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, stanowiła podstawowy akt prawny Unii w tej dziedzinie. Dyrektywa ta ustanawiała ogólne warunki zgodności z prawem przetwarzania tych danych, a także prawa osób, których te dane dotyczą, i przewidywała w szczególności ustanowienie w państwach członkowskich niezależnych organów nadzorczych.

Następnie dyrektywę 95/46 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]. Należy zauważyć, że prawodawca Unii rozważa dokonanie przeglądu tej dyrektywy. W związku z tym w dniu 10 stycznia 2017 r. Komisja przedstawiła wniosek mający na celu zastąpienie tej dyrektywy rozporządzeniem w sprawie życia prywatnego i łączności elektronicznej[4].

Poza tym w przestrzeni wolności, bezpieczeństwa i sprawiedliwości (dawne art. 30 i 31 TUE) decyzja ramowa 2008/977/WSiSW[5] regulowała do maja 2018 r. ochronę danych osobowych w dziedzinach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych.

W 2016 roku Unia Europejska zreformowała kompleksowe ramy prawne w omawianej dziedzinie. W tym celu przyjęła rozporządzenie (UE) 2016/679[6] w sprawie ochrony danych (zwane dalej „RODO"), które uchyla dyrektywę 95/46 i ma zastosowanie od dnia 25 maja 2018 r., a także dyrektywę (UE) 2016/680[7] 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 była w pierwszej kolejności zapewniana przez rozporządzenie (WE) nr 45/2001[8] Rozporządzenie to w szczególności umożliwiło utworzenie w 2004 r. organu o nazwie Europejski

---

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. 1995, L 281, s. 31), wersja skonsolidowana z dnia 20 listopada, uchylona w dniu 25 maja 2018 r. (zob. przypis 5).

2 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa dotycząca prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37), wersja skonsolidowana z dnia 19 grudnia 2009 r.

3 Dyrektywa 2002/58 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. 2006, L 105, 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, zatytułowaną „Zgodność prawa wtórnego Unii z prawem do ochrony danych osobowych" niniejszej broszury).

4 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenia w sprawie życia prywatnego i łączności elektronicznej), COM(2017) 10 final – 2017/03 (COD).

5 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. 2008, L 350, s. 60), uchylona w dniu 6 maja 2018 r. (zob. przypis 6)

6 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. 2016, L 119, s. 1).

7 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. 2016, L 119, s. 89).

8 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. 2001, L 8, s. 1).

Inspektor Ochrony Danych. W 2018 roku Unia Europejska ustanowiła nowe ramy prawne w tej dziedzinie, w szczególności poprzez przyjęcie rozporządzenia (UE) 2018/1725[9], które uchyla rozporządzenie nr 45/2001 i decyzję nr 1247/2002/WE[10] i które obowiązuje od dnia 11 grudnia 2018 r. Z myślą o spójnym podejściu do ochrony danych osobowych w całej Unii nowe rozporządzenie ma na celu dostosowanie w jak największym stopniu przepisów w tej dziedzinie do systemu ustanowionego rozporządzeniem RODO.

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

[10] Decyzja nr 1247/2002/WE Parlamentu Europejskiego, Rady i Komisji z dnia 1 lipca 2002 r. w sprawie regulaminu i ogólnych warunków regulujących wykonywanie obowiązków przez Europejskiego Pełnomocnika ds. Ochrony Danych (Dz.U. 2002, L 183, s. 1).

SPIS TREŚCI

I. PRAWO DO OCHRONY DANYCH OSOBOWYCH UZNANE W KARCIE PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ 5

1. Zgodność prawa wtórnego Unii z prawem do ochrony danych osobowych 5

2. Poszanowanie prawa do ochrony danych osobowych w ramach wprowadzania w życie prawa Unii .. 9

II. PRZETWARZANIE DANYCH OSOBOWYCH W ROZUMIENIU OGÓLNYCH PRZEPISÓW W TYM ZAKRESIE..... 10

1. Przetwarzanie danych osobowych wykluczonych z zakresu stosowania dyrektywy 95/46 10

2. Pojęcie „danych osobowych” 13

3. Pojęcie „przetwarzania danych osobowych” 15

4. Pojęcie „zbioru danych” 20

5. Pojęcie „administratora danych osobowych” 21

6. Warunki zgodności z prawem przetwarzania danych osobowych..... 23

III. PRZETWARZANIE DANYCH OSOBOWYCH W ROZUMIENIU DYREKTYWY 2002/58 33

IV. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH..... 39

V. OCHRONA DANYCH OSOBOWYCH W INTERNECIE 46

1. Prawo do sprzeciwu wobec przetwarzania danych osobowych („prawo do bycia zapomnianym”) ... 46

2. Przetwarzanie danych osobowych a prawa własności intelektualnej 48

3. Usunięcie linków do danych osobowych 52

4. Zgoda użytkownika strony internetowej na przechowywanie informacji..... 56

VI. KRAJOWE ORGANY NADZORCZe 57

1. Zakres wymogu niezależności 57

2. Ustalenie prawa właściwego oraz właściwego organu nadzorczego 60

3. Uprawnienia krajowych organów nadzorczych..... 61

VII. TERYTORIALNE STOSOWANIE PRAWODAWSTWA UNII..... 66

VIII. .....PRAWO PUBLICZNEGO DOSTĘPU DO DOKUMENTÓW INSTYTUCJI UNII EUROPEJSKIEJ A OCHRONA DANYCH OSOBOWYCH 66

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)[11]

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[12] i nr 259/2008[13], 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 szereg pytań dotyczących ważności niektórych przepisów rozporządzenia nr 1290/2005 i rozporządzenia 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

[11] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2010, s. 11.

[12] Rozporządzenia Rady (WE) nr 1290/2005 z dnia 21 czerwca 2005 r. w sprawie finansowania wspólnej polityki rolnej (Dz.U. 2005, L 209, 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. 2013, L 347, s. 549).

[13] 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. 2008, L 76, 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. 2014, L 255, s. 59).

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 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 nr 1290/2005, a także rozporządzenia 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; sentencja, pkt 1). 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; sentencja, pkt 2).

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[14], 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 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 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

[14] 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. 2004, L385, s. 1), zmienione rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 444/2009 z dnia 6 maja 2009 r. (Dz.U. 2009, L 142, s. 1).

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 w stopniu mniejszym niż metoda związana z odciskami palców (pkt 53). Artykuł 1 ust. 2 rozporządzenia 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)[15]

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 wnioskach o wydanie orzeczenia w trybie prejudycjalnym sądy irlandzki i austriacki zwróciły się do Trybunału z zapytaniem o ważność dyrektywy 2006/24 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

[15] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2014, s. 60.

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, 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 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 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 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)[16]

W związku z wydaniem wyroku Digital Rights Ireland i Seitlinger i in., stwierdzającego nieważność dyrektywy 2006/24 (zob. wyżej) do Trybunału 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 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 pytania prejudycjalne w celu uzyskania wykładni art. 15 ust. 1 dyrektywy 2002/58, 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 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; sentencja, pkt 1).

[16] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2016, s. 62.

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; sentencja, pkt 2).

Trybunał natomiast stwierdził, że art. 15 ust. 1 dyrektywy 2002/58 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 ogólnych przepisów w tym zakresie

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

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[17] 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[18] 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 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. 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 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).

---

[17] 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. 2004, L 235, s. 11).

[18] 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. 2004, L 183, s. 83; sprostowanie Dz.U. 2005, L 255, s. 168).

W odniesieniu do decyzji Rady Trybunał stwierdził, że art. 95 WE w związku z art. 25 dyrektywy 95/46 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.

Rozpatrując odwołanie wniesione przez F. Ryneš na orzeczenie wydane przez Městský soud v Praze (sąd miejski w Pradze, Republika Czeska), utrzymujące w mocy decyzję urzędu, Nejvyšší správní soud (naczelny sąd administracyjny) zwrócił się do Trybunału 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 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 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 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)[19]

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 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, 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 (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, 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; sentencja, pkt 1).

Wyrok z dnia 20 grudnia 2017 r., Nowak (C-434/16, EU:C:2017:994)

Peter Nowak, księgowy stażysta, nie zdał egzaminu organizowanego przez irlandzki instytut biegłych rewidentów. Postanowił on złożyć, na podstawie art. 4 ustawy o ochronie danych

[19] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2016, s. 61.

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.

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 z pytaniem, czy art. 2 lit. a) dyrektywy 95/46 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 orzekł w pierwszej kolejności, że do tego, aby dane mogły zostać uznane za „osobowe" w rozumieniu art. 2 lit. a) dyrektywy 95/46, 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") (pkt 31, 36–40).

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 (pkt 42, 43).

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, 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 prawa do dostępu i sprostowania nie obejmują pytań egzaminacyjnych, które nie stanowią jako takie danych osobowych egzaminowanego (pkt 56, 58).

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 (pkt 62; sentencja).

3. Pojęcie „przetwarzania danych osobowych”

Wyrok z dnia 6 listopada 2003 r. (wielka izba), 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 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.

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; sentencja, pkt 1). 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; sentencja, pkt 2).

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.

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

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 (sentencja, pkt 1). 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).

Wyrok z dnia 10 lipca 2018 r. (wielka izba), Jehovan todistajat (C-25/17, EU:C:2018:551)[20]

Fiński organ ochrony danych wydał decyzję zakazującą wspólnocie świadków Jehowy gromadzenia lub przetwarzania danych osobowych w ramach działalności kaznodziejskiej realizowanej przez jej członków poprzez odwiedzanie kolejnych gospodarstw domowych, o ile nie będą przestrzegane określone w ustawodawstwie fińskim warunki przetwarzania takich danych. W ramach działalności kaznodziejskiej realizowanej poprzez odwiedzanie kolejnych gospodarstw domowych członkowie tej wspólnoty sporządzają bowiem notatki o wizytach złożonych osobom nieznanym ani im, ani wspomnianej wspólnocie. Dane te są gromadzone jako zapiski ku pamięci, po to, by można je odnaleźć dla potrzeb ewentualnej późniejszej wizyty, przy czym zainteresowane osoby nie są proszone o wyrażenie na to zgody ani o tym informowane. W tym zakresie wspólnota świadków Jehowy ustaliła dla swoich członków wytyczne dotyczące sporządzania takich notatek, które to wytyczne są zawarte w co najmniej jednym z jej czasopism poświęconych działalności kaznodziejskiej.

Trybunał orzekł, że gromadzenie danych osobowych przez członków wspólnoty religijnej w ramach działalności kaznodziejskiej realizowanej poprzez odwiedzanie kolejnych gospodarstw domowych oraz późniejsze przetwarzanie tych danych nie jest objęte żadnym z wyjątków od zakresu stosowania dyrektywy 95/46, ponieważ nie stanowi ani przetwarzania danych osobowych w ramach działalności, o której mowa w art. 3 ust. 2 tiret pierwsze tej dyrektywy, ani przetwarzania danych osobowych przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze w rozumieniu art. 3 ust. 2 tiret drugie wspomnianej dyrektywy (pkt 51; sentencja, pkt 1).

Wyrok z dnia 14 lutego 2019 r., Buivids (C-345/17, EU:C:2019:122)

W sprawie tej Trybunał zajmował się wykładnią, po pierwsze, zakresu stosowania dyrektywy 95/46, a po drugie, pojęcia „przetwarzania danych osobowych wyłącznie w celach dziennikarskich", o którym mowa w art. 9 tej dyrektywy.

Wyrok ten wpisuje się w ramy wniosku o wydanie orzeczenia w trybie prejudycjalnym, z którym zwrócił się sąd najwyższy Łotwy rozpatrujący spór między S. Buividsem (zwanym dalej „skarżącym") a krajowym urzędem ochrony danych osobowych w przedmiocie skargi o stwierdzenie niezgodności z prawem decyzji tego urzędu, zgodnie z którą osoba ta naruszyła przepisy prawa krajowego w dziedzinie ochrony danych osobowych poprzez opublikowanie na stronie internetowej nagrania wideo, sfilmowanego przez nią samą momentu, w którym składa zeznania na komisariacie policji krajowej w ramach postępowania karno-administracyjnego. W związku z tym, w następstwie oddalenia skargi przez dwa sądy niższej instancji, skarżący wniósł skargę kasacyjną do sądu najwyższego. Przed sądem tym powołał się on na swoje prawo do wolności wypowiedzi, argumentując, że omawiane nagranie wideo pokazuje funkcjonariuszy policji krajowej, którzy mają status osób publicznych, w miejscu dostępnym publicznie i że w związku z tym osoby te nie są objęte stosowaniem przepisów ustawy o ochronie danych osobowych.

[20] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2018, s. 87–88.

W odniesieniu, w pierwszej kolejności, do zakresu stosowania dyrektywy 95/46 Trybunał zauważył, że po pierwsze, obrazy członków policji zarejestrowane na przedmiotowym nagraniu wideo stanowią dane osobowe, a po drugie, że nagranie wideo tych osób przechowywane w pamięci kamery używanej przez skarżącego stanowi przetwarzanie danych osobowych. Trybunał dodał zatem, że opublikowanie nagrania wideo, na którym znajdują się dane osobowe, na stronie internetowej zawierającej materiały wideo, które mogą być oglądane i rozpowszechniane przez użytkowników, stanowi przetwarzanie tych danych w całości lub w części w sposób zautomatyzowany. Ponadto Trybunał podkreślił, że omawiane rejestrowanie i publikowanie nie jest objęte wyjątkami przewidzianymi w zakresie stosowania dyrektywy 95/46, dotyczącymi w szczególności przetwarzania danych osobowych w ramach działalności, która nie wchodzi w zakres stosowania tej dyrektywy, oraz przetwarzania wpisującego się w ramy wykonywania czynności o czysto osobistym lub domowym charakterze. W związku z tym Trybunał stwierdził, że zakresem stosowania tej dyrektywy jest objęte nagranie na wideo policjantów na komisariacie policji w chwili przyjmowania przez nich zeznań oraz opublikowanie tak nagranego wideo na stronie internetowej zawierającej materiały wideo, na której użytkownicy mogą zamieszczać, odtwarzać i rozpowszechniać nagrania wideo (pkt 31, 32, 35, 39, 42, 43; sentencja, pkt 1).

Jeśli chodzi w drugiej kolejności o zakres pojęcia „przetwarzania danych osobowych wyłącznie w celach dziennikarskich", Trybunał przypomniał przede wszystkim, że zgodnie z szeroką wykładnią pojęcia „dziennikarstwa" wyjątki i odstępstwa przewidziane w art. 9 dyrektywy 95/46 mają zastosowanie do każdej osoby prowadzącej działalność dziennikarską. Trybunał orzekł zatem, że okoliczność, iż skarżący nie jest zawodowym dziennikarzem, nie wyklucza możliwości zakwalifikowania nagrania wideo i jego transmisji jako „przetwarzania danych osobowych wyłącznie w celach dziennikarskich". Ponadto Trybunał podkreślił, że wyjątki i odstępstwa przewidziane w art. 9 dyrektywy 95/46 powinny być stosowane tylko w takim zakresie, w jakim jest to konieczne do pogodzenia dwóch praw podstawowych, a mianowicie, prawa do ochrony życia prywatnego i prawa do wolności wypowiedzi. W tym względzie Trybunał uściślił, że nie można wykluczyć, iż zarejestrowanie oraz opublikowanie przedmiotowego nagrania wideo, które miały miejsce bez poinformowania o tym nagraniu i jego celach ujętych na nim policjantów stanowi ingerencję w podstawowe prawo do poszanowania życia prywatnego tych osób. W konsekwencji stwierdził on, że nagranie oraz opublikowanie przedmiotowego nagrania wideo na stronie internetowej zawierającej materiały wideo może stanowić przetwarzanie danych osobowych wyłącznie w celach dziennikarskich, o ile ze wspomnianego nagrania wideo wynika, że wyłącznym celem jego zarejestrowania i opublikowania jest publiczne rozpowszechnienie informacji, opinii lub myśli, czego zbadanie należy do sądu odsyłającego (pkt 51, 52, 55, 63, 67; sentencja, pkt 2).

Wyrok z dnia 22 czerwca 2021 r. (wielka izba), Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU: C:2021:504)

B, osoba fizyczna, otrzymała punkty karne za wykroczenie (wykroczenia) drogowe. Te punkty karne zostały wpisane przez Ceļu satiksmes drošības direkcija (dyrekcję bezpieczeństwa drogowego, Łotwa, zwaną dalej „CSDD") do krajowego rejestru pojazdów i ich kierowców.

Zgodnie z łotewskimi przepisami dotyczącymi ruchu drogowego[21] informacje dotyczące punktów karnych nałożonych na kierowców pojazdów wpisanych do tego rejestru są publicznie dostępne i przekazywane przez CSDD wszystkim osobom, które się o to zwrócą, przy czym nie mają one obowiązku wykazywania szczególnego interesu w uzyskaniu tych informacji, w tym podmiotom gospodarczym w celu ponownego wykorzystania. Rozważywszy zgodność z prawem tych przepisów, B wniósł skargę konstytucyjną do Latvijas Republikas Satversmes tiesa (trybunału konstytucyjnego, Łotwa) w celu zbadania zgodności tych przepisów z prawem do poszanowania życia prywatnego.

Trybunał konstytucyjny uznał, że w ramach oceny tego prawa konstytucyjnego powinien uwzględnić RODO. W związku z tym sąd ten zwrócił się do Trybunału o wyjaśnienie zakresu kilku przepisów RODO w celu ustalenia zgodności łotewskiego uregulowania dotyczącego ruchu drogowego z tym rozporządzeniem.

W wyroku wydanym w składzie wielkiej izby Trybunał orzekł, że przetwarzanie danych osobowych dotyczących punktów karnych stanowi „przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa”[22], w odniesieniu do którego RODO przewiduje zwiększoną ochronę ze względu na szczególną wrażliwość tych danych (pkt 10, 46, 74, 94; sentencja, pkt 1).

W tym kontekście zauważył on na wstępie, że informacje dotyczące punktów karnych są danymi osobowymi i że ich przekazywanie osobom trzecim przez CSDD stanowi przetwarzanie objęte przedmiotowym zakresem stosowania RODO. Ten zakres stosowania jest bowiem bardzo szeroki, a przetwarzanie to nie jest objęte wyjątkami od stosowania tego rozporządzenia (pkt 60, 61, 72).

Z jednej strony przetwarzanie to nie jest objęte wyjątkiem dotyczącym niestosowania RODO do przetwarzania dokonywanego w ramach działalności nieobjętej zakresem prawa Unii[23]. Należy uznać, że jedynym celem tego wyjątku jest wyłączenie z zakresu stosowania tego rozporządzenia przetwarzania danych osobowych dokonywanego przez organy państwowe w ramach działalności mającej na celu ochronę bezpieczeństwa narodowego lub działalności, która może zostać zaliczona do tej samej kategorii. Działalność ta obejmuje w szczególności działania mające na celu ochronę podstawowych funkcji państwa i podstawowych interesów społeczeństwa. Tymczasem czynności związane z bezpieczeństwem na drogach nie realizują tego celu i nie można ich wobec tego zaliczyć do kategorii działań mających na celu ochronę bezpieczeństwa narodowego. (pkt 62, 66–68).

Z drugiej strony ujawnianie danych osobowych dotyczących punktów karnych również nie jest przetwarzaniem objętym wyjątkiem przewidującym niestosowanie RODO do przetwarzania danych osobowych dokonywanego przez organy właściwe w sprawach karnych[24]. Trybunał

[21] Artykuł 14[1] ust. 2, Ceļu satiksmes likums (ustawy o ruchu drogowym) z dnia 1 października 1997 r. (*Latvijas Vēstnesis*, 1997, nr 274/276).
[22] Artykuł 10 RODO.
[23] Artykuł 2 ust. 2 lit. a) RODO.
[24] Artykuł 2 ust. 2 lit. d) RODO.

stwierdził bowiem, że w ramach tego ujawniania CSDD nie może być uważany za taki „właściwy organ”[25] (pkt 69–71).

W celu ustalenia, czy dostęp do danych osobowych dotyczących wykroczeń drogowych, takich jak punkty karne, stanowi przetwarzanie danych osobowych dotyczących „naruszeń prawa”[26], które korzystają ze zwiększonej ochrony, Trybunał stwierdził, opierając się w szczególności na genezie RODO, że pojęcie to odnosi się wyłącznie do przestępstw. Jednakże okoliczność, że w łotewskim systemie prawnym wykroczenia drogowe są kwalifikowane jako administracyjne, nie jest decydująca dla oceny, czy wykroczenia te wchodzą w zakres pojęcia „przestępstwa”, ponieważ chodzi tu o autonomiczne pojęcie prawa Unii, które wymaga w całej Unii autonomicznej i jednolitej wykładni. Przypomniawszy zatem trzy kryteria istotne dla oceny karnego charakteru czynu zabronionego, a mianowicie kwalifikację prawną czynu w prawie krajowym, charakter naruszenia i stopień surowości grożącej sankcji, Trybunał orzekł, że rozpatrywane wykroczenia drogowe wchodzą w zakres pojęcia „naruszenia prawa” w rozumieniu RODO. W odniesieniu do dwóch pierwszych kryteriów Trybunał stwierdził, że nawet jeśli wykroczenia nie są kwalifikowane jako „karne” w prawie krajowym, taki charakter może wynikać z charakteru wykroczenia, a w szczególności z represyjnego celu, jaki realizuje kara, do której może prowadzić wykroczenie. Tymczasem w niniejszej sprawie nałożenie punktów karnych za wykroczenia drogowe, podobnie jak inne sankcje, jakie może spowodować ich popełnienie, realizują między innymi taki cel represyjny. W odniesieniu do trzeciego kryterium Trybunał zauważył, że jedynie wykroczenia drogowe o określonej wadze pociągają za sobą nałożenie punktów karnych i że w związku z tym mogą one prowadzić do sankcji o określonej surowości. Ponadto nałożenie takich punktów zazwyczaj uzupełnia nałożoną sankcję, a kumulacja tych punktów pociąga za sobą skutki prawne, które mogą obejmować nawet zakaz kierowania pojazdami (pkt 77, 80, 85, 87–90, 93).

4. Pojęcie „zbioru danych”

Wyrok z dnia 10 lipca 2018 r. (wielka izba), Jehovan todistajat (C-25/17, EU:C:2018:551)

W tym wyroku (zob. także część II.3, zatytułowaną „Pojęcie »przetwarzania danych osobowych«”) Trybunał wyjaśnił pojęcie „zbioru danych”, o którym mowa w art. 2 lit. c) dyrektywy 95/46.

Po przypomnieniu zatem, że dyrektywa ta stosuje się do ręcznego przetwarzania danych osobowych tylko w przypadku, gdy dane przetwarzane stanowią część zbioru danych lub mają stanowić część zbioru danych, Trybunał wskazał, że rzeczone pojęcie obejmuje zestaw danych osobowych gromadzonych w ramach działalności kaznodziejskiej realizowanej poprzez odwiedzanie kolejnych gospodarstw domowych, zawierających nazwiska i adresy oraz inne informacje dotyczące odwiedzonych osób, o ile dane te są zorganizowane według określonych kryteriów umożliwiających w praktyce ich łatwe odnalezienie celów celu ich późniejszego

[25] Artykuł 3 ust. 7 dyrektywy 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. 2016, L 119, s. 89).

[26] Artykuł 10 RODO.

wykorzystania. Aby zestaw taki był objęty tym pojęciem, nie jest konieczne, by zawierał kartoteki, szczególne rejestry lub inne systemy służące wyszukiwaniu (pkt 62; sentencja, pkt 2).

5. Pojęcie „administratora danych osobowych”

Wyrok z dnia 10 lipca 2018 r. (wielka izba), Jehovan todistajat (C-25/17, EU:C:2018:551)

W tej sprawie (zob. także części II.3 i II.4 zatytułowane „Pojęcie »przetwarzania danych osobowych«” i „Pojęcie »zbioru danych«”) Trybunał wypowiedział się w przedmiocie odpowiedzialności wspólnoty religijnej za przetwarzanie danych osobowych dokonywane w ramach zorganizowanej, koordynowanej i wspieranej przez wspólnotę działalności kaznodziejskiej realizowanej poprzez odwiedzanie kolejnych gospodarstw domowych

Trybunał uznał zatem, że spoczywającego na wszystkich osobach obowiązku dostosowania się do zasad prawa Unii dotyczących ochrony danych osobowych nie można uznać za ingerencję w autonomię organizacyjną wspólnot religijnych. W tej kwestii orzekł on, że art. 2 lit. d) dyrektywy 95/46 w świetle art. 10 ust. 1 karty należy interpretować w ten sposób, że pozwala on uznać wspólnotę religijną wspólnie z jej członkami głosicielami za administratora danych osobowych w odniesieniu do przetwarzania dokonywanego przez tych członków głosicieli w ramach zorganizowanej, koordynowanej i wspieranej przez wspólnotę działalności kaznodziejskiej realizowanej poprzez odwiedzanie kolejnych gospodarstw domowych, przy czym nie jest konieczne, by wspomniana wspólnota miała dostęp do danych, ani nie musi zostać ustalone, że udzielała ona swoim członkom pisemnych wytycznych lub instrukcji dotyczących tego przetwarzania.

Wyrok z dnia 5 czerwca 2018 r. (wielka izba), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388)[27]

Niemiecki organ ochrony danych, jako organ nadzorczy w rozumieniu art. 28 dyrektywy 95/46, nakazał niemieckiej spółce specjalizującej się w edukacji i świadczącej usługi kształcenia przy użyciu fanpage’a prowadzonego na stronie portalu społecznościowego Facebook dezaktywację należącego do niej fanpage’a. Zdaniem tego organu ani ta spółka, ani Facebook nie informowali osób odwiedzających fanpage o gromadzeniu za pomocą plików cookies dotyczących ich danych osobowych, które następnie były przetwarzane przez rzeczoną spółkę i przez Facebook.

W tym kontekście Trybunał sprecyzował pojęcie „administratora danych” osobowych. Trybunał uznał w tym względzie, że administrator fanpage’a prowadzonego na Facebooku, taki jak spółka występująca w sprawie w postępowaniu głównym, uczestniczy, podejmując działania polegające na ustaleniu parametrów (zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakresie zarządzania lub promocji jego działalności), w określeniu celów i sposobów przetwarzania danych osobowych osób odwiedzających fanpage. Z tego względu, zdaniem Trybunału, należy uznać, że ów administrator fanpage’a ponosi na poziomie Unii

[27] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2018, s. 86–87.

wspólną odpowiedzialność z Facebook Ireland (spółką zależną amerykańskiej spółki Facebook na terytorium Unii) za przetwarzanie danych w rozumieniu art. 2 lit. d) dyrektywy 95/46 (pkt 39).

Wyrok z dnia 29 lipca 2019 r., Fashion ID (C-40/17, EU:C:2019:629)

W tej sprawie Trybunał miał okazję rozwinąć pojęcie „administratora danych" w związku z włączeniem tzw. „plug-in" do strony internetowej.

W tym przypadku Fashion ID, spółka zajmująca się sprzedażą online modnej odzieży, umieściła w swojej witrynie internetowej wtyczkę społecznościową „Lubię to" serwisu społecznościowego Facebook. Konsekwencją tego umieszczenia wydaje się być to, że kiedy osoba odwiedzająca przegląda witrynę internetową Fashion ID, dane osobowe tej osoby odwiedzającej są przekazywane do Facebooka Ireland. Wydaje się, że to przekazywanie następuje bez wiedzy wspomnianej osoby odwiedzającej i niezależnie od okoliczności, czy jest ona członkiem serwisu społecznościowego Facebook lub czy kliknęła na przycisk „Lubię to" Facebooka.

Verbraucherzentrale NRW, niemieckie stowarzyszenie użyteczności publicznej ochrony interesów konsumentów, zarzuca Fashion ID przekazywanie Facebook Ireland danych osobowych należących do osób odwiedzających jej witrynę internetową, po pierwsze, bez ich zgody, a po drugie, z naruszeniem obowiązków informacyjnych przewidzianych w przepisach dotyczących ochrony danych osobowych. Rozpatrujący spór Oberlandesgericht Düsseldorf (wyższy sąd krajowy w Düsseldorfie, Niemcy) zwrócił się do Trybunału o dokonanie wykładni kilku przepisów dyrektywy 95/46.

Trybunał stwierdził przede wszystkim, że operatora witryny internetowej, takiego jak Fashion ID, można uznać za administratora danych w rozumieniu art. 2 lit. d) dyrektywy 95/46. Odpowiedzialność ta jest jednak ograniczona do operacji lub do zestawu operacji przetwarzania danych osobowych, której lub których cele i sposoby rzeczywiście on określa, mianowicie gromadzenia rozpatrywanych danych i ich ujawniania poprzez transmisję. Natomiast zdaniem Trybunału wydaje się prima facie wykluczone, by Fashion ID określała cele i sposoby późniejszych operacji przetwarzania danych osobowych, dokonywanych przez Facebook Ireland po przekazaniu tych danych tej ostatniej spółce, wobec czego Fashion ID nie można uznać za administratora w odniesieniu do tych operacji w rozumieniu tego art. 2 lit. d) (pkt 76, 85; sentencja, pkt 2).

Ponadto Trybunał podkreślił, że konieczne jest, aby operator strony internetowej i dostawca wtyczki społecznościowej, taki jak Facebook Ireland, dążyli, w ramach tych operacji przetwarzania, do realizacji uzasadnionych interesów w rozumieniu art. 7 lit. f) dyrektywy 95/46, aby operacje te były względem każdego z nich uzasadnione (pkt 97; sentencja, pkt 3).

Trybunał uściślił wreszcie, że zgoda osoby, której dane dotyczą, o której mowa w art. 2 lit. h) i art. 7 lit. a) dyrektywy 95/46, powinna zostać uzyskana przez operatora strony internetowej wyłącznie w odniesieniu do operacji przetwarzania danych osobowych, których cele i sposoby ten operator określa. W takiej sytuacji obowiązek informacyjny przewidziany w art. 10 tej dyrektywy ciąży również na wspomnianym operatorze, przy czym jednak informacja, jaką ten ostatni musi przedstawić osobie, której dane dotyczą, powinna odnosić się wyłącznie do operacji

lub do zestawu operacji przetwarzania danych osobowych, której lub których cele i sposoby on określa (pkt 106; sentencja, pkt 4).

Wyrok z dnia 9 lipca 2020 r., Land Hessen, C-272/19, EU:C:2020:535

Obywatel, który złożył petycję do komisji ds. petycji parlamentu kraju związkowego Hesja (Niemcy), zażądał od tej komisji dostępu do dotyczących go danych osobowych przechowywanych przez komisję w związku z rozpatrywaniem jego petycji. Swój wniosek oparł on na przepisach RODO, które przewidują prawo osoby, której dane dotyczą, do uzyskania od administratora danych dostępu do dotyczących tej osoby danych osobowych.

Przewodniczący parlamentu kraju związkowego Hesja oddalił wniosek na tej podstawie, że postępowanie w sprawie petycji stanowi działalność parlamentarną i że parlament nie podlega przepisom RODO.

Verwaltungsgericht Wiesbaden (sąd administracyjny w Wiesbaden, Niemcy), do którego wystąpił ze skargą ten obywatel, stwierdził, że prawo niemieckie nie przyznaje żadnego prawa dostępu do danych osobowych w kontekście rozpatrywanej petycji. Uznając jednak, że takie prawo dostępu może wynikać z przepisów RODO, Verwaltungsgericht Wiesbaden (sąd administracyjny w Wiesbaden) skierował w tej kwestii pytania do Trybunału Sprawiedliwości. Ponadto, mając wątpliwości co do własnej niezawisłości, a tym samym swojego statusu jako sądu uprawnionego do przedłożenia Trybunałowi pytań prejudycjalnych, Verwaltungsgericht Wiesbaden (sąd administracyjny w Wiesbaden) zwrócił się również w tej sprawie do Trybunału.

W wyroku Trybunał odpowiedział, że w zakresie, w jakim komisja ds. petycji parlamentu kraju związkowego państwa członkowskiego określa – samodzielnie lub wspólnie z innymi – cele i sposoby przetwarzania danych osobowych, komisja ta powinna zostać uznana za „administratora danych" w rozumieniu RODO[28]. Przetwarzanie danych osobowych przez taką komisję podlega zatem temu rozporządzeniu, w szczególności przepisowi przyznającemu zainteresowanym osobom prawo dostępu do dotyczących je danych osobowych[29].

Trybunał stwierdził w szczególności, że działalność komisji ds. petycji parlamentu kraju związkowego Hesja nie wchodzi w zakres wyjątku przewidzianego w przepisach RODO. Przyznał on, że działalność ta ma charakter publiczny i jest właściwa temu krajowi związkowemu, ponieważ komisja ta pośrednio przyczynia się do działalności parlamentarnej, lecz wskazał, że działalność ta ma również charakter zarówno polityczny, jak i administracyjny. Ponadto z informacji, którymi dysponuje Trybunał, nie wynika w żaden sposób, że działalność ta odpowiada w niniejszym przypadku wyjątkom przewidzianym w przepisach RODO (pkt 71–74; sentencja).

6. Warunki zgodności z prawem przetwarzania danych osobowych

[28] Artykuł 4 pkt 7 RODO.
[29] Artykuł 15 RODO.

Wyrok z dnia 16 grudnia 2008 r. (wielka izba), Huber (C-524/06, EU:C:2008:724)[30]

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 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 (wyższy sąd administracyjny dla kraju związkowego 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).

W odniesieniu do pojęcia konieczności w rozumieniu art. 7 lit. e) dyrektywy 95/46 Trybunał najpierw przypomniał, że jest to autonomiczne pojęcie prawa Unii, którego wykładnia winna w pełni odpowiadać celowi dyrektywy 95/46, 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 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

[30] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2008, s. 45.

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.

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, 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, 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.

Trybunał przede wszystkim stwierdził w tym względzie, że art. 7 dyrektywy 95/46 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.

W konsekwencji Trybunał stwierdził, że art. 7 lit. f) dyrektywy 95/46 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 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 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 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, wykluczając możliwość ważenia celu polegającego na zagwarantowaniu ogólnej funkcjonalności mediów online z interesem lub podstawowymi prawami i wolnościami użytkowników (pkt 62–64; sentencja, pkt 2).

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 pytanie, czy art. 7 lit. f) dyrektywy 95/46 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 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; 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 Slovenskej republiky (sąd najwyższy Republiki Słowackiej) zwrócił się do Trybunału, 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 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 zostały spełnione (pkt 117; sentencja, pkt 3).

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 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).

Wyrok z dnia 11 listopada 2020 r., Orange Romania (C-61/19, EU:C:2020:901)

Orange România SA jest dostawcą usług telefonii ruchomej na rynku rumuńskim. W dniu 28 marca 2018 r. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (krajowy organ nadzoru nad przetwarzaniem danych osobowych, Rumunia) nałożył na Orange România grzywnę za gromadzenie i przechowywanie kopii dokumentów tożsamości swoich klientów bez ich wyraźnej zgody.

Według ANSPDCP, w okresie od 1 do 26 marca 2018 r. Orange România zawarła umowy o świadczenie usług telefonii ruchomej zawierające klauzulę, zgodnie z którą klienci byli informowani i wyrażali zgodę na gromadzenie i przechowywanie kopii ich dokumentu tożsamości do celów identyfikacji. Pole wyboru odnoszące się do tej klauzuli zostało zaznaczone przez administratora danych przed podpisaniem umowy.

W tym właśnie kontekście Tribunalul București (sąd okręgowy w Bukareszcie, Rumunia) zwrócił się do Trybunału o wyjaśnienie warunków, na jakich zgodę klientów na przetwarzanie danych osobowych można uznać za ważną.

Trybunał przypomniał przede wszystkim, że prawo Unii[31] przewiduje wykaz przypadków, w których przetwarzanie danych osobowych może być uznane za zgodne z prawem. W szczególności zgoda osoby, której dane dotyczą, musi być dobrowolna, konkretna, świadoma i jednoznaczna[32]. W tym względzie zgoda nie jest wyrażona w sposób skuteczny w przypadku milczenia, okienek domyślnie zaznaczonych lub niepodjęcia działania (pkt 34, 36, 37, 39).

Ponadto, jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, takie oświadczenie musi zostać przedstawione w zrozumiałej i łatwo dostępnej formie oraz musi zostać wyrażone jasnym i prostym językiem. W celu zapewnienia osobie, której dane dotyczą, rzeczywistej swobody wyboru postanowienia umowne nie powinny wprowadzać tej osoby w błąd co do możliwości zawarcia umowy, nawet jeśli odmawia ona wyrażenia zgody na przetwarzanie jej danych (pkt 34, 36, 37, 39, 41).

Trybunał wskazał, że ponieważ Orange România jest administratorem danych osobowych, powinna być w stanie wykazać zgodność z prawem przetwarzania tych danych, a zatem, w niniejszej sprawie, istnienie ważnej zgody swoich klientów. W tym względzie, ponieważ nie wydaje się, by zainteresowani klienci sami zaznaczyli pole wyboru dotyczące gromadzenia i przechowywania kopii ich dokumentów tożsamości, sam fakt zaznaczenia tego pola nie może świadczyć o pozytywnym wyrażeniu przez nich zgody. Do sądu krajowego należy dokonanie niezbędnych ustaleń w tym zakresie (pkt 42, 46).

Do sądu krajowego należy również, zdaniem Trybunału, ocena, czy przedmiotowe postanowienia umowne mogły wprowadzić danych klientów w błąd co do możliwości zawarcia umowy pomimo odmowy wyrażenia zgody na przetwarzanie ich danych, wobec braku wyjaśnień w tej kwestii. Ponadto, w przypadku odmowy wyrażenia przez klienta zgody na przetwarzanie jego danych, Trybunał zauważył, że Orange România wymagała od takiego klienta złożenia oświadczenia na piśmie, że nie wyraża on zgody ani na pobranie od niego dokumentu tożsamości, ani na przechowywanie kopii tego dokumentu. Zdaniem Trybunału taki dodatkowy wymóg może bezpodstawnie wpłynąć na swobodne podjęcie decyzji o sprzeciwieniu się takiemu gromadzeniu i przechowywaniu danych. W każdym razie, skoro omawiana spółka jest zobowiązana do wykazania, że jej klienci wyrażali zgodę na przetwarzanie ich danych osobowych poprzez czynne zachowanie, owa spółka nie może wymagać od nich, aby poprzez czynne zachowanie wyrażali oni swą odmowę (pkt 49–51).

Trybunał doszedł zatem do wniosku, że umowa o świadczenie usług telekomunikacyjnych zawierająca klauzulę stwierdzającą, że osoba, której dane dotyczą, została poinformowana o skopiowaniu i przechowywaniu kopii swego dokumentu tożsamości do celów identyfikacji i wyraziła na to zgodę, nie pozwala wykazać, że osoba ta skutecznie wyraziła zgodę, w rozumieniu wskazanych przepisów, na sporządzenie tej kopii i jej przechowywanie, gdy okienko wyboru odnoszące się do tej klauzuli zostało zaznaczone przez administratora danych przed

[31] Artykuł 7 dyrektywy 95/46 i art. 6 RODO.
[32] Artykuł 2 lit. h) dyrektywy 95/46 i art. 4 pkt 11 RODO.

podpisaniem umowy, gdy postanowienia rzeczonej umowy mogą wprowadzać osobę, której dane dotyczą, w błąd co do możliwości zawarcia owej umowy pomimo odmowy udzielenia zgody na przetwarzanie danych lub gdy administrator ten bezpodstawnie wpłynął na swobodne podjęcie decyzji o sprzeciwieniu się skopiowaniu i przechowywaniu kopii dokumentu tożsamości poprzez ustanowienie wymogu, aby, celem wyrażenia swojej odmowy na przetwarzanie tych danych, osoba, której dane dotyczą, wypełniła dodatkowy formularz dokumentujący tę odmowę (pkt 52; sentencja).

Wyrok z dnia 12 maja 2021 r. (wielka izba), Bundesrepublik Deutschland (Czerwona nota Interpolu) (C-505/19, EU:C:2021:376)

W 2012 r. Międzynarodowa Organizacja Policji Kryminalnej (zwana dalej „Interpolem") opublikowała, na wniosek Stanów Zjednoczonych i na podstawie nakazu aresztowania wydanego przez organy tego państwa, czerwoną notę dotyczącą WS, będącego obywatelem Niemiec, w celu jego ewentualnej ekstradycji. Gdy osoba, której dotyczy taka nota, zostaje zlokalizowana na terytorium państwa członkowskiego Interpolu, zasadniczo powinno ono tymczasowo zatrzymać tę osobę lub ograniczyć jej przemieszczanie się.

Jednak jeszcze przed opublikowaniem tej czerwonej noty przeciwko WS zostało wszczęte w Niemczech dochodzenie o te same – według sądu odsyłającego – czyny, co czyny leżące u podstaw czerwonej noty. Postępowanie to zostało prawomocnie umorzone w 2010 r., po zapłaceniu przez WS określonej kwoty, w ramach szczególnego postępowania ugodowego przewidzianego w niemieckim prawie karnym. W związku z tym Bundeskriminalamt (federalne biuro policji kryminalnej, Niemcy) poinformowało Interpol, że jego zdaniem, ze względu na to wcześniejsze postępowanie, zastosowanie ma zasada ne bis in idem. Zasada ta, zapisana zarówno w art. 54 konwencji wykonawczej do układu z Schengen[33], jak i w art. 50 karty, zabrania w szczególności, by osoba, której proces zakończył się prawomocnym wyrokiem, była ponownie ścigana za to samo przestępstwo.

W 2017 r. WS złożył do Verwaltungsgericht Wiesbaden (sądu administracyjnego w Wiesbaden, Niemcy) skargę przeciwko Republice Federalnej Niemiec, wnosząc o nakazanie temu państwu podjęcia wszelkich niezbędnych działań zmierzających do usunięcia tej czerwonej noty. W tej kwestii, oprócz naruszenia zasady ne bis in idem, WS powołał się na naruszenie jego prawa do swobodnego przemieszczania się, gwarantowanego w art. 21 TFUE, ponieważ nie mógł udać się do państwa będącego stroną układu z Schengen lub do państwa członkowskiego, nie ryzykując zatrzymania. Podnosił również, że z powodu tych naruszeń przetwarzanie jego danych osobowych zawartych w czerwonej nocie jest sprzeczne z dyrektywą 2016/680, dotyczącą ochrony danych osobowych w sprawach karnych[34].

W tym właśnie kontekście sąd administracyjny w Wiesbaden postanowił zwrócić się do Trybunału z pytaniem o stosowanie zasady ne bis in idem, a dokładniej – o możliwość tymczasowego

[33] Konwencja wykonawcza do układu z Schengen z dnia 14 czerwca 1985 r. między rządami państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz.U. 2000, L 239, s. 19, zwana dalej „KWUS").

[34] 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. 2016, L 119, s. 89).

zatrzymania osoby, której dotyczy czerwona nota w sytuacji takiej, jak przez niego rozpatrywana. Ponadto, na wypadek możliwości stosowania tej zasady, sąd ten chciałby ustalić konsekwencje dla przetwarzania przez państwa członkowskie danych osobowych zawartych w takiej nocie.

Wyrokiem wielkiej izby Trybunał orzekł, między innymi, że przepisy dyrektywy 2016/680 w związku z art. 54 KWUS i z art. 50 karty należy interpretować w ten sposób, że nie stoją one na przeszkodzie przetwarzaniu danych osobowych zawartych w czerwonej nocie wydanej przez Interpol, dopóki nie zostanie wykazane, poprzez takie orzeczenie sądowe, że w odniesieniu do czynów, na których opiera się ta nota, ma zastosowanie zasada ne bis in idem, pod warunkiem że takie przetwarzanie spełnia wymogi przewidziane w tej dyrektywie (pkt 121; sentencja, pkt 2).

Jeżeli chodzi o pytanie dotyczące danych osobowych zawartych w czerwonej nocie Interpolu, Trybunał wskazał, że operacja wykonywana na tych danych, taka jak ich utrwalanie w bazach osób poszukiwanych państwa członkowskiego, stanowi „przetwarzanie" objęte zakresem dyrektywy 2016/680[35]. Ponadto stwierdził on, po pierwsze, że przetwarzanie to zmierza do osiągnięcia prawnie uzasadnionego celu, oraz, po drugie, że nie można uznać go za niezgodne z prawem wyłącznie na tej podstawie, że do czynów, na których opiera się czerwona nota, mogłaby znaleźć zastosowanie zasada ne bis in idem[36]. Wspomniane przetwarzanie przez organy państwa członkowskiego może okazać się niezbędne właśnie w celu sprawdzenia, czy zasada ta ma zastosowanie (pkt 111, 114, 116, 117, 119).

W tych okolicznościach Trybunał orzekł również, że dyrektywa 2016/680 w związku z art. 54 KWUS i z art. 50 karty nie stoi na przeszkodzie przetwarzaniu danych osobowych zawartych w czerwonej nocie, dopóki prawomocne orzeczenie sądowe nie wykaże, że w danej sprawie znajduje zastosowanie zasada ne bis in idem. Takie przetwarzanie musi jednak spełniać wymogi przewidziane w tej dyrektywie. W tym kontekście musi ono być w szczególności niezbędne do wykonania zadania realizowanego przez właściwy organ krajowy w celach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar[37] (pkt 121; sentencja, pkt 2).

Jeżeli natomiast zasada ne bis in idem znajduje zastosowanie, to utrwalenie w bazach osób poszukiwanych państw członkowskich danych osobowych zawartych w czerwonej nocie Interpolu nie jest już niezbędne, jako że dana osoba nie może być już w państwach członkowskich ścigana za czyny objęte rzeczoną notą, a w konsekwencji nie może być już zatrzymana ze względu na te same czyny. Wynika stąd, że zainteresowana osoba powinna móc zażądać usunięcia swoich danych. Jeżeli jednak to utrwalenie zostaje utrzymane, powinna mu towarzyszyć wzmianka, że osoba ta nie może już być ścigana za te same czyny w państwie członkowskim lub w umawiającym się państwie ze względu na zasadę ne bis in idem (pkt 120).

[35] Zobacz art. 2 ust. 1 i art. 3 pkt 2 dyrektywy 2016/680.

[36] Zobacz art. 4 ust. 1 lit. b) i art. 8 ust. 1 dyrektywy 2016/680.

[37] Zobacz art. 1 ust. 1 i art. 8 ust. 1 dyrektywy 2016/680.

Wyrok z dnia 22 czerwca 2021 r. (wielka izba), Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU:C:2021:504)

W wyroku tym (zob. także część II.3, zatytułowaną „Pojęcie »przetwarzania danych osobowych«") Trybunał orzekł, że RODO stoi na przeszkodzie uregulowaniu zobowiązującemu Ceļu satiksmes drošības direkcija (dyrekcję bezpieczeństwa ruchu drogowego, Łotwa) (zwaną dalej „CSDD") do publicznego udostępniania danych dotyczących punktów karnych nakładanych na kierowców pojazdów za wykroczenia drogowe, bez konieczności wykazywania przez osobę wnioskującą o dostęp szczególnego interesu w ich uzyskaniu. Stwierdził on, że konieczność udostępnienia danych osobowych dotyczących punktów karnych za wykroczenia drogowe, w szczególności w świetle celu poprawy bezpieczeństwa na drogach, na który powołuje się rząd łotewski, nie została wykazana. Ponadto zdaniem Trybunału ani prawo publicznego dostępu do dokumentów urzędowych, ani prawo do wolności informacji nie uzasadniają takiego uregulowania (pkt 113, 120–122; sentencja, pkt 2).

W tym kontekście Trybunał podkreślił, że poprawa bezpieczeństwa na drogach, o którym mowa w łotewskich przepisach, stanowi cel interesu ogólnego uznawany przez Unię i że w związku z tym państwa członkowskie mogą zakwalifikować bezpieczeństwo na drogach jako „zadanie realizowane w interesie publicznym"[38]. Jednakże konieczność łotewskiego systemu przekazywania danych osobowych dotyczących punktów karnych dla osiągnięcia zamierzonego celu nie została wykazana. Z jednej strony bowiem ustawodawca łotewski dysponuje wieloma sposobami działania, które pozwoliłyby mu na osiągnięcie tego celu za pomocą innych środków, w mniejszym stopniu naruszających prawa podstawowe zainteresowanych osób. Z drugiej strony należy mieć na uwadze wrażliwość danych dotyczących punktów karnych oraz fakt, że ich publiczne udostępnianie może stanowić poważną ingerencję w prawa do poszanowania życia prywatnego i do ochrony danych osobowych, ponieważ może ono prowadzić do dezaprobaty społeczeństwa i do stygmatyzacji osoby, której dane dotyczą (pkt 109–113).

Ponadto Trybunał uznał, że biorąc pod uwagę wrażliwość tych danych i wagę tej ingerencji w te dwa prawa podstawowe, prawa te są nadrzędne zarówno wobec interesu publicznego w uzyskaniu dostępu do dokumentów urzędowych, takich jak krajowy rejestr pojazdów i ich kierowców, jak i wobec prawa do wolności informacji (pkt 120, 121).

W dodatku, z tych samych względów Trybunał orzekł, że RODO sprzeciwia się również przepisom łotewskim w zakresie, w jakim upoważniają one CSDD do przekazywania danych dotyczących punktów karnych nałożonych na kierowców pojazdów za wykroczenia drogowe podmiotom gospodarczym, tak aby te ostatnie mogły je ponownie wykorzystywać i ujawniać publicznie (pkt 126; sentencja, pkt 3).

Wreszcie Trybunał uściślił, że zasada pierwszeństwa prawa Unii sprzeciwia się temu, by sąd odsyłający, do którego wniesiono skargę na przepisy łotewskie uznane przez Trybunał za niezgodne z prawem Unii, postanowił utrzymać w mocy skutki prawne tych przepisów do dnia ogłoszenia swojego ostatecznego wyroku (pkt 137; sentencja, pkt 4).

[38] Zgodnie z art. 6 ust. 1 lit. e) RODO przetwarzanie danych jest zgodne z prawem, jeśli jest ono „niezbędne do wykonania zadania realizowanego w interesie publicznym".

III. Przetwarzanie danych osobowych w rozumieniu dyrektywy 2002/58

Wyrok z dnia 2 października 2018 r. (wielka izba), Ministerio Fiscal (C-207/16, EU:C:2018:788)[39]

Niniejsza sprawa dotyczyła oddalenia przez hiszpański sąd śledczy wniosku złożonego w ramach śledztwa w sprawie rozboju, w wyniku którego skradziono portfel i telefon komórkowy. W szczególności policja zwróciła się do wspomnianego sądu o udzielenie jej dostępu do danych identyfikacyjnych użytkowników numerów telefonów aktywowanych ze skradzionego telefonu w okresie 12 dni od daty kradzieży. Oddalenie to zostało umotywowane tym, że czyny objęte dochodzeniem nie stanowiły przestępstwa „poważnego", to znaczy, zgodnie z prawem hiszpańskim, zagrożonego karą powyżej pięciu lat pozbawienia wolności, a dostęp do danych identyfikacyjnych jest możliwy wyłącznie w przypadku tego typu przestępstw.

Po wskazaniu, że dostęp organów publicznych do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej w ramach dochodzenia w postępowaniu karnym wchodzi w zakres zastosowania dyrektywy 2002/58, Trybunał przypomniał, że dostęp organów publicznych do danych mających na celu identyfikację posiadaczy kart SIM aktywowanych przy użyciu skradzionego telefonu komórkowego, takich jak nazwiska, imiona i ewentualnie adresy tych posiadaczy, stanowi ingerencję w podstawowe prawo do poszanowania życia prywatnego oraz w prawo podstawowe do ochrony danych osobowych, zapisane w karcie, nawet w braku okoliczności pozwalających na zakwalifikowanie tej ingerencji jako „poważnej", i nie ma znaczenia, czy informacje związane z życiem prywatnym osób, których dotyczą, mają charakter wrażliwy czy nie, lub czy zainteresowane osoby poniosły jakiekolwiek negatywne konsekwencje z powodu tej ingerencji. Trybunał podkreślił jednak, że ingerencja ta nie jest na tyle poważna, aby dostęp ten należało ograniczyć – w zakresie zapobiegania, dochodzenia, wykrywania i ścigania przestępstw kryminalnych – do walki z poważną przestępczością. O ile bowiem dyrektywa 2002/58 w sposób wyczerpujący wymienia cele, które mogą uzasadniać uregulowanie krajowe normujące dostęp organów publicznych do odnośnych danych i tym samym stanowiące odstępstwo od zasady poufności łączności elektronicznej, a dostęp ten powinien odpowiadać rzeczywiście i ściśle jednemu z tych celów, o tyle Trybunał zauważa, że jeżeli chodzi o cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu przestępstw, brzmienie dyrektywy 2002/58 nie ogranicza tego celu do zwalczania poważnych przestępstw, lecz odnosi się ogólnie do „przestępstw kryminalnych" (pkt 38, 42, 59–63; sentencja).

W tym kontekście Trybunał wyjaśnił, że o ile w wyroku Tele2 Sverige i Watson i in.[40] orzekł on, że jedynie walka z poważną przestępczością może usprawiedliwiać dostęp organów publicznych do danych osobowych zatrzymywanych przez dostawców usług łączności elektronicznej, których całokształt może dostarczyć precyzyjnych wskazówek dotyczących życia prywatnego osób, o których dane chodzi, o tyle wykładnia taka była uzasadniona okolicznością, że cel realizowany przez uregulowanie normujące ten dostęp powinien być powiązany z wagą ingerencji w odnośne prawa podstawowe, jaką dostęp taki pociąga za sobą. I tak, zgodnie z zasadą proporcjonalności, poważna ingerencja może bowiem być uzasadniona w tej dziedzinie jedynie przez cel polegający

[39] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2018, s. 88–89.
[40] Wyrok Trybunału z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970),

na zwalczaniu przestępczości, którą można uznać za „poważną". Jeżeli natomiast ingerencja wynikająca z takiego dostępu nie jest poważna, to dostęp ów może być uzasadniony celem polegającym na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu „przestępstw kryminalnych" (pkt 54–57).

W niniejszej sprawie Trybunał uznał, że dostęp wyłącznie do danych objętych spornym wnioskiem nie może zostać uznany za „poważną" ingerencję w prawa podstawowe osób, o których dane chodzi, ponieważ dane te nie pozwalają na wyciągnięcie konkretnych wniosków dotyczących ich życia prywatnego. Trybunał wywiódł stąd, że ingerencja, którą spowodowałby dostęp do takich danych, może być zatem uzasadniona przez cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu ogółu „przestępstw kryminalnych", bez konieczności zakwalifikowania tych przestępstw jako „poważnych" (pkt 61, 62).

Wyroki z dnia 6 października 2020 r (wielka izba), Privacy International (C-623/17, EU:C:2020:790) i La Quadrature du Net i in. (C-511/18, C-512/18 i i C-520/18 i C-520/18, EU:C:2020:791)[41]

Orzecznictwo dotyczące zatrzymywania danych osobowych i dostępu do nich w dziedzinie komunikacji elektronicznej, w szczególności wyrok Tele2 Sverige i Watson i in., w którym stwierdzono między innymi, że państwa członkowskie nie mogą nakładać na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, wzbudziło zaniepokojenie niektórych państw członkowskich, obawiających się pozbawienia ich instrumentu koniecznego do ochrony bezpieczeństwa narodowego i do zwalczania przestępczości.

To na tym tle do Investigatory Powers Tribunal (sądu ds. uprawnień dochodzeniowych, Zjednoczone Królestwo) (Privacy International, C-623/17), Conseil d'État (rady stanu, Francja) (La Quadrature du Net i in., sprawy połączone C-511/18 i C-512/18), a także Cour constitutionnelle (trybunału konstytucyjnego, Belgia) (Ordre des barreaux francophones et germanophone i in., C-520/18) wpłynęły sprawy dotyczące zgodności z prawem uregulowań przyjętych przez niektóre państwa członkowskie, przewidujących w szczególności zobowiązanie dostawców usług elektronicznych do transmitowania organowi publicznemu lub do zatrzymywania w sposób uogólniony i niezróżnicowany danych użytkowników dotyczących ruchu i lokalizacji.

W dwóch wyrokach wydanych w dniu 6 października 2020 r. w składzie wielkiej izby Trybunał orzekł przede wszystkim, że uregulowania krajowe nakładające na dostawców usług łączności elektronicznej obowiązek zatrzymywania danych o ruchu i danych o lokalizacji lub też transmitowania w tym celu owych danych służbom wywiadu i bezpieczeństwa są objęte zakresem zastosowania dyrektywy 2002/58 (pkt 49; sentencja, pkt 1 wyroku Privacy International; pkt 104 wyroku La Quadrature du Net i in.)

Następnie Trybunał przypomniał, że dyrektywa 2002/58[42] nie pozwala na to, by odstępstwo od zasadniczego obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych oraz od zakazu przechowywania tych danych stało się regułą. Oznacza to, że

[41] Wyroki te zostały przedstawione w sprawozdaniu rocznym 2020, s. 29–32

[42] Artykuł 15 ust. 1 i 3 dyrektywy 2002/58.

dyrektywa ta zezwala państwom członkowskim na przyjmowanie – między innymi do celów bezpieczeństwa narodowego – środków ustawodawczych mających na celu ograniczenie praw i obowiązków przewidzianych w tej dyrektywie, zwłaszcza obowiązku zapewnienia poufności łączności elektronicznej i danych o ruchu[43], wyłącznie z poszanowaniem ogólnych zasad prawa Unii, wśród których figuruje zasada proporcjonalności, oraz praw podstawowych gwarantowanych w karcie[44] (pkt 59, 60 wyroku Privacy International; pkt 111, 113 wyroku La Quadrature du Net i in.).

W tym kontekście Trybunał po pierwsze stwierdził, w sprawie Privacy International, że dyrektywa 2002/58 w związku z kartą stoi na przeszkodzie uregulowaniu krajowemu nakładającemu na dostawców usług łączności elektronicznej, do celów ochrony bezpieczeństwa narodowego, obowiązku uogólnionego i niezróżnicowanego transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji. Po drugie, w sprawach połączonych La Quadrature du Net i in., jak również w sprawie Ordre des barreaux francophones et germanophone i in., Trybunał orzekł, że ta sama dyrektywa stoi na przeszkodzie środkom ustawodawczym nakładającym na dostawców usług łączności elektronicznej obowiązek prewencyjnego, uogólnionego i niezróżnicowanego, zatrzymywania danych o ruchu i danych o lokalizacji.

Wspomniane bowiem obowiązki transmisji i uogólnionego i niezróżnicowanego zatrzymywania takich danych stanowią szczególnie poważne ingerencje w prawa podstawowe gwarantowane kartą mimo braku związku zachowania osób, których danych to dotyczy, z celem rozpatrywanego uregulowania. Analogicznie Trybunał dokonał wykładni art. 23 ust. 1 RODO w świetle karty w ten sposób, że stoi on na przeszkodzie środkom ustawodawczym nakładającym na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych obowiązek uogólnionego i niezróżnicowanego zatrzymywania między innymi danych osobowych dotyczących tych usług (pkt 71, 82; sentencja, pkt 2 wyroku Privacy International; pkt 146, 168, 174, 177, 212; sentencja, pkt 1, 3 wyroku La Quadrature du Net i in.).

Trybunał stwierdził natomiast, że w sytuacjach, gdy dane państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia, dyrektywa 2002/58 w związku z kartą nie stoi na przeszkodzie nakazaniu dostawcom usług łączności elektronicznej zatrzymywania w sposób uogólniony i niezróżnicowany danych o ruchu i danych o lokalizacji. W tym kontekście Trybunał sprecyzował, że decyzja o wydaniu takiego nakazu, wydana na określony czas ograniczony do tego, co ściśle niezbędne, powinna podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, w celu weryfikacji występowania jednej z takich sytuacji oraz poszanowania przewidzianych warunków i gwarancji. W takich warunkach rzeczona dyrektywa nie stoi na przeszkodzie również zautomatyzowanej analizie danych, w szczególności danych o ruchu i o lokalizacji, ogółu użytkowników środków łączności elektronicznej (pkt 137–139, 177–179; sentencja, pkt 1, 2 wyroku La Quadrature du Net i in.).

Trybunał dodał, że dyrektywa 2002/58 w związku z kartą nie stoi na przeszkodzie środkom ustawodawczym zezwalającym na ukierunkowane zatrzymywanie na określony czas ograniczony

[43] Artykuł 5 ust. 1 dyrektywy 2002/58.
[44] W szczególności art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

do tego, co ściśle niezbędne, danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego. Podobnie dyrektywa ta nie stoi na przeszkodzie takim środkom przewidującym uogólnione i niezróżnicowane zatrzymywanie adresów IP przypisanych do źródła połączenia, jeżeli czas tego zatrzymania jest ograniczony do tego, co ściśle niezbędne, ani środkom przewidującym uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; w tym ostatnim przypadku państwa członkowskie nie mają obowiązku ograniczenia zatrzymania w czasie. Ponadto wspomniana dyrektywa nie stoi na przeszkodzie środkowi ustawodawczemu umożliwiającemu szybkie zatrzymanie danych, którymi dysponują dostawcy usług, jeżeli pojawią się sytuacje, w których zaistnieje konieczność zatrzymania tych danych poza ustawowymi terminami zatrzymywania danych do celów wyjaśnienia poważnych przestępstw lub naruszeń bezpieczeństwa narodowego, jeżeli te przestępstwa lub naruszenia zostały już stwierdzone lub ich istnienie można racjonalnie podejrzewać (pkt 161, 163, 168; sentencja, pkt 1 wyroku La Quadrature du Net i in.).

Ponadto Trybunał orzekł, że dyrektywa 2002/58 w związku z kartą nie stoi na przeszkodzie uregulowaniu krajowemu nakładającemu na dostawców usług łączności elektronicznej obowiązek gromadzenia w czasie rzeczywistym między innymi danych o ruchu i danych o lokalizacji, jeżeli to gromadzenie ogranicza się do osób, co do których istnieje ważny powód, by podejrzewać, że są one zaangażowane w taki lub inny sposób w działalność terrorystyczną, oraz podlega uprzedniej kontroli przeprowadzanej albo przez sąd, albo przez niezależny organ administracyjny, którego decyzja ma skutek wiążący, przy czym ten sąd lub ten organ upewni się, że zezwolenie na takie gromadzenie w czasie rzeczywistym zostało wydane jedynie w granicach tego, co jest ściśle niezbędne. W przypadkach pilnych kontrola powinna nastąpić w krótkim czasie (pkt 192; sentencja, pkt 2 wyroku La Quadrature du Net i in.).

Wreszcie Trybunał zajął się kwestią pozostawienia w mocy skutków uregulowania krajowego uznanego za niezgodne z prawem Unii. W tej kwestii Trybunał orzekł, że sąd krajowy nie może zastosować przepisu prawa krajowego, który upoważnia go do ograniczenia w czasie skutków stwierdzenia przez niego niezgodności z prawem uregulowania krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, uznanego za niezgodne z dyrektywą 2002/58 w związku z kartą.

Mimo to, w celu udzielenia sądowi krajowemu użytecznej odpowiedzi, Trybunał przypomniał, że dopuszczalność i ocena dowodów uzyskanych w wyniku sprzecznego z prawem Unii zatrzymania danych w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie poważnych przestępstw podlegają, w obecnym stanie prawa Unii, wyłącznie prawu krajowemu. Trybunał uściślił jednak, że dyrektywa 2002/58, interpretowana w świetle zasady skuteczności, wymaga, by w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstwa krajowy sąd karny nie uwzględnił dowodów uzyskanych w drodze uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii, jeżeli osoby te nie są w stanie skutecznie ustosunkować się do tych dowodów (pkt 222, 228; sentencja, pkt 4 wyroku La Quadrature du Net i in.).

Wyrok z dnia 2 marca 2021 r. (wielka izba), Prokuratuur (Warunki dostępu do danych związanych z łącznością elektroniczną) (C-746/18, EU:C:2021:152)

W Estonii wszczęto postępowanie karne przeciwko H. K. pod zarzutem kradzieży, wykorzystania karty bankowej osoby trzeciej oraz przemocy wobec osób uczestniczących w postępowaniu sądowym. H. K. została skazana za popełnienie tych przestępstw na karę dwóch lat pozbawienia wolności przez sąd pierwszej instancji. Orzeczenie to zostało następnie utrzymane w mocy w postępowaniu apelacyjnym. Protokoły, na których opiera się ustalenie popełnienia tych przestępstw, zostały w szczególności sporządzone na podstawie danych osobowych generowanych w ramach świadczenia usług łączności elektronicznej. Riigikohus (sąd najwyższy, Estonia), do którego H. K. wniosła skargę kasacyjną, wyraził wątpliwości co do zgodności z prawem Unii[45] warunków dostępu do tych danych przez służby prowadzące dochodzenie.

Wątpliwości te dotyczą w pierwszej kolejności kwestii, czy długość okresu, w którym służby prowadzące dochodzenie miały dostęp do danych, stanowi kryterium pozwalające ocenić wagę ingerencji, jaką stanowi ów dostęp, w prawa podstawowe zainteresowanych osób. Tak więc, w sytuacji gdy okres ten jest bardzo krótki lub gdy ilość zebranych danych jest bardzo ograniczona, sąd odsyłający zastanawiał się nad tym, czy cel polegający na zwalczaniu ogółu przestępczości, a nie tylko zwalczaniu poważnej przestępczości, może uzasadniać taką ingerencję. W drugiej kolejności sąd odsyłający powziął wątpliwości co do możliwości uznania estońskiej prokuratury – biorąc pod uwagę różne zadania powierzone jej przez przepisy krajowe – za „niezależny" organ administracyjny, w rozumieniu wyroku Tele2 Sverige i Watson i in.[46], który może zezwolić organowi dochodzeniowemu na dostęp do rozpatrywanych danych.

W wyroku wydanym w składzie wielkiej izby Trybunał orzekł, że dyrektywa 2002/58, interpretowana w świetle karty praw podstawowych, stoi na przeszkodzie przepisom krajowym umożliwiającym dostęp organów władzy publicznej do danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego. Zdaniem Trybunału długość okresu, na jaki wniesiono o dostęp do tych danych, oraz ilość bądź rodzaj danych dostępnych przez taki okres, nie ma w tym względzie znaczenia. Ponadto Trybunał stwierdził, że dyrektywa ta, interpretowana w świetle karty, stoi na przeszkodzie przepisom krajowym przyznającym prokuraturze kompetencję do udzielania zezwoleń na dostęp organu władzy publicznej do danych o ruchu i danych o lokalizacji w celu prowadzenia postępowania przygotowawczego (pkt 45, 59; sentencja, pkt 1, 2).

Jeśli chodzi o realizowany przez przepisy rozpatrywane w postępowaniu głównym cel polegający na dochodzeniu, wykrywaniu i karaniu przestępstw lub zapobieganiu im, Trybunał orzekł, że zgodnie z zasadą proporcjonalności jedynie cele w postaci zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego mogą uzasadniać

[45] Dokładniej mówiąc, z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.
[46] Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970, pkt 120).

dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które umożliwiają wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane dotyczą, przy czym inne czynniki związane z proporcjonalnością wniosku o udzielenie dostępu, takie jak długość okresu, na jaki wniesiono o dostęp do takich danych, nie mogą skutkować tym, by cel polegający na dochodzeniu, wykrywaniu i karaniu ogółu przestępstw lub zapobieganiu im mógł uzasadniać taki dostęp (pkt 33, 35).

Odnośnie do przyznanej prokuraturze kompetencji do udzielania zezwoleń organowi władzy publicznej na dostęp do danych o ruchu i danych o lokalizacji w celu przeprowadzenia postępowania przygotowawczego, Trybunał przypomniał, że do prawa krajowego należy określenie warunków, na jakich dostawcy usług łączności elektronicznej powinni udzielić właściwym organom państwowym dostępu do danych będących w ich posiadaniu. Jednakże, aby spełnić wymóg proporcjonalności, takie uregulowanie musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć. To uregulowanie musi być prawnie wiążące w prawie wewnętrznym i wskazywać, w jakich okolicznościach i pod jakimi warunkami materialnymi i proceduralnymi można przyjąć środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja zostanie ograniczona do tego, co ściśle niezbędne (pkt 48).

Zdaniem Trybunału w celu zapewnienia w praktyce pełnej zgodności z tymi warunkami ważne jest, aby dostęp właściwych organów państwowych do zatrzymanych danych był uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, a decyzja tego sądu lub organu była wydawana na uzasadniony wniosek owych organów państwowych, złożony w szczególności w ramach postępowań mających na celu wykrywanie lub karanie przestępstw lub zapobieganie im. W pilnych i należycie uzasadnionych przypadkach kontrola powinna nastąpić w krótkim czasie (pkt 51).

W tym względzie Trybunał wyjaśnił, że uprzednia kontrola wymaga między innymi, aby sąd lub organ odpowiedzialny za przeprowadzenie tej kontroli dysponował wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia poszczególnych wchodzących w grę interesów i praw. Jeśli chodzi w szczególności o dochodzenie karne, taka kontrola wymaga, aby ten sąd lub organ był w stanie zapewnić właściwą równowagę pomiędzy z jednej strony interesami związanymi z potrzebami dochodzenia w ramach zwalczania przestępczości, a z drugiej strony prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych osób, których dane są udostępniane. Jeżeli kontrola ta jest dokonywana nie przez sąd, lecz przez niezależny organ administracyjny, musi on posiadać status pozwalający mu działać przy wykonywaniu swoich obowiązków w sposób obiektywny i bezstronny i w tym celu powinien on pozostawać poza jakimkolwiek wpływem z zewnątrz (pkt 52, 53).

Według Trybunału z powyższego wynika, że wymóg niezależności, który powinien spełniać organ odpowiedzialny za przeprowadzenie uprzedniej kontroli, wymaga, aby organ ten miał status strony trzeciej w stosunku do organu wnoszącego o udzielenie dostępu do danych, tak aby ten pierwszy był w stanie przeprowadzić tę kontrolę w sposób obiektywny i bezstronny, poza jakimkolwiek wpływem z zewnątrz. W szczególności w dziedzinie prawa karnego wymóg niezależności oznacza, że organ odpowiedzialny za tę uprzednią kontrolę, po pierwsze, nie jest zaangażowany w prowadzenie omawianego dochodzenia karnego, a po drugie, zajmuje

neutralną pozycję wobec stron postępowania karnego. Tymczasem nie jest tak w przypadku prokuratury, która, tak jak prokuratura estońska, kieruje dochodzeniem i, w stosownych przypadkach, sprawuje funkcję oskarżyciela publicznego. Prokuratura nie jest zatem w stanie przeprowadzić wspomnianej uprzedniej kontroli (pkt 54, 55, 57).

IV. Przekazywanie danych osobowych do państw trzecich

Wyrok z dnia 6 listopada 2003 r. (wielka izba), Lindqvist (C-101/01, EU:C:2003:596)[47]

W tej sprawie (zob. także część II.3, zatytułowaną „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 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; sentencja, pkt 4).

Jeśli uwzględnić z jednej strony stan rozwoju Internetu w okresie trwania prac nad dyrektywą 95/46 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 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)[48]

Maximillian Schrems, obywatel austriacki i użytkownik sieci społecznościowej Facebook, wniósł skargę do Data Protection Commissionner (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

[47] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2003, s. 67.
[48] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2015, s. 53.

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[49] Komisja stwierdziła, iż w ramach systemu zwanego „bezpieczną przystanią" (ang. „safe harbour")[50] Stany Zjednoczone zapewniają odpowiedni poziom ochrony przekazywanych danych osobowych.

W tym kontekście High Court (wysoki trybunał, Irlandia) zwrócił się do Trybunału z wnioskiem o wykładnię art. 25 ust. 6 dyrektywy 95/46, 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, przyjętej przez Komisję na podstawie wspomnianego art. 25 ust. 6 dyrektywy 95/46.

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 tego nie uczyniła, art. 1 tej decyzji narusza wymogi ustanowione w art. 25 ust. 6 dyrektywy 95/46 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 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; sentencja, pkt 2).

Poza tym Trybunał stwierdził nieważność art. 3 decyzji 2000/520, ponieważ pozbawia on krajowe organy nadzorcze ich kompetencji wynikających z art. 28 dyrektywy 95/46, 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 miała wpływ na ważność tej decyzji w całości (pkt 105, 106).

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 bezprawnym wykorzystywaniem. Konieczność zapewnienia takich

[49] Decyzja 2000/520/WE Komisji 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. 2000, L 215, s. 7).

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

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 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 rządowym 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).

Wyrok z dnia 16 lipca 2020 r. (wielka izba), Facebook Ireland i Schrems (C-311/18, EU:C:2020:559)[51]

RODO stanowi, że przekazywanie danych do państwa trzeciego może nastąpić co do zasady tylko wtedy, gdy dane państwo trzecie zapewni odpowiedni stopień ich ochrony. Zgodnie z tym rozporządzeniem Komisja może stwierdzić, że państwo trzecie – poprzez swoje ustawodawstwo krajowe lub zobowiązania międzynarodowe – zapewnia odpowiedni stopień ochrony[52]. W braku takiej decyzji stwierdzającej odpowiedni stopień ochrony przekazanie to może nastąpić tylko wtedy, gdy podmiot przekazujący dane osobowe, mający siedzibę w Unii, ustanowi odpowiednie zabezpieczenia, które mogą wynikać w szczególności ze standardowych klauzul ochrony danych przyjętych przez Komisję, i jeżeli zainteresowane osoby dysponują egzekwowalnymi prawami i skutecznymi środkami ochrony prawnej[53]. Poza tym RODO ustala w szczegółowy sposób

[51] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2020, s. 26–29.
[52] Artykuł 45 RODO.
[53] Artykuł 46 ust. 1, art. 46 ust. 2 lit. c) RODO.

warunki, w których przekazywanie danych może mieć miejsce w braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń[54].

Maximilian Schrems, obywatel austriacki zamieszkały w Austrii, jest użytkownikiem Facebooka od 2008 roku. Podobnie jak w przypadku innych użytkowników zamieszkałych w Unii, dane osobowe M. Schremsa są w całości lub w części przekazywane przez Facebook Ireland do serwerów należących do Facebook Inc., znajdujących się na terytorium Stanów Zjednoczonych, gdzie są przetwarzane. M. Schrems wniósł skargę do irlandzkiego organu nadzorczego zmierzającą zasadniczo do zakazania tego przekazywania. Podniósł on, że prawo i praktyka Stanów Zjednoczonych nie zapewniają wystarczającej ochrony przed dostępem organów publicznych do danych przekazywanych do tego kraju. Skarga ta została oddalona, w szczególności ze względu na to, że w decyzji 2000/520[55] Komisja stwierdziła, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony. Wyrokiem z dnia 6 października 2015 r. Trybunał, do którego High Court (wysoki trybunał, Irlandia) zwrócił się z pytaniem prejudycjalnym, orzekł nieważność tej decyzji (zwany dalej „wyrokiem Schrems I")[56] (pkt 52, 53).

W następstwie wyroku Schrems i późniejszego stwierdzenia przez sąd irlandzki nieważności decyzji oddalającej skargę M. Schremsa irlandzki organ nadzorczy wezwał go do przeformułowania skargi, mając na względzie stwierdzenie nieważności decyzji 2000/520 przez Trybunał. W przeformułowanej skardze M. Schrems utrzymuje, że Stany Zjednoczone nie zapewniają wystarczającej ochrony danych przekazywanych do tego państwa. Żąda on zawieszenia lub zakazania na przyszłość przekazywania jego danych osobowych z Unii do Stanów Zjednoczonych, które Facebook Ireland prowadzi obecnie na podstawie standardowych klauzul ochrony zawartych w załączniku do decyzji 2010/87/UE[57]. Uznawszy, że rozpatrzenie skargi M. Schremsa zależy w szczególności od ważności decyzji 2010/87, irlandzki organ nadzorczy wszczął postępowanie przed High Court, aby ten przedłożył Trybunałowi wniosek o wydanie orzeczenia w trybie prejudycjalnym. Po wszczęciu tego postępowania Komisja przyjęła decyzję (UE) 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA[58] (pkt 54, 55, 57).

We wniosku o wydanie orzeczenia w trybie prejudycjalnym sąd odsyłający zwraca się do Trybunału o wyjaśnienie, czy RODO ma zastosowanie do przekazywania danych osobowych opartego na standardowych klauzulach ochrony zawartych w decyzji 2010/87, jaki jest stopień ochrony wymagany przez to rozporządzenie w ramach takiego przekazywania danych oraz jakie obowiązki spoczywają w tym kontekście na organach nadzorczych. Ponadto High Court podnosi kwestię ważności zarówno decyzji 2010/87, jak i decyzji 2016/1250.

Trybunał stwierdza, że analiza decyzji 2010/87 w świetle Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą") nie ujawnia żadnego elementu, który mógłby wpłynąć na jej

---

54 Artykuł 49 RODO.

55 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. 2000, L 215, s. 7).

56 Wyrok Trybunału z dnia 6 października 2015 r., Schrems (C-362/14, EU:C:2015:650) (zob. także komunikat prasowy nr 117/15).

57 Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46 Parlamentu Europejskiego i Rady (Dz.U. 2010, L 39, s. 5), zmieniona decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r. (Dz.U. 2016, L 344, s. 100).

58 Decyzja wykonawcza Komisji z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA (Dz.U. 2016, L 207, s. 1).

ważność. Stwierdza natomiast nieważność decyzji 2016/1250 (sentencja, pkt 4, 5).

Trybunał uważa przede wszystkim, że prawo Unii, a w szczególności RODO, ma zastosowanie do przekazywania danych osobowych w celach handlowych przez podmiot gospodarczy mający siedzibę w jednym państwie członkowskim do innego podmiotu gospodarczego z siedzibą w państwie trzecim, nawet jeśli w trakcie lub w następstwie tego przekazania dane te mogą być przetwarzane do celów bezpieczeństwa publicznego, obronności i bezpieczeństwa państwa przez organy danego państwa trzeciego. Wyjaśnia on, że ten rodzaj przetwarzania danych przez organy państwa trzeciego nie może wykluczyć takiego przekazania z zakresu stosowania RODO (pkt 86, 88, 89; sentencja, pkt 1).

Co się tyczy poziomu ochrony wymaganego w ramach takiego przekazywania, Trybunał stwierdza, że wymogi przewidziane w tym celu w przepisach RODO, które dotyczą odpowiednich zabezpieczeń, egzekwowalnych praw oraz skutecznych środków ochrony prawnej, należy interpretować w ten sposób, że osoby, których dane osobowe są przekazywane do państwa trzeciego na podstawie klauzul ochrony danych, powinny korzystać z poziomu ochrony merytorycznie równoważnego poziomowi gwarantowanemu w Unii na podstawie tego rozporządzenia, interpretowanego w świetle karty. W tym kontekście wyjaśnia on, że ocena tego stopnia ochrony powinna uwzględniać zarówno postanowienia umowne uzgodnione między podmiotem przekazującym dane, mającym siedzibę w Unii, a podmiotem odbierającym z siedzibą w danym państwie trzecim, jak i – w odniesieniu do ewentualnego dostępu organów władzy publicznej tego państwa trzeciego do przekazanych w ten sposób danych – istotne elementy jego systemu prawnego (pkt 105; sentencja, pkt 2).

Co się tyczy obowiązków spoczywających na organach nadzorczych w kontekście takiego przekazywania, Trybunał stwierdza, że – o ile nie istnieje ważna decyzja Komisji stwierdzająca odpowiedni stopień ochrony danych – same te organy są zobowiązane do zawieszenia lub zakazania przekazywania danych osobowych do państwa trzeciego, jeżeli uznają w świetle okoliczności towarzyszących temu przekazywaniu, że standardowe klauzule ochrony danych nie są lub nie mogą być przestrzegane w tym państwie trzecim, a ochrona przekazywanych danych, jakiej wymaga prawo Unii, nie może być zapewniona innymi środkami (pkt 121; sentencja, pkt 3).

Trybunał bada następnie ważność decyzji 2010/87. Zdaniem Trybunału ważności tej decyzji nie podważa fakt, że standardowe klauzule ochrony danych zawarte w tej decyzji ze względu na ich umowny charakter nie wiążą organów państwa trzeciego, do którego może nastąpić przekazanie danych. Wyjaśnia natomiast, że ważność ta zależy od tego, czy wspomniana decyzja przewiduje skuteczne mechanizmy umożliwiające w praktyce zapewnienie przestrzegania stopnia ochrony wymaganego przez prawo Unii i czy odbywające się na podstawie takich klauzul przekazywanie danych osobowych zostanie w przypadku ich naruszenia lub niemożności ich przestrzegania zawieszone lub zakazane. Trybunał stwierdza, że decyzja 2010/87 wprowadza takie mechanizmy. W tym względzie podkreśla on w szczególności, że decyzja ta nakłada na podmiot przekazujący dane i na podmiot odbierający obowiązek uprzedniego sprawdzenia, czy w danym państwie trzecim jest przestrzegany ten stopień ochrony, i że zobowiązuje ona ten podmiot odbierający do poinformowania podmiotu przekazującego o swej ewentualnej niemożności zastosowania się do standardowych klauzul ochrony, w którym to przypadku do tego ostatniego należy zawieszenie przekazywania danych lub rozwiązanie umowy z pierwszym (pkt 132, 136, 137, 142, 148; sentencja, pkt 4).

Wreszcie Trybunał przeprowadza badanie ważności decyzji 2016/1250 w świetle wymogów wynikających z RODO, interpretowanych w świetle postanowień karty gwarantujących poszanowanie życia prywatnego i rodzinnego, ochronę danych osobowych i prawo do skutecznej ochrony sądowej. W tym względzie Trybunał zauważa, że decyzja ta ustanawia, podobnie jak decyzja 2000/520, pierwszeństwo wymogów dotyczących bezpieczeństwa narodowego, interesu publicznego i przestrzegania ustawodawstwa amerykańskiego, umożliwiając w ten sposób ingerencje w prawa podstawowe osób, których dane są przekazywane do tego państwa trzeciego. Zdaniem Trybunału ograniczenia ochrony danych osobowych wynikające z wewnętrznych regulacji Stanów Zjednoczonych dotyczących dostępu i wykorzystywania przez amerykańskie organy władz publicznych takich danych przekazywanych z Unii do tego państwa trzeciego, a które Komisja oceniła w decyzji 2016/1250, nie są uregulowane w sposób odpowiadający wymogom, które są merytorycznie równoważne wymogom ustanowionym w prawie Unii przez zasadę proporcjonalności, ponieważ programy monitorowania oparte na tych regulacjach nie są ograniczone do tego, co ściśle konieczne. Opierając się na stwierdzeniach zawartych w tej decyzji, Trybunał zauważa, że w odniesieniu do niektórych programów nadzoru wspomniane regulacje nie wskazują w żaden sposób na istnienie ograniczeń ustanowionego w nim uprawnienia odnoszącego się do wdrażania programów, ani też na istnienie gwarancji dla osób nieamerykańskich potencjalnie objętych tymi programami. Trybunał dodaje, że o ile regulacje te przewidują wymogi, które władze amerykańskie powinny spełnić przy wdrażaniu danych programów nadzoru, o tyle nie przyznają one zainteresowanym osobom praw, które mogłyby być egzekwowalne wobec władz amerykańskich przed sądami (pkt 164, 165, 180–182, 184, 185).

Co się tyczy wymogu ochrony sądowej, Trybunał stwierdza, że wbrew temu, co Komisja ustaliła w decyzji 2016/1250, mechanizm mediacji, o którym mowa w tej decyzji, nie zapewnia tym osobom środka odwoławczego przed organem oferującym zabezpieczenia merytorycznie równoważne z zabezpieczeniami wymaganymi w prawie Unii, tak aby zapewnić zarówno niezależność Rzecznika przewidzianego w tym mechanizmie, jak i istnienie norm upoważniających Rzecznika do wydawania wiążących decyzji w odniesieniu do amerykańskich służb wywiadowczych. Z tych wszystkich względów Trybunał stwierdza nieważność decyzji 2016/1250 (pkt 195–197, 201; sentencja, pkt 5).

V. 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, zatytułowaną „Pojęcie »przetwarzania danych osobowych«”) Trybunał wyjaśnił zakres przewidzianych w dyrektywie 95/46 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, 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; sentencja, pkt 3).

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 mającego za punkt wyjścia to imię i nazwisko, pozostaje bez związku z tym, czy zawarcie na liście wyników wyszukiwania danej informacji wyrządza szkodę osobie, której dotyczą dane (pkt 96; sentencja, pkt 4).

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; sentencja, pkt 4).

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)[59]

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 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 elektronicznym")[60], 2001/29/WE w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym[61], 2004/48/WE w sprawie egzekwowania praw własności intelektualnej[62] oraz dyrektywa 2002/58 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.

---

59 Wyrok ten został przedstawiony w sprawozdaniu rocznym 2008, s. 46.

60 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. 2000, L 178, s. 1).

61 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. 2001, L 167, s. 10).

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

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; sentencja).

Wyrok z dnia 24 listopada 2011 r., Scarlet Extended (C-70/10, EU:C:2011:771)[63]

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 w trybie prejudycjalnym odpowiedzi na pytanie, czy taki nakaz jest zgodny z prawem Unii.

Trybunał orzekł, że dyrektywy 95/46, 2000/31, 2001/29, 2002/58 i 2004/48, 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; sentencja).

Zdaniem Trybunału tego typu nakaz narusza bowiem wprowadzony przez art. 15 ust. 1 dyrektywy 2000/31 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).

W tym kontekście Trybunał orzekł po pierwsze, że nakaz ustanowienia spornego systemu filtrowania pociągałby za sobą konieczność przeprowadzania systematycznej analizy wszelkich

[63] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2011, s. 37.

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 (sąd najwyższy, Szwecja) zwrócił się do Trybunału w trybie prejudycjalnym w celu uzyskania wykładni dyrektyw 2002/58 i 2004/48, 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 z pytaniem, czy prawo Unii stoi na przeszkodzie stosowaniu przepisu krajowego, opartego na art. 8 dyrektywy 2004/48, 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 w związku z art. 15 ust. 1 dyrektywy 2002/58 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 i 2004/48 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; sentencja).

Wyrok z dnia 17 czerwca 2021 r., M.I.C.M. (C-597/19, EU:C:2021:492)

Przedsiębiorstwo Mircom International Content Management & Consulting (M.I.C.M.) Limited (zwane dalej „Mircomem") złożyło do Ondernemingsrechtbank Antwerpen (sądu gospodarczego w Antwerpii, Belgia, zwanego dalej „sądem odsyłającym") żądanie udzielenia informacji skierowane do Telenet BVBA, dostawcy usług dostępu do Internetu. Podnosząc to żądanie, Mircom zmierzał do uzyskania decyzji zobowiązującej Telenet do przedstawienia danych identyfikacyjnych jego klientów na podstawie adresów IP zgromadzonych dla Mircomu przez wyspecjalizowaną spółkę. Łącza internetowe klientów Telenetu były wykorzystywane do wzajemnego udostępniania w sieci równorzędnej (peer-to-peer) za pomocą protokołu BitTorrent filmów znajdujących się w katalogu Mircomu. Telenet sprzeciwił się temu żądaniu.

W tym kontekście sąd odsyłający zwrócił się do Trybunału przede wszystkim z pytaniem, czy wzajemne udostępnianie w tej sieci segmentów pliku multimedialnego zawierającego chroniony utwór stanowi publiczne udostępnianie na mocy prawa Unii. Następnie sąd ten chciał ustalić, czy podmiot praw własności intelektualnej, taki jak Mircom, który sam z nich nie korzysta, lecz ogranicza się do dochodzenia roszczeń odszkodowawczych od podmiotów, które w jego ocenie naruszają te prawa, może korzystać ze środków, procedur i środków naprawczych przewidzianych w prawie Unii w celu zapewnienia poszanowania tych praw, na przykład poprzez żądanie udzielenia informacji. Wreszcie sąd odsyłający zwrócił się do Trybunału o wyjaśnienie kwestii zgodności z prawem, po pierwsze, sposobu, w jaki Mircom zbierał adresy IP klientów, i, po drugie, udostępnienia danych, którego ten zażądał od Telenetu.

Trybunał orzekł, że prawo Unii[64] co do zasady nie stoi na przeszkodzie ani systematycznej rejestracji przez podmiot praw własności intelektualnej lub przez osoby trzecie adresów IP użytkowników sieci równorzędnych (peer-to-peer), których łącza internetowe miały być wykorzystywane do działań naruszających prawo (uprzednie przetwarzanie danych), ani podawaniu nazw i adresów pocztowych użytkowników do wiadomości tego podmiotu lub osoby trzeciej w celu wniesienia powództwa o odszkodowanie (późniejsze przetwarzanie danych). Jednakże inicjatywy i kierowane żądania powinny być uzasadnione, proporcjonalne i nie mieć znamion nadużycia, a ponadto winny one być przewidziane w krajowym środku ustawodawczym ograniczającym zakres praw i obowiązków wynikających z przepisów prawa Unii. Trybunał uściślił, że prawo to nie nakłada na spółkę taką jak Telenet obowiązku udostępniania osobom prywatnym danych osobowych po to, aby umożliwić im wnoszenie do sądów cywilnych powództw o naruszenie praw autorskich. Prawo Unii zezwala jednak państwom członkowskim na nałożenie takiego obowiązku (pkt 97, 125–127; sentencja, pkt 3).

3. Usunięcie linków do danych osobowych

Wyrok z dnia 24 września 2019 r. (wielka izba), GC i in. (Usunięcie linków do danych wrażliwych) (C-136/17, EU:C:2019:773)[65]

W wyroku tym Trybunał, orzekając w składzie wielkiej izby, wyjaśnił obowiązki operatora wyszukiwarki w ramach żądania usunięcia linków do danych wrażliwych.

Spółka Google odmówiła uwzględnienia żądań, wniesionych przez cztery osoby, usunięcia z wyświetlanej w wyszukiwarce listy wyników wyszukiwania mającego za punkt wyjścia ich imiona i nazwiska, różnego rodzaju linków kierujących do prowadzonych przez osoby trzecie stron internetowych, w szczególności do artykułów prasowych. W następstwie skarg wniesionych przez te cztery osoby, Commission nationale de l'informatique et des libertés (krajowa komisja ds. informatyki i swobód, CNIL) (Francja) odmówiła wezwania spółki Google do żądanego usunięcia linków. Rozpatrująca sprawę Conseil d'État (rada stanu, Francja) zwróciła się do Trybunału o wyjaśnienie obowiązków spoczywających na operatorze wyszukiwarki przy rozpatrywaniu żądania usunięcia linków na podstawie dyrektywy 95/46.

Po pierwsze, Trybunał przypomniał, że przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego jest zakazane[66], z zastrzeżeniem pewnych wyjątków i odstępstw. Jeśli chodzi o przetwarzanie danych dotyczących przestępstw (czynów zabronionych), wyroków skazujących lub środków bezpieczeństwa, to może ono zasadniczo odbywać się jedynie pod kontrolą władz publicznych lub też wówczas, gdy zgodnie z prawem krajowym ustanowiono odpowiednie i określone środki zabezpieczające[67] (pkt 39, 40).

64 Artykuł 6 ust. 1 lit. f) RODO i art. 15 ust. 1 dyrektywy 2002/58.
65 Wyrok ten został przedstawiony w sprawozdaniu rocznym 2019, s. 117 i 118.
66 Artykuł 8, ust. 1 dyrektywy 95/46 i art. 9 ust 1 rozporządzenia 2016/679.
67 Artykuł 8 ust. 5 dyrektywy 95/46 i art. 10 rozporządzenia 2016/679.

Trybunał orzekł, że zakaz oraz ograniczenia przetwarzania tych szczególnych kategorii danych mają zastosowanie do operatora wyszukiwarki, podobnie jak do każdego innego administratora danych osobowych. Celem tych zakazów i ograniczeń jest bowiem zapewnienie zwiększonej ochrony przed takim przetwarzaniem, które ze względu na szczególną wrażliwość tych danych może stanowić szczególnie poważną ingerencję w prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych (pkt 42–44).

Jednakże operator wyszukiwarki odpowiada nie za to, że dane osobowe znajdują się na stronie internetowej opublikowanej przez osobę trzecią, lecz za odsyłanie do tej strony. W tych okolicznościach zakaz oraz ograniczenia przetwarzania danych wrażliwych mają zastosowanie do tego operatora, ale tylko w zakresie dotyczącym wspomnianego odsyłania do stron internetowych, w rezultacie kontroli przeprowadzanej pod nadzorem właściwych organów krajowych po wniesieniu żądania przez osobę, której dane dotyczą (pkt 46, 47).

Po drugie, Trybunał stwierdził, że gdy do operatora skierowano żądanie usunięcia linków dotyczące danych wrażliwych, operator ten jest zasadniczo zobowiązany, z zastrzeżeniem pewnych wyjątków, do uwzględnienia takiego żądania. Jeśli chodzi o wspomniane wyjątki, operator może w szczególności odmówić uwzględnienia takiego żądania, jeżeli stwierdzi, że linki prowadzą do danych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą[68], pod warunkiem że odesłanie do takich linków spełnia pozostałe warunki zgodności przetwarzania danych osobowych z prawem, chyba że osoba ta ma prawo sprzeciwić się wspomnianemu odesłaniu z przyczyn związanych z jej szczególną sytuacją[69] (pkt 65, 69).

W każdym wypadku operator wyszukiwarki, do którego skierowano żądanie usunięcia linków, musi sprawdzić, czy umieszczenie linku do danej strony internetowej, na której zostały opublikowane dane wrażliwe, na liście wyświetlanej w wyniku wyszukiwania mającego za punkt wyjścia imię i nazwisko tej osoby, jest ściśle niezbędne do ochrony prawa do wolności informacji przysługującego internautom potencjalnie zainteresowanym uzyskaniem dostępu do tej strony internetowej dzięki takiemu wyszukiwaniu. W tym względzie Trybunał podkreślił, że choć prawa do poszanowania życia prywatnego i ochrony danych osobowych są co do zasady nadrzędne wobec prawa do wolności informacji przysługującego internautom, to jednak równowaga ta może, w szczególnych przypadkach, zależeć od charakteru rozpatrywanych informacji i od tego, jak istotne są one dla prywatności osoby, której dane dotyczą, oraz od publicznego interesu w dysponowaniu tą informacją, który to z kolei interes może być uzależniony w szczególności od roli odgrywanej przez tę osobę w życiu publicznym (pkt 66, 68).

Po trzecie, Trybunał orzekł, że w ramach żądania usunięcia linków do stron internetowych, na których są opublikowane informacje dotyczące postępowania sądowego w sprawie karnej prowadzonej przeciwko osobie, której dane dotyczą, które odnoszą się do wcześniejszego etapu takiego postępowania i nie odpowiadają już aktualnej sytuacji, do operatora wyszukiwarki należy dokonanie oceny, czy, biorąc pod uwagę wszystkie okoliczności sprawy, osoba ta jest uprawniona do tego, by rozpatrywane informacje nie były już aktualnie wiązane z jej imieniem i nazwiskiem za pomocą wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia to imię i nazwisko. Jednakże, nawet jeśli operator wyszukiwarki stwierdzi, że tak nie jest ze względu

[68] Artykuł 8 ust. 2 lit. e) dyrektywy 95/46 i art. 9 ust. 2 lit. e) rozporządzenia 2016/679.
[69] Artykuł 14 akapit pierwszy lit. a) dyrektywy 95/46 i art. 21 ust. 1 rozporządzenia 2016/679.

na fakt, że umieszczenie danego linku jest ściśle niezbędne do pogodzenia prawa do poszanowania życia prywatnego i ochrony danych osobowych osoby, której dane dotyczą, z prawem do wolności informacji przysługującym potencjalnie zainteresowanym internautom, operator ten jest zobowiązany, najpóźniej w momencie skierowania żądania usunięcia linków, do uporządkowania listy wyników w taki sposób, aby wynikający z niej dla internauty ogólny obraz odzwierciedlał aktualną sytuację prawną, co wymaga w szczególności, aby linki do stron internetowych zawierających informacje na ten temat znajdowały się na pierwszym miejscu na tej liście (pkt 77, 78).

Wyrok z dnia 24 września 2019 r. (wielka izba), Google (Terytorialny zakres usunięcia linków) (C-507/17, EU:C:2019:772)[70]

Commission nationale de l'informatique et des libertés (krajowa komisja ds. informatyki i swobód, CNIL, Francja) wezwała spółkę Google, w związku z uwzględnieniem przez tę spółkę wniosku o usunięcie linków, do usunięcia z listy wyników wyświetlanej po przeprowadzeniu wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby, linków prowadzących do stron internetowych zawierających dane osobowe dotyczące wskazanej osoby, w odniesieniu do wszystkich rozszerzeń nazwy domeny w tej wyszukiwarce. W obliczu odmowy zastosowania się przez Google do tego wezwania CNIL nałożyła na nią karę w wysokości 100 000 EUR. Conseil d'État (rada państwa, Francja), do której spółka Google wniosła skargę, zwróciła się do Trybunału z wnioskiem o ustalenie zakresu terytorialnego ciążącego na operatorze wyszukiwarki internetowej obowiązku wprowadzenia w życie prawa do usunięcia linków w myśl przepisów dyrektywy 95/46.

Przede wszystkim Trybunał przypomniał, że osoby fizyczne mogą, na podstawie prawa Unii, powoływać się przeciwko operatorowi wyszukiwarki internetowej, który na terytorium Unii ma swój zakład lub kilka zakładów, na przysługujące im prawo do usunięcia linków, niezależnie od tego, czy przetwarzanie danych osobowych (w tym wypadku zamieszczanie linków odsyłających do stron internetowych, na których znajdują się dane osobowe dotyczące osoby, która powołuje się na to prawo), ma miejsce na terenie Unii czy poza nią[71].

Co się tyczy zakresu prawa do usunięcia linków, Trybunał uznał, że operator wyszukiwarki internetowej jest zobowiązany do usunięcia linków nie ze wszystkich wersji swej wyszukiwarki, ale z tych jej wersji, które odpowiadają wszystkim państwom członkowskim. Trybunał wskazał w tym względzie, że o ile usunięcie wszystkich istniejących linków pozwoliłoby – zważywszy na charakterystyczne cechy Internetu i wyszukiwarek internetowych – na pełne urzeczywistnienie celu prawodawcy Unii, jakim jest zapewnienie wysokiego poziomu ochrony danych osobowych w całej Unii, o tyle z prawa Unii[72] nie wynika wcale, że dążąc do osiągnięcia tego celu prawodawca postanowił nadać prawu do usunięcia linków zakres, który wykraczałby poza terytorium państw członkowskich. W szczególności, podczas gdy w prawie Unii ustanowiono mechanizmy współpracy między organami nadzorczymi państw członkowskich umożliwiające wypracowanie wspólnej decyzji, opartej na osiągnięciu równowagi między prawem do ochrony

[70] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2019, s. 118 i 119.
[71] Artykuł 4 ust. 1 lit. a) dyrektywy 95/46 i art. 3 ust. 1 rozporządzenia nr 2016/679.
[72] Artykuł 12 lit. b) i art. 14 akapit pierwszy lit. a) dyrektywy 95/46; art. 17 ust. 1 rozporządzenia nr 2016/679.

życia prywatnego i danych osobowych z jednej strony a interesem publicznym różnych państw członkowskich w dostępie do informacji z drugiej strony, tego rodzaju mechanizmy nie są obecnie przewidziane w odniesieniu do usuwania linków poza Unią (pkt 62, 73).

Na obecnym etapie rozwoju prawa Unii operator wyszukiwarki internetowej ma obowiązek zastosować się do żądania usunięcia linków nie tylko w odniesieniu do wersji wyszukiwarki odpowiadającej państwu członkowskiemu, w którym ma miejsce zamieszkania beneficjent prawa do usunięcia linków, lecz w odniesieniu do wersji wyszukiwarki odpowiadających wszystkim państwom członkowskim, w szczególności w celu zapewnienia spójnego i wysokiego poziomu ochrony w całej Unii. Ponadto operator taki powinien w razie konieczności podjąć wystarczająco skuteczne środki w celu uniemożliwienia internautom z terenu Unii uzyskiwania dostępu, w stosownym wypadku za pomocą wersji wyszukiwarki odpowiadającej państwu trzeciemu, do linków podlegających usunięciu, a przynajmniej w celu poważnego zniechęcenia ich do uzyskiwania dostępu do takich linków, zaś do sądu krajowego należy ustalenie, czy środki zastosowane przez operatora spełniają ten wymóg (pkt 70).

Trybunał podkreślił wreszcie, że o ile prawo Unii nie zobowiązuje operatora wyszukiwarki internetowej do usunięcia linków ze wszystkich wersji jego wyszukiwarki o tyle nie zakazuje również, aby to uczynił. W związku z tym organ nadzorczy lub organ sądowy państwa członkowskiego zachowuje kompetencje w zakresie wypracowania, w świetle krajowych standardów ochrony praw podstawowych, równowagi między prawem danej osoby do poszanowania jej życia prywatnego oraz do ochrony jej danych osobowych z jednej strony, a prawem do wolności informacji z drugiej strony, zaś po wyważeniu tych praw – wezwania w stosownym wypadku operatora wyszukiwarki internetowej do usunięcia linków ze wszystkich wersji owej wyszukiwarki (pkt 65, 72).

4. Zgoda użytkownika strony internetowej na przechowywanie informacji

Wyrok z dnia 1 października 2019 r. (wielka izba), Planet49 (C-673/17, EU:C:2019:801)[73]

W wyroku tym Trybunał orzekł, że zgoda na przechowywanie informacji lub na dostęp do informacji za pośrednictwem plików cookie zainstalowanych na urządzeniu końcowym użytkownika strony internetowej nie jest ważna, jeżeli akceptacja ta wynika z domyślnie zaznaczonego pola wyboru, niezależnie od tego, czy przedmiotowe informacje stanowią dane osobowe. Ponadto Trybunał orzekł, że usługodawca musi poinformować użytkownika strony internetowej o tym, jaki jest okres funkcjonowania plików cookie oraz czy osoby trzecie mogą uzyskać dostęp do takich plików.

Spór w postępowaniu głównym dotyczył organizacji przez spółkę Planet49 loterii promocyjnej na stronie internetowej www.dein-macbook.de. Aby wziąć w niej udział, internauci musieli podać swe imię, nazwisko i adres na stronie internetowej, na której zamieszczono okienka wyboru. Okienko wyboru umożliwiające instalację plików cookie zostało zaznaczone domyślnie. Bundesgerichtshof (federalny trybunał sprawiedliwości, Niemcy), rozpatrujący skargę wniesioną przez niemiecki związek organizacji konsumenckich, powziął wątpliwości co do ważności uzyskania zgody użytkowników za pomocą domyślnie zaznaczonego okienka wyboru oraz co do zakresu obowiązku informacyjnego ciążącego na usługodawcy.

Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczył zasadniczo wykładni pojęcia „zgody" w rozumieniu dyrektywy 2002/58[74] w związku z dyrektywą 95/46[75], jak również RODO[76].

Po pierwsze, Trybunał zaznaczył, że art. 2 lit. h) dyrektywy 95/46, do którego odsyła art. 2 lit. f) dyrektywy 2002/58, definiuje zgodę jako „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych". Trybunał wskazał, że wymóg „wskazania" woli osoby, której dane dotyczą, wyraźnie sugeruje zachowanie czynne, a nie bierne. Tymczasem zgoda udzielona za pomocą zaznaczonego domyślnie okienka wyboru nie oznacza czynnego zachowania użytkownika strony internetowej. Ponadto geneza art. 5 ust. 3 dyrektywy 2002/58, który to przepis przewiduje, od chwili jego zmiany dyrektywą 2009/136, że użytkownik musi „wyrazić zgodę" na zainstalowanie plików cookie, sugeruje, że zgoda użytkownika nie może być dłużej domniemana i musi wynikać z jego czynnego zachowania. Wreszcie czynną zgodę przewiduje obecnie RODO[77], którego art. 4 pkt 11 wymaga w szczególności wyrażenia woli w formie „wyraźnego aktu potwierdzającego" i którego motyw 32 wyraźnie wyklucza wyrażenie zgody poprzez „milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania" (pkt 49, 52, 56, 62).

---

73 Wyrok ten został przedstawiony w sprawozdaniu rocznym 2019, s. 120 i 121.

74 Artykuł 2 lit. f) i art. 5 ust. 3 dyrektywy 2002/58, zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11).

75 Artykuł 2 lit. h) dyrektywy 95/46.

76 Artykuł 6 ust. 1 lit. a) rozporządzenia nr 2016/679.

77 Ibidem.

Trybunał orzekł zatem, że zgoda nie jest ważna, jeżeli przechowywanie informacji lub dostęp do informacji już przechowywanych w urządzeniu końcowym użytkownika strony internetowej zostały zaakceptowane za pomocą domyślnie zaznaczonego okienka wyboru, którego zaznaczenie użytkownik ten musi usunąć, aby odmówić udzielenia zgody. Sąd dodał, że okoliczność, iż użytkownik aktywuje przycisk uczestnictwa w loterii promocyjnej, o której mowa w tej sprawie, nie może być wystarczająca do uznania, że dany użytkownik skutecznie wyraził zgodę na zainstalowanie plików cookie (pkt 63).

Po drugie, Trybunał stwierdził, że art. 5 ust. 3 dyrektywy 2002/58 ma na celu ochronę użytkownika przed każdą ingerencją w sferę prywatną bez względu na to, czy ingerencja ta obejmuje dane osobowe. W związku z tym pojęcie „zgody" nie powinno być interpretowane w różny sposób w zależności od tego, czy informacje przechowywane lub udostępniane w urządzeniu końcowym użytkownika strony internetowej stanowią dane osobowe (pkt 69, 71).

Po trzecie, Trybunał zauważył, że art. 5 ust. 3 dyrektywy 2002/58 wymaga, aby użytkownik wyrażał zgodę, po otrzymaniu jasnych i wyczerpujących informacji, w szczególności o celach przetwarzania. Jasne i wyczerpujące informacje powinny umożliwiać użytkownikowi łatwe ustalenie konsekwencji zgody, której może udzielić, oraz gwarantować, że zgoda ta zostanie udzielona przy pełnej znajomości stanu rzeczy. W tym względzie Trybunał uznał, wskazanie okresu funkcjonowania plików cookie oraz określenie, czy osoby trzecie mogą uzyskać dostęp do takich plików, są to elementy jasnych i wyczerpujących informacji, jakie powinny zostać udzielone użytkownikowi strony internetowej przez usługodawcę (pkt 73–75, 81).

VI. 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)[78]

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.

Republika Federalna Niemiec twierdziła z kolei, że art. 28 ust. 1 akapit drugi dyrektywy 95/46 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

[78] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2010, s. 34.

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.

Trybunał orzekł, że przewidziane w dyrektywie 95/46 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 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 kontrolujących, 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; 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.

Trybunał stwierdził uchybienie ze strony Austrii, orzekając w istocie, że nie czyni zadość ustanowionemu w dyrektywie 95/46 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; sentencja).

Trybunał najpierw przypomniał, że zawarte w art. 28 ust. 1 akapit drugi dyrektywy 95/46 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, krajowy organ nadzorczy nie musi posiadać niezależnej linii budżetowej takiej jak przewidziana w art. 43 ust. 3 rozporządzenia nr 45/2001. Państwa członkowskie nie mają bowiem obowiązku powtarzania w ich krajowym ustawodawstwie przepisów analogicznych do przepisów rozdziału V rozporządzenia 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 (pkt 58).

Wyrok z dnia 8 kwietnia 2014 r. (wielka izba), Komisja/Węgry (C-288/12, EU:C:2014:237)[79]

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

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

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

[79] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2014, s. 62.

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)[80]

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.

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. W konsekwencji sąd ten zwrócił się do Trybunału z kilkoma pytaniami prejudycjalnymi.

W odniesieniu do mającego zastosowanie prawa Trybunał orzekł, że art. 4 ust. 1 lit. a) dyrektywy 95/46 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

[80] Wyrok ten został przedstawiony w sprawozdaniu rocznym 2015, s. 55.

przynależności państwowej osób, których dotyczy to przetwarzanie danych, nie ma znaczenia (pkt 41; sentencja, pkt 1).

W odniesieniu do właściwości i uprawnień organu nadzorczego rozpatrującego skargi zgodnie z art. 28 ust. 4 dyrektywy 95/46, 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; sentencja, pkt 2).

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 IV, zatytułowaną „Przekazywanie danych osobowych do państw trzecich") Trybunał 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, 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 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, 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).

Wyrok z dnia 5 czerwca 2018 r. (wielka izba), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

W tym wyroku (zob. także część II.5 zatytułowaną „Pojęcie »administratora danych osobowych"), dotyczącym m.in. wykładni art. 4 i 28 dyrektywy 95/46, Trybunał orzekł w sprawie zakresu uprawnień interwencyjnych, jakimi dysponują organy nadzorcze w odniesieniu do przetwarzania danych osobowych, które obejmuje udział kilku podmiotów.

Trybunał orzekł zatem, że w przypadku gdy przedsiębiorstwo z siedzibą poza Unią Europejską (takie jak amerykańska spółka Facebook) ma kilka oddziałów w różnych państwach członkowskich, organ nadzorczy państwa członkowskiego może wykonywać uprawnienia przyznane mu przez art. 28 ust. 3 tej dyrektywy w stosunku do oddziału tego przedsiębiorstwa, znajdującego się na terytorium tego państwa członkowskiego (tutaj: Facebook Germany), nawet jeżeli zgodnie z podziałem zadań w obrębie grupy, po pierwsze, ów oddział jest wyłącznie odpowiedzialny za sprzedaż przestrzeni reklamowej i inne działania marketingowe na terytorium rzeczonego państwa członkowskiego, a po drugie, wyłączną odpowiedzialność za gromadzenie i przetwarzanie danych osobowych ponosi w zakresie całego terytorium Unii Europejskiej oddział położony w innym państwie członkowskim (tutaj: Facebook Ireland) (pkt 64; sentencja, pkt 2).

Ponadto Trybunał uściślił, że w przypadku gdy organ nadzorczy państwa członkowskiego zamierza wykonać w stosunku do podmiotu mającego siedzibę na terytorium tego państwa członkowskiego uprawnienia interwencyjne, o których mowa w art. 28 ust. 3 dyrektywy 95/46, z powodu naruszeń przepisów o ochronie danych osobowych popełnionych przez administrującą tymi danymi osobę trzecią mającą siedzibę w innym państwie członkowskim (tutaj: Facebook Ireland), ów organ nadzorczy jest właściwy do dokonania oceny, w sposób niezależny od organu nadzorczego tego ostatniego państwa członkowskiego (Irlandii), zgodności z prawem takiego przetwarzania danych i może wykonywać przysługujące mu uprawnienia interwencyjne w stosunku do podmiotu mającego siedzibę na jego terytorium bez uprzedniego zwrócenia się do organu nadzorczego drugiego państwa członkowskiego o podjęcie działań (pkt 74; sentencja, pkt 3).

Wyrok z dnia 15 czerwca 2021 r. (wielka izba), Facebook Ireland i in. (C-645/19, EU:C:2021:483)

W dniu 11 września 2015 r. przewodniczący Commission belge de la protection de la vie priveé (belgijskiej komisji do spraw ochrony prywatności, zwanej dalej „KOP") wystąpił do Nederlandstalige rechtbank van eerste aanleg Brussel (niderlandzkojęzycznego sądu pierwszej instancji w Brukseli, Belgia) przeciwko Facebook Ireland, Facebook Inc. i Facebook Belgium z powództwem o zaniechanie mającym na celu położenie kresu naruszeniom przepisów dotyczących ochrony danych, których miał dopuszczać się Facebook. Naruszenia te polegały w szczególności na gromadzeniu i wykorzystywaniu informacji o zachowaniach w Internecie internautów belgijskich, niezależnie od tego, czy posiadają oni konto na Facebooku, przy użyciu różnego rodzaju technologii, takich jak pliki cookie, wtyczki społecznościowe[81] czy też piksele monitorujące.

[81] Przykładowo przyciski „lubię to" lub „udostępnij".

W dniu 16 lutego 2018 r. sąd ten uznał się za właściwy do orzekania w przedmiocie tego powództwa i orzekł co do istoty, że sieć społecznościowa Facebook nie informowała dostatecznie belgijskich internautów o gromadzeniu i wykorzystywaniu dotyczących ich informacji. Ponadto uznał on za nieważną udzielaną przez internautów zgodę na gromadzenie i przetwarzanie tych informacji.

W dniu 2 marca 2018 r. Facebook Ireland, Facebook Inc. i Facebook Belgium zaskarżyły to rozstrzygnięcie przed Hof van beroep te Brussel (sądem apelacyjnym w Brukseli, Belgia), czyli sądem odsyłającym w omawianej sprawie. W postępowaniu przed tym sądem belgijski organ ochrony danych (zwany dalej „ODO") występował jako następca prawny przewodniczącego KOP. Sąd odsyłający stwierdził swoją właściwość do rozpoznania odwołania wniesionego przez Facebook Belgium.

Sąd odsyłający powziął wątpliwości co do wpływu, jaki ma stosowanie przewidzianego w RODO[82] mechanizmu kompleksowej współpracy na kompetencje ODO i, w szczególności, zadał sobie pytanie, czy, w odniesieniu do okoliczności, które zaszły po wejściu w życie RODO, czyli po dniu 25 maja 2018 r., ODO może wystąpić z powództwem przeciwko Facebook Belgium, skoro to Facebook Ireland został uznany za administratora rozpatrywanych danych. Począwszy bowiem od tej daty, a w szczególności w zastosowaniu przewidzianej w RODO zasady kompleksowej współpracy, jedynie irlandzki komisarz ds. ochrony danych jest właściwy do wytoczenia powództwa o zaniechanie, nad czym kontrolę sprawują sądy irlandzkie (pkt 36, 37).

W wydanym w składzie wielkiej izby wyroku Trybunał doprecyzowuje uprawnienia przysługujące krajowym organom nadzorczym w ramach RODO. Podkreślił on w szczególności, że rozporządzenie to pod pewnymi warunkami zezwala na wykonywanie przez krajowy organ nadzorczy danego państwa członkowskiego przysługujących mu uprawnień do podnoszenia wszelkich zarzucanych naruszeń RODO przed sądami tego państwa członkowskiego i do wszczęcia postępowania sądowego w przedmiocie transgranicznego przetwarzania danych[83], nawet jeśli nie jest on w odniesieniu do tego przetwarzania wiodącym organem nadzorczym (sentencja, pkt 1).

W pierwszej kolejności Trybunał dokonał uszczegółowienia warunków, w jakich krajowy organ nadzorczy, który nie jest wiodącym organem w zakresie przetwarzania transgranicznego, powinien wykonywać przysługujące mu uprawnienia do podnoszenia wszelkich zarzucanych naruszeń RODO przed sądami danego państwa członkowskiego i, w odpowiednim przypadku, do wszczynania postępowania sądowego w celu zapewnienia stosowania tego rozporządzenia. Tak więc, po pierwsze, RODO winno przyznawać temu organowi nadzorczemu uprawnienie do wydania decyzji stwierdzającej, że to przetwarzanie narusza zasady przewidziane w tym rozporządzeniu, i, po drugie, uprawnienie to powinno być wykonywane przy poszanowaniu ustanowionych w tym rozporządzeniu procedur współpracy i kontroli spójności[84] (pkt 75; sentencja, pkt 1).

---

82 Zgodnie z brzmieniem art. 56 ust. 1 RODO: „Bez uszczerbku dla art. 55 organ nadzorczy głównej lub pojedynczej [jedynej] jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy względem transgranicznego przetwarzania dokonywanego przez tego administratora lub ten podmiot przetwarzający".

83 W rozumieniu art. 4 pkt 23 RODO.

84 Przewidzianych art. 56 i 60 RODO.

W odniesieniu do operacji przetwarzania transgranicznego RODO przewiduje bowiem mechanizm kompleksowej współpracy[85], który opiera się na podziale kompetencji między „wiodącym organem nadzorczym" a innymi krajowymi organami nadzorczymi, których to przetwarzanie dotyczy. Mechanizm ten wymaga ścisłej, lojalnej i skutecznej współpracy między tymi organami, a to w celu zapewnienia spójnej i jednolitej ochrony zasad dotyczących ochrony danych osobowych i zachowania w ten sposób skuteczności (effet utile) tego rozporządzenia. W RODO zostało w tym względzie ustanowiona przysługująca co do zasady wiodącemu organowi nadzorczemu właściwość do wydania decyzji stwierdzającej, że dana operacja przetwarzania transgranicznego narusza zasady zawarte w tym rozporządzeniu[86], podczas gdy przysługująca innym organom nadzorczym, których sprawa dotyczy, kompetencja do wydania takiej decyzji, choćby tylko czasowej, stanowi wyjątek od tej zasady[87]. Niemniej jednak wiodący organ nadzorczy nie może w ramach wykonywania swoich kompetencji zrezygnować z prowadzenia niezbędnego dialogu oraz lojalnej i skutecznej współpracy z innymi organami nadzorczymi, których sprawa dotyczy. Z tego względu wiodący organ nadzorczy nie może zignorować opinii innych organów nadzorczych, których sprawa dotyczy, zaś wszelkie mające znaczenie dla sprawy i uzasadnione sprzeciwy ze strony któregokolwiek z tych organów skutkują zablokowaniem, przynajmniej czasowo, możliwości przyjęcia projektu decyzji przez wiodący organ nadzorczy (pkt 50–53, 56–59, 63–65).

Trybunał uściślił ponadto, że okoliczność polegająca na tym, iż organ nadzorczy państwa członkowskiego, który nie jest wiodącym organem nadzorczym w odniesieniu do danej operacji transgranicznego przetwarzania danych, może wykonywać uprawnienia do podnoszenia wszelkich zarzucanych naruszeń RODO przed sądami tego państwa członkowskiego i do wszczynania postępowania sądowego jedynie z poszanowaniem zasad podziału kompetencji decyzyjnych pomiędzy wiodącym organem nadzorczym a innymi organami nadzorczymi[88] jest zgodna z art. 7, 8 i 47 karty, gwarantującej danej osobie, odpowiednio, prawo do ochrony danych osobowych i prawo do skutecznego środka prawnego (pkt 67).

W drugiej kolejności Trybunał orzekł, iż w przypadku transgranicznego przetwarzania danych wykonywanie przysługujących organowi nadzorczemu państwa członkowskiego innemu niż organ wiodący uprawnień do wszczęcia postępowania przed sądem[89] nie ma wymogu, aby administrator danych lub podmiot dokonujący transgranicznego przetwarzania danych osobowych, którego dotyczy to powództwo, posiadał główną czy też inną jednostkę organizacyjną na terenie tego państwa członkowskiego. Niemniej jednak wykonywanie tego uprawnienia powinno być objęte terytorialnym zakresem stosowania RODO[90], co wiąże się z przyjęciem założenia, że administrator danych lub podmiot dokonujący ich transgranicznego przetwarzania muszą posiadać jednostkę organizacyjną na terytorium Unii (pkt 80, 83, 84; sentencja, pkt 2).

---

85 Artykuł 56 ust. 1 RODO.
86 Artykuł 60 ust. 7 RODO.
87 Wyjątki od zasady kompetencji decyzyjnych wiodącego organu nadzorczego zostały ustanowione w art. 56 ust. 2 i art. 66 RODO.
88 Przewidzianych w art. 55 i 56 w związku z art. 60 RODO.
89 Zgodnie z art. 58 ust. 5 RODO.
90 Artykuł 3 ust. 1 RODO stanowi, że rozporządzenie to ma zastosowanie do przetwarzania danych osobowych „w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii".

W trzeciej kolejności Trybunał orzekł, że w przypadku transgranicznego przetwarzania danych przysługujące organowi nadzorczemu danego państwa członkowskiego innemu niż wiodący uprawnienia do podnoszenia wszelkich zarzucanych naruszeń tego rozporządzenia przed sądami tego państwa członkowskiego oraz, w odpowiednim przypadku, do wszczynania postępowania sądowego, mogą być wykonywane zarówno w odniesieniu do głównej jednostki organizacyjnej administratora danych, która znajduje się w państwie członkowskim, do którego przynależy ten organ, jak i w odniesieniu do innej jednostki organizacyjnej tego administratora, pod warunkiem, że to powództwo dotyczy przetwarzania danych dokonywanego w ramach działalności tej jednostki organizacyjnej, a organ ten jest właściwy do wykonywania tego uprawnienia.

Trybunał potwierdził jednak, że wykonywanie tego uprawnienia wiąże się z przyjęciem założenia, że RODO ma zastosowanie. W niniejszym przypadku, ze względu na to, że działalność jednostki organizacyjnej grupy Facebook znajdującej się w Belgii jest nierozerwalnie związana z rozpatrywanym w postępowaniu głównym przetwarzaniem danych osobowych, za które, w odniesieniu do terytorium Unii, odpowiedzialny jest Facebook Ireland, przetwarzanie to jest dokonywane „w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora", a zatem wchodzi w zakres zastosowania RODO (pkt 94–96; sentencja, pkt 3).

W czwartej kolejności Trybunał orzekł, że jeżeli organ nadzorczy państwa członkowskiego, który nie jest „wiodącym organem nadzorczym", skierował przed dniem wejścia w życie RODO powództwo dotyczące transgranicznego przetwarzania danych osobowych, powództwo to może na mocy prawa Unii zostać podtrzymane na podstawie przepisów dyrektywy 95/46**,** która nadal ma zastosowanie w odniesieniu do naruszeń przewidzianych w niej zasad popełnionych do dnia, w którym została ona uchylona. Ponadto powództwo to może zostać wniesione przez ten organ w związku z naruszeniami popełnionymi po wejściu w życie RODO pod warunkiem, że jest to jeden z przypadków, w którym rozporządzenie to przyznaje temu organowi uprawnienie do przyjęcia decyzji stwierdzającej, że dana operacja przetwarzania danych narusza reguły ustanowione w tym rozporządzeniu, i dzieje się to przy poszanowaniu ustanowionych w tym rozporządzeniu procedur współpracy i kontroli spójności (pkt 105; sentencja, pkt 4).

W piątej i ostatniej kolejności Trybunał potwierdził bezpośrednią skuteczność przepisu RODO, zgodnie z którym każde państwo członkowskie przewiduje w swoich przepisach, że jego organ nadzorczy jest uprawniony do podnoszenia przed organami wymiaru sprawiedliwości wszelkich naruszeń tego rozporządzenia i, w odpowiednim przypadku, do wszczynania postępowania sądowego. Organ taki może więc powołać się na ten przepis w celu wszczęcia lub dalszego prowadzenia postępowania przeciwko jednostkom, nawet jeśli ten konkretny przepis jako taki nie został transponowany do ustawodawstwa danego państwa członkowskiego (pkt 113; sentencja, pkt 5).

VII. 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, zatytułowaną „Pojęcie »przetwarzania danych osobowych«" i część V.1, zatytułowaną „Prawo do sprzeciwu wobec przetwarzania danych osobowych (»prawo do bycia zapomnianym«)"] Trybunał wypowiedział się także w przedmiocie terytorialnego zakresu stosowania dyrektywy 95/46.

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, 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; sentencja, pkt 2).

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).

VIII. 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 45/2001.

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, popierana przez Zjednoczone Królestwo i Radę, wniosła następnie do Trybunału odwołanie od tego wyroku Sądu.

Trybunał najpierw stwierdził, że jeżeli wniosek sporządzony w oparciu o rozporządzenie nr 1049/2001[91] w sprawie dostępu do dokumentów, ma na celu uzyskanie dostępu do dokumentów zawierających dane osobowe, przepisy rozporządzenia 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 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).

W przypadku bowiem, gdy w ramach wniosku o dostęp do protokołu na podstawie rozporządzenia nr 1049/2001, nie dostarczono żadnego wyraźnego i uprawnionego uzasadnienia ani żadnego przekonywającego argumentu w celu wykazania konieczności

[91] 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. 2001, L 145, s. 43).

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 nr 45/2001 (pkt 78)[92].

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[93], 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 nr 1049/2001 oraz z przepisami Unii dotyczącymi ochrony danych osobowych, a zwłaszcza rozporządzenia nr 45/2001. EFSA zaznaczyła w tym względzie, że ujawnienie nazwisk biegłych odpowiadałoby przekazaniu danych osobowych w rozumieniu art. 8 rozporządzenia 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[94] Sądu do Trybunału.

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 nr 45/2001. Ponieważ nie należy mylić pojęcia „danych osobowych" w rozumieniu art. 2 lit. a) rozporządzenia 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).

92 Wyrok ten został przedstawiony w sprawozdaniu rocznym 2010, s. 14.

93 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. 2009, L 309, s. 1).

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

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 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, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07 i 4.11.11.01.