ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3744
PRZEGLĄD PRAWA I ADMINISTRACJI CVII
WROCŁAW 2016
DOI: 10.19195/0137-1134.107.10

SYLWIA MAJKOWSKA-SZULC
Uniwersytet Gdański

TARCZA PRYWATNOŚCI UE–USA PO KOLIZJI W „BEZPIECZNEJ PRZYSTANI". ZAKRES OCHRONY PRYWATNOŚCI PO WYROKU W SPRAWIE C-362/14 SCHREMS

Kolizja w „bezpiecznej przystani" doprowadziła do ustanowienia „Tarczy Prywatności UE–USA". Tak w skrócie można przedstawić skutki wyroku Trybunału Sprawiedliwości z 6 października 2015 roku w sprawie C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner[1]. Tytułowa kolizja, mimo marynistycznych skojarzeń, dotyczy niezgodności prawa i praktyk Stanów Zjednoczonych z prawem Unii Europejskiej w dziedzinie ochrony danych osobowych w sytuacji, w której dane obywateli Unii są przekazywane do Stanów Zjednoczonych. Instytucje Unii działają na rzecz ułatwiania przepływu danych, stawiając jednak warunek zapewnienia wysokiego poziomu ochrony danych osobowych. W związku z tym Komisja przyjęła w 2000 r. decyzję 2000/520 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[2]. Decyzja ta dotyczyła adekwatności ochrony zapewnianej w Stanach Zjednoczonych w celu spełnienia wymagań art. 25 ust. 1 dyrektywy 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[3].

[1] Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner, ECLI:EU:C:2015:650.

[2] Decyzja Komisji z dnia 26 lipca 2000 r. nr 2000/520/WE 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 (notyfikowana jako dokument nr C(2000) 2441). Tekst mający znaczenie dla EOG (Dz.U. L 215 z dnia 25 sierpnia 2000 r.), s. 7–47.

[3] Art. 2 decyzji Komisji z dnia 26 lipca 2000 r. nr 2000/520/WE przyjętej 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.

Uznanie Stanów Zjednoczonych za państwo trzecie, które nie zapewnia odpowiedniego stopnia ochrony danych osobowych, spowodowało, że Trybunał Sprawiedliwości w wyroku w sprawie C-362/14 Schrems stwierdził nieważność wspomnianej decyzji 2000/520. W konsekwencji, wspólny amerykańsko-europejski program „bezpiecznej przystani" zakończył się fiaskiem[4]. Od tej pory transfery danych osobowych, na przykład z Polski do USA, nie mogły odbywać się na podstawie systemu „bezpiecznej przystani", lecz nadal były możliwe po spełnieniu jednej z przesłanek określonych w art. 47 albo art. 48 ustawy o ochronie danych osobowych[5], w szczególności nadal możliwe było stosowanie w odniesieniu do takich transferów standardowych klauzul umownych oraz zatwierdzonych przez Generalnego Inspektora wiążących reguł korporacyjnych[6].

Tymczasem przekazywanie danych stanowi integralną część wymiany handlowej. Jak wynika z samej decyzji 2000/520, zasady ochrony prywatności w ramach „bezpiecznej przystani" zostały opracowane w konsultacji z kręgami przemysłowymi i publicznością w celu ułatwienia handlu między Stanami Zjednoczonymi a Unią Europejską[7]. Wyrok w sprawie C-362/14 Schrems ma więc doniosłe znaczenie w kontekście rozbudowanych stosunków transatlantyckich. Unia Europejska i USA są dla siebie nawzajem najważniejszymi partnerami handlowymi[8]. Problem związany ze stwierdzeniem nieważności decyzji 2000/520 dotknął nie tylko Facebook Inc., lecz ponad cztery tysiące przedsiębiorców przesyłających dane obywateli Unii do Stanów Zjednoczonych, dlatego wyrok wywołał ożywioną reakcję mediów i zainteresowanych podmiotów[9].

---

[4] F. Moos, J. Schefzig, *„Safe Harbor" hat Schiffbruch erlitten. Auswirkungen des EuGH-Urteils C-362/14 in Sachen Schrems ./. Data Protection Commissioner*, Computer Und Recht: Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation, 31, 2015, nr 10, s. 625–633.

[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133, poz. 833 ze zm.) Ustawa wdraża dyrektywę 95/46. Art. 47 ustawy określa warunki przekazania danych osobowych do państwa trzeciego, a art. 48 ustawy reguluje przypadki, w których wymagana jest zgoda Generalnego Inspektora Ochrony Danych Osobowych na przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych.

[6] W celach informacyjnych na stronach polskiego Generalnego Inspektora Danych Osobowych opublikowano komunikat pt. *Stanowisko GIODO w sprawie przekazywania danych osobowych do USA*, http://giodo.gov.pl/560/id_art/9054/j/pl (dostęp: 20.09.2016).

[7] Załącznik I akapit 2 decyzji Komisji z dnia 26 lipca 2000 r. nr 2000/520/WE…

[8] Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 6 listopada 2015 w sprawie przekazywania danych osobowych z UE do Stanów Zjednoczonych na mocy dyrektywy 95/46/WE w następstwie wyroku Trybunału Sprawiedliwości w sprawie C-362/14 (Schrems), COM/2015/0566 final, s. 1.

[9] Na przykład: J. Titcomb, *Facebook can be blocked from passing data to US after treaty ruled invalid*, „The Telegraph", 6 Oct 2015; K. Szymielewicz, *Koniec „Bezpiecznej Przystani" — początek nowej polityki na linii UE–USA?*, Fundacja Panoptykon, 6 października 2016, www.panoptykon.org.

Ponadto wyrok w sprawie Schrems nie pozostaje bez znaczenia dla toczących się między Unią Europejską a USA negocjacji dotyczących transatlantyckiego partnerstwa w dziedzinie handlu i inwestycji (ang. *Transatlantic Trade and Investment Partnership — TTIP*). Wśród korzyści, jakie mają wynikać z zawarcia TTIP, instytucje Unii wymieniają: otwarcie amerykańskiego rynku dla europejskich przedsiębiorstw, ograniczenie formalności administracyjnych, jakich muszą dopełniać eksporterzy, czy też ustanowienie nowych przepisów, które ułatwią eksport, import oraz inwestowanie za granicą na uczciwych warunkach. Tymczasem Komisja bezdyskusyjnie musi uwzględniać wnioski wypływające z wyroku w sprawie Schrems, co z pewnością nie ułatwia negocjacji na temat otwarcia amerykańskiego rynku dla przedsiębiorstw z Europy[10].

Jak najszybsze osiągnięcie nowego porozumienia było więc kluczowe między innymi z punktu widzenia stosunków gospodarczych. Po intensywnych miesiącach pracy instytucji unijnych i ich partnerów amerykańskich 12 lipca 2016 roku wydana została decyzja wykonawcza Komisji 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA[11]. Nowe ramy prawne mają zapewnić ochronę praw podstawowych obywatelom Unii, których dane osobowe są przekazywane do Stanów Zjednoczonych oraz gwarantować przejrzystość prawa przedsiębiorcom dokonującym transatlantyckich transferów danych[12].

Tytułowa sprawa rozpoczęła się w Austrii. Maximillian Schrems, zamieszkały w Austrii obywatel austriacki, wówczas student prawa[13], był użytkownikiem sieci społecznościowej Facebook od 2008 roku. Z kolei użytkownikiem Facebooka można było stać się wyłącznie po zawarciu umowy ze spółką Facebook Ireland, co następowało w chwili rejestracji użytkownika. Trybunał Sprawiedliwości nie poddał sprawy analizie w aspekcie zasady swobody umów, choć w doktrynie zwraca się niekiedy uwagę na trudności związane z oceną klauzul umownych w konfrontacji z zasadą swobody umów[14]. Facebook Ireland jest spółką zależną spółki dominującej Facebook Inc. z siedzibą w Stanach Zjednoczonych. Serwery spółki Facebook Inc. były zlokalizowane na terytorium Stanów Zjednoczonych i to tam były przekazywane w całości lub w części, a następnie przetwarzane, dane

[10] G. Greenleaf, *International data privacy agreements after the GDPR and Schrems*, „Privacy Laws & Business International Report” 12–15, 139, 30 January 2016, s. 6.

[11] Decyzja wykonawcza Komisji (UE) 2016/1250 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 (notyfikowana jako dokument nr C(2016) 4176) (Tekst mający znaczenie dla EOG), C/2016/4176, Dz.U. L 207 z 1.8.2016, s. 1–112.

[12] Komisja Europejska — Komunikat prasowy, Komisja Europejska uruchamia Tarczę Prywatności UE–USA: lepsza ochrona transatlantyckiego przepływu danych, Bruksela, 12 lipca 2016 r., s. 1.

[13] Informacja podawana przez media światowe. Na przykład: J. Titcomb, *op. cit*.

[14] *L'extraterritorialité du droit entre souveraineté et mondialisation des droits*, red. N. Maziau, La Semaine Juridique Entreprise et Affaires n° 28, 9 Juillet 2015, 1343, pkt 5.

osobowe użytkowników Facebooka zamieszkałych na terytorium Unii Europejskiej, w tym M. Schremsa[15].

W 2013 roku M. Schrems skierował skargę do Data Protection Commissioner (komisarz ds. ochrony danych), żądając, by organ ten zakazał spółce Facebook Ireland przekazywania jego danych osobowych do Stanów Zjednoczonych. Skargę swą uzasadniał tym, że prawo i praktyka obowiązujące w USA nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na tym terytorium przed działaniami nadzorczymi prowadzonymi przez władze publiczne. M. Schrems działał pod wpływem informacji ujawnionych przez Edwarda Snowdena na temat działalności amerykańskich służb wywiadowczych, w szczególności National Security Agency[16]. Komisarz ds. ochrony danych odmówił rozpatrzenia skargi, ponieważ uznał, że nie miał obowiązku przeprowadzenia dochodzenia w przedmiocie okoliczności faktycznych wskazanych przez M. Schremsa. W efekcie komisarz ds. ochrony danych odrzucił skargę jako bezpodstawną. Jednym z powodów była decyzja 2000/520, w której Komisja Europejska stwierdziła, że Stany Zjednoczone zapewniały odpowiedni stopień ochrony[17].

M. Schrems wniósł następnie skargę do High Court (sądu najwyższego), który wprawdzie stwierdził, że nadzór elektroniczny i przechwytywanie danych osobowych przekazywanych z Unii do Stanów Zjednoczonych służyło realizacji koniecznych i niezbędnych celów interesu publicznego, lecz jednocześnie przyznał, że informacje ujawnione przez E. Snowdena wskazały na „istotne przekroczenie granic kompetencji" przez służby National Security Agency i innych organów federalnych[18]. W tej sytuacji High Court postanowił skierować do Trybunału Sprawiedliwości pytania prejudycjalne zmierzające do wyjaśnienia, jakie stanowisko mają zająć krajowe organy nadzorcze i Komisja wobec nieprawidłowości w stosowaniu decyzji 2000/520, przy czym kluczowe w sprawie okazały się nowe okoliczności faktycznie zaistniałe po dacie publikacji decyzji Komisji. Ponadto pytania High Court zmierzały do określenia znaczenia decyzji 2000/520 w świetle art. 7, 8 i 47 Karty Praw Podstawowych Unii Europejskiej, ponieważ w ocenie tego sądu sprawa dotyczyła stosowania prawa Unii w rozumieniu art. 51 Karty[19]. Austriacki sąd najwyższy nie spytał wprost o kwestię ważności unijnego aktu prawa wtór-

[15] Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14…, pkt 26–27.

[16] Tego samego dnia, w którym Trybunał Sprawiedliwości wydał wyrok w sprawie C-362/14 Schrems, sam Edward Snowden zamieścił na Twitterze wpis z gratulacjami dla Maximiliana Schremsa: „Congratulations, @MaxSchrems. You've changed the world for the better". Przedruk dostępny w elektronicznej wersji artykułu J. Titcomb, *op. cit*.

[17] Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14…, pkt 28–29.

[18] *Ibidem*, pkt 30.

[19] *Ibidem*, pkt 36.

nego, pytania jednak były bezpośrednio związane z prawem Unii Europejskiej, więc Trybunał Sprawiedliwości mógł stwierdzić nieważność decyzji 2000/520[20].

W sprawie najważniejsza okazała się analiza kompetencji krajowych organów nadzorczych w rozumieniu art. 28 dyrektywy 95/46 w świetle decyzji Komisji 2000/520, ocena ważności tej decyzji, jak również wykładnia art. 25 ust. 1 dyrektywy 95/46 zakazująca przekazywania danych osobowych do państw trzecich, które nie zapewniają odpowiedniego stopnia ochrony. Ponadto zadaniem Trybunału Sprawiedliwości było dokonanie wykładni art. 1 decyzji 2000/520 w kontekście wyjątku, zgodnie z którym stosowanie zasad „bezpiecznej przystani” może być ograniczone między innymi „wymaganiami bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa”. Ostatecznie Trybunał Sprawiedliwości musiał dokonać wykładni art. 3 decyzji 2000/520 zmierzającej do ustalenia, czy kompetencje wykonawcze Komisji dają jej możliwość ograniczania kompetencji krajowych organów nadzorczych działających w dziedzinie ochrony danych.

Zasady ochrony prywatności w ramach „bezpiecznej przystani” były wyrazem kompromisu między amerykańskim i unijnym podejściem do ochrony prywatności, które zasadniczo się różnią, mimo iż Stany Zjednoczone i Unia Europejska dążą do tego samego celu, jakim jest podniesienie poziomu ochrony prywatności swoich obywateli. Stany Zjednoczone stosują podejście sektorowe polegające na połączeniu ustawodawstwa, regulacji i samoregulacji. Przyjęte mocą decyzji Komisji 2000/520 zasady były przeznaczone do wyłącznego użytku przez amerykańskie organizacje otrzymujące dane osobowe z Unii Europejskiej w celu zakwalifikowania ich jako „bezpiecznej przystani” i domniemania „adekwatności”, jakie ta przystań stwarza. Decyzje amerykańskich organizacji były całkowicie dobrowolne, zaś te, które zdecydowały się przyjąć zasady, musiały je stosować w celu uzyskania i utrzymania przywilejów płynących z zasad ochrony prywatności w ramach „bezpiecznej przystani”, jak również publicznie oświadczyć, że tak postępują. Przyjęcie zasad mogło być ograniczone między innymi ze względu na wymagania bezpieczeństwa narodowego, co z kolei leżało u podstaw działania takich organów, jak amerykańska National Security Agency.

Z perspektywy europejskiej strażnikami podstawowych praw i wolności określonych w Karcie Praw Podstawowych są przede wszystkim krajowe organy nadzorcze[21]. Jak stwierdził Trybunał Sprawiedliwości w wyroku w sprawie C-362/14 Schrems[22], zadaniem niezależnych organów nadzorczych jest zapewnienie prawidłowej równowagi między przestrzeganiem podstawowego prawa do poszanowania życia prywatnego a interesami, które wymagają swobodnego przepływu

[20] M. Safjan, D. Düsterhaus, A. Guérin, *La Charte des droits fondamentaux de l’Union européenne et les ordres juridiques nationaux, de la mise en oeuvre à la mise en balance*, RTDEUlr. Revue trimestrielle de droit européen, NO.2 2016, s. 226–230.

[21] Chodzi o krajowe organy nadzorcze w rozumieniu art. 28 dyrektywy 95/46 w świetle decyzji Komisji 2000/520/WE przyjętej na podstawie art. 25 ust. 6 ww. dyrektywy.

[22] Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14…

danych osobowych[23]. Z utrwalonej linii orzeczniczej Trybunału Sprawiedliwości wynika, że przepisy dyrektywy 95/46 muszą być bezwzględnie interpretowane pod kątem ich zgodności z prawami podstawowymi ustanowionymi w Karcie Praw Podstawowych[24]. Sama dyrektywa 95/46 potwierdza, że jej celem jest nie tylko zapewnienie skutecznej i pełnej ochrony podstawowych praw i wolności osób fizycznych, w tym prawa podstawowego do poszanowania prywatności w zakresie przetwarzania danych osobowych, lecz także utrzymanie wysokiego poziomu ochrony tych praw i wolności[25]. Między innymi z tego względu normy wynikające z ww. dyrektywy bywają interpretowane w świetle gwarantowanego w art. 7 KPP prawa do poszanowania życia prywatnego, jak również gwarantowanego w art. 8 KPP prawa do ochrony danych osobowych[26]. Przede wszystkim jednak prawo każdej osoby do ochrony danych osobowych ma swoje źródło w prawie pierwotnym (art. 16 ust. 1 TFUE) i tam też znajduje się podstawa prawna powołania oraz działania niezależnych organów.

Ustanowienie w państwach członkowskich niezależnych organów nadzorczych jest istotnym elementem ochrony osób w związku z przetwarzaniem danych osobowych[27]. Organy te są niezbędne dla zapewnienia efektywności unormowań materialnych w zakresie ochrony prywatności. Parlament Europejski i Rada ustanawiają zasady ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii, jak również przez państwa członkowskie w zakresie, w jakim stosują one prawo UE. Zasady dotyczące swobodnego przepływu danych osobowych określa również Parlament Europejski wspólnie z Radą. We wszystkich tych przypadkach znajduje zastosowanie zwykła procedura ustawodawcza. Zgodnie z Traktatem przestrzeganie zasad ustanowionych w tym celu podlega kontroli niezależnych organów[28]. Wspomniany przepis prawa pierwotnego znalazł odzwierciedlenie między innymi w przepisach dyrektywy 95/46, która nałożyła na państwa członkowskie obowiązek utworzenia jednego lub więcej niezależnych organów nadzorujących poszanowanie unijnych

[23] *Ibidem*, pkt 42–43.

[24] Wyrok w sprawach połączonych C 465/00, C 138/01 i C 139/01 Österreichischer Rundfunk i in., EU:C:2003:294, pkt 68; Wyrok w sprawie C 131/12 Google Spain i Google Inc., EU:C:2014:317, pkt 68; Wyrok w sprawie C 212/13 Ryneš, EU:C:2014:2428, pkt 29.

[25] Art. 1, motywy 2 i 10 dyrektywy 95/46 Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z dnia 23 listopada 1995, s. 31–50.

[26] Wyrok w sprawie C 553/07 Rijkeboer, EU:C:2009:293, pkt 47; Wyrok w sprawach połączonych C 293/12 i C 594/12 Digital Rights Ireland i in., EU:C:2014:238, pkt 53; Wyrok w sprawie C 131/12 Google Spain i Google Inc., EU:C:2014:317, pkt 53, 66, 74.

[27] Motyw 62 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

[28] Art. 16 ust. 2 TFUE.

zasad ochrony osób fizycznych w zakresie przetwarzania danych w przypadku ich przekazywania z Unii Europejskiej do państw trzecich.

Kryterium niezależności krajowych organów nadzorczych zostało wprowadzone mocą dyrektywy 95/46[29]. Zgodnie z utrwalonym orzecznictwem Trybunału Sprawiedliwości pojęcie niezależności tych organów powinno być przedmiotem wykładni autonomicznej opartej na brzmieniu stosownego przepisu ww. dyrektywy, jak również na celach i systematyce całej dyrektywy[30]. Organy nadzorcze w zakresie ochrony danych osobowych powinny korzystać z niezależności pozwalającej im na wykonywanie ich zadań bez wpływu z zewnątrz. Oznacza to, że krajowe organy nadzorcze powinny pozostawać poza jakimkolwiek bezpośrednim czy pośrednim wpływem z zewnątrz mogącym nadawać kierunek ich decyzjom[31]. W odniesieniu do organu publicznego określenie „niezależny” oznacza zwykle status, który daje możliwość w pełni swobodnego działania, z wyłączeniem jakichkolwiek instrukcji czy nacisków. Trybunał Sprawiedliwości podkreśla, że organy kontroli przewidziane w art. 28 dyrektywy 95/46 są strażnikami podstawowych praw i wolności, natomiast rola strażników prawa do poszanowania życia prywatnego wymaga, by decyzje tych organów, jak również one same, pozostawały poza jakimkolwiek podejrzeniem stronniczości[32].

Za niezgodną z wymogiem niezależności uznał Trybunał Sprawiedliwości kontrolę państwową wykonywaną nad niemieckimi organami kontroli właściwymi w zakresie przetwarzania danych osobowych w sektorze niepublicznym. Republika Federalna Niemiec błędnie implementowała wymóg z art. 28 ust. 1 akapit 2 dyrektywy 95/46, zgodnie z którym organy te wykonują zadania „całkowicie niezależnie”, ponieważ poddała nadzorowi państwowemu organy kontroli właściwe w zakresie przetwarzania danych osobowych przez instytucje niepubliczne i przedsiębiorstwa publiczne działające na konkurencyjnym rynku w niektórych krajach związkowych[33].

Krajowym organom nadzorczym powinny przysługiwać odpowiednie kompetencje, w tym kompetencje dochodzeniowe, takie jak prawo do gromadzenia wszelkich informacji potrzebnych do wykonywania ich funkcji nadzorczych, a ponadto skuteczne kompetencje interwencyjne, takie jak prawo nakładania czasowego lub ostatecznego zakazu przetwarzania danych oraz prawo pozywania[34]. Zasięg terytorialny kompetencji krajowych organów nadzorczych nie wykracza

[29] Zgodnie z art. 28 ust. 1 dyrektywy 95/46 „Organy te postępują w sposób całkowicie niezależny przy wykonywaniu powierzonych im funkcji”.

[30] Wyrok Trybunału (wielka izba) z dnia 9 marca 2010 r. w sprawie C-518/07 Komisja Europejska przeciwko Republice Federalnej Niemiec, pkt 17 i 29.

[31] *Ibidem*, pkt 19, 25, 30, 50.

[32] *Ibidem*, pkt 18, 36, 37, 56, sentencja.

[33] *Ibidem*, sentencja.

[34] Art 28 ust. 3 dyrektywy 95/46 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.

poza terytorium państwa członkowskiego, do którego te organy należą, ponieważ kompetencje obejmują przetwarzanie danych osobowych dokonywane na terytorium państwa pochodzenia organów[35]. Na uwagę zasługuje jednak wykładnia przyjęta przez Trybunał Sprawiedliwości, zgodnie z którą operacja przekazywania danych osobowych z państwa członkowskiego do państwa trzeciego polega na przetwarzaniu danych osobowych w rozumieniu dyrektywy 95/46 dokonywanym na terytorium państwa członkowskiego. Definicja „przetwarzania danych osobowych" obejmuje „każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych" i wskazuje jako przykład „ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób"[36].

Trybunał Sprawiedliwości wydedukował, że skoro przekazywanie danych osobowych do państw trzecich może następować wyłącznie w całkowitej zgodności z przepisami państw członkowskich przyjętymi na podstawie dyrektywy 95/46[37], a krajowe organy nadzorcze są zobowiązane do kontrolowania poszanowania unijnych zasad w tym zakresie, to każdy z krajowych organów jest wyposażony w kompetencję do zbadania, czy przekazywanie danych osobowych do państwa trzeciego następuje z poszanowaniem ww. dyrektywy[38]. Wnioski, do których doszedł Trybunał Sprawiedliwości w wyroku w sprawie Schrems odnośnie zakresu kompetencji krajowych organów nadzorczych, wydają się rewolucyjne w stosunku do wydanego pięć dni wcześniej wyroku Trybunału Sprawiedliwości w sprawie C-230/14 Weltimmo s.r.o.[39] W wyroku tym Trybunał również dokonał wykładni art. 28 ust. 3 dyrektywy 95/46, stwierdzając jednak, że organ nadzorczy może wykonywać skuteczne uprawnienia interwencyjne wyłącznie na terytorium państwa członkowskiego, któremu podlega. W konsekwencji organ ten nie może nałożyć sankcji na podstawie prawa państwa członkowskiego na administratora danych, który nie prowadzi działalności gospodarczej na jego terytorium, tylko powinien, na podstawie art. 28 ust. 6 tej dyrektywy, wystąpić o podjęcie działań do organu nadzorczego podległego państwu członkowskiemu, którego prawo jest właściwe[40]. Sprawa dotyczyła wprawdzie przesyłania danych osobowych między państwami członkowskimi UE, ale fakt ten nie wydaje się wystarczający dla uzasadnienia tak diametralnie różnej wykładni art. 28 dyrektywy 95/46, jakiej dokonał Trybunał Sprawiedliwości w wyroku w sprawie C-230/14 Weltimmo s.r.o. i w wydanym

[35] Art. 28 ust. 1 i 6 dyrektywy 95/46 Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. …

[36] Art. 2 lit. b) dyrektywy 95/46 Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. …

[37] Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14…, pkt 46.

[38] *Ibidem*, pkt 47.

[39] Wyrok Trybunału (trzecia izba) z dnia 1 października 2015 r. w sprawie C-230/14 Weltimmo s.r.o. przeciwko Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639.

[40] *Ibidem*, pkt 60 i pkt 2 sentencji wyroku.

pięć dni później wyroku w sprawie C-362/14 Schrems. O ile w wyroku w sprawie C-230/14 Weltimmo s.r.o. Trybunał Sprawiedliwości brał pod uwagę zasadę terytorialności celem ograniczenia zakresu kompetencji krajowych organów nadzorczych do terytorium państwa, z którego one pochodzą, to w wyroku w sprawie C-362/14 Schrems całkowicie odszedł od tej zasady[41]. Ponadto w wyroku w sprawie C-230/14 Weltimmo s.r.o. niedosyt budzą te części uzasadnienia, w których Trybunał Sprawiedliwości jawi się zwolennikiem teorii siedziby w przypadku transgranicznego świadczenia usług drogą elektroniczną. Tymczasem stanowisko przyjęte w wyroku w sprawie C-362/14 Schrems zostało uzasadnione w sposób detaliczny, a na poparcie swych tez Trybunał Sprawiedliwości podał kilka istotnych argumentów.

Po pierwsze, w świetle art. 25 dyrektywy 95/46 ustalenia dotyczące tego, czy państwo trzecie zapewnia odpowiedni stopień ochrony, czy też nie, mogą zostać dokonane albo przez państwa członkowskie, albo przez Komisję, co stanowi przypadek kompetencji dzielonych[42]. Po drugie, fakt, że akty instytucji Unii korzystają zasadniczo z domniemania ważności, a zatem wywołują skutki prawne do czasu ich uchylenia, nie uniemożliwia osobom, których dane zostały przekazane do państwa trzeciego, wniesienia do krajowych organów nadzorczych skargi w rozumieniu innego przepisu dyrektywy, jakim jest art. 28 ust. 4 dyrektywy 95/46. Decyzja Komisji, taka jak decyzja 2000/520, nie może zanegować ani ograniczyć kompetencji wyraźnie przyznanych krajowym organom nadzorczym w art. 8 ust. 3 Karty Praw Podstawowych oraz w art. 28 dyrektywy 95/46. Po trzecie, żaden z wymienionych przepisów nie wyklucza z zakresu kompetencji krajowych organów nadzorczych kontroli przekazywania danych osobowych do państw trzecich objętych zakresem zastosowania decyzji Komisji wydanych na podstawie art. 25 ust. 6 dyrektywy 95/46. Również art. 28 ust. 4 ww. dyrektywy nie przewiduje żadnego wyjątku w tym względzie. Zdaniem rzecznika generalnego Yves'a Bota sytuacja, w której omawiana decyzja Komisji uniemożliwiałaby krajowemu organowi nadzorczemu rozpatrzenie skargi złożonej przez osobę, której dane zostały lub mogły zostać przekazane do państwa trzeciego, byłaby sprzeczna zarówno z celem art. 25 i 28 ww. dyrektywy, jak również z systemem wprowadzonym przez dyrektywę. W konsekwencji, jeśli osoba, której dane osobowe zostały lub mogły zostać przekazane do państwa trzeciego będącego przedmiotem decyzji Komisji przyjętej na mocy art. 25 ust. 6 dyrektywy 95/46, wnosi do krajowego organu nadzorczego skargę dotyczącą ochrony jej praw i wolności w zakresie przetwarzania tych danych, a także podważa zgodność tej decyzji z ochroną życia prywatnego

[41] Na temat zasady terytorialności w kontekście transgranicznego przetwarzania danych osobowych: K. Kowalik-Bańczyk, O. Pollicino, *Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information*, „German Law Journal" 17, 2016, nr 3, s. 321.

[42] Opinia rzecznika generalnego Y. Bota przedstawiona w dniu 23 września 2015 r., ECLI:EU:C:2015:627, pkt 86.

oraz podstawowych praw i wolności jednostek, to krajowy organ nadzorczy zobowiązany jest do rozpatrzenia tej skargi z wszelką wymaganą starannością[43].

Sprawa Schrems zbiegła się w czasie z pracami nad nowym ogólnym rozporządzeniem o ochronie danych. Po kilku latach prac, 27 kwietnia 2016 roku, przyjęte zostało rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[44]. Rozporządzenie weszło w życie 20 dni po ogłoszeniu w Dzienniku Urzędowym Unii Europejskiej, to jest 24 maja 2016 roku, ale będzie miało zastosowanie od 25 maja 2018 roku[45]. Wśród powodów przygotowania nowego rozporządzenia wskazywano na szybki postęp techniczny i globalizację oraz wzrost skali zbierania i wymiany danych osobowych. Z jednej strony, dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą wykorzystywać dane osobowe w swojej działalności na niespotykaną wcześniej skalę. Z drugiej strony, osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Uznano, że technologia powinna w dalszym ciągu ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, jednak równocześnie powinna zapewniać wysoki stopień ich ochrony[46]. Podkreślenie znaczenia przepływu danych do państw trzecich może być przejawem doświadczeń wynikających z wyroku w sprawie Schrems. Jak stwierdził Europejski Rzecznik Ochrony Danych, rozporządzenie to stanowi pierwszy etap modernizacji, a jego wdrożenie pozwoli na skuteczne wyciągnięcie wniosków z wyroku w sprawie Schrems[47].

Ponadto w motywach ogólnego rozporządzenia o ochronie danych przyznano, że przy wdrażaniu dyrektywy 95/46 nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w Internecie. Różnice w stopniu ochrony praw i wolności osób fizycznych w państwach członkowskich w związku z przetwarzaniem danych osobowych mogły utrudniać swobodny przepływ danych osobowych w Unii i w rezultacie stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, w tym zakłócać konkurencję oraz utrudniać organom wykonywanie obowiązków nałożonych na nie prawem Unii.

---

[43] Opinia rzecznika generalnego Y. Bota przedstawiona w dniu 23 września 2015 r., ECLI:EU:C:2015:627, pkt 61, 93, 95, 113, 116 i in. oraz wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14…, pkt 50–63.

[44] 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 (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz.U. L 119 z dnia 4 maja 2016, s. 1–88.

[45] Art. 99 ogólnego rozporządzenia o ochronie danych.

[46] Motyw 6 ogólnego rozporządzenia o ochronie danych.

[47] Contrôleur européen de la protection des données, Le Rapport Annuel 2015, Résumé, ed. Union européenne 2016, s. B3.

Skoro różnice w stopniu ochrony wynikały z różnic we wdrażaniu i stosowaniu dyrektywy 95/46, to zdecydowano się na zastąpienie dyrektywy rozporządzeniem ogólnym, którego celem jest zapewnienie równorzędnego stopnia ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych we wszystkich państwach członkowskich. Rozporządzenie ze swej natury daje większe możliwości zapewnienia spójnego i jednolitego w całej Unii stosowania przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Niezależnie od tego, rozporządzenie umożliwia państwom członkowskim doprecyzowanie jego przepisów, między innymi w odniesieniu do przetwarzania szczególnych kategorii danych osobowych („dane wrażliwe"). W tym kontekście rozporządzenie nie wyklucza możliwości określenia w prawie krajowym okoliczności dotyczących konkretnych sytuacji związanych z przetwarzaniem danych[48]. Zaproponowane w ogólnym rozporządzeniu o ochronie danych zmiany bywają określane mianem przewrotu kopernikańskiego w unijnym prawie ochrony danych[49].

Przyjęcie w 1995 roku dyrektywy 95/46 sygnalizowało nadejście drugiej generacji standardów ochrony danych, które przez dwie dekady wpływały na ochronę danych także poza Europą i to w takim stopniu, że globalny standard ochrony danych jest bliższy dyrektywie 95/46 niż wytycznym OECD. Ważne globalne pytanie dotyczące ogólnego rozporządzenia o ochronie danych powinno odnosić się do kwestii, które z nowych zasad i wymogów w zakresie wykonania mogą stać się standardowymi elementami ochrony danych poza Unią Europejską, to znaczy trzecią generacją zmieniających się globalnych standardów ochrony danych osobowych. Pamiętać przy tym należy, że część rozwiązań przyjętych w ogólnym rozporządzeniu o ochronie danych jest już przyjęta w zrewidowanych w 2013 roku Wytycznych OECD[50]. Ożywienie kwestii ochrony danych i prawa do prywatności, jak również wdrożenie jej jest wspólnym elementem reform przeprowadzanych zarówno w Europie, jak i poza jej granicami[51].

Przyjęta w lipcu 2016 roku przez Komisję Europejską Tarcza Prywatności UE–USA ma na celu lepszą ochronę transatlantyckiego przepływu danych po unieważnieniu decyzji Komisji 2000/520 wyrokiem w sprawie C-362/14 Schrems. Z jednej strony chodzi o zapewnienie ochrony praw podstawowych obywatelom Unii, których dane osobowe są przekazywane do USA. Z drugiej zaś o zagwarantowanie jasności prawa przedsiębiorcom, którzy dokonują transatlantyckich

---

[48] Motywy 9 i 10 ogólnego rozporządzenia o ochronie danych.

[49] Giovanni BUTTARELLI — European Data Protection Supervisor, Keynote speech for session "*Global Personal Data Protection Policy Trend*", Speech delivered at occasion of Korea EU Personal information International Seminar, Seoul, Korea, 18 July 2016, s. 2.

[50] G. Greenleaf, *op. cit.*, s. 4–5.

[51] D. Wright, P. De Hert, *Introduction to Enforcing Privacy*, [w:] *Enforcing Privacy — Regulatory, Legal and Technical Approaches, Governance and Technology*, red. D. Wright, P. De Hert, Series 25, Springer International Publishing Switzerland 2016, s. 2.

transferów danych. Tarcza prywatności UE–USA przewiduje rygorystyczne obowiązki nałożone na przedsiębiorstwa przetwarzające dane, wyraźne zabezpieczenia i wymogi przejrzystości regulujące dostęp administracji rządowej USA do danych osobowych, skuteczną ochronę praw osób fizycznych oraz wspólny mechanizm corocznego przeglądu. Departament Handlu Stanów Zjednoczonych będzie prowadził regularne aktualizacje i przeglądy uczestniczących przedsiębiorstw. Jeśli przedsiębiorstwa nie będą przestrzegały zasad w praktyce, mogą spotkać się z sankcjami i zostać usunięte z listy. Stany Zjednoczone zapewniły Unię Europejską, że dostęp organów publicznych do danych, uzasadniony względami bezpieczeństwa narodowego, jest ograniczony oraz że będzie podlegać zabezpieczeniom i mechanizmom nadzoru. USA wykluczyły bezkrytyczną masową inwigilację danych osobowych przekazywanych im w ramach uzgodnienia Tarczy Prywatności UE–USA. Każdy obywatel, który uważa, że jego dane zostały niewłaściwie wykorzystane w ramach systemu Tarczy Prywatności, będzie mógł skorzystać z kilku dostępnych i przystępnych cenowo mechanizmów rozstrzygania sporów. Osoby fizyczne będą mogły między innymi zwrócić się do krajowych organów ochrony danych w swoim państwie, które skontaktują się z Federalną Komisją Handlu, aby zagwarantować, że skargi europejskich obywateli zostaną zbadane i rozpatrzone[52].

Na marginesie rozważań warto wspomnieć, że w 2013 roku spółka Facebook Inc. uruchomiła w mieście Luleå w północnej Szwecji nowoczesne centrum danych Facebooka, przez co nie musiała korzystać z serwerów usytuowanych w USA. Szwedzki kompleks danych Facebooka został wybudowany według najnowszych technologii. Całość zapotrzebowania na energię czerpie ze źródeł odnawialnych. Główny budynek jest wielkości sześciu boisk piłkarskich. Miasto jest położne w odległości kilkudziesięciu kilometrów od koła podbiegunowego, dzięki czemu serwery mogą być chłodzone w naturalny sposób powietrzem polarnym. Produkowane przez serwery ciepło jest wykorzystane do ogrzewania budynków. Mark Zuckerberg, założyciel i główny udziałowiec Facebook Inc., nie stroni od mediów, by pokazać światu swoje centra danych. Jest to możliwe, zwłaszcza że serwerownie zaprojektowano zgodnie z ideą Open Compute Project, co oznacza, że specyfikacja wykorzystanego w centrum danych sprzętu i infrastruktury jest udostępniana za darmo[53]. Facebook Inc. jest kolejną po Google Inc.[54] amerykańską spółką, która

[52] Komisja Europejska — Komunikat prasowy, *Komisja Europejska uruchamia Tarczę Prywatności UE–USA: lepsza ochrona transatlantyckiego przepływu danych*, Bruksela, 12 lipca 2016 r., s. 1–2.

[53] J. Fryc, *Mark Zuckerberg zabiera w podróż do północnej Szwecji. Pokazuje centrum danych Facebooka*, Business Insider Polska — Technologie, 29 września 2016, http://businessinsider.com.pl/technologie. Ponadto, R. Miller, *Live in Lulea: Facebook Goes Global and Gets Greener*, Data Center Knowledge, 12 czerwca, 2013, www.datacenterknowledge.com.

[54] Wyrok Trybunału (wielka izba) z dnia 13 maja 2014 r. w sprawie C-131/12 Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi, ECLI:EU:C:2014:317.

dostosowała swoją działalność do wymogów prawa Unii Europejskiej określonych w orzecznictwie Trybunału Sprawiedliwości.

Tytułem podsumowania warto podkreślić, że swobodny przepływ danych osobowych stanowi integralną część wymiany handlowej zarówno między podmiotami pochodzącymi z Unii Europejskiej, jak i w ramach stosunków z podmiotami pochodzącymi z państw trzecich. Wyrok Trybunału Sprawiedliwości w sprawie Schrems został wydany 6 października 2015 roku i w związku ze stwierdzeniem nieważności decyzji Komisji 2000/520 wywołał konieczność uregulowania od nowa pewnych aspektów transatlantyckiego przepływu danych osobowych. W wyroku w sprawie Schrems Trybunał Sprawiedliwości potwierdził, że przepisy Karty Praw Podstawowych Unii Europejskiej określające prawa podstawowe odnoszące się do ochrony danych osobowych znajdują zastosowanie także w sytuacji przekazywania danych osobowych poza Unię Europejską. W ten sposób dookreślony został zewnętrzny zakres stosowania prawa Unii Europejskiej regulującego ochronę danych osobowych i prawo do poszanowania prywatności. W następstwie tego wyroku na nowo uregulowano transatlantyckie przekazywanie danych, uruchamiając w 2016 roku Tarczę Prywatności UE–USA.

EU–U.S. PRIVACY SHIELD AFTER A COLLISION IN THE "SAFE HARBOUR". THE SCOPE OF PRIVACY PROTECTION AFTER THE JUDGEMENT IN THE C-362/14 SCHREMS CASE

Summary

Transfer of personal data is an essential element of the transatlantic trade relationship, because the EU and the United States are for each other the most important trading partners. Data transfers increasingly form an integral part of their commercial exchanges. The Court of Justice of the European Union ruling of 6 October 2015 in case C-362/14 Schrems reaffirmed the importance of the fundamental right to the protection of personal data, as enshrined in the Charter of Fundamental Rights of the EU, including the situation when such data are transferred outside the EU. In the wake of the hereinabove judgement the transatlantic data transfer has been regulated anew. European Commission has launched EU-U.S. Privacy Shield in order to ensure stronger protection for transatlantic data flows. This article aims to analyse the importance and results of the above-mentioned judgement.

Przegląd Prawa i Administracji 107, 2016