TRYBUNAŁ SPRAWIEDLIWOŚCI
UNII EUROPEJSKIEJ

PL

Broszury tematyczne

Ochrona danych osobowych

Dyrekcja Badań i Dokumentacji

curia.europa.eu

Wstęp

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

Zostało ono usankcjonowane w prawie pierwotnym, a w szczególności w art. 8 Karty praw podstawowych Unii Europejskiej(zwanej dalej „Kartą"), a także w art. 16 ust. 1 traktatu o funkcjonowaniu Unii Europejskiej (TFUE). To prawo podstawowe jest ściśle związane z prawem do poszanowania życia prywatnego i rodzinnego uznanego w art. 7 karty.

W odniesieniu do prawa wtórnego należy wskazać, że od połowy lat 90 Wspólnota Europejska wprowadza różnego rodzaju 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], uchylona w 2018 r., stanowiła podstawowy akt prawny Unii w tej dziedzinie.

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 w celu uwzględnienia ostatnich zmian technologicznych i komercyjnych, prawodawca UE zainicjował w 2017 r. przegląd tej dyrektywy[4], który jest nadal w toku [5].

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

---

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 6).

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 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.

5 W dniu 10 lutego 2021 r. Rada Unii Europejskiej zatwierdziła wytyczne do negocjacji w przedmiocie zmiany przepisów o ochronie prywatności i poufności w związku z korzystaniem z usług łączności elektronicznej, umożliwiając rozpoczęcie negocjacji z Parlamentem Europejskim. Tekst wniosku dotyczącego 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) jest dostępny (w języku angielskim) tutaj: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

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).

25 maja 2018 r., a także dyrektywę (UE) 2016/680 [7] dotyczącą ochrony wspomnianych danych w sprawach karnych, której przepisy mają zastosowanie począwszy od dnia 6 maja 2018 r.

Jeżeli chodzi o przetwarzanie danych osobowych przez instytucje i organy UE, począwszy od dnia 11 grudnia 2018 r. ochronę tych danych zapewnia rozporządzenie (UE) 2018/1725 [8]. Realizując interes polegający na zapewnieniu spójnego podejścia do ochrony danych osobowych w całej Unii, rozporządzenie to ma na celu dostosowanie przepisów dotyczących ochrony danych osobowych w możliwie największym stopniu do systemu ustanowionego w RODO.

Wreszcie, aby sprostać wyzwaniom związanym z nowymi technologiami, prawodawca Unii rozpoczął począwszy od 2020 r. przyjmowanie nowych środków ustawodawczych [9], które są zgodne z przepisami prawa Unii dotyczącymi ochrony danych osobowych.

Biorąc pod uwagę istnienie bogatego orzecznictwa Trybunału Sprawiedliwości w zakresie ochrony danych osobowych, niniejsza broszura została opracowana w celu przedstawienie wyboru najważniejszych wyroków w tym przedmiocie oraz tych wyroków, które wniosły istotny wkład w rozwój tego orzecznictwa, ze szczególnym uwzględnieniem wyroków wydanych przez wielką izbę Trybunału. W szczególności niniejsza broszura ma obejmować zarówno orzecznictwo dotyczące ogólnych uregulowań dotyczących ochrony danych osobowych, które wynikają z wykładni dyrektywy 95/46 i RODO, jak i orzecznictwo dotyczące uregulowań sektorowych, obejmujących w szczególności łączność elektroniczną i prawo karne. Ponadto broszura ta ma na celu przedstawienie wybranych wyroków dotyczących uregulowań mających zastosowanie we wszystkich dziedzinach, przy jednoczesnym podkreśleniu decydującej roli, jaką od samego początku w rozwoju orzecznictwa odgrywała Karta.

---

[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 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 (Dz.U. 2018, L 295, s. 39).

[9] W tych ramach należy zwrócić uwagę na trzy inicjatywy legislacyjne: *i)* rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.U. L 152 z 3.6.2022, s. 1) oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.U. 2023, L 2854, s. 1) ; *ii)* pakiet legislacyjny dotyczący usług i rynków cyfrowych, składający się z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. L 277 z 27.10.2022, s. 1) oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. L 265 z 21.9.2022, s. 1); i *iii)* pierwszy w historii wniosek ustawodawczy zmierzający do stworzenia ram regulacyjnych dla sztucznej inteligencji, który doprowadził do przyjęcia rozporządzenia w sprawie sztucznej inteligencji (Dz.U. 2024, L, 1689).

Spis treści

WSTĘP 3
I. PRAWO DO OCHRONY DANYCH OSOBOWYCH UZNANE W KARCIE PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ 7
1. Zgodność prawa wtórnego Unii z prawem do ochrony danych osobowych 7
2. Poszanowanie prawa do ochrony danych osobowych w ramach wprowadzania w życie prawa Unii 19
II. PRZETWARZANIE DANYCH OSOBOWYCH W ROZUMIENIU OGÓLNYCH PRZEPISÓW W TYM ZAKRESIE 21
1. Zakres zastosowania przepisów ogólnych 21
2. Pojęcie „danych osobowych” 26
3. Pojęcie „przetwarzania danych osobowych” 29
4. Pojęcie „zbioru danych” 34
5. Pojęcie „administratora danych osobowych” 35
6. Pojęcie „współadministratora danych” 37
7. Warunki zgodności z prawem przetwarzania danych osobowych 38
III. PRZETWARZANIE DANYCH OSOBOWYCH W ROZUMIENIU UREGULOWAŃ SEKTOROWYCH W TYM ZAKRESIE 44
1. Przetwarzanie danych osobowych w sektorze łączności elektronicznej 44
2. Przetwarzanie danych osobowych w sprawach karnych 64
IV. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH 68
V. OCHRONA DANYCH OSOBOWYCH W INTERNECIE 77
1. Prawo do sprzeciwu wobec przetwarzania danych osobowych („prawo do bycia zapomnianym”) 77
2. Przetwarzanie danych osobowych a prawa własności intelektualnej 78
3. Usunięcie linków do danych osobowych 81
4. Zgoda użytkownika strony internetowej na przechowywanie informacji 90
5. Przetwarzanie danych osobowych w internetowych sieciach społecznościowych 92
VI. KRAJOWE ORGANY NADZORCZE 96
1. Zakres wymogu niezależności 96
2. Ustalenie prawa właściwego oraz właściwego organu nadzorczego 99
3. Uprawnienia krajowych organów nadzorczych 100
4. Warunki nakładania administracyjnych kar pieniężnych 106
5. Związek między uprawnieniami krajowych organów nadzorczych a uprawnieniami innych organów krajowych 110

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)

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

W tym kontekście Verwaltungsgericht Wiesbaden (sąd administracyjny w Wiesbaden, Niemcy) skierował do Trybunału 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.

---

[10] 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).

[11] Rozporządzenie Komisji (WE) nr 259/2008 z dnia 18 marca 2008 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1290/2005 w zakresie publikowania informacji na temat beneficjentów środków pochodzących z Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW) (Dz.U. 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).

Aby tego rodzaju ingerencja mogła być uzasadniona, powinna ona być przewidziana ustawowo, z poszanowaniem istoty omawianych praw oraz, zgodnie z zasadą proporcjonalności, być niezbędna i rzeczywiście odpowiadać uznanym przez Unię celom interesu ogólnego, a odstępstwa od tych praw i ich ograniczenia powinny sprowadzać się do tego, co ściśle niezbędne. 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.

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. Jednakże Trybunał nie zakwestionował skutków publikacji wykazów beneficjentów takiej pomocy, dokonanej przez organy krajowe na podstawie tych przepisów w okresie przed dniem wydania wyroku.

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)

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 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.

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. 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. 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. 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.

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.

Wyrok z dnia 21 czerwca 2022 r. (wielka izba), Ligue des droits humains (C-817/19, EU:C:2022:491)

Dane PNR (Passenger Name Record) są informacjami dotyczącymi rezerwacji, przechowywanymi przez przewoźników lotniczych w ich systemach rezerwacji i systemach odpraw pasażerskich. Dyrektywa PNR [12] zobowiązuje tych przewoźników do przekazywania danych wszystkich pasażerów odbywających lot pozaunijny, wykonywany między państwem trzecim a Unią Europejską, jednostce do spraw informacji o pasażerach (zwanej dalej „JIP") państwa członkowskiego przeznaczenia lub wylotu danego lotu w celu zwalczania terroryzmu i poważnej przestępczości. Przekazywane w ten sposób dane PNR są przedmiotem wstępnej oceny dokonywanej przez JIP [13], a następnie są zatrzymywane do celów ewentualnej późniejszej oceny przez właściwe organy zainteresowanego państwa członkowskiego lub organy innego państwa członkowskiego. Państwa członkowskie mogą postanowić o stosowaniu dyrektywy również do lotów wewnątrzunijnych [14].

Ligue des droits humains wniosła do Cour constitutionnelle (trybunału konstytucyjnego, Belgia) skargę o stwierdzenie nieważności belgijskiej ustawy, w drodze której dokonano transpozycji do prawa belgijskiego zarówno dyrektywy PNR, jak i dyrektywy API [15]. Zdaniem skarżącej ustawa ta narusza prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych. Skarżąca zakwestionowała, po pierwsze, dopuszczalność bardzo szerokiego ujęcia danych PNR, a po drugie, niezróżnicowany charakter gromadzenia, przekazywania i przetwarzania tych danych. W przekonaniu skarżącej ustawa ta narusza również swobodę przepływu osób, ponieważ pośrednio przywraca

[12] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.U. 2016, L 119, s. 132, zwana dalej „dyrektywą PNR")

[13] Ta wstępna ocena ma na celu zidentyfikowanie osób, w odniesieniu do których wymagane jest bardziej szczegółowe badanie przez właściwe organy ze względu na to, że osoby te mogą być zaangażowane w przestępstwa terrorystyczne lub poważną przestępczość. Ocena ta jest dokonywana w sposób systematyczny i zautomatyzowany poprzez zestawienie danych PNR z bazami danych, „które mają znaczenie", lub w drodze przetwarzania tych danych w świetle ustalonych wcześniej kryteriów w art. 6 ust. 2 lit. a) i art. 6 ust. 3 dyrektywy PNR.

[14] Korzystając z możliwości przewidzianej w art. 2 dyrektywy PNR.

[15] Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (Dz.U. 2004, L 261, s. 24) (zwanej dalej również „dyrektywą API"). W dyrektywie tej uregulowano przekazywanie przez przewoźników lotniczych właściwym organom krajowym danych pasażera przekazanych przed podróżą (takich jak rodzaj i numer i rodzaj używanego dokumentu podróży oraz obywatelstwa) w celu poprawy kontroli granicznej i zwalczania nielegalnej imigracji.

kontrole graniczne poprzez rozszerzenie systemu PNR na loty wewnątrzunijne i przewozy dokonywane innymi środkami transportu w obrębie Unii.

W tym kontekście belgijski Cour constitutionnelle (Trybunał Konstytucyjny) zwrócił się do Trybunału z pytaniami prejudycjalnymi dotyczącymi ważności dyrektywy PNR.

W wyroku wydanym w składzie wielkiej izby Trybunał potwierdził ważność dyrektywy PNR z tego względu, że poddaje się ona wykładni zgodnej z Kartą.

Trybunał orzekł w tym względzie, że ponieważ dokonana przez Trybunał wykładnia dyrektywy 2016/681 w świetle praw podstawowych zagwarantowanych w art. 7, 8 i 21 oraz art. 52 ust. 1 Karty [16] zapewnia zgodność tej dyrektywy ze wskazanymi postanowieniami Karty, analiza zadanych pytań nie doprowadziła do żadnych ustaleń, które mogłyby mieć wpływ na ważność owej dyrektywy.

Tytułem wstępu Trybunał przypomniał, że akt prawa Unii powinien być interpretowany tak dalece, jak to możliwe, w sposób, który nie podważa jego ważności, i w zgodzie z całością prawa pierwotnego, w tym w szczególności z postanowieniami Karty, a co za tym idzie, państwa członkowskie nie powinny opierać się na takiej wykładni Karty, która pozostawałaby w konflikcie z prawami podstawowymi chronionymi przez porządek prawny Unii lub z innymi ogólnymi zasadami uznanymi przez ten porządek prawny. W odniesieniu do dyrektywy PNR Trybunał wyjaśnił, że szereg jej motywów i przepisów wymaga takiej wykładni zgodnej, podkreślając wagę, jaką ustawodawca Unii przykłada, gdy odnosi się do wysokiego poziomu ochrony danych, do pełnego poszanowania praw podstawowych zagwarantowanych w Karcie.

Trybunał stwierdził, że dyrektywa PNR ustanawia istotne ingerencje w prawa zagwarantowane na mocy art. 7 i 8 Karty ze względu między innymi na to, ze jej celem jest wprowadzenie systemu nadzoru o charakterze stałym, nieukierunkowanym i systematycznym, przewidującego zautomatyzowaną ocenę danych osobowych wszystkich pasażerów korzystających z usług transportu lotniczego. Przypomniał on, że możliwość uzasadnienia przez państwa członkowskie takiej ingerencji należy oceniać, badając jej wagę oraz sprawdzając, czy znaczenie zamierzonego celu interesu ogólnego pozostaje w relacji do tej wagi.

Trybunał stwierdził, że przekazywanie, przetwarzanie i zatrzymywanie danych PNR przewidziane w tej dyrektywie można uznać za ograniczone do tego, co ściśle konieczne do celów walki z przestępstwami terrorystycznymi i poważną przestępczością, pod warunkiem, że uprawnienia przewidziane w owej dyrektywie podlegają wykładni zawężającej. W tym względzie w tym wyroku stwierdzono między innymi, że:

[16] Zgodnie z tym postanowieniem wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Ponadto ograniczenia tych praw i wolności mogą być wprowadzane wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

- system ustanowiony w dyrektywie PNR powinien obejmować jedynie informacje jednoznacznie możliwe do określenia i o oznaczonym zakresie w rubrykach zawartych w załączniku I do tej dyrektywy, dotyczące wykonanego lotu i danego pasażera, co w odniesieniu do niektórych rubryk zawartych w tym załączniku oznacza, że objęte są jedynie informacje wyraźnie wskazane [17].
- stosowanie systemu ustanowionego dyrektywą PNR powinno być ograniczone do przestępstw terrorystycznych i tylko do poważnych form przestępczości wykazujących obiektywny związek, przynajmniej pośredni, z lotniczym przewozem pasażerów. Jeśli chodzi o te formy, stosowanie wspomnianego systemu nie może zostać rozszerzone na przestępstwa, które – choć spełniają przewidziane przez tę dyrektywę kryterium dotyczące wagi i mowa o nich w szczególności w załączniku II do wspomnianej dyrektywy – należą do przestępstw pospolitych, stosownie do specyfiki krajowych systemów prawa karnego.
- Ewentualne rozszerzenie stosowania dyrektywy PNR na całość lub część lotów wewnątrzunijnych, o którym państwo członkowskie może postanowić, czyniąc użytek z uprawnienia przewidzianego w tej dyrektywie, powinno zostać ograniczone do tego, co ściśle konieczne. Takie rozszerzenie powinno podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek. W tym względzie Trybunał uściślił, że:
    - jedynie w sytuacji, gdy rzeczone państwo członkowskie stwierdzi istnienie wystarczająco konkretnych okoliczności pozwalających na uznanie, że stoi ono w obliczu zagrożenia terrorystycznego, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia, zastosowanie tej dyrektywy przez ograniczony do tego co ściśle konieczne lecz odnawialny okres do wszystkich lotów wewnątrzunijnych rozpoczynających się lub kończących w tym państwie nie wykracza poza to co ściśle konieczne [18].
    - W braku takiego zagrożenia terrorystycznego stosowanie wspomnianej dyrektywy nie może obejmować wszystkich lotów wewnątrzunijnych, lecz powinno być ograniczone do lotów wewnątrzunijnych związanych w szczególności z niektórymi trasami lotniczymi lub planami podróży, lub niektórymi lotniskami, w odniesieniu do których istnieją przesłanki mogące uzasadnić takie zastosowanie. Ściśle konieczny charakter tego stosowania do tak wybranych lotów wewnątrzunijnych powinien być regularnie poddawany przeglądowi pod kątem ewolucji okoliczności uzasadniających ich wybór.

[17] W szczególności „wszystkie informacje o formie płatności" (rubryka 6 załącznika) powinny być ograniczone do sposobu płatności i faktury za bilet lotniczy, z pominięciem wszelkich innych informacji niemających bezpośredniego związku z lotem, a „uwagi ogólne" (rubryka 12) mogą dotyczyć jedynie informacji wyraźnie wymienionych w tej rubryce, dotyczących pasażerów małoletnich.

[18] Istnienie takiego zagrożenia może bowiem samo w sobie ustanowić związek między przekazaniem i przetwarzaniem danych a walką z terroryzmem. W związku z tym wprowadzenie stosowania dyrektywy PNR do wszystkich lotów wewnątrzunijnych z lub do danego państwa członkowskiego, na czas określony, nie wykracza poza to co ściśle konieczne, przy czym decyzja przewidująca to stosowanie powinna podlegać kontroli przez sąd lub niezależny organ administracyjny.

- Do celów wstępnej oceny danych PNR mającej na celu identyfikację osób wymagających dalszego sprawdzenia przed ich przylotem lub wylotem, która w pierwszym etapie odbywa się w drodze zautomatyzowanego przetwarzania, JIP może jedynie, po pierwsze, zestawić te dane z bazami danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem [19]. Te bazy danych powinny mieć charakter niedyskryminacyjny i być użytkowane przez właściwe organy w związku ze zwalczaniem przestępstw terrorystycznych i poważnej przestępczości oraz mieć obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów. Co się tyczy, po drugie, wstępnej oceny w świetle wcześniej ustalonych kryteriów, JIP nie może wykorzystywać technologii sztucznej inteligencji w ramach systemu uczenia maszynowego (machine learning), który może, bez interwencji i udziału ludzi, zmieniać proces oceny, a w szczególności kryteria oceny, na których opiera się rezultat zastosowania takiego procesu, jak i wagę tych kryteriów. Wspomniane kryteria powinny być sformułowane w taki sposób, by ukierunkować je ściśle na osoby, wobec których może istnieć racjonalne podejrzenie ich udziału w przestępstwach terrorystycznych lub poważnej przestępczości, z uwzględnieniem zarówno elementów „obciążających", jak i „odciążających" i pomijając wszelką dyskryminację, zarówno bezpośrednią, jak i pośrednią [20].

- Biorąc pod uwagę odsetek błędów nieodłącznie związany ze zautomatyzowanym przetwarzaniem danych PNR, a zwłaszcza znaczną liczbę wyników „fałszywie pozytywnych", które zostały uzyskane w latach 2018 i 2019, przydatność systemu wprowadzonego dyrektywą PNR do realizowania zamierzonych celów zależy zasadniczo od dobrego funkcjonowania następczej weryfikacji pozytywnych wyników uzyskanych w ramach takiego przetwarzania przeprowadzanej przez JIP – w drugim etapie – za pomocą środków niezautomatyzowanych. W tym względzie państwa członkowskie muszą zapewnić jasne i precyzyjne zasady, które będą wytyczać kierunek i ramy analizy przeprowadzanej przez pracowników JIP odpowiedzialnych za tę indywidualną kontrolę, aby zapewnić pełne poszanowanie praw podstawowych zapisanych w art. 7, 8 i 21 Karty, a w szczególności zagwarantować spójną praktykę administracyjną w ramach JIP, która respektuje zasadę niedyskryminacji. W szczególności państwa członkowskie mają obowiązek zapewnienia, by JIP określała w sposób jasny i precyzyjny obiektywne kryteria oceny pozwalające jej pracownikom zweryfikować, po

[19] To znaczy baz danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem w rozumieniu art. 6 ust. 3 lit. a) dyrektywy PNR. Natomiast analizy oparte na różnych bazach danych mogą przybrać formę eksploracji danych (data mining) i prowadzić do nieproporcjonalnego wykorzystania tych danych, umożliwiając ustalenie precyzyjnego profilu osób zainteresowanych tylko dlatego, że mają one zamiar podróżować samolotem.

[20] Wcześniej ustalone kryteria muszą być ukierunkowane, proporcjonalne i szczegółowe oraz poddawane regularnym przeglądom (art. 6 ust. 4 dyrektywy PNR). Wstępna ocena w świetle wcześniej ustalonych kryteriów powinna być przeprowadzona w sposób niedyskryminacyjny. Zgodnie z art. 6 ust. 4 zdanie czwarte dyrektywy PNR kryteria te w żadnym przypadku nie mogą opierać się na rasie ani pochodzeniu etnicznym, na poglądach politycznych, przekonaniach religijnych lub światopoglądowych, przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby.

pierwsze, czy i w jakim stopniu wynik pozytywny (hit) dotyczy w istocie jednostki, która może być zaangażowana w przestępstwa terrorystyczne lub poważną przestępczość, oraz, po drugie, niedyskryminacyjny charakter zautomatyzowanego przetwarzania. W tym kontekście Trybunał podkreślił ponadto, że właściwe organy powinny zagwarantować, by osoba zainteresowana mogła zrozumieć działanie zastosowanych kryteriów wstępnej oceny i programów stosujących te kryteria, w sposób pozwalający jej na podjęcie w sposób w pełni świadomy decyzji, czy skorzysta z prawa do sądowego środka ochrony prawnej. Podobnie, w ramach sądowego środka ochrony prawnej zarówno sąd dokonujący kontroli legalności decyzji wydanej przez właściwe organy, jak i osoba zainteresowana, z wyłączeniem przypadków zagrożenia bezpieczeństwa narodowego, powinny mieć możliwość zapoznania się z całością zarówno motywów, jak i odnośnych dowodów, na podstawie których decyzja ta została wydana, w tym z wcześniej ustalonymi kryteriami oceny oraz działaniem programów stosujących te kryteria.

- późniejsze ujawnianie i ocena danych PNR, to jest po przylocie lub wylocie zainteresowanej osoby, muszą być oparte na nowych okolicznościach i obiektywnych przesłankach – na których można oprzeć racjonalne podejrzenie zaangażowania danej osoby w poważną przestępczość, która ma związek, choćby pośredni, z lotniczym przewozem pasażerów – albo które pozwalają stwierdzić, że dane te mogą w konkretnym przypadku skutecznie przyczynić się do zwalczania przestępstw terrorystycznych wykazujących taki związek. Ujawnianie danych PNR do celów takiej późniejszej oceny powinno, co do zasady, z wyjątkiem należycie uzasadnionych pilnych przypadków, być uzależnione od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, przeprowadzanej na uzasadniony wniosek właściwych organów, niezależnie od tego, czy ten wniosek został złożony przed upływem sześciu miesięcy od przekazania tych danych JIP czy przed jego upływem [21].

Wyrok z dnia 22 listopada 2022 r. (wielka izba), Luxembourg Business Registers (C-37/20 i C-601/20, EU:C:2022:912)

W celu zwalczania prania pieniędzy i finansowania terroryzmu oraz zapobiegania im dyrektywa o przeciwdziałaniu praniu pieniędzy [22] nakłada na państwa członkowskie obowiązek prowadzenia rejestru zawierającego informacje o beneficjentach

[21] Zgodnie z brzmieniem art. 12 ust. 1 i 3 dyrektywy PNR taka kontrola jest wyraźnie przewidziana jedynie w odniesieniu do wniosków o ujawnienie danych PNR składanych po upływie sześciu miesięcy od przekazania tych danych do JIP.

[22] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. 2015 L 141, s. 73, zwana dalej „dyrektywą o przeciwdziałaniu praniu pieniędzy").

rzeczywistych [23] podmiotów o charakterze korporacyjnym i innych podmiotów prawnych utworzonych na ich terytorium. W następstwie zmiany tej dyrektywy wprowadzonej dyrektywą 2018/843 [24] niektóre z tych informacji powinny być udostępniane we wszystkich przypadkach każdej osobie. Zgodnie ze zmienioną w ten sposób dyrektywą o przeciwdziałaniu praniu pieniędzy (zwaną dalej „zmienioną dyrektywą o przeciwdziałaniu praniu pieniędzy") przepisy luksemburskie wprowadziły rejestr beneficjentów rzeczywistych (zwany dalej „RBE") przeznaczony do przechowywania i udostępniania szeregu informacji o beneficjentach rzeczywistych zarejestrowanych podmiotów, do których dostęp jest otwarty dla każdej osoby.

W tym kontekście do tribunal d'arrondissement de Luxembourg (sądu okręgowego w Luksemburgu) wpłynęły dwie sprawy, wniesione odpowiednio przez WM i Sovim SA, którzy kwestionują odmowę przez Luxembourg Business Registers, administratora RBE, uwzględnienia ich wniosków mających na celu uniemożliwienie publicznego dostępu do informacji dotyczących w pierwszej sprawie WM jako beneficjenta rzeczywistego spółki cywilnej nieruchomości, a w drugiej sprawie beneficjenta rzeczywistego Sovim SA. W ramach tych dwóch spraw, powziąwszy wątpliwości w szczególności co do ważności przepisów prawa Unii wprowadzających system publicznego dostępu do informacji dotyczących beneficjentów rzeczywistych, tribunal d'arrondissement de Luxembourg (sąd okręgowy w Luksemburgu) zwrócił się do Trybunału z pytaniem prejudycjalnym dotyczącym oceny ważności.

W swoim wyroku Trybunał, orzekający w składzie wielkiej izby, stwierdził nieważność dyrektywy 2018/843 w zakresie, w jakim zmieniła ona dyrektywę o przeciwdziałaniu praniu pieniędzy w ten sposób, że państwa członkowskie zapewniają, aby informacje o beneficjentach rzeczywistych podmiotów o charakterze korporacyjnym i innych podmiotów prawnych utworzonych na ich terytorium były we wszystkich przypadkach udostępniane każdej osobie [25].

W pierwszej kolejności Trybunał stwierdził, że publiczny dostęp do informacji o beneficjentach rzeczywistych przewidziany przez zmienioną dyrektywę o przeciwdziałaniu praniu pieniędzy stanowi poważną ingerencję w prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych, zapisane odpowiednio w art. 7 i 8 Karty.

W tym względzie Trybunał zauważył, że skoro dane te zawierają informacje o konkretnych osobach fizycznych, a mianowicie o beneficjentach rzeczywistych podmiotów o charakterze korporacyjnym i innych podmiotów prawnych utworzonych na

[23] Zgodnie z brzmieniem art. 3 pkt 6 dyrektywy o przeciwdziałaniu praniu pieniędzy beneficjentem rzeczywistym jest osoba fizyczna lub osoby fizyczne będące ostatecznymi właścicielami klienta lub sprawujące kontrolę nad tym klientem lub osoba fizyczna lub osoby fizyczne, w imieniu których przeprowadzana jest transakcja lub działalność.

[24] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Dz.U. L 2018, L 156, s. 43).

[25] Nieważność art. 1 pkt 15 lit. c) dyrektywy 2018/843 zmieniającej art. 30 ust. 5 lit. c) akapit pierwszy dyrektywy w sprawie prania pieniędzy.

terytorium państw członkowskich, dostęp do nich każdej osoby ma wpływ na podstawowe prawo do poszanowania życia prywatnego. Ponadto ich publiczne udostępnianie stanowi przetwarzanie danych osobowych. Dodał on, że takie publiczne udostępnianie stanowi ingerencję w dwa wyżej wymienione prawa podstawowe, niezależnie od tego, w jaki sposób przekazane informacje zostaną później wykorzystane.

Co się tyczy wagi tej ingerencji, Trybunał zauważył, że w zakresie, w jakim informacje udostępniane publicznie dotyczą tożsamości beneficjenta rzeczywistego, jak również posiadanej własności lub charakteru sprawowanej kontroli w podmiotach o charakterze korporacyjnym lub innych podmiotach prawnych, mogą one pozwolić na określenie profilu dotyczącego niektórych danych osobowych o charakterze identyfikacyjnym, stanu majątkowego danej osoby, jak również konkretnych sektorów gospodarczych, krajów i przedsiębiorstw, w które zainwestowała. Co więcej, informacje te stają się wówczas dostępne dla potencjalnie nieograniczonej liczby osób, tak że takie przetwarzanie danych osobowych może umożliwić swobodny dostęp do tych informacji również osobom, które ze względów niezwiązanych z celem realizowanym przez ten środek dążą do uzyskania informacji na temat sytuacji w szczególności materialnej i finansowej beneficjenta rzeczywistego. Możliwość ta wydaje się tym łatwiejsza, gdy dane te można przeglądać w Internecie. Ponadto potencjalne konsekwencje dla zainteresowanych osób wynikające z ewentualnego niewłaściwego wykorzystania ich danych pogłębia fakt, że po ich publicznym udostępnieniu mogą one być nie tylko swobodnie przeglądane, ale także przechowywane i rozpowszechniane, a więc trudniejsza, a nawet iluzoryczna staje się dla tych osób skuteczna obrona przed niewłaściwym wykorzystaniem.

W drugiej kolejności, w ramach badania uzasadnienia rozpatrywanej ingerencji, po pierwsze, Trybunał zauważył, że w niniejszej sprawie przestrzegana jest zasada legalności. Ograniczenie korzystania z ww. praw podstawowych, wynikające z publicznego dostępu do informacji dotyczących beneficjentów rzeczywistych, jest bowiem przewidziane w akcie prawodawczym, a mianowicie w zmienionej dyrektywie o przeciwdziałaniu praniu pieniędzy. Ponadto, z jednej strony, dyrektywa ta precyzuje, że informacje te powinny być odpowiednie, dokładne i aktualne, oraz wyraźnie wymienia niektóre z tych danych, które mają być udostępniane publicznie. Z drugiej strony, ustanawia ona warunki, na jakich państwa członkowskie mogą przewidzieć odstępstwa od takiego dostępu.

Po drugie, wyjaśnił on, że omawiana ingerencja nie stanowi zagrożenia dla istoty praw podstawowych zagwarantowanych w art. 7 i 8 Karty. O ile prawdą jest, że zmieniona dyrektywa o przeciwdziałaniu praniu pieniędzy nie zawiera wyczerpującego wykazu danych, do których każda osoba powinna mieć dostęp, oraz że państwa członkowskie są uprawnione do udzielenia dostępu do dodatkowych informacji, o tyle jedynie odpowiednie informacje dotyczące beneficjentów rzeczywistych i informacje o posiadanej własności lub charakterze sprawowanej kontroli mogą zostać uzyskane, być posiadane, a w związku z tym zostać potencjalnie udostępnione publicznie, co w

szczególności wyklucza informacje, które nie są odpowiednio związane z celami zmienionej dyrektywy o przeciwdziałaniu praniu pieniędzy. Tymczasem nie wydaje się, by udostępnienie każdej osobie informacji mających taki związek w jakikolwiek sposób naruszało istotę wskazanych praw podstawowych.

Po trzecie, Trybunał podkreślił, że przewidując publiczny dostęp do informacji o beneficjentach rzeczywistych, prawodawca Unii ma na celu zapobieganie praniu pieniędzy i finansowaniu terroryzmu poprzez stworzenie, za pomocą zwiększonej przejrzystości, środowiska, w którym prawdopodobieństwo wykorzystania go do tych celów jest mniejsze, co stanowi cel leżący w interesie ogólnym, który może uzasadniać ingerencje, nawet poważne, w prawa podstawowe ustanowione w art. 7 i 8 Karty.

Po czwarte, w ramach badania odpowiedniego, koniecznego i proporcjonalnego charakteru rozpatrywanej ingerencji Trybunał stwierdził, że prawdą jest, iż publiczny dostęp do informacji o beneficjentach rzeczywistych może przyczynić się do realizacji tego celu.

Niemniej jednak uznał on, że owa ingerencja nie może być uznana za ograniczoną do tego, co bezwzględnie konieczne. Po pierwsze, nie można wykazać bezwzględnej konieczności wspomnianej ingerencji, opierając się na okoliczności, że kryterium „uzasadnionego interesu", jaki zgodnie z dyrektywą o przeciwdziałaniu praniu pieniędzy, w brzmieniu sprzed zmiany wprowadzonej dyrektywą 2018/843, powinien przysługiwać każdej osobie pragnącej uzyskać dostęp do informacji dotyczących beneficjentów rzeczywistych, było trudne do wprowadzenia i że jego stosowanie mogło prowadzić do arbitralnych decyzji. Ewentualne istnienie trudności w dokładnym określeniu przesłanek i warunków, na jakich każda osoba może uzyskać dostęp do informacji o beneficjentach rzeczywistych, nie może bowiem uzasadniać tego, że prawodawca Unii przewiduje publiczny dostęp do tych informacji.

Po drugie, zawarte w dyrektywie 2018/843 wyjaśnienia również nie świadczą o bezwzględnej konieczności rozpatrywanej ingerencji [26]. W zakresie, w jakim według tych wyjaśnień publiczny dostęp do informacji o beneficjentach rzeczywistych ma umożliwić zwiększoną kontrolę informacji przez społeczeństwo obywatelskie, w szczególności prasę i organizacje społeczeństwa obywatelskiego, Trybunał zauważył, że zarówno prasa, jak i organizacje społeczeństwa obywatelskiego mające związek z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu i ich zwalczaniem mają uzasadniony interes w dostępie do danych informacji. To samo dotyczy osób, które chcą znać tożsamość beneficjentów rzeczywistych podmiotu o charakterze korporacyjnym lub innego podmiotu prawnego ze względu na to, że mogą one zawierać transakcje z nimi, a także instytucji finansowych i władz zaangażowanych w zwalczanie przestępstw prania pieniędzy lub finansowania terroryzmu.

[26] Są to wyjaśnienia zawarte w motywie 30 dyrektywy 2018/843.

Ponadto rozpatrywana ingerencja nie ma również proporcjonalnego charakteru. W tym względzie Trybunał stwierdził, że przepisy materialne regulujące tę ingerencję nie spełniają wymogu jasności i precyzji. Zmieniona dyrektywa o przeciwdziałaniu praniu pieniędzy przewiduje bowiem dostęp każdej osoby „co najmniej" do danych, o których w niej mowa, i przyznaje państwom członkowskim możliwość udzielenia dostępu do dodatkowych informacji, obejmujących „co najmniej" datę urodzenia lub dane kontaktowe danego beneficjenta rzeczywistego. Tymczasem poprzez użycie wyrażenia „co najmniej" dyrektywa ta zezwala na publiczne udostępnianie danych, które nie są wystarczająco zdefiniowane ani możliwe do zidentyfikowania.

Poza tym, co się tyczy wyważenia wagi tej ingerencji ze znaczeniem zamierzonego celu leżącego w interesie ogólnym, Trybunał uznał, że ze względu na swoje znaczenie, cel ten może uzasadniać ingerencje, nawet poważne, w prawa podstawowe ustanowione w art. 7 i 8 Karty.

Niemniej jednak, z jednej strony zwalczanie prania pieniędzy i finansowania terroryzmu należy przede wszystkim do kompetencji władz publicznych oraz podmiotów takich jak instytucje kredytowe lub finansowe, które ze względu na swoją działalność podlegają szczególnym obowiązkom w tym zakresie. Z tego powodu zmieniona dyrektywa o przeciwdziałaniu praniu pieniędzy przewiduje, że informacje o beneficjentach rzeczywistych powinny być dostępne we wszystkich przypadkach właściwym organom i jednostkom analityki finansowej bez żadnych ograniczeń, a także podmiotom zobowiązanym, w kontekście należytej staranności wobec klienta [27].

Z drugiej strony, w porównaniu z wcześniejszym systemem, który przewidywał, poza dostępem właściwych organów i niektórych podmiotów do informacji o beneficjentach rzeczywistych, dostęp każdej osoby lub organizacji, które mogą wykazać uzasadniony interes, system wprowadzony przez dyrektywę 2018/843 stanowi znacznie poważniejsze naruszenie praw podstawowych zagwarantowanych w art. 7 i 8 Karty, które nie może zostać zrekompensowane ewentualnymi korzyściami, jakie mogłyby wyniknąć z tego ostatniego systemu w porównaniu z pierwszym, w zakresie zwalczania prania pieniędzy i finansowania terroryzmu.

[27] Artykuł 30 ust. 5 akapit pierwszy lit. a) i b) zmienionej dyrektywy o przeciwdziałaniu praniu pieniędzy.

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), EU:C:2016:970***)***

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.

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.

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 namierzenie 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.

II. Przetwarzanie danych osobowych w rozumieniu ogólnych przepisów w tym zakresie

1. Zakres zastosowania przepisów ogólnych

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[28] 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 [29] 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

[28] 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).

[29] 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, biura ceł i ochrony granic (Dz.U. 2004, L 183, s. 83; sprostowanie Dz.U. 2005, L 255, s. 168).

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.

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.

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.

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 wyroku tym Trybunał zajął również stanowisko w przedmiocie terytorialnego zakresu zastosowania 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.

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.

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.

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 prywatności, muszą być bezwzględnie interpretowane z punktu widzenia praw podstawowych, które zostały zawarte w wyżej wskazanej Karcie, odstępstwo przewidziane w art. 3 ust. 2 tiret drugie tej dyrektywy musi podlegać ścisłej wykładni. 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.

Wyrok z dnia 16 stycznia 2024 r. (wielka izba), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Wspomniana komisja śledcza (zwana dalej „komisją śledczą BVT") została powołana przez Nationalrat (zgromadzenie narodowe, Austria) w celu zbadania możliwego wywierania nacisków politycznych na Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (federalny urząd ochrony konstytucji i zwalczania terroryzmu, Austria) [30]. Jedną z osób przesłuchiwanych przez tę komisję w charakterze świadka był WK. Protokół z tego przesłuchania, który zawierał pełne imię i nazwisko WK, został opublikowany na stronie internetowej Parlament Österreich (parlamentu austriackiego), pomimo wniosku WK o jego utajnienie. Uznawszy, że ujawnienie jego tożsamości odbyło się z naruszeniem przepisów RODO i austriackiego prawa, WK wniósł skargę do Österreichische Datenschutzbehörde (organu ochrony danych, Austria) (zwanego dalej „Datenschutzbehörde"). Decyzją z dnia 18 września 2019 r. Datenschutzbehörde stwierdził brak właściwości do rozpoznania skargi, wyjaśniając, że jako organ władzy wykonawczej nie może kontrolować działalności komisji śledczej BVT, będącej częścią władzy ustawodawczej, gdyż jest to sprzeczne z zasadą podziału władz.

[30] W dniu 1 grudnia 2021 r. podmiot ten przekształcił się w "Direktion Staatsschutz und Nachrichtendienst" (Dyrekcję ds. Bezpieczeństwa Państwowego i Służb Wywiadowczych, Austria).

WK zaskarżył decyzję Datenschutzbehörde do Bundesverwaltungsgericht (federalnego sądu administracyjnego), który orzekł po jego myśli i uchylił ją, w następstwie czego wspomniany organ wniósł skargę rewizyjną do trybunału administracyjnego, będącego sądem odsyłającym.

Sąd ten zwrócił się w tym kontekście do Trybunału o ustalenie, czy działalność komisji śledczej powołanej przez parlament państwa członkowskiego wchodzi w zakres stosowania RODO oraz czy owo rozporządzenie znajduje zastosowanie, jeżeli wspomniana działalność dotyczy ochrony bezpieczeństwa narodowego.

W pierwszej kolejności Trybunał przypomniał, że jedynym celem art. 2 ust. 2 lit. a) RODO, w myśl którego RODO nie stosuje się do przetwarzania danych osobowych dokonywanego w ramach działalności nieobjętej zakresem prawa Unii, jest wyłączenie z zakresu stosowania tego rozporządzenia przetwarzania danych dokonywanego przez organy państwowe w ramach działalności mającej na celu ochronę bezpieczeństwa narodowego lub działalności należącej do tej samej kategorii. Sam fakt, iż dana działalność jest właściwa państwu lub organowi publicznemu, nie wystarcza, aby wyłączyć ją spod reżimu RODO.

Taka wykładnia, wynikająca z braku rozróżnienia ze względu na tożsamość podmiotu przetwarzającego, znajduje potwierdzenie w art. 4 ust. 7 RODO [31].

Trybunał wyjaśnił, że parlamentarny charakter komisji śledczej BVT nie oznacza, że jej działalność sytuuje się poza zakresem stosowania RODO. Przewidziany w art. 2 ust. 2 lit. a) tego rozporządzenia wyjątek odnosi się bowiem wyłącznie do kategorii działań, które ze względu na swój charakter nie są objęte zakresem stosowania prawa Unii, nie zaś do kategorii osób. W związku z tym sama okoliczność, że przetwarzanie danych osobowych jest dokonywane przez komisję śledczą powołaną przez parlament państwa członkowskiego w ramach wykonywania przez niego uprawnień z zakresu kontroli władzy wykonawczej, nie pozwala na ustalenie, że takie przetwarzanie jest dokonywane w ramach działalności nieobjętej zakresem prawa Unii.

W drugiej kolejności Trybunał wskazał, że chociaż to do państw członkowskich należy określenie ich podstawowych interesów bezpieczeństwa i podjęcie środków zmierzających do ich zagwarantowania [32], sama okoliczność, że dany środek krajowy został podjęty w celu ochrony bezpieczeństwa narodowego, nie powoduje wyłączenia zastosowania prawa Unii i nie zwalnia państw członkowskich z konieczności jego przestrzegania. Przewidziany w art. 2 ust. 2 lit. a) RODO wyjątek odnosi się bowiem wyłącznie do kategorii działań, które ze względu na swój charakter nie są objęte zakresem stosowania prawa Unii. W tym względzie sama okoliczność, że administratorem danych jest organ publiczny, którego główna działalność polega na

[31] Zgodnie z zawartą w RODO definicją „»administrator« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych."

[32] Zgodnie z art. 4 ust. 2 TUE.

zapewnieniu ochrony bezpieczeństwa narodowego, nie wystarcza do wyłączenia z zakresu stosowania RODO przetwarzania danych osobowych dokonywanego przez ten organ w ramach innych prowadzonych przez niego czynności.

W niniejszej sprawie nie wydaje się, aby sama kontrola polityczna przeprowadzona przez komisję śledczą BVT stanowiła działalność mającą na celu ochronę bezpieczeństwa narodowego lub działalność należącą do takiej kategorii. W związku z tym – z zastrzeżeniem zweryfikowania tego stwierdzenia przez sąd odsyłający – działalność ta nie jest wyłączona z zakresu stosowania RODO.

Niezależnie od powyższego parlamentarna komisja śledcza może mieć dostęp do danych osobowych, które ze względów związanych z bezpieczeństwem narodowym, zasługują na szczególną ochronę. W tym względzie ograniczenia praw i obowiązków wynikających z RODO w celu zapewnienia między innymi bezpieczeństwa narodowego mogą zostać wprowadzone w drodze aktu prawnego [33]. Na tej podstawie można wprowadzić ograniczenia w odniesieniu do gromadzenia danych osobowych, informowania osób, których dane dotyczą, i ich dostępu do tych danych, a także ich ujawniania bez zgody osób, których dane dotyczą, osobom innym niż administrator danych, pod warunkiem że takie ograniczenia nie naruszają istoty podstawowych praw i wolności osób, których dane dotyczą, i są w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym.

Trybunał zwrócił jednak uwagę, że z informacji, którymi dysponuje, nie wynika, aby komisja śledcza BVT twierdziła, iż ujawnienie danych osobowych zainteresowanej osoby było konieczne dla ochrony bezpieczeństwa narodowego i oparte na przewidzianym w tym celu krajowym akcie prawnym, czego ustalenie należy jednak w stosownym wypadku do sądu odsyłającego.

2. Pojęcie „danych osobowych”

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

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

[33] Zgodnie z art. 23 RODO.

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.

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.

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 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, tak jak w niniejszym przypadku, egzaminu, na którym można korzystać z własnych materiałów referencyjnych („open book exam").

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

osiągniętych przez osobę przystępującą do egzaminu i mogą pociągnąć za sobą pewne skutki dla tej osoby.

W czwartej kolejności Trybunał orzekł, że pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi mogą zostać poddane weryfikacji, w szczególności pod kątem ich prawidłowości i potrzeby ich przechowywania w rozumieniu art. 6 ust. 1 lit. d) i e) dyrektywy 95/46, 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.

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.

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. Bodil 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. 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.

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

W tym wyroku (zobacz również sekcję II.1., zatytułowaną „Zakres zastosowania przepisów ogólnych”), 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. 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.

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

Finlandzki 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 finlandzkim 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.

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 [34] 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

[34] Artykuł 14[1] ust. 2, Ceļu satiksmes likums (ustawy o ruchu drogowym) z dnia 1 października 1997 r. (Latvijas Vēstnesis, 1997, nr 274/276).

dotyczących wyroków skazujących i naruszeń prawa” [35], w odniesieniu do którego RODO przewiduje zwiększoną ochronę ze względu na szczególną wrażliwość tych danych.

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.

Z jednej strony przetwarzanie to nie jest objęte wyjątkiem dotyczącym niestosowania RODO do przetwarzania dokonywanego w ramach działalności nieobjętej zakresem prawa Unii [36]. 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.

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 [37]. Trybunał stwierdził bowiem, że w ramach tego ujawniania CSDD nie może być uważany za taki „właściwy organ” [38].

W celu ustalenia, czy dostęp do danych osobowych dotyczących wykroczeń drogowych, takich jak punkty karne, stanowi przetwarzanie danych osobowych dotyczących „naruszeń prawa” [39], 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,

[35] Artykuł 10 RODO.
[36] Artykuł 2 ust. 2 lit. a) RODO.
[37] Artykuł 2 ust. 2 lit. d) RODO.
[38] 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).
[39] Artykuł 10 RODO.

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.

Wyrok z dnia 5 grudnia 2023 r. (wielka izba), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

W 2020 r., aby lepiej zarządzać pandemią COVID-19, władze litewskie postanowiły zorganizować nabycie mobilnej aplikacji informatycznej. Aplikacja ta miała przyczynić się do monitorowania epidemiologicznego umożliwiając rejestrowanie i monitorowanie danych osób narażonych na kontakt z wirusem COVID-19.

W tym celu Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (krajowe centrum zdrowia publicznego przy ministerstwie zdrowia, Litwa, zwane dalej „NVSC"), odpowiedzialne za to nabycie, skontaktowało się ze spółką UAB „IT sprendimai sėkmei" (zwaną dalej „spółką ITSS"), zwracając się do niej o utworzenie takiej aplikacji mobilnej. Następnie pracownicy NVSC skierowali do tej spółki wiadomości elektroniczne dotyczące między innymi pytań, które powinny znaleźć się w tej aplikacji.

W okresie od kwietnia do maja 2020 r. aplikacja mobilna utworzona przez tę spółkę ITSS została udostępniona publicznie. W konsekwencji 3802 osoby skorzystały z tej aplikacji i dostarczyły wymagane na podstawie tej aplikacji dotyczące ich dane. Jednakże ze względu na brak środków finansowych NVSC nie udzieliła spółce ITSS żadnego zamówienia publicznego na oficjalne nabycie swojej aplikacji mobilnej i zakończyła związane z tym postępowanie.

W międzyczasie krajowy organ nadzorczy wszczął dochodzenie dotyczące przetwarzania danych osobowych wynikającego z zastosowania tej aplikacji. Decyzją tego organu, wydaną po zakończeniu dochodzenia, zarówno na NVSC, jak i na spółkę ITSS, którą uznano za współadministratora danych, zostały nałożone administracyjne kary pieniężne.

NVSC zaskarżyło tę decyzję do Vilniaus apygardos administracinis teismas (regionalnego sądu administracyjnego w Wilnie, Litwa). Powziąwszy wątpliwości co do wykładni szeregu

przepisów RODO, sąd ten zwrócił się do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym.

W swoim wyroku Trybunał w składzie wielkiej izby wyjaśnił między innymi pojęcie "przetwarzania". W tym względzie wskazał on, że wykorzystywanie danych osobowych do celów testowania systemów informatycznych zintegrowanych z aplikacją mobilną stanowi przetwarzanie w rozumieniu RODO. Jednakże inaczej jest w sytuacji, gdy takie dane zostały zanonimizowane w taki sposób, że osoby, której te dane dotyczą, nie można lub już nie można zidentyfikować, lub gdy chodzi o dane fikcyjne, które nie odnoszą się do istniejącej osoby fizycznej.

Po pierwsze bowiem kwestia, czy dane osobowe są wykorzystywane do testowania systemów informatycznych, czy też w innym celu, nie ma wpływu na zakwalifikowanie danej operacji jako „przetwarzania”. Po drugie jedynie przetwarzanie, które dotyczy danych osobowych, może zostać zakwalifikowane jako „przetwarzanie” w rozumieniu RODO. Fikcyjne i zanonimizowane dane nie stanowią zaś danych osobowych.

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 sekcję 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 wykorzystania. Aby zestaw taki był objęty tym pojęciem, nie jest konieczne, by zawierał kartoteki, szczególne rejestry lub inne systemy służące wyszukiwaniu.

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 sekcje 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)

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 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.

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. Należy uznać, 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).

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.

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.

Wyrok z dnia 5 grudnia 2023 r. (wielka izba), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

W tej sprawie (zob. także sekcję II.3, zatytułowaną „Pojęcie »przetwarzania danych osobowych«") Trybunał zauważył, że podmiot, który zlecił danemu przedsiębiorstwu opracowanie mobilnej aplikacji informatycznej i który w tym kontekście uczestniczył w określaniu celów i sposobów przetwarzania danych osobowych dokonywanego za pośrednictwem tej aplikacji, może zostać uznany za administratora [40]. Stwierdzenia tego nie może podważyć okoliczność, że ów podmiot sam nie przeprowadził operacji przetwarzania takich danych, nie udzielił wyraźnej zgody na realizację konkretnych operacji takiego przetwarzania lub na publiczne udostępnienie wspomnianej aplikacji mobilnej i nie nabył tejże aplikacji mobilnej, chyba że przed tym publicznym udostępnieniem wspomniany podmiot wyraźnie sprzeciwił się temu udostępnieniu i przetwarzaniu danych osobowych, które z niego wynikło.

6. Pojęcie „współadministratora danych"

Wyrok z dnia 5 grudnia 2023 r. (wielka izba), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

W tej sprawie (zob. także sekcje II.3 i II.5, zatytułowane „Pojęcie »przetwarzania danych osobowych«" i „Pojęcie »administratora danych«") Trybunał zauważył, że uznanie dwóch podmiotów za współadministratorów nie zakłada ani istnienia uzgodnień między tymi podmiotami w przedmiocie określenia celów i sposobów przetwarzania danych osobowych, ani istnienia uzgodnień ustalających warunki odnoszące się do współadministrowania danymi. Prawdą jest, że zgodnie z RODO [41] współadministratorzy winni w drodze wspólnych uzgodnień w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z tego rozporządzenia. Istnienie takich uzgodnień nie jest jednak warunkiem wstępnym uznania co najmniej dwóch podmiotów za „współadministratorów", lecz obowiązkiem, który RODO nakłada na współadministratorów, po zakwalifikowaniu ich jako takich,

[40] W rozumieniu art. 4 pkt 7 RODO.
[41] Artykuł 26 ust. 1 RODO w związku z jego motywem 79.

celem zapewnienia, że spełniają oni nałożone na nich wypływające z tego rozporządzenia wymogi. Taka kwalifikacja wynika zatem z samego faktu, że w określaniu celów i sposobów przetwarzania uczestniczyło kilka podmiotów.

Co się tyczy wspólnego określania przez zainteresowane podmioty celów i sposobów przetwarzania, Trybunał wyjaśnił, że ich udział w tym ustalaniu może przybierać różne formy i wynikać zarówno z ich wspólnej decyzji, jak i z ich zbieżnych decyzji. W tym ostatnim przypadku zaś decyzje te powinny uzupełniać się w taki sposób, aby każda z nich miała konkretny wpływ na określanie celów i sposobów przetwarzania.

7. Warunki zgodności z prawem przetwarzania danych osobowych

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

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. Heinz 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.

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.

Ponadto w odniesieniu do kwestii wykorzystywania danych zawartych w rejestrze do celów zwalczania przestępczości Trybunał orzekł w szczególności, że cel ten odnosi się do ścigania popełnionych zbrodni i występków, niezależnie od przynależności państwowej osób, które się ich dopuściły. Wobec tego w świetle celu zwalczania przestępczości z punktu widzenia państwa członkowskiego sytuacja jego obywateli nie może różnić się od sytuacji obywateli Unii niebędących obywatelami tego państwa członkowskiego, którzy zamieszkują na jego terytorium. Tak więc 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.

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

W tym wyroku (zob. także sekcję 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. W tym przypadku zaś 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.

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.

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.

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.

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.

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 Naţională 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 [42] 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 [43]. W tym względzie zgoda nie jest wyrażona w sposób skuteczny w przypadku milczenia, okienek domyślnie zaznaczonych lub niepodjęcia działania.

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.

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.

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.

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

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 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.

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

W tym wyroku (zob. także sekcję 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.

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” [44]. 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

[44] 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”.

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.

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.

Ponadto 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.

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.

III. Przetwarzanie danych osobowych w rozumieniu uregulowań sektorowych w tym zakresie

1. Przetwarzanie danych osobowych w sektorze łączności elektronicznej

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

Niniejsza sprawa dotyczyła oddalenia przez hiszpański sąd śledczy wniosku złożonego w ramach śledztwa w sprawie rozboju, w wyniku którego skradziono portfel i telefon komórkowy. Konkretnie rzecz ujmując, policja zwróciła się do sędziego o przyznanie jej dostępu do danych identyfikacyjnych użytkowników numerów telefonów aktywowanych ze skradzionego telefonu przez okres dwunastu dni od daty kradzieży. Wniosek ten został odrzucony na tej podstawie, że okoliczności, na podstawie których wszczęto dochodzenie, nie miały znamion "poważnego" przestępstwa – to znaczy, zgodnie z prawem hiszpańskim, przestępstwa zagrożonego karą pozbawienia wolności powyżej pięciu lat – a uzyskanie dostępu do tych danych identyfikacyjnych jest możliwy tylko w przypadku tego rodzaju przestępstwa.

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".

W tym kontekście Trybunał wyjaśnił, że o ile w wyroku Tele2 Sverige i Watson i in. [45] 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 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".

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

[45] 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),

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".

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 C-520/18, EU:C:2020:791)

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.

Następnie Trybunał przypomniał, że dyrektywa 2002/58 [46] 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 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 [47],

[46] Artykuł 15 ust. 1 i 3 dyrektywy 2002/58.
[47] Artykuł 5 ust. 1 dyrektywy 2002/58.

wyłącznie z poszanowaniem ogólnych zasad prawa Unii, wśród których figuruje zasada proporcjonalności, oraz praw podstawowych gwarantowanych w Karcie [48].

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 wykładni art. 23 ust. 1 RODO w świetle Karty Trybunał dokonał 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.

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.

Trybunał dodał, że dyrektywa 2002/58 w związku z kartą nie stoi na przeszkodzie środkom ustawodawczym zezwalającym na ukierunkowane zatrzymywanie na określony czas ograniczony do tego, co ściśle niezbędne, danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych

[48] W szczególności art. 7, 8 i 11 oraz art. 52 ust. 1 Karty.

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.

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.

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.

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. Za popełnienie tych przestępstw sąd pierwszej instancji skazał H. K. na karę dwóch lat pozbawienia wolności. Orzeczenie to zostało następnie utrzymane w mocy w postępowaniu apelacyjnym. Protokoły, w oparciu o które ustalono, że doszło do 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 [49] 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. [50], 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

[49] Dokładniej mówiąc, z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.
[50] 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).

ma w tym względzie znaczenia. Ponadto Trybunał stwierdził, że dyrektywa ta, interpretowana w świetle karty praw podstawowych, 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.

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 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.

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.

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.

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.

Według Trybunału z powyższego wynika, że zgodnie z wymogiem niezależności, który powinien spełniać organ odpowiedzialny za przeprowadzenie uprzedniej kontroli, organ ten musi mieć 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. Nie ma to zaś miejsca 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.

Wyrok z dnia 5 kwietnia 2022 r. (wielka izba), Commissioner of An Garda Síochána i in. (C-140/20, EU:C:2022:258)

W niniejszej sprawie wniosek o wydanie orzeczenia w trybie prejudycjalnym został przedstawiony przez Supreme Court (sąd najwyższy, Irlandia) w ramach postępowania cywilnego wszczętego przez osobę skazaną na karę dożywotniego pozbawienia wolności za zabójstwo popełnione w Irlandii. Osoba ta kwestionowała zgodność z prawem Unii niektórych przepisów ustawy krajowej dotyczącej zatrzymywania danych generowanych w ramach łączności elektronicznej. Na podstawie tej ustawy dane o ruchu i dane o lokalizacji dotyczące rozmów telefonicznych oskarżonego zostały zatrzymane przez dostawców usług łączności elektronicznej i udostępnione organom policji. Wątpliwości wyrażone przez sąd odsyłający dotyczyły w szczególności zgodności z dyrektywą 2002/58, interpretowaną w świetle karty, systemu uogólnionego i niezróżnicowanego zatrzymywania tych danych w związku z walką z poważną przestępczością.

W wyroku, wydanym w składzie wielkiej izby, Trybunał potwierdził, uściślając zarazem jego zakres, orzecznictwo wynikające z wyroku La Quadrature du Net i in. [51], przypominając, że uogólnione i niezróżnicowane zatrzymywanie danych o ruchu

[51] Wyrok z dnia 6 października 2020 r., La Quadrature du Net i in. (C- 511/18, C- 512/18 i C- 520/18, EU:C:2020:791).

i danych o lokalizacji dotyczących łączności elektronicznej nie jest dozwolone do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego. Potwierdził również orzecznictwo wynikające z wyroku Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej)[52], w szczególności w odniesieniu do obowiązku uzależnienia dostępu właściwych organów krajowych do owych zatrzymanych danych od uprzedniej kontroli sprawowanej wobec funkcjonariusza policji bądź przez sąd, bądź przez niezależną jednostkę administracyjną.

Trybunał orzekł w pierwszej kolejności, że dyrektywa 2002/58, interpretowana w świetle karty, stoi na przeszkodzie środkom ustawodawczym przewidującym, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji. Biorąc bowiem pod uwagę, po pierwsze, zniechęcający wpływ na wykonywanie praw podstawowych [53], jaki może wywrzeć to zatrzymywanie danych, a po drugie, wagę ingerencji, jaką ono za sobą pociąga, takie zatrzymywanie musi stanowić wyjątek, a nie regułę, od systemu ustanowionego w tej dyrektywie, tak aby dane te nie mogły być zatrzymywane w sposób systemowy i stały. Przestępczość, nawet szczególnie poważna, nie może być utożsamiana z zagrożeniem dla bezpieczeństwa narodowego, gdyż takie utożsamienie mogłoby wprowadzić kategorię pośrednią między bezpieczeństwem narodowym a bezpieczeństwem publicznym w celu zastosowania do tego drugiego wymogów właściwych dla tego pierwszego.

Natomiast dyrektywa 2002/58, interpretowana w świetle Karty, nie stoi na przeszkodzie środkom ustawodawczym przewidującym, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kategorii osób, których dane dotyczą, lub za pomocą kryterium geograficznego, przez okres ograniczony do tego, co ściśle niezbędne, ale odnawialny. Trybunał dodał, że taki środek polegający na zatrzymywaniu danych odnoszący się do miejsc lub infrastruktury, w których regularnie przebywa bardzo wiele osób, lub też do miejsc strategicznych, takich jak porty lotnicze, dworce, porty morskie lub strefy poboru opłat za przejazd, może pozwolić właściwym organom na uzyskanie informacji na temat obecności w tych miejscach lub strefach geograficznych osób korzystających tam ze środka łączności elektronicznej oraz na wyciągnięcie, do celów zwalczania poważnej przestępczości, wniosków co do ich obecności i ich działalności w tych miejscach lub strefach geograficznych. W każdym wypadku ewentualne istnienie trudności w dokładnym określeniu przesłanek i warunków, na jakich można dokonać ukierunkowanego

[52] Wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152).
[53] Ustanowionych w art. 7–11 Karty.

zatrzymywania danych, nie może uzasadniać wprowadzenia przez państwa członkowskie uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji.

Dyrektywa ta, interpretowana w świetle Karty, nie stoi również na przeszkodzie środkom ustawodawczym przewidującym, do tych samych celów, uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia przez okres ograniczony do tego, co ściśle niezbędne oraz danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej. W tym ostatnim aspekcie Trybunał wyjaśnił w szczególności, że ani dyrektywa 2002/58, ani żaden inny akt prawa Unii nie stoją na przeszkodzie uregulowaniu krajowemu, mającemu na celu zwalczanie poważnej przestępczości, na podstawie którego nabycie środka łączności elektronicznej, takiego jak opłaconej z góry karty SIM, jest uzależnione od sprawdzenia urzędowych dokumentów ustalających tożsamość nabywcy i od zarejestrowania przez sprzedawcę wynikających z nich informacji, gdyż sprzedawca jest w stosownym wypadku zobowiązany do udzielenia dostępu do tych informacji właściwym organom krajowym.

Nie inaczej jest w przypadku środków ustawodawczych przewidujących, również do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, posłużenie się skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, nakazem szybkiego zatrzymania („quick freeze”) przez określony czas danych o ruchu i danych o lokalizacji, którymi dysponują ci dostawcy usług. Jedynie bowiem walka z poważną przestępczością i, a fortiori, ochrona bezpieczeństwa narodowego mogą uzasadniać takie zatrzymywanie danych, pod warunkiem że środek ten oraz dostęp do zatrzymanych danych przestrzegają granic tego, co ściśle niezbędne. Trybunał przypomniał, że taki środek polegający na szybkim zatrzymaniu danych może zostać rozszerzony na dane o ruchu i dane o lokalizacji dotyczące osób innych niż te, które są podejrzewane o planowanie lub popełnienie poważnego przestępstwa lub naruszenie bezpieczeństwa narodowego, o ile dane te mogą w oparciu o obiektywne i niedyskryminacyjne kryteria przyczynić się do wyjaśnienia takiego przestępstwa lub takiego naruszenia bezpieczeństwa narodowego, takie jak dane ofiary tego przestępstwa lub naruszenia, jej otoczenia społecznego lub zawodowego.

Trybunał wskazał jednak następnie, że wszystkie wymienione wyżej środki ustawodawcze muszą za pomocą jasnych i precyzyjnych przepisów zapewniać, że odnośne zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych warunków oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć. Różnego rodzaju środki polegające na zatrzymywaniu danych o ruchu i danych o lokalizacji mogą – zgodnie z wyborem ustawodawcy krajowego i przy poszanowaniu granic tego, co ściśle niezbędne – znaleźć wspólnie zastosowanie.

Ponadto Trybunał wyjaśnił, że zezwolenie, do celów zwalczania poważnej przestępczości, na dostęp do takich danych zatrzymywanych w uogólniony i niezróżnicowany sposób, aby stawić czoła poważnemu zagrożeniu dla bezpieczeństwa narodowego,

pozostawałoby w sprzeczności z tą hierarchią celów interesu ogólnego mogących uzasadniać środek przyjęty na podstawie dyrektywy 2002/58. Oznaczałoby to bowiem dopuszczenie sytuacji, w której dostęp mógłby zostać uzasadniony celem o mniejszym znaczeniu niż cel, który uzasadniał zatrzymanie danych, czyli ochrona bezpieczeństwa narodowego, grożąc tym samym pozbawieniem wszelkiej skuteczności (effet utile) zakazu uogólnionego i niezróżnicowanego zatrzymywania danych do celów zwalczania poważnej przestępczości.

W drugiej kolejności Trybunał orzekł, że dyrektywa 2002/58, interpretowana w świetle Karty, stoi na przeszkodzie uregulowaniu krajowemu, na podstawie którego scentralizowane rozpatrywanie wniosków o udzielenie dostępu do danych zatrzymanych przez dostawców usług łączności elektronicznej, pochodzących od policji w ramach wykrywania i ścigania poważnych przestępstw, należy do funkcjonariusza policji, nawet jeżeli jest on wspierany przez ustanowioną w obrębie policji jednostkę, której przysługuje pewien stopień autonomii w wykonywaniu powierzonego jej zadania i której decyzje mogą być następnie przedmiotem kontroli sądowej. Po pierwsze, taki funkcjonariusz nie spełnia bowiem wymogów niezależności i bezstronności, które obowiązują organ administracyjny sprawujący uprzednią kontrolę wniosków o udzielenie dostępu do danych pochodzących od właściwych organów krajowych, ponieważ nie ma on statusu osoby trzeciej w stosunku do tych organów. Po drugie, choć decyzja takiego funkcjonariusza może być przedmiotem dokonanej a posteriori kontroli sądowej, kontrola ta nie może jednak zastąpić niezależnej i – z wyjątkiem pilnych i należycie uzasadnionych przypadków – uprzedniej kontroli.

Wreszcie, w trzeciej kolejności Trybunał potwierdził swoje orzecznictwo, zgodnie z którym prawo Unii stoi na przeszkodzie temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji ze względu na niezgodność tego uregulowania z dyrektywą 2002/58. Niezależnie od powyższego Trybunał przypomniał, że kwestia dopuszczalności dowodów uzyskanych za pomocą takiego uogólnionego i niezróżnicowanego zatrzymywania danych należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

Wyrok z dnia 20 września 2022 r. (wielka izba), VD i SR (C-339/20 i C-397/20, EU:C:2022:703)

W następstwie dochodzenia przeprowadzonego przez Autorité des marchés financières (urząd rynków finansowych, Francja, zwany dalej „AMF”) wszczęto postępowania karne przeciwko VD i SR, dwóm osobom fizycznym oskarżonym o popełnienie przestępstw wykorzystywania i ukrywania informacji poufnych, współsprawstwa, korupcji i prania pieniędzy. W ramach tego dochodzenia AMF wykorzystał dane osobowe pochodzące z rozmów telefonicznych VD i SR, wygenerowane na podstawie code des postes et des

communications électroniques (kodeksu pocztowego i łączności elektronicznej) w ramach świadczenia usług łączności elektronicznej.

Ponieważ ich oskarżenie było oparte na danych o ruchu dostarczonych przez AMF, VD i SR wnieśli osobno do cour d'appel de Paris (sądu apelacyjnego w Paryżu, Francja) skargi, podnosząc w szczególności zarzut dotyczący naruszenia art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty. Ściślej rzecz ujmując, opierając się na orzecznictwie wynikającym z wyroku Tele2 Sverige i Watson i in. [54], VD i SR kwestionowali fakt, że w celu zgromadzenia wspomnianych danych organ ten oparł się na przepisach krajowych, podczas gdy przepisy te z jednej strony nie były zgodne z prawem Unii w zakresie, w jakim przewidywały uogólnione i niezróżnicowane zatrzymywanie danych dotyczących połączeń, a z drugiej strony nie określały żadnych ograniczeń w zakresie uprawnień śledczych AMF do uzyskania dostępu do zatrzymanych danych.

Dwoma wyrokami z dnia 20 grudnia 2018 r. i z dnia 7 marca 2019 r. cour d'appel de Paris (sąd apelacyjny w Paryżu) oddalił skargi VD i SR. W celu oddalenia wspomnianego wyżej zarzutu sędziowie orzekający co do istoty oparli się w szczególności na fakcie, że rozporządzenie w sprawie nadużyć na rynku [55] umożliwia właściwym organom uzyskanie – w zakresie dozwolonym prawem krajowym – istniejących zapisów danych o ruchu przechowywanych przez operatorów usług łączności elektronicznej w przypadku uzasadnionego podejrzenia naruszenia zakazu wykorzystywania informacji poufnych i gdy takie zapisy mogą mieć znaczenie dla czynności wyjaśniających w sprawie tego naruszenia

VD i SR wnieśli następnie odwołanie do Cour de cassation (sądu kasacyjnego, Francja), będącego sądem odsyłającym w niniejszych sprawach.

W tym kontekście sąd ten zastanawia się nad pogodzeniem art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej, interpretowanego w świetle karty, z wymogami wynikającymi z art. 12 ust. 2 lit. a) i d) dyrektywy w sprawie nadużyć na rynku [56] oraz z art. 23 ust. 2 lit. g) i h) rozporządzenia w sprawie nadużyć na rynku. Wątpliwość ta ma swoje źródło w przepisach ustawowych będących przedmiotem postępowania głównego, które nakładają na operatorów usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu zapobiegawczo przez okres jednego roku od dnia zapisu dla celów zwalczania naruszeń stanowiących nadużycie na rynku, do których zalicza się wykorzystywanie informacji poufnych. Na wypadek gdyby Trybunał uznał, że rozpatrywane w postępowaniu głównym przepisy dotyczące zatrzymywania danych dotyczących połączeń nie są zgodne z prawem Unii,

[54] Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C- 203/15 i C- 698/15, EU:C:2016:970).

[55] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6 i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE (Dz.U. 2014, L 173, s. 1).

[56] Dyrektywa 2003/6/WE Parlamentu Europejskiego i Rady z dnia 28 stycznia 2003 r. w sprawie wykorzystywania poufnych informacji i manipulacji na rynku (nadużyć na rynku) (Dz.U. 2003, L 96, s. 16).

sąd odsyłający zastanawia się nad kwestią tymczasowego utrzymania w mocy skutków tego ustawodawstwa w celu uniknięcia niepewności prawnej i umożliwienia wykorzystania danych zgromadzonych wcześniej i zatrzymanych do celów wykrywania i ścigania wykorzystywania informacji poufnych.

W swoim wyroku Trybunał, orzekający w składzie wielkiej izby, uznał, że uogólnione i niezróżnicowane zatrzymywanie danych o ruchu przez okres jednego roku od dnia rejestracji przez operatorów usług łączności elektronicznej nie jest dozwolone zapobiegawczo w celu zwalczania naruszeń w postaci nadużyć na rynku. Ponadto potwierdził on swoje orzecznictwo, zgodnie z którym prawo Unii sprzeciwia się temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego ma on dokonać w odniesieniu do krajowych przepisów ustawowych niezgodnych z prawem Unii.

Trybunał przypomniał przede wszystkim, że w celu dokonania wykładni przepisu prawa Unii należy nie tylko odwołać się do jego brzmienia, lecz także uwzględnić jego kontekst oraz cele regulacji, której część on stanowi.

W odniesieniu do brzmienia przepisów, o których mowa w pytaniach prejudycjalnych, Trybunał stwierdził, że podczas gdy art. 12 ust. 2 lit. d) dyrektywy w sprawie nadużyć na rynku odnosi się do uprawnienia AMF do „żądania wydania rejestrów połączeń i rejestrów przesyłu danych", art. 23 ust. 2 lit. g) i h) rozporządzenia w sprawie nadużyć na rynku odsyła do uprawnienia tego organu do żądania wydania z jednej strony „zapisów danych o ruchu przechowywanych przez firmy inwestycyjne, instytucje kredytowe lub instytucje finansowe", a z drugiej strony „żądania, w zakresie dozwolonym prawem krajowym, wydania istniejących zapisów danych o ruchu przechowywanych przez operatora telekomunikacyjnego". Zdaniem Trybunału z brzmienia tych przepisów wynika jednoznacznie, że ograniczają się one do zakreślenia ram uprawnienia AMF do „żądania" lub „żądania wydania" danych, którymi dysponują ci operatorzy, co odpowiada dostępowi do tych danych. Ponadto odwołanie się do zapisów „istniejących", takich jak „przechowywane" przez wspomnianych operatorów, sugeruje, że prawodawca Unii nie zamierzał regulować możliwości ustanowienia przez ustawodawcę krajowego obowiązku przechowywania takich zapisów. Zdaniem Trybunału za taką wykładnią przemawia zarówno kontekst, w jaki wpisują się wspomniane przepisy, jak i cele uregulowania, którego część stanowią te przepisy.

Co się tyczy kontekstu, w jaki wpisują się przepisy, o których mowa w pytaniach prejudycjalnych, Trybunał zauważył, że o ile zgodnie z właściwymi przepisami dyrektywy w sprawie nadużyć na rynku [57] i rozporządzenia w sprawie nadużyć na rynku prawodawca Unii zamierzał zobowiązać państwa członkowskie do podjęcia niezbędnych środków w celu zapewnienia, aby organy właściwe w sprawach finansowych dysponowały zestawem narzędzi, kompetencji i odpowiednich zasobów, jak również

[57] Odpowiednio art. 12 ust. 1 dyrektywy w sprawie nadużyć na rynku i art. 23 ust. 3 rozporządzenia w sprawie nadużyć na rynku w świetle motywu 62 tego rozporządzenia.

uprawnień nadzorczych i śledczych niezbędnych do zapewnienia skuteczności ich zadań, o tyle przepisy te nie mówią nic o tym, czy państwa członkowskie mogą w tym celu nałożyć na operatorów usług łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, ani o warunkach, na jakich dane te powinny być zatrzymywane przez tych operatorów w celu przekazania ich w stosownych przypadkach właściwym organom.

Co się tyczy celów spornej regulacji, Trybunał wskazuje, że zarówno z dyrektywy w sprawie nadużyć na rynku, jak i z rozporządzenia w sprawie nadużyć [58] na rynku wynika, iż celem tych instrumentów jest zapewnienie integralności rynków finansowych Unii i zwiększenie zaufania inwestorów do tych rynków, które to zaufanie opiera się w szczególności na tym, że będą one traktowane na równych zasadach i chronione przed bezprawnym wykorzystywaniem informacji poufnych. Zakaz wykorzystywania informacji poufnych ustanowiony we wspomnianych instrumentach [59] ma zatem na celu zagwarantowanie równości stron transakcji giełdowej poprzez uniknięcie sytuacji, w której jedna z nich, posiadająca informacje poufne i znajdująca się w związku z tym w uprzywilejowanej sytuacji w stosunku do pozostałych inwestorów, osiąga w ten sposób korzyść ze szkodą dla innych inwestorów, którzy nie posiadają takich informacji. O ile zgodnie z rozporządzeniem w sprawie nadużyć na rynku [60] zapisy danych o połączeniach stanowią istotny, a niekiedy jedyny dowód pozwalający na wykrycie i udowodnienie wykorzystywania informacji poufnych lub manipulacji na rynku, o tyle motyw ten odnosi się jedynie do zapisów „przechowywanych" przez operatorów usług łączności elektronicznej, a także do uprawnienia organu właściwego w sprawach finansowych do „zażądania" od tych operatorów udostępnienia „istniejących" danych. Z tekstu tego nie wynika zatem w żaden sposób, że prawodawca Unii zamierzał w ten sposób przyznać państwom członkowskim uprawnienie do nałożenia na operatorów świadczących usługi łączności elektronicznej uogólnionego obowiązku zatrzymywania danych. Wynika z tego, że ani dyrektywa w sprawie nadużyć na rynku, ani rozporządzenie w sprawie nadużyć na rynku nie mogą stanowić podstawy prawnej ogólnego obowiązku zatrzymywania zapisów danych o ruchu przechowywanych przez operatorów usług łączności elektronicznej w celu wykonywania uprawnień powierzonych organowi właściwemu w sprawach finansowych na podstawie tych aktów.

Następnie Trybunał przypomniał, że dyrektywa 2002/58 jest uregulowaniem stanowiącym punkt odniesienia w dziedzinie zatrzymywania i, bardziej ogólnie, przetwarzania danych osobowych w sektorze łączności elektronicznej, wobec czego wykładnia dokonana przez Trybunał w świetle tej dyrektywy stosuje się również do zapisów danych o ruchu przechowywanych przez operatorów usług łączności elektronicznej, których organy właściwe w sprawach finansowych w rozumieniu

[58] Odpowiednio motywy 2 i 12 dyrektywy w sprawie nadużyć na rynku i art. 1 rozporządzenia w sprawie nadużyć na rynku w świetle motywów 2 i 24 tego rozporządzenia.
[59] Artykuł 2 ust. 1 dyrektywy w sprawie nadużyć na rynku i art. 8 ust. 1 rozporządzenia w sprawie nadużyć na rynku.
[60] Motyw 62 rozporządzenia w sprawie nadużyć na rynku.

dyrektywy w sprawie nadużyć na rynku i rozporządzenia w sprawie nadużyć na rynku [61] mogą zażądać od tych operatorów. Ocena zgodności z prawem przetwarzania zapisów przechowywanych przez operatorów usług łączności elektronicznej [62] powinna być dokonywana zatem w świetle przesłanek przewidzianych w dyrektywie 2002/58, a także wykładni tej dyrektywy dokonanej przez Trybunał w jego orzecznictwie.

W konsekwencji Trybunał orzekł, że dyrektywa w sprawie nadużyć na rynku i rozporządzenie w sprawie nadużyć na rynku w związku z dyrektywą 2002/58 oraz w świetle Karty sprzeciwiają się środkom ustawodawczym przewidującym zapobiegawczo w celu zwalczania przestępstw polegających na nadużyciach na rynku, do których zalicza się wykorzystywanie informacji poufnych, ogólne i niezróżnicowane zatrzymywanie danych o ruchu przez rok od dnia ich zapisu.

Wreszcie, Trybunał potwierdził swoje orzecznictwo, zgodnie z którym prawo Unii sprzeciwia się temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego na mocy prawa krajowego ma on dokonać w odniesieniu do przepisów krajowych, które z jednej strony nakładają na operatorów świadczących usługi łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, a z drugiej strony pozwalają na przekazywanie tych danych organowi właściwemu w sprawach finansowych bez uprzedniego zezwolenia sądu lub niezależnego organu administracyjnego, ze względu na niezgodność tych przepisów z dyrektywą 2002/58 interpretowaną w świetle karty. Niezależnie od powyższego Trybunał przypomniał, że kwestia dopuszczalności dowodów uzyskanych za pomocą takiego uogólnionego i niezróżnicowanego zatrzymywania danych należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności. Ta ostatnia zasada wymaga od krajowego sądu karnego, aby pominął informacje i dowody uzyskane w drodze uogólnionego i niezróżnicowanego zatrzymywania danych niezgodnego z prawem Unii, jeżeli zainteresowane osoby nie są w stanie skutecznie ustosunkować się do tych informacji i dowodów należących do dziedziny niepodlegającej rozpoznaniu przez sąd i mogących mieć decydujący wpływ na ocenę okoliczności faktycznych.

Wyrok z dnia 30 kwietnia 2024 r. (pełny skład Trybunału), La Quadrature du Net i in. (Dane osobowe i walka z naruszeniami praw własności intelektualnej) (C-470/21, EU:C:2024:370)

Trybunał, do którego z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym zwróciła się Conseil d'État (rada stanu, Francja), rozwinął swe orzecznictwo w przedmiocie dyrektywy 2002/58, przedstawiając w wyroku, który zapadł w pełnym składzie, wyjaśnienia dotyczące, po pierwsze, warunków, w jakich uogólnionego przechowywania adresów IP przez dostawców usług łączności elektronicznej nie można

[61] Odpowiednio art. 11 dyrektywy w sprawie nadużyć na rynku i art. 22 rozporządzenia w sprawie nadużyć na rynku.
[62] W rozumieniu art. 12 ust. 2 lit. d) dyrektywy w sprawie nadużyć na rynku i art. 23 ust. 2 lit. g) i h) rozporządzenia w sprawie nadużyć na rynku.

postrzegać jako wiążącego się z poważną ingerencją w zagwarantowane w Karcie [63] prawa do poszanowania życia prywatnego, do ochrony danych osobowych oraz do wolności wypowiedzi, oraz, po drugie, możliwości uzyskania przez organ publiczny dostępu do niektórych przechowywanych w poszanowaniu owych warunków danych osobowych w ramach zwalczania naruszeń praw własności intelektualnej, do których dochodzi w Internecie.

W rozpatrywanym wypadku cztery stowarzyszenia złożyły do premiera (Francja) wniosek o uchylenie décret relatif au traitement automatisé de données à caractère personnel (dekretu w sprawie zautomatyzowanego przetwarzania danych osobowych) [64]. Z uwagi na to, że wniosek ten nie wywołał zamierzonych skutków, wspomniane stowarzyszenia wniosły do Conseil d'État (rady stanu) skargę o uchylenie tej dorozumianej decyzji oddalającej. Ich zdaniem ów dekret oraz przepisy, które stanowią jego podstawę prawną[65], naruszają prawo Unii.

Zgodnie z prawem francuskim Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi, wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie) – aby móc identyfikować osoby, które dopuściły się naruszeń praw autorskich lub praw pokrewnych w Internecie – jest upoważniony do dostępu do niektórych danych, które dostawcy usług łączności elektronicznej mają obowiązek przechowywać. Dane te odnoszą się do tożsamości cywilnej danej osoby, odpowiadającej jej adresowi IP zebranemu wcześniej przez organizacje zrzeszające uprawnionych. Po zidentyfikowaniu posiadacza adresu IP wykorzystanego do aktywności wiążącej się z takim naruszeniem Hadopi wszczyna tzw. procedurę stopniowej odpowiedzi. Konkretnie jest on uprawniony do wysłania tej osobie dwóch zaleceń, które są podobne do ostrzeżeń, a w przypadku kontynuacji aktywności – pisma informującego ją, że jej aktywność może być przedmiotem ścigania. Wreszcie ma on prawo zawiadomić prokuraturę w celu ścigania owej osoby [66].

W tym kontekście Conseil d'État (rada stanu) zwróciła się do Trybunału z pytaniami dotyczącymi wykładni dyrektywy o prywatności i łączności elektronicznej w świetle Karty[67].

---

63 Artykuły 7, 8 i 11 Karty.

64 Décret no 2010- 236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331- 29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (dekret nr 2010- 236 z dnia 5 marca 2010 r. w sprawie zautomatyzowanego przetwarzania danych osobowych dopuszczonego w art. L. 331- 29 kodeksu własności intelektualnej, zwanego „systemem zarządzania środkami ochrony utworów w Internecie") (JORF nr 56 z dnia 7 marca 2010 r., akt nr 19), zmieniony décret no 2017- 924 du 6 mai 2017 relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (dekretem nr 2017- 924 z dnia 6 maja 2017 r. w sprawie zarządzania prawami autorskimi i prawami pokrewnymi przez organizację zarządzania prawami, zmieniającym kodeks własności intelektualnej) (JORF nr 109 z dnia 10 maja 2017 r., akt nr 176).

65 W szczególności art. L. 331- 21 akapity od trzeciego do piątego code de la propriété intellectuelle (kodeksu własności intelektualnej).

66 W dniu 1 stycznia 2022 r. Hadopi połączono z Conseil supérieur de l'audiovisuel (CSA, wyższą radą ds. radiofonii i telewizji), będącą innym niezależnym organem publicznym, tworząc Autorité de régulation de la communication audiovisuelle et numérique (ARCOM, organ ds. regulacji komunikacji radiowo- telewizyjnej i cyfrowej). Procedura stopniowej odpowiedzi pozostała jednak w swej istocie niezmieniona.

67 Artykuł 15 ust. 1 dyrektywy 2002/58.

W pierwszej kolejności, co się tyczy przechowywania danych dotyczących tożsamości cywilnej i odpowiadających im adresów IP, Trybunał podkreślił, że nie każde uogólnione i niezróżnicowane przechowywanie adresów IP stanowi w sposób konieczny poważną ingerencję w zagwarantowane w Karcie prawa do poszanowania życia prywatnego, do ochrony danych osobowych oraz do wolności wypowiedzi.

Obowiązek zapewnienia takiego przechowywania może być uzasadniony celem polegającym na zwalczaniu ogółu czynów zabronionych, jeżeli rzeczywiście wykluczono ewentualność wywołania przez owo przechowywanie poważnej ingerencji w życie prywatne osoby, której dane dotyczą, ze względu na możliwość wyciągnięcia precyzyjnych wniosków na temat jej życia prywatnego w szczególności poprzez powiązanie tych adresów IP ze zbiorem danych o ruchu lub danych dotyczących lokalizacji.

W związku z tym państwo członkowskie, które zamierza nałożyć na dostawców usług łączności elektronicznej taki obowiązek, musi zapewnić, by zasady przechowywania tych danych wykluczały możliwość wyciągnięcia precyzyjnych wniosków na temat życia prywatnego osób, których dane dotyczą.

Trybunał uściślił, że aby osiągnąć ten skutek, zasady przechowywania muszą odnosić się do samej struktury przechowywania, która zasadniczo musi być zorganizowana w taki sposób, aby gwarantować rzeczywiście szczelne odseparowanie poszczególnych kategorii przechowywanych danych. Przepisy krajowe dotyczące tych zasad muszą zatem zapewniać, aby każda kategoria danych, w tym dane dotyczące tożsamości cywilnej i adresy IP, była przechowywana w sposób w pełni odseparowany od pozostałych kategorii przechowywanych danych i aby to odseparowanie było rzeczywiście szczelne dzięki wykorzystaniu bezpiecznego i niezawodnego systemu informatycznego. Ponadto w zakresie, w jakim owe przepisy przewidują możliwość powiązania przechowywanych adresów IP z tożsamością cywilną osoby, której dane dotyczą, na potrzeby zwalczania czynów zabronionych, muszą one pozwalać na dokonanie takiego powiązania wyłącznie poprzez zastosowanie efektywnego rozwiązania technicznego, które nie wpływa na skuteczność szczelnego odseparowania tych kategorii danych. Niezawodność tego odseparowania musi podlegać regularnej kontroli osobnego organu publicznego. Pod warunkiem, że we właściwych przepisach krajowych przewidziano takie rygorystyczne wymogi, wynikającej z tego przechowywania adresów IP ingerencji nie można uznać za „poważną”.

W związku z tym Trybunał doszedł do wniosku, że w przypadku przyjęcia regulacji prawnej gwarantującej, że żadne powiązanie danych nie pozwala na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane są przechowywane, dyrektywa 2002/58 w świetle Karty nie stoi na przeszkodzie nałożeniu przez państwo członkowskie obowiązku uogólnionego i niezróżnicowanego przechowywania adresów IP przez okres nieprzekraczający tego, co ściśle niezbędne, do celów zwalczania ogółu czynów zabronionych.

W drugiej kolejności, co się tyczy dostępu do danych dotyczących tożsamości cywilnej odpowiadających adresom IP, Trybunał orzekł, że dyrektywa 2002/58 interpretowana w świetle Karty co do zasady nie stoi na przeszkodzie uregulowaniu krajowemu zezwalającemu organowi publicznemu na dostęp do tych danych przechowywanych przez dostawców usług łączności elektronicznej w sposób odseparowany i rzeczywiście szczelny, wyłącznie w tym celu, aby ów organ publiczny mógł zidentyfikować posiadaczy tych adresów podejrzewanych o dopuszczenie się naruszeń praw autorskich lub praw pokrewnych w Internecie i zastosować wobec nich środki. W takim przypadku uregulowanie krajowe musi zakazywać urzędnikom mającym taki dostęp, po pierwsze, ujawniania w jakiejkolwiek formie informacji na temat zawartości plików przeglądanych przez tych posiadaczy, z jedynym wyjątkiem wiążącym się z ujawnieniem ich w celu zawiadomienia prokuratury, po drugie, wszelkiego śledzenia historii treści przeglądanych przez owych posiadaczy, oraz po trzecie, wykorzystywania tych adresów IP do celów innych niż zastosowanie owych środków.

W tym kontekście Trybunał przypomniał w szczególności, że chociaż wolność wypowiedzi i poufność danych osobowych są kwestiami o fundamentalnym znaczeniu, to jednak te prawa podstawowe nie mają charakteru absolutnego. Przy dokonywaniu wyważenia wchodzących w grę praw i interesów muszą one bowiem niekiedy ustąpić przed innymi prawami podstawowymi i nadrzędnymi względami interesu ogólnego, takimi jak ochrona porządku publicznego, zapobieganie czynom zabronionym czy ochrona praw i wolności innych osób. Jest tak zwłaszcza w przypadku, gdy nadrzędna rola przypisywana owym kwestiom o fundamentalnym znaczeniu mogłaby prowadzić do ograniczenia skuteczności dochodzenia karnego, w szczególności poprzez uniemożliwienie lub nadmierne utrudnienie skutecznej identyfikacji sprawcy czynu zabronionego i nałożenia na niego kary.

W tym samym kontekście Trybunał odniósł się również do swojego orzecznictwa, zgodnie z którym w zakresie zwalczania czynów zabronionych naruszających prawa autorskie lub prawa pokrewne, do których dochodzi w Internecie, okoliczność, że dostęp do adresów IP może stanowić jedyny środek dochodzeniowy umożliwiający ustalenie tożsamości danej osoby, skłania do stwierdzenia, że przechowywanie tych adresów i dostęp do nich są ściśle niezbędne do osiągnięcia zamierzonego celu, a zatem spełniają wymóg proporcjonalności. Nieumożliwienie takiego dostępu wiązałoby się ponadto z rzeczywistym ryzykiem systemowej bezkarności w zakresie czynów zabronionych, które popełniono w Internecie bądź których popełnienie lub do których przygotowanie ułatwiają szczególne cechy Internetu. Istnienie takiego ryzyka stanowi zaś okoliczność istotną dla oceny, w ramach dokonywania wyważenia różnych wchodzących w grę praw i interesów, czy dana ingerencja w prawa do poszanowania życia prywatnego, do ochrony danych osobowych oraz do wolności wypowiedzi jest środkiem proporcjonalnym w świetle celu polegającego na zwalczaniu czynów zabronionych.

W trzeciej kolejności, wypowiadając się w kwestii, czy dostęp organu publicznego do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP powinien być

uzależniony od dokonania uprzedniej kontroli przez sąd lub niezależny organ administracyjny, Trybunał uznał, że wymóg takiej kontroli znajduje zastosowanie, gdy w kontekście uregulowania krajowego dostęp ten wiąże się z ryzykiem poważnej ingerencji w prawa podstawowe osoby, której dane dotyczą, w tym znaczeniu, że mógłby on pozwolić temu organowi publicznemu na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego tej osoby i, w stosownych przypadkach, na ustalenie jej szczegółowego profilu. Ów wymóg uprzedniej kontroli nie ma natomiast zastosowania, gdy ingerencji w prawa podstawowe nie można uznać za poważną.

W tym względzie Trybunał wyjaśnił, że w razie wprowadzenia mechanizmu przechowywania gwarantującego rzeczywiście szczelne odseparowanie poszczególnych kategorii przechowywanych danych dostęp organu publicznego do danych dotyczących tożsamości cywilnej odpowiadających adresom IP co do zasady nie jest uzależniony od wymogu uprzedniej kontroli. Taki dostęp wyłącznie w celu zidentyfikowania posiadacza adresu IP zasadniczo nie stanowi bowiem poważnej ingerencji w wyżej wymienione prawa.

Trybunał nie wykluczył jednak istnienia – w nietypowych sytuacjach – ryzyka, że w ramach procedury takiej jak procedura stopniowej odpowiedzi rozpatrywana w postępowaniu głównym organ publiczny może wyciągnąć precyzyjne wnioski na temat życia prywatnego osoby, której dane dotyczą, w szczególności wtedy, gdy osoba ta podejmuje aktywność naruszającą prawa autorskie lub prawa pokrewne w sieciach peer-to-peer wielokrotnie, czy wręcz na dużą skalę, w związku z chronionymi utworami określonego rodzaju, co może prowadzić do ujawnienia informacji, potencjalnie wrażliwych, na temat jej życia prywatnego.

W rozpatrywanym wypadku posiadacze adresów IP mogli być szczególnie narażeni na takie ryzyko wtedy, gdy organ publiczny miał podjąć decyzję o ewentualnym zawiadomieniu prokuratury w celu ich ścigania. Intensywność naruszenia prawa do poszanowania życia prywatnego mogła bowiem wzrastać w miarę osiągania przez procedurę stopniowej odpowiedzi, która przebiega w trybie sekwencyjnym, poszczególnych etapów, które się na nią składają. Dostęp właściwego organu do zbioru zgromadzonych na poszczególnych etapach tej procedury danych osoby, której one dotyczą, mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat jej życia prywatnego. W związku z tym uregulowanie krajowe musi przewidywać uprzednią kontrolę, która powinna mieć miejsce, zanim organ publiczny będzie mógł powiązać dane dotyczące tożsamości cywilnej z takim zbiorem danych, a także przed ewentualnym wysłaniem pisma informującego, w którym stwierdza się, że osoba ta dopuściła się czynów, które mogą być przedmiotem ścigania. Kontrola ta musi ponadto pozwolić na zachowanie skuteczności procedury stopniowej odpowiedzi poprzez umożliwienie w szczególności wykrywania przypadków możliwego kolejnego ponowienia danego zachowania noszącego znamiona czynu zabronionego. Aby osiągnąć ten skutek, procedura ta powinna być zorganizowana i ustrukturyzowana w taki sposób, aby dane dotyczące tożsamości cywilnej danej osoby odpowiadające zebranym wcześniej

w Internecie adresom IP nie mogły być przez osoby odpowiedzialne w ramach właściwego organu publicznego za analizę zdarzeń automatycznie powiązane z elementami, którymi organ ten już dysponuje i które mogłyby pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego tej osoby.

Ponadto, co się tyczy przedmiotu uprzedniej kontroli, Trybunał zauważył, że w przypadku gdy osobę, której dane dotyczą, podejrzewa się o to, że dopuściła się naruszenia należącego do czynów zabronionych w ujęciu ogólnym, sąd lub niezależny organ administracyjny odpowiedzialny za tę kontrolę musi odmówić dostępu, gdyby dostęp ten pozwalał organowi publicznemu, który zawnioskował o jego udzielenie, na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego wspomnianej osoby. Należy natomiast dopuścić możliwość udzielenia nawet takiego dostępu, który pozwala na wyciągnięcie takich precyzyjnych wniosków, w przypadku gdy osobę, której dane dotyczą, podejrzewa się o to, że dopuściła się występków, które dane państwo członkowskie uznało za naruszające jeden z podstawowych interesów społeczeństwa i należące w związku z tym do form poważnej przestępczości.

Trybunał wyjaśnił również, że uprzednia kontrola w żadnym razie nie może być w pełni zautomatyzowana, ponieważ – w odniesieniu do dochodzenia karnego – taka kontrola wymaga wyważenia uzasadnionych interesów związanych ze zwalczeniem przestępczości z jednej strony oraz poszanowania życia prywatnego i ochrony danych osobowych z drugiej strony. Owo wyważenie wymaga udziału osoby fizycznej, który jest tym bardziej niezbędny, że zautomatyzowanie i duża skala rozpatrywanego przetwarzania danych wiążą się z ryzykiem dla życia prywatnego.

Trybunał doszedł zatem do wniosku, że możliwość powiązania, przez osoby odpowiedzialne w ramach organu publicznego za analizę zdarzeń, danych dotyczących tożsamości cywilnej danej osoby odpowiadających adresowi IP z plikami zawierającymi elementy umożliwiające poznanie tytułów utworów chronionych, których udostępnienie w Internecie uzasadniało zebranie adresów IP przez organizacje zrzeszające uprawnionych, musi być uzależniona – w przypadkach kolejnego ponowienia aktywności naruszającej prawa autorskie lub prawa pokrewne przez tę samą osobę – od dokonania przez sąd lub niezależny organ administracyjny kontroli. Kontrola ta nie może być w pełni zautomatyzowana i powinna mieć miejsce przed dokonaniem takiego powiązania, które może w takich przypadkach pozwolić na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego wspomnianej osoby, której adres IP wykorzystano do aktywności mogącej naruszać prawa autorskie lub prawa pokrewne.

W czwartej i ostatniej kolejności Trybunał wskazał, że system przetwarzania danych wykorzystywany przez organ publiczny musi podlegać w regularnych odstępach czasu kontroli niezależnego organu mającego status strony trzeciej w stosunku do tego organu publicznego. Kontrola ta ma na celu weryfikację integralności systemu, w tym skutecznych gwarancji chroniących przed ryzykiem takiego dostępu do tych danych lub takiego ich wykorzystywania, które nosiłyby znamiona nadużycia lub byłyby niezgodne

z prawem, oraz jego skuteczności i niezawodności w wykrywaniu ewentualnych uchybień.

W tym kontekście Trybunał zauważył, że w rozpatrywanym wypadku zautomatyzowane przetwarzanie danych osobowych dokonywane przez organ publiczny na podstawie informacji dotyczących naruszeń praw własności intelektualnej stwierdzanych przez organizacje zrzeszające uprawnionych mogło wiązać się z pewną liczbą „fałszywych alarmów" oraz, przede wszystkim, z ryzykiem niewłaściwego wykorzystania przez osoby trzecie potencjalnie bardzo dużej ilości danych w celach noszących znamiona nadużycia lub niezgodnych z prawem, co uzasadnia konieczność takiej kontroli. Trybunał dodał ponadto, że przetwarzanie to musi być zgodne z dotyczącymi ochrony danych osobowych przepisami szczególnymi przewidzianymi w dyrektywie 2016/680. Nawet bowiem jeżeli w rozpatrywanym wypadku organ publiczny nie posiadał własnych uprawnień decyzyjnych w ramach tzw. procedury stopniowej odpowiedzi, należało uznać, że jest on „organem publicznym" zaangażowanym w zapobieganie czynom zabronionym i wykrywanie takich czynów, w związku z czym jest objęty jej zakresem stosowania. Osobom uczestniczącym w takiej procedurze musi wobec tego przysługiwać szereg gwarancji materialnych i proceduralnych, jakich wymaga dyrektywa 2016/680, a do sądu odsyłającego należy zweryfikowanie, czy przepisy krajowe je przewidują.

2. Przetwarzanie danych osobowych w sprawach karnych

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 [68], 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 [69].

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 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.

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 [70]. Ponadto stwierdził on, po pierwsze, że przetwarzanie to zmierza do osiągnięcia prawnie uzasadnionego celu, oraz,

[68] 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").

[69] 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).

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

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 [71]. Wspomniane przetwarzanie przez organy państwa członkowskiego może okazać się niezbędne właśnie w celu sprawdzenia, czy zasada ta ma zastosowanie.

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 [72].

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.

Wyrok z dnia 21 czerwca 2022 r. (wielka izba), Ligue des droits humains (C-817/19, EU:C:2022:491)

W tej sprawie (zob. również sekcja I.1. zatytułowana "Zgodność prawa wtórnego Unii z prawem do ochrony danych osobowych") po stwierdzeniu ważności dyrektywy PNR Trybunał sformułował dalsze wyjaśnienia co do wykładni tej dyrektywy [73].

Po pierwsze, wskazał on, że dyrektywa wylicza cele przetwarzania danych PNR w sposób wyczerpujący. W związku z tym dyrektywa ta stoi na przeszkodzie uregulowaniu krajowemu, które zezwala na przetwarzanie danych PNR w celach innych niż zwalczanie przestępstw terrorystycznych i poważnej przestępczości. Tym samym uregulowanie krajowe dopuszczające ponadto, jako cel przetwarzania danych PNR, monitorowanie działalności będącej przedmiotem zainteresowania służb wywiadowczych i bezpieczeństwa może naruszać wyczerpujący charakter tego wyliczenia. Podobnie,

[71] Zobacz art. 4 ust. 1 lit. b) i art. 8 ust. 1 dyrektywy 2016/680.
[72] Zobacz art. 1 ust. 1 i art. 8 ust. 1 dyrektywy 2016/680.
[73] W szczególności art. 2 („Stosowanie [dyrektywy] do lotów wewnątrzunijnych"), art. 6 („Przetwarzanie danych PNR") i art. 12 („Okres zatrzymania danych i depersonalizacja") dyrektywy PNR.

system ustanowiony przez dyrektywę PNR nie może być wykorzystywany do celów poprawy kontroli granicznej i zwalczania nielegalnej imigracji. Z powyższego wynika również, że dane PNR nie mogą być zatrzymywane w pojedynczej bazie danych, z której można by korzystać na potrzeby realizacji zarówno celów dyrektywy PNR, jak i innych celów.

Po drugie, Trybunał uściślił pojęcie niezależnego organu krajowego, właściwego do sprawdzenia, czy są spełnione przesłanki ujawnienia danych PNR do celów ich późniejszej oceny, i do zatwierdzenia takiego ujawnienia. W szczególności organ wyznaczony jako JIP nie może zostać uznany za niezależny organ krajowy, ponieważ nie ma statusu podmiotu trzeciego względem organu, który wnosi o udzielenie dostępu do danych. Pracownicy JIP mogą bowiem być oddelegowani z organów właściwych do wnoszenia o taki dostęp, a zatem JIP jawi się w sposób jednoznaczny jako podmiot powiązany z tymi organami. W konsekwencji dyrektywa PNR stoi na przeszkodzie uregulowaniu krajowemu, zgodnie z którym organ wyznaczony jako JIP ma również status właściwego organu krajowego upoważnionego do zatwierdzania ujawniania danych PNR po upływie sześciu miesięcy od przekazania tych danych do JIP.

Po trzecie, co się tyczy okresu zatrzymywania danych PNR, Trybunał orzekł, że art. 12 dyrektywy PNR w związku z art. 7, 8 i art. 52 ust. 1 karty stoi na przeszkodzie uregulowaniu krajowemu, które przewiduje ogólny pięcioletni okres zatrzymywania tych danych, mający zastosowanie bez rozróżnienia do wszystkich pasażerów lotniczych.

Zdaniem Trybunału, po upływie początkowego sześciomiesięcznego okresu przechowywania danych, przechowywanie danych PNR nie jawi się bowiem jako ograniczone do tego, co jest ściśle niezbędne w odniesieniu do tych pasażerów lotniczych, dla których ani wstępna ocena, ani ewentualne kontrole przeprowadzone w początkowym sześciomiesięcznym okresie przechowywania, ani żadne inne okoliczności nie wykazały istnienia obiektywnych elementów – takich jak fakt, że dane PNR odnośnych pasażerów dały wynik pozytywny, zweryfikowany w ramach wstępnej oceny – o takim charakterze, który pozwala stwierdzić ryzyko popełnienia przestępstw terrorystycznych lub udziału w poważnej przestępczości, które mają obiektywny związek, przynajmniej pośredni, z podróżą lotniczą odbytą przez tych pasażerów. Trybunał doszedł natomiast do wniosku, że zatrzymywanie, w pierwotnym okresie sześciu miesięcy, danych PNR wszystkich pasażerów lotniczych objętych systemem ustanowionym przez tę dyrektywę nie wydaje się, co do zasady, wykraczać poza to, co jest ściśle konieczne.

Po czwarte, Trybunał dostarczył wskazówek dotyczących ewentualnego stosowania dyrektywy PNR – do celów walki z przestępstwami terrorystycznymi i poważną przestępczością – do innych środków transportu przewożących pasażerów w obrębie Unii. Dyrektywa ta zaś, interpretowana w świetle art. 3 ust. 2 TUE, art. 67 ust. 2 TFUE i art. 45 karty stoi na przeszkodzie systemowi przekazywania i przetwarzania danych PNR w odniesieniu do ogółu operacji transportu dokonywanych przez inne środki transportu w obrębie Unii przy braku rzeczywistego i aktualnego lub dającego się

przewidzieć zagrożenia terrorystycznego, z którym zmaga się państwo członkowskie. W takiej sytuacji, tak jak w przypadku lotów wewnątrzunijnych, stosowanie systemu ustanowionego przez dyrektywę PNR powinno być ograniczone do danych PNR odnoszących się do przewozów dotyczących, w szczególności, niektórych połączeń lub planów podróży, lub niektórych lotnisk, dworców lub portów morskich, co do których istnieją przesłanki uzasadniające takie stosowanie. Do danego państwa członkowskiego należy wybór środka transportu, w odniesieniu do którego takie przesłanki istnieją, oraz dokonywanie regularnych przeglądów takiego stosowania w zależności od ewolucji warunków, które uzasadniały ich wybór.

IV. Przekazywanie danych osobowych do państw trzecich

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

W tej sprawie (zob. także sekcję 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.

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.

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

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 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 [74] Komisja stwierdziła, iż w ramach systemu zwanego „bezpieczną przystanią" (ang. „safe harbour") [75] 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.

---

[74] 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).

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

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. Trybunał stwierdził, że nieważność art. 1 i 3 decyzji 2000/520 miała wpływ na ważność tej decyzji w całości.

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 gwarancji ma znaczenie tym większe, że dane osobowe przetwarzane są automatycznie i istnieje znaczne ryzyko bezprawnego uzyskania dostępu do nich.

Ponadto i przede wszystkim ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne. 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 przewidzenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu władz 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 absolutnie konieczne. 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 zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 Karty.

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, a w szczególności z postanowieniami dotyczącymi poszanowania życia prywatnego oraz ochrony danych osobowych.

Unia Europejska i Kanada wynegocjowały 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 zatwierdzenie umowy, Parlament postanowił skierować sprawę do Trybunału w celu ustalenia, czy umowa ta 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.

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.)

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. W tej sprawie brak zaś jest 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.

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.

W trzeciej kolejności Trybunał stwierdził, że uznane w art. 7 Karty 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.

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

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 [76]. 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 [77]. Poza tym RODO ustala w szczegółowy sposób warunki, w których przekazywanie danych może mieć miejsce w braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń [78].

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,

[76] Artykuł 45 RODO.
[77] Artykuł 46 ust. 1, art. 46 ust. 2 lit. c) RODO.
[78] Artykuł 49 RODO.

w szczególności ze względu na to, że w decyzji 2000/520 [79] 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") [80].

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 [81]. 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 [82].

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 stwierdził, że analiza decyzji 2010/87 w świetle Karty nie wykazała istnienia żadnego elementu, który mógłby mieć wpływ na jej ważność. Stwierdził on natomiast nieważność decyzji 2016/1250.

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,

---

[79] 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).

[80] Wyrok Trybunału z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650.

[81] 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).

[82] 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).

obronności i bezpieczeństwa państwa przez organy danego państwa trzeciego. Komisja wyjaśniła, że ten rodzaj przetwarzania danych przez organy państwa trzeciego nie może wykluczyć takiego przekazania z zakresu stosowania RODO.

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.

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.

Trybunał zbadał 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. Wyjaśnił on 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 stwierdził, że decyzja 2010/87 wprowadza takie mechanizmy. W tym względzie podkreślił 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.

Wreszcie Trybunał przeprowadził 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 zauważył, 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 zauważył, 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 dodał, że choć regulacje te przewidują wymogi, które władze amerykańskie powinny spełnić przy wdrażaniu danych programów nadzoru, to nie przyznają one zainteresowanym osobom praw, które mogłyby być egzekwowalne wobec władz amerykańskich przed sądami.

Co się tyczy wymogu ochrony sądowej, Trybunał stwierdził, 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 stwierdził nieważność decyzji 2016/1250.

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 sekcje II.1 i II.3, zatytułowane „Zakres zastosowania przepisów ogólnych” i „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.

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. 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. W tym względzie stwierdzenie, iż danej osobie przysługuje prawo, aby dotycząca jej informacja nie była już, w aktualnym stanie rzeczy, 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.

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 umieszczeniu na liście, dostępu do danej informacji

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)

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") [83], 2001/29/WE w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym [84], 2004/48/WE w sprawie egzekwowania praw własności intelektualnej [85] 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. Ponadto przy przyjmowaniu środków mających na celu transpozycję tych dyrektyw, władze 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 pozostawałby w konflikcie z wspomnianymi prawami podstawowymi lub z innymi ogólnymi zasadami prawa wspólnotowego, takimi jak zasada proporcjonalności.

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

[83] 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).

[84] 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).

[85] 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).

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.

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.

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.

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)

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 [86], 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 [87].

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.

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

[86] Artykuł 8, ust. 1 dyrektywy 95/46 i art. 9 ust 1 RODO.
[87] Artykuł 8 ust. 5 dyrektywy 95/46 i art. 10 RODO.

odsyłania do stron internetowych, w rezultacie kontroli przeprowadzanej pod nadzorem właściwych organów krajowych po wniesieniu żądania przez osobę, której dane dotyczą.

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 [88], 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 [89].

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.

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 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

[88] Artykuł 8 ust. 2 lit. e) dyrektywy 95/46 i art. 9 ust. 2 lit. e) RODO.
[89] Artykuł 14 akapit pierwszy lit. a) dyrektywy 95/46 i art. 21 ust. 1 RODO.

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.

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

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 [90].

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 [91] 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

[90] Artykuł 4 ust. 1 lit. a) dyrektywy 95/46 i art. 3 ust. 1 RODO.
[91] Artykuł 12 lit. b) i art. 14 akapit pierwszy lit. a) dyrektywy 95/46; art. 17 ust. 1 RODO.

prawem do ochrony 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.

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.

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.

Wyrok z dnia 8 grudnia 2022 r. (wielka izba), Google (Usunięcie linków do treści, która może okazać się nieprawdziwa) (C-460/20, EU:C:2022:962)

Na stronie internetowej G-LLC opublikowano w 2015 r. trzy artykuły o powodach w postępowaniu głównym: TU, zajmującym stanowiska kierownicze i posiadającym udziały w różnych spółkach, oraz RE, która była partnerką TU i do maja 2015 r. pełniła funkcję prokurenta w jednej z tych spółek. Artykuły te, z których jeden był zilustrowany czterema zdjęciami przedstawiającymi powodów i sugerującymi, że prowadzili oni luksusowe życie, przedstawiały w krytyczny sposób model inwestycyjny szeregu ich spółek. Uzyskanie dostępu do tych artykułów było możliwe po wprowadzeniu do wyszukiwarki Google LLC (zwanej dalej „Google”) imion i nazwisk powodów – zarówno jako takich, jak i w połączeniu z określonymi nazwami spółek. Lista wyników wyszukiwania zawierała link odsyłający do tych artykułów oraz do zdjęć wyświetlanych w formie miniatur („thumbnails”).

Powodowie w postępowaniu głównym zwrócili się do Google jako administratora danych osobowych odpowiedzialnego za ich przetwarzanie przez jej wyszukiwarkę, po pierwsze, o usunięcie z listy wyników wyszukiwania linków do artykułów ze względu na to, że miały one zawierać nieprawdziwe twierdzenia i zniesławiające opinie, i po drugie, o usunięcie z tej listy wyników wyszukiwania miniatur. Google odmówił uwzględnienia takiego żądania.

Ponieważ ich żądania nie zostały uwzględnione w dwóch pierwszych instancjach, powodowie w postępowaniu głównym skierowali do Bundesgerichtshof (federalnego trybunału sprawiedliwości, Niemcy) skargę rewizyjną, w ramach rozpatrywania której Bundesgerichtshof zwrócił się do Trybunału o dokonanie wykładni RODO i dyrektywy 95/46 [92].

W wydanym w składzie wielkiej izby wyroku Trybunał rozwinął orzecznictwo dotyczące wymogów mających zastosowanie do żądań usunięcia linków skierowanych do operatora wyszukiwarki na podstawie przepisów o ochronie danych osobowych. W szczególności zbadał on, po pierwsze, zakres obowiązków i odpowiedzialności spoczywających na operatorze wyszukiwarki przy rozpatrywaniu żądania usunięcia linków opartego na wskazanej nieprawdziwości informacji zawartych w treści, do której odsyłają linki, i po drugie, ciężar dowodu nałożonego na osobę, której dane dotyczą, w odniesieniu do tej nieprawdziwości. Trybunał wydał ponadto rozstrzygnięcie w przedmiocie konieczności uwzględnienia, do celów zbadania żądania usunięcia zdjęć wyświetlanych na liście wyników wyszukiwania grafiki w postaci miniatur, pierwotnego kontekstu publikacji tych zdjęć w Internecie.

W pierwszej kolejności Trybunał rozstrzygnął, że w ramach dokonywania wyważenia między z jednej strony prawami do poszanowania życia prywatnego i ochrony danych osobowych i z drugiej strony prawem do wolności wypowiedzi i informacji [93], którego to wyważenia należy dokonać w celu zbadania skierowanego do operatora wyszukiwarki żądania usunięcia z listy wyników wyszukiwania linku prowadzącego do treści zawierającej informacje wskazane jako nieprawdziwe, to usunięcie linków nie jest uzależnione od tego, czy kwestia prawdziwości treści, do której odesłano, została, przynajmniej tymczasowo, rozstrzygnięta w ramach postępowania sądowego wszczętego przez tę osobę przeciwko dostawcy tej treści.

Na wstępie, aby zbadać, w jakich warunkach operator wyszukiwarki jest zobowiązany do uwzględnienia żądania usunięcia linków, i co za tym idzie, do usunięcia z wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko osoby, której dane dotyczą, linku do strony internetowej zawierającej twierdzenia, które mogą okazać się nieprawdziwe, Trybunał przypomniał w szczególności, co następuje:

---

[92] Odpowiednio art. 17 ust. 3 lit. a) RODO oraz art. 12 lit. b) i art. 14 lit. a) akapit pierwszy dyrektywy 95/46.

[93] Prawa podstawowe zagwarantowane odpowiednio w art. 7, 8 i 11 Karty.

ze względu na to, że działalność wyszukiwarki internetowej może znacząco oddziaływać na prawa podstawowe do poszanowania prywatności i ochrony danych osobowych w sposób dodatkowy w stosunku do działalności prowadzonej przez wydawców stron internetowych, operator tej wyszukiwarki, jako osoba określająca cele i sposoby prowadzenia tej działalności, winien w ramach spoczywającej na nim odpowiedzialności zapewnić – w granicach jego odpowiedzialności, kompetencji i możliwości – aby przewidziane w dyrektywie 95/46 i w RODO gwarancje były w pełni skuteczne i aby można było rzeczywiście zrealizować ich cel polegający na skutecznej i pełnej ochronie objętych nią osób;

gdy do operatora wyszukiwarki internetowej skierowane zostaje żądanie usunięcia linków, musi on sprawdzić, czy umieszczenie na liście wyników wyszukiwania linku do danej strony internetowej jest niezbędne do skorzystania przez internautów – potencjalnie zainteresowanych uzyskaniem dzięki takiemu wyszukiwaniu dostępu do tej strony internetowej – z prawa do wolności informacji, która to wolność jest chroniona na mocy prawa do wolności wypowiedzi i informacji;

w RODO ustanowiony został wyraźnie wymóg dokonania wyważenia między z jednej strony prawami podstawowymi do poszanowania życia prywatnego i do ochrony danych osobowych, a z drugiej strony prawem podstawowym do wolności informacji.

Przede wszystkim Trybunał wskazał, że choć przysługujące osobie, której dane dotyczą, prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych są co do zasady nadrzędne wobec istniejącego po stronie internautów uzasadnionego interesu w uzyskaniu dostępu do danej informacji, to jednak równowaga ta może być uzależniona od szczególnych okoliczności danego przypadku, a w szczególności od charakteru tej 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.

Kwestia prawdziwości treści, do której odsyłają linki (bądź jej braku) również stanowi istotny element, który należy wziąć pod uwagę w ramach tej oceny. Niewątpliwie w pewnych okolicznościach prawo do wolności wypowiedzi i informacji ma pierwszeństwo przed prawem do ochrony życia prywatnego i prawem do ochrony danych osobowych, w szczególności wówczas, gdy osoba, której dane dotyczą, odgrywa znaczącą rolę w życiu publicznym. Niemniej jednak stosunek ten ulega odwróceniu, w przypadku gdy okaże się, że przynajmniej część informacji, których dotyczy żądanie usunięcia linków, niemająca nikłego znaczenia dla całokształtu tej treści, jest nieprawdziwa. W takim przypadku prawo do przekazywania informacji i prawo do otrzymywania informacji nie mogą być brane pod uwagę, ponieważ nie mogą one obejmować prawa do rozpowszechniania takich informacji i dostępu do nich.

Następnie, co się tyczy z jednej strony obowiązków dotyczących ustalenia, czy informacje zawarte w treści, do której odsyłają linki, są prawdziwe, Trybunał wyjaśnił, że to do

osoby, która żąda usunięcia linków z uwagi na nieprawdziwość takich informacji, należy wykazanie oczywistej nieprawdziwości tych informacji lub co najmniej tej części tych informacji, która nie ma nikłego znaczenia dla całokształtu tej treści. Niemniej jednak, aby uniknąć nakładania na tę osobę nadmiernego ciężaru mogącego podważyć skuteczność (effet utile) prawa do usunięcia linków, winna ona przedstawić jedynie takie dowody, jakich zgromadzenia, biorąc pod uwagę okoliczności danego przypadku, można od niej racjonalnie wymagać. Co do zasady osoba ta nie może być co zobowiązana do przedstawienia, na etapie przedsądowym, na poparcie podnoszonego przez nią żądania usunięcia linków wydanego przeciw wydawcy strony internetowej orzeczenia sądowego, nawet jeśli dotyczy ono środków tymczasowych.

Co się tyczy z drugiej strony obowiązków i odpowiedzialności operatora wyszukiwarki, Trybunał podkreślił, że aby sprawdzić, czy po ustosunkowaniu się przezeń do żądania usunięcia linków, dana treść może nadal znajdować się na liście wyników wyszukiwania przeprowadzonego za pomocą jego wyszukiwarki, musi on oprzeć się na wszystkich wchodzących w grę prawach i interesach, jak również na całokształcie okoliczności danego przypadku. Niemniej jednak nie można nałożyć na tego operatora obowiązku zbadania okoliczności faktycznych i przeprowadzenia kontradyktoryjnej debaty z dostawcą treści celem uzyskania w ten sposób brakujących dowodów na prawdziwość treści, do której odsyłają linki. W przypadku nałożenia na tego operatora obowiązku przyczynienia się do ustalenia tego, czy treść, do której odsyłają linki, jest prawdziwa, nałożony na niego ciężar wykraczałby poza to, czego można od niego racjonalnie oczekiwać, biorąc pod uwagę jego odpowiedzialność, kompetencje i możliwości. Przyjęcie takiego rozwiązania wiązałoby się zatem z poważnym ryzykiem, że linki do treści, które zaspokajają uzasadnioną i nadrzędną potrzebę informowania opinii publicznej, zostaną usunięte i w ten sposób odnalezienie ich w Internecie stanie się utrudnione. Gdyby więc taki operator wyszukiwarki dokonywałby usuwania linków niemalże automatycznie po to, aby uniknąć ciężaru związanego z badaniem okoliczności faktycznych w celu ustalenia, czy treść, do której odsyłają linki, jest prawdziwa, prawdopodobne byłoby wystąpienie skutku zniechęcającego do korzystania z wolności wypowiedzi i informacji.

Tak więc w przypadku gdy osoba, która zażądała usunięcia linków, przedstawi dowody świadczące o oczywiście nieprawdziwym charakterze informacji zawartych w treści, do której odsyłają linki, lub co najmniej tej części tych informacji, która nie ma nikłego znaczenia dla całokształtu tej treści, operator wyszukiwarki jest zobowiązany do uwzględnienia tego żądania usunięcia linków. Podobnie rzecz ma się, w przypadku gdy osoba, która zażądała usunięcia linków, przedstawia wydane przeciwko wydawcy strony internetowej orzeczenie sądowe, które opiera się na stwierdzeniu, że zawarte w treści, do której odsyłają linki, informacje niemające nikłego znaczenia dla całokształtu tej treści są, przynajmniej na pierwszy rzut oka, nieprawdziwe. Natomiast jeśli nieprawdziwy charakter takich informacji nie wydaje się oczywisty w świetle dowodów przedstawionych przez osobę żądającą usunięcia linków, operator wyszukiwarki, w braku takiego orzeczenia sądowego, nie jest zobowiązany do uwzględnienia żądania

usunięcia linków. Jeżeli rozpatrywane informacje mogą stanowić wkład w prowadzoną w interesie ogólnym debatę, należy, uwzględniając całokształt okoliczności danego przypadku, przypisać prawu do wolności wypowiedzi i informacji szczególne znaczenie.

Wreszcie Trybunał dodał, że w sytuacji gdy operator wyszukiwarki nie nada dalszego biegu złożonemu doń żądaniu usunięcia linków, osoba, której dane dotyczą, może zwrócić się do organu nadzorczego czy też organu sądowego, aby organ ów przeprowadził konieczną kontrolę i nakazał temu operatorowi przyjęcie odpowiednich środków. W tym względzie to wyważenie sprzecznych ze sobą interesów należy do organów sądowych, ponieważ to one są najbardziej odpowiednie do dokonania złożonego i pogłębionego wyważenia, uwzględniającego wszystkie kryteria i czynniki, jakie zostały ustalone w mającym zastosowanie orzecznictwie.

W drugiej kolejności Trybunał rozstrzygnął, że w ramach dokonywania wyważenia między wyżej wskazanymi prawami podstawowymi, którego to wyważenia należy dokonać w celu przeanalizowania skierowanego do operatora wyszukiwarki żądania usunięcia z listy wyników wyszukiwania grafiki mającego za punkt wyjścia imię i nazwisko osoby fizycznej przedstawiających tę osobę zdjęć wyświetlanych w postaci miniatur, wartość informacyjna tych zdjęć powinna być uwzględniana niezależnie od pierwotnego kontekstu ich publikacji na stronie internetowej, z której pochodzą. Niemniej jednak należy uwzględnić wszelkie treści, które bezpośrednio towarzyszą wyświetlaniu tych zdjęć w wynikach wyszukiwania i które mogą stanowić wyjaśnienie wartości informacyjnej tych zdjęć.

Dochodząc do tego wniosku, Trybunał podkreślił, że przeprowadzone za pomocą wyszukiwarki internetowej wyszukiwanie grafiki mające za punkt wyjścia imię i nazwisko danej osoby podlega zasadom takim samym jak te mające zastosowanie do wyszukiwania stron internetowych i zawartych w nich informacji. Wskazał on, że wyświetlanie, po przeprowadzeniu wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby, przedstawiających tę osobę zdjęć może stanowić szczególnie poważną ingerencję w prawa do poszanowania życia prywatnego i do ochrony danych osobowych tej osoby.

Tak więc w sytuacji gdy do operatora wyszukiwarki skierowano żądanie usunięcia linków zmierzające do usunięcia z listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby przedstawiających tę osobę zdjęć w postaci miniatur, operator ten musi sprawdzić, czy to wyświetlanie zdjęć jest niezbędne do wykonywania przez internautów – potencjalnie zainteresowanych uzyskaniem dzięki takiemu wyszukiwaniu dostępu do tych zdjęć – prawa do wolności informacji.

W zakresie zaś, w jakim wyszukiwarka wyświetla zdjęcia danej osoby poza kontekstem, w jakim są one publikowane na stronie internetowej, do której odsyłają linki, najczęściej w celu zilustrowania treści zawartych w tej stronie, należy ustalić, czy kontekst ten winien jednak zostać uwzględniony przy wyważaniu sprzecznych ze sobą praw i interesów, jakiego należy dokonać. W tych ramach, kwestia tego, czy ta ocena winna obejmować

również treść strony internetowej, na której zamieszczono zdjęcie, którego wyświetlania w postaci miniatury dotyczy żądanie usunięcia, zależy od przedmiotu danego przetwarzania i charakteru tego przetwarzania.

Co się tyczy, po pierwsze, przedmiotu rozpatrywanego przetwarzania, Trybunał zauważył, że publikacja zdjęcia jako środka komunikacji pozawerbalnej może mieć większy wpływ na internautów niż publikacje w postaci tekstowej. Zdjęcia jako takie są bowiem ważnym środkiem służącym do przyciągania uwagi internautów i mogą budzić zainteresowanie dostępem do ilustrowanych przez nie artykułów. W szczególności zaś ze względu na fakt, że zdjęcia często można różnie interpretować, ich wyświetlanie na liście wyników wyszukiwania w postaci miniatur może prowadzić do szczególnie poważnej ingerencji w przysługujące danej osobie prawo do ochrony jej wizerunku, co należy wziąć pod uwagę w ramach wyważenia sprzecznych ze sobą praw i interesów. Należy dokonać odrębnego wyważenia w zależności od tego, czy rozpatrywane są z jednej strony opatrzone zdjęciami artykuły opublikowane przez wydawcę strony internetowej, które to zdjęcia, umieszczone w ich pierwotnym kontekście, ilustrują informacje podane w tych artykułach i wyrażone w nich opinie, i z drugiej strony zdjęcia wyświetlane przez operatora wyszukiwarki w postaci miniatur na liście wyników wyszukiwania poza kontekstem, w którym zostały one opublikowane na stronie internetowej, z której pochodzą.

W tym względzie Trybunał przypomniał, że nie tylko względy uzasadniające publikację danych osobowych na stronie internetowej nie muszą wcale pokrywać się z tymi mającymi zastosowanie do działalności wyszukiwarek internetowych, lecz również, że nawet jeśli sytuacja taka zachodzi, efekt wyważenia wchodzących w grę praw i interesów, jakiego należy dokonać, może być różny w zależności od tego, czy w grę będzie wchodzić przetwarzanie dokonywane przez operatora wyszukiwarki internetowej, czy też to przetwarzanie będzie dokonywane przez wydawcę tej strony internetowej. Z jednej strony zgodne z prawem interesy uzasadniające to przetwarzanie mogą różnić się między sobą, z drugiej zaś strony przetwarzanie to nie zawsze musi mieć w obu przypadkach dla osoby, której dane dotyczą, a zwłaszcza dla jej prywatności, takie same skutki.

Co się tyczy, po drugie, charakteru przetwarzania, jakiego dokonuje operator wyszukiwarki internetowej, Trybunał stwierdził, że znajdując zdjęcia osób fizycznych opublikowane w Internecie i wyświetlając je w wynikach wyszukiwania grafiki w postaci miniatur, niezależnie od treści, które one ilustrują, operator wyszukiwarki oferuje usługę, w ramach której dokonuje przetwarzania danych osobowych w sposób niezależny i odrębny zarówno od przetwarzania danych przez wydawcę strony internetowej, z której pochodzą zdjęcia, jak i od przetwarzania danych w ramach odsyłania do tej strony, za które ten operator jest również odpowiedzialny.

W konsekwencji należy przeprowadzić osobną ocenę prowadzonej przez operatora wyszukiwarki działalności polegającej na wyświetlaniu wyników wyszukiwania grafiki w postaci miniatur, ponieważ wynikające z takiej działalności dodatkowe naruszenie praw

podstawowych może być szczególnie spotęgowane z powodu mającego miejsce podczas wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby łączenia w jedną całość wszystkich dotyczących jej informacji, które znajdują się w Internecie. W ramach tej osobnej oceny należy uwzględnić okoliczność polegającą na tym, że to wyświetlanie stanowi samo w sobie zamierzony przez internautę wynik, niezależnie od tego, jaka będzie jego późniejsza decyzja co do tego, czy przejdzie on na stronę internetową, z której pochodzą treści graficzne, czy też nie.

Trybunał dodał jednak, że takie szczególne wyważenie, w ramach którego uwzględniony zostaje autonomiczny charakter przetwarzania dokonywanego przez operatora wyszukiwarki, pozostaje bez uszczerbku dla ewentualnego znaczenia treści, jakie mogą bezpośrednio towarzyszyć wyświetlaniu danego zdjęcia w wykazie wyników wyszukiwania, ponieważ takie treści mogą stanowić dla opinii publicznej wyjaśnienie wartości informacyjnej tego zdjęcia i tym samym mieć wpływ na wyważenie wchodzących w grę praw i interesów.

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)

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 [94] w związku z dyrektywą 95/46 [95], jak również RODO [96].

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. Zgoda udzielona za pomocą zaznaczonego domyślnie okienka wyboru nie oznacza jednak 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 [97], 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".

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.

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.

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.

---

[94] 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).
[95] Artykuł 2 lit. h) dyrektywy 95/46.
[96] Artykuł 6 ust. 1 lit. a) RODO.
[97] Ibidem.

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.

5. Przetwarzanie danych osobowych w internetowych sieciach społecznościowych

Wyrok z dnia 4 lipca 2023 r. (wielka izba), Meta Platforms i in. (Ogólne warunki korzystania z sieci społecznościowej) (C-252/21, EU:C:2023:537)

Spółka Meta Platforms jest właścicielem internetowej sieci społecznościowej „Facebook", która jest bezpłatna dla użytkowników prywatnych. Model biznesowy tej sieci społecznościowej opiera się na finansowaniu z reklam internetowych, które są dostosowane do indywidualnego użytkownika sieci społecznościowej. Pod względem technicznym tego typu reklama jest możliwa dzięki zautomatyzowanemu tworzeniu bardzo szczegółowych profili użytkowników sieci i usług internetowych oferowanych na poziomie grupy. Tak więc użytkownicy tej sieci społecznościowej, aby móc z niej korzystać, muszą w chwili rejestracji zaakceptować ogólne warunki ustalone przez Meta Platforms, które zawierają odesłanie do określonej przez tę spółkę polityki w zakresie korzystania z danych i plików cookie. Na podstawie tych warunków, oprócz danych, które użytkownicy ci dostarczają bezpośrednio przy swej rejestracji, Meta Platforms zbiera również dane dotyczące działań użytkowników w ramach sieci społecznościowej i poza nią i łączy je z kontami Facebook tych użytkowników. W przypadku tych ostatnich danych, określanych również jako „dane off Facebook", chodzi, po pierwsze, o dane dotyczące przeglądania stron internetowych i aplikacji osób trzecich, i, po drugie, o dane dotyczące korzystania z innych należących do grupy Meta usług internetowych (takich jak Instagram i WhatsApp). Dokonanie całościowego przeglądu zbieranych w ten sposób danych pozwala na wyciągnięcie szczegółowych wniosków na temat preferencji i zainteresowań tych użytkowników.

Decyzją z dnia 6 lutego 2019 r. Bundeskartellamt (federalny organ ochrony konkurencji, Niemcy) zakazał Meta Platforms, po pierwsze, uzależniania w obowiązujących wówczas ogólnych warunkach umownych korzystania z sieci społecznościowej Facebook przez użytkowników prywatnych zamieszkałych w Niemczech od przetwarzania ich danych off Facebook, i, po drugie, przetwarzania tych danych bez ich zgody. Ponadto ten federalny organ ochrony konkurencji nałożył na Meta Platforms obowiązek dostosowania tych ogólnych warunków w taki sposób, aby jasno z nich wynikało, iż dane te nie będą zbierane, łączone z kontami użytkowników Facebooka i wykorzystywane bez zgody użytkowników, których te dane dotyczą. Wreszcie, organ ten podkreślił, że taka zgoda jest nieważna, jeżeli stanowi warunek korzystania z tej sieci społecznościowej. Uzasadnił

on swoją decyzję tym, że przetwarzanie rozpatrywanych danych, które nie byłoby zgodne z RODO, stanowiłoby nadużycie pozycji dominującej zajmowanej przez Meta Platforms na rynku internetowych sieci społecznościowych.

Meta Platforms wniosła na tę decyzję skargę do Oberlandesgericht Düsseldorf (wyższego sądu krajowego w Düsseldorfie, Niemcy). Mając wątpliwości między innymi co do wykładni i stosowania niektórych przepisów RODO, wyższy sąd krajowy w Düsseldorfie zwrócił się do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym.

W swym wydanym w składzie wielkiej izby wyroku Trybunał przedstawił wyjaśnienia w przedmiocie możliwości przetwarzania przez operatora danej sieci społecznościowej „wrażliwych" danych osobowych użytkowników tej sieci, w przedmiocie przesłanek zgodności z prawem przetwarzania danych osobowych przez takiego operatora oraz w przedmiocie ważności zgody udzielonej w celu takiego przetwarzania przez tych użytkowników przedsiębiorstwu zajmującemu pozycję dominującą na krajowym rynku internetowych sieci społecznościowych.

Jeśli chodzi o przetwarzanie szczególnych kategorii danych osobowych [98] Trybunał uznał, że w przypadku, gdy użytkownik internetowej sieci społecznościowej przegląda strony internetowe lub aplikacje powiązane z jedną lub kilkoma z tych kategorii i, w stosownym przypadku, zamieszcza tam dane, rejestrując się na tych stronach czy też w tych aplikacjach lub składając zamówienia online, przetwarzanie danych osobowych przez operatora tej internetowej sieci społecznościowej [99] należy uznać za „przetwarzanie szczególnych kategorii danych osobowych" w rozumieniu art. 9 ust. 1 RODO, jeżeli pozwala ono na ujawnienie informacji należących do jednej z tych szczególnych kategorii, niezależnie od tego, czy informacje te dotyczą użytkownika tej sieci, czy jakiejkolwiek innej osoby fizycznej. Przetwarzanie danych jest co do zasady zakazane, z zastrzeżeniem pewnych odstępstw od tego zakazu [100].

W tym ostatnim względzie Trybunał wyjaśnił, że w sytuacji, gdy użytkownik internetowej sieci społecznościowej przegląda strony internetowe czy też aplikacje powiązane z jedną lub kilkoma ze szczególnych kategorii danych, nie upublicznia on w sposób oczywisty [101]

---

[98] O których mowa w art. 9 ust. 1 RODO. Zgodnie z tym przepisem „[z]abrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby".

[99] Przetwarzanie to polega na zbieraniu, za pomocą zintegrowanych interfejsów, plików cookie lub podobnych technologii rejestracji, danych pochodzących z przeglądania tych stron internetowych lub aplikacji osób, a także danych zamieszczonych przez użytkownika, łączeniu wszystkich tych danych z kontem sieci społecznościowej tego użytkownika i wykorzystywaniu tych danych przez tego operatora.

[100] O których mowa w art. 9 ust. 2 RODO. Przepis ten stanowi: „Ustęp 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1; […]

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

[…]".

[101] W rozumieniu art. 9 ust. 2 RODO.

dotyczących tego przeglądania danych zbieranych przez operatora tej sieci społecznościowej za pomocą plików cookie lub podobnych technologii rejestracji. Ponadto w sytuacji, gdy taki użytkownik zamieszcza dane na takich stronach internetowych lub w takich aplikacjach lub też gdy aktywuje zintegrowane z tymi stronami i aplikacjami przyciski wyboru, takie jak przyciski „lubię to" lub „udostępnij", lub też przyciski umożliwiające użytkownikowi zidentyfikowanie się na tych stronach lub w tych aplikacjach za pomocą identyfikatorów połączenia związanych z jego kontem użytkownika w internetowej sieci społecznościowej, z jego numerem telefonu lub jego adresem elektronicznym, upublicznia on w oczywisty sposób dane zamieszczone w ten sposób lub wynikające z aktywowania tych przycisków jedynie w przypadku, gdy uprzednio wyraźnie wyraził swój wybór – w stosownym przypadku poprzez indywidualne zdefiniowanie z pełną znajomością rzeczy parametrów – publicznego udostępnienia dotyczących go danych nieograniczonej liczbie osób.

W trzeciej kolejności, jeśli chodzi o, bardziej ogólnie rzecz ujmując, warunki, po spełnieniu których dane przetwarzanie danych osobowych jest zgodne z prawem, Trybunał przypomniał, że zgodnie z RODO przetwarzanie danych jest zgodne z prawem jeśli – i w takim zakresie, w jakim – osoba, której dane dotyczą, wyraziła na to zgodę w określonym celu lub określonych celach [102]. W braku takiej zgody lub gdy zgoda ta nie została udzielona w sposób dobrowolny, konkretny, świadomy i jednoznaczny, przetwarzanie takie jest niemniej jednak uzasadnione w sytuacji, gdy spełnia ono jeden z wymogów dotyczących niezbędności [103] , które należy interpretować w sposób ścisły. Dokonywane przez operatora sieci społecznościowej przetwarzanie danych osobowych jej użytkowników można uznać za niezbędne do wykonania umowy, której użytkownicy ci są stronami, jedynie pod warunkiem, że przetwarzanie to jest obiektywnie niezbędne do osiągnięcia celu, który stanowi integralną część świadczenia umownego na rzecz tych samych użytkowników, skutkiem czego główny cel umowy nie mógłby zostać osiągnięty w braku tego przetwarzania.

Ponadto zdaniem Trybunału rozpatrywane przetwarzanie danych może zostać uznane za niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią jedynie pod warunkiem, że operator ten wskazał użytkownikom, od których dane zostały pozyskane, prawnie uzasadniony interes, do którego realizacji służy przetwarzanie tych danych, że przetwarzanie to odbywa się w granicach tego, co jest absolutnie niezbędne do realizacji tego prawnie uzasadnionego interesu, oraz że z wyważenia przeciwstawnych interesów w świetle wszystkich istotnych okoliczności danej sprawy wynika, iż interesy lub podstawowe prawa i wolności tych użytkowników nie mają pierwszeństwa przed tym prawnie

[102] Zgodnie z brzmieniem art. 6 ust. 1 akapit pierwszy lit. a) RODO.

[103] O których mowa w art. 6 ust. 1 akapit pierwszy lit. b)-f) RODO. Zgodnie z tymi przepisami przetwarzanie jest zgodne z prawem tylko wtedy gdy – i w takim zakresie, w jakim – jest ono niezbędne między innymi do wykonania umowy, której stroną jest osoba, której dane dotyczą [art. 6 ust. 1 akapit pierwszy lit. b) RODO], do wypełnienia obowiązku prawnego ciążącego na administratorze [art. 6 ust. 1 akapit pierwszy lit. c) RODO] lub do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią [art. 6 ust. 1 akapit pierwszy lit. f) RODO].

uzasadnionym interesem administratora lub osoby trzeciej. Trybunał uznał zaś w szczególności, że, w braku zgody z ich strony, interesy i prawa podstawowe wspomnianych użytkowników mają pierwszeństwo przed interesem operatora internetowej sieci społecznościowej w zakresie personalizacji reklamy, poprzez którą finansuje on swoją działalność.

Wreszcie, Trybunał wyjaśnił, że rozpatrywane przetwarzanie danych jest uzasadnione w sytuacji, gdy jest rzeczywiście niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych na podstawie przepisu prawa Unii lub prawa danego państwa członkowskiego, a ta podstawa prawna służy realizacji celu leżącego w interesie publicznym i jest proporcjonalna do prawnie uzasadnionego celu, a przetwarzanie to jest dokonywane w granicach tego, co jest absolutnie niezbędne.

Co się tyczy ważności wyrażonej przez użytkowników, których dane dotyczą, zgody na przetwarzanie na podstawie RODO ich danych osobowych, Trybunał uznał, że okoliczność polegająca na tym, iż operator internetowej sieci społecznościowej zajmuje pozycję dominującą na rynku internetowych sieci społecznościowych, nie stoi sama w sobie na przeszkodzie temu, by użytkownicy takiej sieci mogli skutecznie wyrazić zgodę na przetwarzanie ich danych osobowych przez tego operatora. Jednakże zważywszy, że taka pozycja może mieć wpływ na swobodę wyboru tych użytkowników i prowadzić do wyraźnego braku równowagi między nimi a tym operatorem, stanowi ona element istotny dla ustalenia tego, czy zgoda ta została rzeczywiście udzielona skutecznie i – w szczególności – dobrowolnie, czego udowodnienie należy do tego operatora [104].

W szczególności użytkownicy danej sieci społecznościowej powinni mieć swobodę odmówienia indywidualnie, w ramach procesu zmierzającego do zawarcia umowy, wyrażenia zgody na poszczególne operacje przetwarzania danych, które nie są niezbędne do wykonania umowy, przy czym nie są oni jednak zobowiązani do całkowitego zrezygnowania z korzystania z oferowanej internetowej sieci społecznościowej, co oznacza, że użytkownikom tym oferuje się, w stosownym przypadku za odpowiednim wynagrodzeniem, równoważną alternatywę, która nie jest powiązana z takimi operacjami przetwarzania danych. Ponadto musi istnieć możliwość wyrażenia odrębnej zgody na przetwarzanie danych off Facebook.

[104] Zgodnie z art. 7 ust. 1 RODO.

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)

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 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.

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.

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.

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.

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 środków 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.

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

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 państwo członkowskie, które skraca kadencję organu nadzorczego ochrony danych osobowych uchybia zobowiązaniom, jakie na nim ciążą na mocy dyrektywy 95/46.

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.

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

2. Ustalenie prawa właściwego oraz właściwego organu nadzorczego

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

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 przynależności państwowej osób, których dotyczy to przetwarzanie danych, nie ma znaczenia.

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. 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 prawa i o nałożenie sankcji, o ile prawo właściwe na to pozwala, w razie potrzeby w oparciu o przekazane przez niego informacje.

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 sekcję 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 kompetencje dochodzeniowe, takie jak prawo do gromadzenia wszelkich informacji potrzebnych do wykonywania ich funkcji nadzorczych, skuteczne kompetencje interwencyjne, takie jak prawo nakładania czasowego lub ostatecznego zakazu przetwarzania danych oraz prawo pozywania.

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.

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.

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

W tym wyroku (zob. także sekcję 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).

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.

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 [105] czy też piksele monitorujące.

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 [106] 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.

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 [107], nawet jeśli nie jest on w odniesieniu do tego przetwarzania wiodącym organem nadzorczym.

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

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

[106] Zgodnie z 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".

[107] W rozumieniu art. 4 pkt 23 RODO.

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 [108] procedur współpracy i kontroli spójności.

W odniesieniu do operacji przetwarzania transgranicznego RODO przewiduje bowiem mechanizm kompleksowej współpracy [109], 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 [110], podczas gdy przysługująca innym organom nadzorczym, których sprawa dotyczy, kompetencja do wydania takiej decyzji, choćby tylko czasowej, stanowi wyjątek od tej zasady [111]. 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.

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 [112] jest zgodna z art. 7, 8 i 47 karty, gwarantującej danej osobie, odpowiednio, prawo do ochrony danych osobowych i prawo do skutecznego środka prawnego.

W drugiej kolejności Trybunał orzekł, iż w przypadku transgranicznego przetwarzania danych wykonywanie przysługujących organowi nadzorczemu państwa członkowskiego

[108] Przewidzianych art. 56 i 60 RODO.
[109] Artykuł 56 ust. 1 RGPD
[110] Artykuł 60 ust. 7 RGPD
[111] Wyjątki od zasady kompetencji decyzyjnych wiodącego organu nadzorczego zostały ustanowione w art. 56 ust. 2 i art. 66 RODO.
[112] Przewidzianych w art. 55 i 56 w związku z art. 60 RODO.

innemu niż organ wiodący uprawnień do wszczęcia postępowania przed sądem [113] 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 [114], co wiąże się z przyjęciem założenia, że administrator danych lub podmiot dokonujący ich transgranicznego przetwarzania muszą posiadać jednostkę organizacyjną na terytorium 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, odpowiedzialna jest Facebook Ireland, przetwarzanie to jest dokonywane „w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora", a zatem wchodzi w zakres zastosowania RODO.

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

[113] Zgodnie z art. 58 ust. 5 RODO.

[114] 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".

ustanowione w tym rozporządzeniu, i dzieje się to przy poszanowaniu ustanowionych w tym rozporządzeniu procedur współpracy i kontroli spójności.

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.

Wyrok z dnia 16 stycznia 2024 r. (wielka izba), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

W tej sprawie (zobacz również sekcję II.1, zatytułowaną „Wyłączenia poszczególnych przypadków przetwarzania danych osobowych z zakresu stosowania przepisów ogólnych”) Trybunał zauważył, że przepisy RODO dotyczące właściwości krajowych organów nadzorczych i prawa do wniesienia skargi do nich [115] nie wymagają przyjęcia krajowych środków wykonawczych oraz są wystarczająco jasne, precyzyjne i bezwarunkowe, aby mogły być bezpośrednio skuteczne. Wynika z tego, że chociaż RODO przyznało państwom członkowskim uprawnienia dyskrecjonalne co do liczby organów nadzorczych, które chcą one ustanowić [116], to określiło ono zakres ich kompetencji do nadzorowania stosowania tego rozporządzenia. W przypadku gdy państwo członkowskie zdecyduje się na ustanowienie jednego krajowego organu nadzorczego, organ ten musi posiadać całość kompetencji przewidzianych w RODO. Odmienna wykładnia pozbawiłaby bezpośredniej skuteczności przepisy RODO i mogłaby osłabić skuteczność (effet utile) wszystkich pozostałych przepisów tego rozporządzenia, na których może opierać się skarga.

Co się tyczy okoliczności, że możliwość kontrolowania przez organ nadzorczy, który podlega władzy wykonawczej, stosowania RODO przez organ podlegający władzy ustawodawczej została wyłączona przez krajowe przepisy rangi konstytucyjnej, Trybunał podkreślił, że RODO zobowiązuje państwa członkowskie do ustanowienia co najmniej jednego organu nadzorczego, dając im jednocześnie możliwość ustanowienia kilku takich organów, właśnie z myślą o poszanowaniu ich struktury konstytucyjnej. Omawiane rozporządzenie przyznaje zatem każdemu państwu członkowskiemu uprawnienia dyskrecjonalne pozwalające mu na ustanowienie takiej liczby organów nadzorczych, jaką narzucają mu w szczególności wymogi związane ze strukturą konstytucyjną tego państwa.

[115] Artykuł 55 ust. 1 i art. 77 ust. 1 RODO.
[116] Zgodnie z art. 51 ust. 1 RODO.

Należy ponadto przypomnieć, że powołanie się przez państwo członkowskie na przepisy prawa krajowego nie może naruszać jedności i skuteczności prawa Unii. Skutki wynikające z zasady pierwszeństwa prawa Unii wiążą bowiem wszystkie organy państwa członkowskiego, czemu nie mogą stanąć na przeszkodzie w szczególności przepisy wewnętrzne, w tym również przepisy rangi konstytucyjnej

W związku z tym, jeżeli państwo członkowskie zdecydowało się na ustanowienie jednego organu nadzorczego, nie może ono powoływać się na przepisy prawa krajowego, nawet rangi konstytucyjnej, w celu wyłączenia przetwarzania danych osobowych objętego zakresem stosowania RODO spod nadzoru tego organu.

4. Warunki nakładania administracyjnych kar pieniężnych

Wyrok z dnia 5 grudnia 2023 r. (wielka izba), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

W tej sprawie (zobacz również sekcje I.3, I.5 i I.6, zatytułowane "Pojęcie »przetwarzania danych osobowych«, »Pojęcie "administratora danych osobowych« i »Pojęcie "współadministratora danych osobowych«), Trybunał zauważył, że zgodnie z art. 83 RODO administracyjną karę pieniężną można nałożyć na administratora wyłącznie wtedy, gdy zostanie wykazane, że dopuścił się on, umyślnie lub nieumyślnie, naruszenia przepisów zawartych w tym rozporządzeniu [117].

W tym względzie uściślił on, że prawodawca Unii nie pozostawił państwom członkowskim zakresu uznania w odniesieniu do przesłanek materialnych, które organ nadzorczy powinien spełnić, gdy postanawia nałożyć administracyjną karę pieniężną na administratora danych na mocy tego przepisu. Okoliczność, że RODO daje państwom członkowskim możliwość ustanowienia wyjątków w stosunku do organów publicznych i podmiotów publicznych mających siedzibę na ich terytorium [118], a także wymogów dotyczących procedury stosowanej przez organy nadzorcze w celu nałożenia administracyjnej kary pieniężnej [119] w żaden sposób nie oznacza, że państwa te są również uprawnione do ustanowienia tych materialnych przesłanek.

W odniesieniu do tych przesłanek Trybunał zauważył, że wśród wymienionych w RODO elementów, w świetle których organ nadzorczy nakłada na administratora administracyjną karę pieniężną, figuruje „umyślny lub nieumyślny charakter naruszenia" [120]. Natomiast żaden z elementów nie wskazuje na jakąkolwiek możliwość pociągnięcia

[117] Naruszenie, o którym mowa w art. 83 ust. 4–6.
[118] Zgodnie z art. 83 ust. 7 RODO, który przewiduje, że „[...] każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim".
[119] Zgodnie z art. 83 ust. 8 RODO w związku z jego motywem 129.
[120] Artykuł 83 ust. 2 lit. b) RODO.

do odpowiedzialności administratora w braku jego zawinionego zachowania. Tak więc jedynie naruszenia przepisów RODO popełnione umyślnie lub nieumyślnie mogą prowadzić do nałożenia na niego administracyjnej kary pieniężnej na podstawie art. 83 tego rozporządzenia.

Trybunał dodał, że wykładnia ta znajduje potwierdzenie w ogólnej systematyce i celu RODO. W tym kontekście wyjaśnił on, że istnienie systemu kar na podstawie RODO pozwalającego na nakładanie, o ile uzasadniają to szczególne okoliczności danej sprawy, administracyjnej kary pieniężnej, stanowi zachętę dla administratorów i podmiotów przetwarzających do przestrzegania tego rozporządzenia oraz że ze względu na swój odstraszający skutek administracyjne kary pieniężne przyczyniają się do wzmocnienia ochrony osób, których dane dotyczą. Jednakże prawodawca Unii nie uznał za konieczne aby przewidzieć nakładanie administracyjnych kar pieniężnych w przypadku braku winy. Biorąc pod uwagę fakt, że RODO ma na celu równoważny i jednolity poziom ochrony oraz że w tym celu należy je stosować w sposób spójny w całej Unii, umożliwienie państwom członkowskim ustanowienia takiego systemu nakładania kary pieniężnej byłoby sprzeczne z tym celem.

Ponadto Trybunał uznał, że taka kara pieniężna może zostać nałożona na administratora danych w związku z operacjami przetwarzania danych osobowych dokonywanymi przez podmiot przetwarzający w jego imieniu, z wyjątkiem sytuacji, gdy w ramach tych operacji podmiot przetwarzający dokonywał przetwarzania danych do swoich własnych celów lub przetwarzał te dane w sposób niezgodny z ramami lub sposobami przetwarzania określonymi przez administratora lub w taki sposób, że nie można racjonalnie uznać, że administrator ten wyraził na to zgodę. W takim przypadku podmiot przetwarzający należy uznać za administratora w odniesieniu do takiego przetwarzania.

Wyrok z dnia 5 grudnia 2023 r. (wielka izba), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (zwana dalej „DW") jest spółką nieruchomościową, która posiada pośrednio, poprzez udziały w różnych spółkach, liczne lokale użytkowe i mieszkalne. W ramach swojej działalności gospodarczej przetwarza ona dane osobowe najemców tych lokali.

W następstwie dwóch kontroli przeprowadzonych w 2017 r. i 2019 r. Berliner Beauftragte für den Datenschutz (organ nadzorczy w Berlinie, Niemcy) stwierdził szereg naruszeń RODO popełnionych przez DW. Decyzją z dnia 30 października 2019 r. ten organ nadzorczy nałożył na nią z tego tytułu administracyjne kary pieniężne.

DW wniosła skargę na tę decyzję do Landgericht Berlin (sądu krajowego w Berlinie, Niemcy), który umorzył postępowanie. Sąd ten wskazał, że zgodnie z prawem

niemieckim [121], wykroczenie administracyjne może zostać stwierdzone wyłącznie przeciwko osobie fizycznej, a nie przeciwko osobie prawnej. Ponadto w przypadku powstania odpowiedzialności osoby prawnej można jej przypisać jedynie działania członków jej organów lub jej przedstawicieli. Staatsanwaltschaft Berlin (prokuratura w Berlinie, Niemcy) wniosła skargę na tę decyzję do Kammergericht Berlin (wyższego sądu krajowego w Berlinie, Niemcy). W tym kontekście sąd ten zwrócił się do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w przedmiocie wykładni RODO.

W swoim wyroku Trybunał, orzekający w składzie wielkiej izby, wypowiedział się w przedmiocie przesłanek nałożenia administracyjnych kar pieniężnych na podstawie RODO. W pierwszej kolejności zbadał on kwestię, czy państwa członkowskie mogą uzależnić nałożenie administracyjnej kary pieniężnej na osobę prawną od uprzedniego przypisania naruszenia tego rozporządzenia zidentyfikowanej osobie fizycznej. W drugiej kolejności, podobnie jak w wyroku w sprawie Nacionalinis visuomenės sveikatos centras (patrz powyżej) sąd ten rozważył kwestię, czy podlegające sankcji naruszenie przepisów RODO musi zostać popełnione umyślnie lub nieumyślnie.

Co się tyczy nakładania administracyjnej kary pieniężnej na podstawie RODO na osobę prawną, Trybunał zauważył przede wszystkim, że zasady, zakazy i obowiązki przewidziane w RODO są skierowane w szczególności do „administratorów", których odpowiedzialność obejmuje wszelkie przetwarzanie danych osobowych przez nich samych lub w ich imieniu. To właśnie ta odpowiedzialność stanowi, w przypadku naruszeń przepisów RODO, podstawę nałożenia administracyjnej kary pieniężnej na administratora na podstawie art. 83 tego rozporządzenia. Jednakże prawodawca Unii nie dokonał w celu ustalenia takiej odpowiedzialności, rozróżnienia między osobami fizycznymi a osobami prawnymi, uzależniając tę odpowiedzialność wyłącznie od warunku, że osoby te, samodzielnie lub wspólnie z innymi osobami, określają cele i sposoby przetwarzania danych osobowych [122]. W związku z tym co do zasady każda osoba spełniająca ten warunek ponosi odpowiedzialność w szczególności za wszelkie naruszenia RODO popełnione przez nią lub w jej imieniu. Oznacza to, po pierwsze, że osoby prawne ponoszą odpowiedzialność nie tylko za naruszenia popełnione przez ich przedstawicieli, dyrektorów lub osoby zarządzające, lecz również przez każdą inną osobę działającą w ramach działalności gospodarczej tych osób prawnych i w ich imieniu. Po drugie, administracyjne kary pieniężne przewidziane w RODO w przypadku takich naruszeń powinny móc być nakładane bezpośrednio na osoby prawne, jeżeli można je uznać za administratorów.

Następnie Trybunał zauważył, że żaden przepis RODO nie pozwala uznać, że nałożenie administracyjnej kary pieniężnej na osobę prawną działającą w charakterze

[121] Gesetz über Ordnungswidrigkeiten (ustawa o wykroczeniach administracyjnych) z dnia 24 maja 1968 r. (BGBl. 1968 I, s. 481), w wersji komunikatu z dnia 19 lutego 1987 r. (BGBl. 1987 I, s. 602), zmieniona ustawą z dnia 19 czerwca 2020 r. (BGBl. 2020 I, s. 1350).

[122] Zgodnie z art. 4 pkt 7 RODO.

administratora jest uzależnione od uprzedniego stwierdzenia, że naruszenie to zostało popełnione przez zidentyfikowaną osobę fizyczną. Ponadto prawodawca Unii nie pozostawił państwom członkowskim zakresu uznania w tym względzie. Okoliczność, że RODO daje im możliwość ustanowienia wymogów dotyczących procedury, jaką powinny stosować organy nadzorcze w celu nałożenia administracyjnej kary pieniężnej [123], w żaden sposób nie oznacza, że są one również uprawnione do ustanowienia przesłanek materialnych dodatkowych w stosunku do tych określonych w RODO.

W tym kontekście Trybunał wyjaśnił, że zezwolenie państwom członkowskim na jednostronne nałożenie wymogu, będącego konieczną przesłanką nałożenia administracyjnej kary pieniężnej na podstawie art. 83 RODO na administratora będącego osobą prawną, aby dane naruszenie zostało uprzednio przypisane lub mogło zostać przypisane zidentyfikowanej osobie fizycznej, byłoby sprzeczne z celem RODO. Ponadto taki dodatkowy wymóg mógłby ostatecznie osłabić skuteczność i odstraszający skutek administracyjnych kar pieniężnych nakładanych na osoby prawne jako administratorów.

Wreszcie Trybunał podkreślił, że pojęcie „przedsiębiorstwa" w rozumieniu art. 101 i 102 TFUE [124] nie ma wpływu na to, czy i na jakich warunkach administracyjna kara pieniężna może zostać nałożona na podstawie RODO na administratora będącego osobą prawną i ma znaczenie wyłącznie dla ustalenia kwoty takiej kary pieniężnej.

Trybunał stwierdził zatem, że RODO [125] stoi na przeszkodzie uregulowaniu krajowemu, na mocy którego administracyjna kara pieniężna może zostać nałożona na osobę prawną działającą w charakterze administratora za naruszenie przepisów tego rozporządzenia [126], tylko wtedy, gdy naruszenie to zostało uprzednio przypisane zidentyfikowanej osobie fizycznej.

W odniesieniu do kwestii, czy państwa członkowskie mogą przewidzieć nałożenie administracyjnej kary pieniężnej, nawet jeżeli sankcjonowane naruszenie nie zostało popełnione umyślnie lub nieumyślnie, Trybunał przypomniał przede wszystkim, że przesłanki materialne, których organ nadzorczy musi przestrzegać przy nakładaniu administracyjnej kary pieniężnej na administratora, są regulowane wyłącznie prawem Unii i że państwa członkowskie nie dysponują w tym względzie żadnym marginesem swobody. Przyjmując rozumowanie identyczne z rozumowaniem przyjętym w ww. wyroku Nacionalinis visuomenės sveikatos centras Trybunał stwierdził, że zgodnie z art. 83 RODO administracyjna kara pieniężna może zostać nałożona tylko wtedy, gdy zostanie wykazane, że administrator, będący jednocześnie osobą prawną i przedsiębiorstwem, dopuścił się, umyślnie lub nieumyślnie, naruszenia przepisów zawartych w tym rozporządzeniu.

[123] Jak wynika z art. 58 ust. 4 i art. 83 ust. 8 RODO w świetle motywu 129 RODO.
[124] Do którego odsyła motyw 150 RODO.
[125] Artykuł 58 ust. 2 lit. i) i art. 83 ust. 1-6 RODO.
[126] Wskazanych w art. 83 ust. 4-6 RODO.

5. Związek między uprawnieniami krajowych organów nadzorczych a uprawnieniami innych organów krajowych

Wyrok z dnia 4 lipca 2023 r. (wielka izba), Meta Platforms i in. (Ogólne warunki korzystania z sieci społecznościowej) (C-252/21, EU:C:2023:537)

W tej sprawie (zobacz również sekcję V.5, zatytułowaną „Przetwarzanie danych osobowych w internetowych sieciach społecznościowych"), co się tyczy kompetencji organu ochrony konkurencji do stwierdzenia niezgodności przetwarzania danych osobowych z RODO, Trybunał uznał, że, z zastrzeżeniem poszanowania ciążącego na nim obowiązku lojalnej współpracy [127] z organami nadzorczymi ds. ochrony danych, organ ten może, w ramach badania nadużycia pozycji dominującej przez dane przedsiębiorstwo [128], stwierdzić, iż ogólne warunki korzystania określone przez to przedsiębiorstwo w dziedzinie przetwarzania danych osobowych i wdrażanie tych warunków nie są zgodne z tym rozporządzeniem, jeżeli stwierdzenie to jest konieczne do wykazania istnienia takiego nadużycia. Niemniej jednak w przypadku, gdy dany organ ochrony konkurencji w ramach stwierdzenia przezeń nadużycia pozycji dominującej podnosi, że doszło do naruszenia przepisów RODO, nie wchodzi on w rolę organów nadzorczych.

Tak więc, biorąc pod uwagę zasadę lojalnej współpracy, w sytuacji gdy organy ochrony konkurencji w ramach wykonywania swoich uprawnień mają zbadać zgodność zachowania danego przedsiębiorstwa z przepisami RODO, powinny one konsultować się i lojalnie współpracować z krajowymi organami nadzorczymi, których sprawa dotyczy, lub z wiodącym organem nadzorczym. Wszystkie te organy łącznie są zatem zobowiązane do poszanowania przysługujących im odpowiednio uprawnień i kompetencji w taki sposób, aby wynikające z RODO obowiązki oraz cele tego rozporządzenia były respektowane, przy jednoczesnym zachowaniu ich skuteczności (effet utile). Wynika z tego, że w przypadku, gdy w ramach badania mającego na celu stwierdzenie nadużycia przez przedsiębiorstwo pozycji dominującej organ ochrony konkurencji uzna, iż konieczne jest zbadanie zgodności zachowania tego przedsiębiorstwa z przepisami RODO, organ ten powinien sprawdzić, czy to zachowanie lub zachowanie do niego podobne było już przedmiotem rozstrzygnięcia wydanego przez właściwy krajowy organ nadzorczy lub przez wiodący organ nadzorczy bądź też przez Trybunał. W takim przypadku organ ochrony konkurencji nie może odejść od tej zasady, zachowując jednak swobodę w wyciąganiu z tej sytuacji swoich własnych wniosków z perspektywy zastosowania prawa konkurencji.

---

[127] O którym mowa w art. 4 ust. 3 TUE.
[128] W rozumieniu art. 102 TFUE.

Gdy ten organ ochrony konkurencji ma wątpliwości co do zakresu oceny dokonanej przez właściwy krajowy organ nadzorczy lub wiodący organ nadzorczy, gdy dane zachowanie lub zachowanie do niego podobne jest jednocześnie przedmiotem badania ze strony tych organów lub gdy, w braku przeprowadzenia przez te organy dochodzenia, uznaje on, że zachowanie przedsiębiorstwa nie jest zgodne z przepisami RODO, organ ten powinien skonsultować się z tymi organami i zwrócić się do nich o współpracę mającą na celu rozwianie wątpliwości lub ustalenie, czy przed dokonaniem swej własnej oceny winien on zaczekać na wydanie decyzji przez organ nadzorczy, którego sprawa dotyczy. W braku zgłoszenia przez te organy zastrzeżeń lub też w braku ustosunkowania się do takiego wniosku w rozsądnym terminie organ ochrony konkurencji może kontynuować prowadzone dochodzenie.

TRYBUNAŁ SPRAWIEDLIWOŚCI
UNII EUROPEJSKIEJ

Dyrekcja Badań i Dokumentacji

Lipiec 2024 r.