Wprowadzenie

Znaczenie wzajemnych, złożonych relacji gospodarczych, politycznych, naukowych, kulturalnych i społecznych między Polską (oraz innymi państwami członkowskimi Unii Europejskiej) a Stanami Zjednoczonymi jest w globalizującym się świecie, przy rosnącej roli Chin i państw regionu Pacyfiku, nie do przecenienia.

O doniosłości tych relacji świadczy już sama wartość wymiany handlowej pomiędzy UE a USA, szacowana na początku XXI w. na sumę około 120 mld dolarów rocznie, przy czym szacunek ten nie ujmuje niewymiernych korzyści płynących z wymiany naukowej i kulturalnej. Stany Zjednoczone były i są dla Unii Europejskiej największym odbiorcą towarów i usług. Według danych publikowanych przez Komisję Europejską blisko 17% towarów eksportowanych z UE trafia do USA (import do drugiej na tej liście Szwajcarii stanowi niecałe 10%, a do Chin – 8,5%)[1].

Jednocześnie „paliwem" napędzającym obecnie światową gospodarkę są przekazywane informacje i dane, w tym zwłaszcza dane osobowe, zawierające informacje na temat poszczególnych osób fizycznych. Mówi się wręcz, że to właśnie dane stanowią „nowy węgiel" współczesnej gospodarki[2].

Ta cyfrowa gospodarka kształtuje się m.in. na skutek bezprecedensowego rozwoju technologii przetwarzania i wymiany danych na ogromną skalę[3].

---

[1] *R. Bendini*, Unia Europejska i jej partnerzy handlowi, dokumenty informacyjne o Unii Europejskiej, http://www.europarl.europa.eu/ftu/pdf/pl/FTU_6.2.1.pdf (dostęp: 1.6.2017 r.). Zob. też: *M. Krzysztofek*, Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, Warszawa 2016, s. 238.

[2] *C. Schwab*, The Fourth Industrial Revolution. What It Means and How to Respond, w: Foreign Affairs Anthology Series, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution (dostęp: 12.12.2015 r.).

[3] Pkt 4 preambuły Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 1995 r., Nr 281, s. 31, wydanie specjalne Dz.Urz. UE WS, rozdz. 13, t. 15, s. 355) oraz Explonatory Memorandum – Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regula-

Marek Safjan akcentuje, że doświadczamy „eksplozji niewiarygodnych do niedawna możliwości gromadzenia danych i ich przetwarzania"[4].

Ilustracją tego postępu jest m.in. powszechność i łatwość dostępu do internetu oraz oferowanych przezeń funkcji. Już w sierpniu 2011 r. liczba użytkowników internetowego portalu społecznościowego Facebook wynosiła w skali globu 750 mln osób, a od roku 2008 w skali świata dostęp do internetu miało więcej urządzeń mobilnych (telefonów komórkowych i tabletów) niż komputerów stacjonarnych, co niebywale ułatwia i upowszechnia dostępność sieci komputerowej, istotnie przy tym zmieniając sposób i cel jej wykorzystania[5]. Co więcej, Facebook i inne portale społecznościowe mogą aktywnie kreować postawy i wpływać na zachowania i ludzkie decyzje, w tym na decyzje wyborcze[6].

Jednocześnie, eliminacja barier nadmiernie czy bezzasadnie zakłócających transatlantyckie relacje na rozmaitych płaszczyznach, może stanowić jeden ze sposobów powstrzymania dostrzegalnych tendencji schyłkowych w odniesieniu do globalnej pozycji Europy i Ameryki Północnej, a dalszy rozwój cywilizacji można coraz silniej wiązać z dostępem do informacji[7].

Taką barierę mogą stanowić w szczególności ewentualne nadmierne ograniczenia transferów danych osobowych z Polski (oraz innych państw członkowskich UE) do Stanów Zjednoczonych, przybierające niekiedy formę pozataryfowych barier handlowych[8].

---

tion), Brussels 25.1.2012 r., COM(2012) 11 final, 2012/0011 (COD) (Text with EEA relevance), {SEC(2012) 72 final}, {SEC(2012) 73 final}, s. 2.

[4] *M. Safjan*, Ochrona danych osobowych – granice autonomii informacyjnej, w: *M. Wyrzykowski* (red.), Ochrona danych osobowych, Warszawa 1999, s. 9.

[5] *T. Craig*, *M. Ludloff*, Privacy and Big Data, Sebastopol 2011, s. 3. Zob. też *Y.A. de Montjoye*, *C.A. Hidalgo*, *M. Verleysen*, *V.D. Blondel*, Unique in the Crowd: The privacy bounds of human mobility, Nature.com Scientific Reports, http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html#ref20 (dostęp: 25.3.2013 r.) oraz *P.P. Swire*, The Second Wave of Global Privacy Protection. Symposium Introduction, Ohio State Law Journal 2013, Nr 74, s. 842–852.

[6] Zob. United States of America, Federal Trade Commission: Complaint on Facebook, Inc. (0923184), http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf (dostęp: 1.6.2017 r.). Na temat prawnych aspektów serwisów społecznościowych zob. *P. Fajgielski*, Przetwarzanie danych osobowych w serwisach społecznościowych – wybrane aspekty prawne, w: *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Media elektroniczne. Współczesne problemy prawne, Warszawa 2016, s. 152 i n.

[7] Zob. *I. Lipowicz*, Polska administracja publiczna w świetle standardów europejskich, w: *Z. Niewiadomski* (red.), Prawo administracyjne, Warszawa 2011, s. 335. W odniesieniu do skutków znoszenia barier handlowych zob. *Z. Lewicki*, Historia cywilizacji amerykańskiej. Era sprzeczności 1787–1865, Warszawa 2010, s. 111 i 112.

[8] *P.M. Regan*, American Business and the European Data Protection Directive: Lobbying Strategies and Tactics, w: *C.J. Bennett*, *R. Grant* (red.), Visions of Privacy. Policy Choices for the Digital

Jak stwierdzono w Agendzie Cyfrowej UE: „Europejczykom często łatwiej jest przeprowadzać transakcje transgraniczne [głównie internetowe – przyp. *B.M.*] z przedsiębiorstwem amerykańskim niż z przedsiębiorstwem z innego kraju europejskiego”[9], a dane na temat preferencji i upodobań indywidualnych mieszkańców Unii Europejskiej od lat znajdują się w Stanach Zjednoczonych[10]. Wspomniane ograniczenia dotyczą jednak, co wzmiankowano, także innych sfer życia, w tym np. praktyki udzielania pomocy prawnej[11].

Biorąc pod uwagę opisane uwarunkowania, regulacje mogące negatywnie wpłynąć na wymianę między Polską i USA oraz – szerzej – na transatlantycką wspólnotę wartości – stanowią fascynujący temat badawczy. Dotyczy to zwłaszcza, z uwagi na centralną pozycję we współczesnym świecie, prawnych ograniczeń transatlantyckich przepływów danych osobowych.

Pojęcie odpowiedniego poziomu ochrony danych osobowych występuje w prawie polskim (a także w prawie Unii Europejskiej) jako zasadnicze kryterium oceny bezpieczeństwa danych w państwie trzecim (czyli np. w Stanach Zjednoczonych). Dopiero stwierdzona „odpowiedniość poziomu ochrony” pozwala na przekazanie danych osobowych do konkretnego państwa trzeciego. Niemniej obowiązujące przepisy nie definiują wskazanego pojęcia.

Niedookreślone sformułowanie „odpowiedni poziom ochrony danych osobowych”, pozostawiające znaczną przestrzeń interpretacyjną, ma zatem fundamentalne znaczenie dla swobody i sposobu przepływów danych osobowych z Polski (a także innych państw członkowskich Unii Europejskiej) do Stanów Zjednoczonych, co z kolei bezpośrednio i wprost oddziałuje na rozmiary i intensywność transatlantyckiej wymiany handlowej, kulturalnej, naukowej oraz procesy inwestycyjne.

Age, Toronto–Buffalo–London 1999, s. 211 oraz *P.P. Swire*, *R.E. Litan*, None of your business. World Data Flows, Electronic Commerce, and the European Privacy Directive, Washington D.C. 1998, s. 144 i n.

9 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejska agenda cyfrowa, Bruksela 26.8.2010 r., KOM(2010) 245 wersja ostateczna/2, Corrigendum: Annule et remplace le document COM(2010) 245 final du 19.5.2010 r., s. 6. Tekst Agendy cyfrowej: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PL:PDF (dostęp: 1.6.2017 r.).

10 *P.M. Schwartz*, *J.R. Reidenberg*, Data Privacy Law, A Study of United States Data Protection, Charlottesville, Virginia 1996, s. 308–309.

11 Zob. *M.J. Daley*, *K.N. Rashbaum* (red.), Framework for Anaslysis of Cross-Boarder Discovery Conflicts: A Practical Guide to Navigating the Competitive Currents of International Data protection and e-Discovery, The Sedona Conference Working Group Series, Phoenix 2008.

Utrwalony w Polsce (oraz w Unii Europejskiej) pogląd głosi, że Stany Zjednoczone nie zapewniają odpowiedniego poziomu ochrony danych osobowych, co rodzi poważne konsekwencje i utrudnia, a niekiedy wręcz uniemożliwia przekazywanie danych osobowych do USA. Paraliż transatlantyckiej wymiany handlowej, naukowej czy kulturalnej nie następuje przede wszystkim na skutek stosowania szczególnych i wyjątkowych rozwiązań *ad hoc*, pozwalających na transfer danych do USA pomimo utrzymującego się braku pewności co do ich bezpieczeństwa i dalszych losów.

Obraz dodatkowo komplikuje się w razie stwierdzenia, że współczesne demokratyczne państwa prawa, a do takich zalicza się zarówno Rzeczpospolitą Polską, jak i Stany Zjednoczone Ameryki Północnej, dążą do możliwie pełnego zabezpieczenia praw i wolności obywateli, a elementarne prawa obywatelskie obowiązujące w Polsce nie odbiegają drastycznie od praw obywatelskich uznawanych w USA.

Mimo że zainteresowaniu dziedziną ochrony danych osobowych towarzyszy znaczna liczba naukowych publikacji i konferencji, stosunkowo niewiele uwagi w piśmiennictwie polskim poświęcono przyczynom opisanych wyżej różnic i ich skutków. W szczególności brakuje szczegółowych analiz wykraczających poza opisanie konkretnych, doraźnych rozwiązań normatywnych stosowanych w celu dokonywanej nierzadko *ad hoc* legalizacji przepływu danych z Polski do USA. I choć należy przychylić się do oceny wyrażonej przez *Mariusza Jagielskiego*, że doraźne akcesoryjne środki prawne skutkują pewnym podniesieniem poziomu ochrony danych w państwie takim jak USA, to dostrzegalna jest znikoma refleksja nad przyczynami trudności wprowadzenia powszechnych, transatlantyckich rozwiązań systemowych[12].

Równie znikoma refleksja towarzyszy problematyce dążenia w omawianej dziedzinie do konwergencji, której jeden z przejawów może stanowić interoperacyjność (*interoperability*) systemów prawnych, pojmowaną jako „budowanie mostów między różniącymi się systemami ochrony danych"[13]. Konwergencja rozumiana jest tutaj jako proces zbliżenia poglądów i, w konsekwencji, moż-

[12] *M. Jagielski*, Prawo do ochrony danych osobowych. Standardy europejskie, Warszawa 2010, s. 197.

[13] *C. Kuner*, Transborder Data Flows, s. 176. Obszernie na temat interoperacyjności zob. *B. Szafrański*, Interoperacyjność rejestrów publicznych, w: *A. Gryszczyńska* (red.), Rejestry publiczne. Jawność i interoperacyjność, Warszawa 2016, s. 57 i n. Zob. też *K. v. Beyme*, Implementation: ein Paradigma der Synergieeffekte zwischen Verwaltungswissenschaft und Politikwissenschaft, w: *H.-H. Trute*, *T. Groß*, *H.C. Röhl*, *C. Möllers* (red.), Allgemeines Verwaltungsrecht – zur Tragfähigkeit eines Konzeptes, Tübingen 2008, s. 3 i n.

liwie jednolitego uregulowania identycznych bądź przynajmniej istotnie zbliżonych dziedzin[14].

Niniejsza praca poświęcona jest analizie przyczyn wskazanego stanu, przedstawieniu różnic i podobieństw systemowych, opisowi wyznaczonego przepisami polskiego prawa administracyjnego testu na odpowiedniość poziomu ochrony danych w państwie trzecim oraz ocenie przydatności owego testu, wraz z rekomendacjami wynikającymi ze stanowiska gremiów zajmujących się w Unii Europejskiej ochroną danych osobowych, w odniesieniu do amerykańskiego federalnego systemu prawnego.

W końcowej części pracy zaprezentowane zostały uwagi *de lege ferenda*, obejmujące m.in. wskazania możliwości poszukiwania systemowej konwergencji oraz postulowanych rozwiązań nakierowanych na zniwelowanie istniejących różnic systemowych, m.in. przez odwołanie do prawnie chronionych transatlantyckich wartości i wspólnoty tychże wartości.

Należy wspomnieć, że potrzeba dokonania analizy stanowiącej przedmiot pracy wynika również z faktu przyjęcia 27.4.2016 r. przez Parlament Europejski i Radę UE ogólnego rozporządzenia o ochronie danych (rozporządzenie będzie mieć zastosowanie od 18.5.2018 r.).

Unijne rozporządzenie nie tylko zmodyfikuje aktualne i ukształtuje nowe zasady przetwarzania danych osobowych w UE, lecz także zrodzi potrzebę oceny prawnego unormowania zasad i sposobów transferów danych osobowych z państw członkowskich UE – w tym oczywiście z Polski – do Stanów Zjednoczonych.

Stąd usystematyzowany przegląd stanowisk i regulacji przyjętych po obu stronach Atlantyku ma zatem obecnie elementarne znacznie, a wnioski formułowane w pracy mogą stanowić wkład do wypracowania polskiego stanowiska w transatlantyckiej debacie. Debacie, która w znacznej mierze może przesądzić o przyszłości coraz bardziej cyfrowego świata, a która toczyć się będzie w obliczu Brexitu, prawdopodobnego – w razie wyboru *Donalda Trumpa* na prezydenta USA – zakwestionowania potrzeby i idei zawarcia porozumienia Transatlantic Trade and Investment Partnership (TTIP) oraz wzrostu postaw izolacjonistycznych USA.

Oś dalszych rozważań stanowią pytania, czy ocena braku odpowiedniości poziomu ochrony danych w USA wciąż jest zasadna, a jeśli tak, czy ist-

[14] Szerzej w tej kwestii, w tym na temat zatracania przez systemy prawne swojej konstrukcyjnej jednorodności, zob. *R.D. Kelemen*, Eurolegalism, Cambridge–London 2011, s. 5 i n. oraz *M. Ancel*, Znaczenie i metody prawa porównawczego, Warszawa 1979, s. 12.

nieją możliwości wypracowania rozwiązań zapewniających odpowiedni poziom ochrony danych przekazywanych z Polski do USA, przy możliwie najmniejszym publicznoprawnym ograniczeniu swobody działalności.

Rozdział I. Materia i metody badania

§ 1. Hipoteza i pytania badawcze

Pojęcie odpowiedniego poziomu ochrony danych osobowych występuje w prawie polskim i unijnym i stanowi, jak była o tym mowa we Wprowadzeniu, istotne kryterium decydujące o możliwości przekazywania danych osobowych do państw trzecich, w tym do Stanów Zjednoczonych.

Pojęciem tym posługuje się polski ustawodawca w art. 47 ustawy z 29.8.1997 r. o ochronie danych osobowych[1], a także prawodawca unijny w art. 25 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2] oraz art. 41 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[3], które będzie mieć zastosowanie od 25.5.2018 r.

Zgodnie z definicją słownikową odpowiedniość to „fakt, że jakieś rzeczy, zjawiska itp. odpowiadają sobie wzajemnie", a adekwatność to „zgodność z czymś"[4].

Niemniej obowiązujące akty prawne regulujące dziedzinę ochrony danych osobowych pojęcia odpowiedniości nie definiują ani też nie wskazują precyzyjnie, jak badać ową „odpowiedniość" w państwie trzecim. Podobnie, zagadnienie to nie było poddane pogłębionej analizie w piśmiennictwie, co rodzi zasadnicze dylematy.

Informacje, w tym dane osobowe, przepływają przez systemy informatyczne niezależnie od granic geograficznych, politycznych czy kulturowych,

---

1 T.j. Dz.U. z 2016 r. poz. 922.

2 Dz.Urz. UE L 1995 r., Nr 281, s. 31, wydanie specjalne Dz.Urz. UE WS, rozdz. 13, t. 15, s. 355.

3 Dz.Urz. UE L 2016 r. Nr 119, s. 1 i n.

4 *E. Sobol, L. Drabik, A. Kubiak-Sokół* (red.), Słownik języka polskiego PWN, Warszawa 2016.

zachowując się, jak pisze *Christopher Kuner*, niczym „ciecz w systemie rurociągów"[5], co rodzi wielopłaszczyznowe konsekwencje, w tym np. w sferze społecznej (wiązanej m.in. z wolnością wypowiedzi), jednostkowej (dotyczącej zaspokajania indywidualnych potrzeb i kwestii życiowych), urzędowej czy korporacyjnej[6].

Już same tytuły dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz rozporządzenia UE 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych wskazują obszary regulacji obejmujący ochronę osób fizycznych wobec faktu przetwarzania ich danych oraz swobodę przepływu danych[7], a europejski – w tym także polski – system prawnej ochrony danych osobowych uchodzi za najbardziej zaawansowany na świecie[8].

W Polsce regulacja ochrony danych osobowych została wprowadzona przez Konstytucję Rzeczypospolitej Polskiej z 2.4.1997 r.[9], a następnie szczegółowo uregulowana przepisami ustawy z 29.8.1997 r. o ochronie danych osobowych[10], przy czym należy zaakcentować, że wskazane akty weszły w życie – odpowiednio – 17.10.1997 i 30.4.1998 r., a zatem na kilka lat przed przystąpieniem Polski do Unii Europejskiej (1.5.2004 r.).

Rozwiązania przyjęte w polskiej ustawie w znacznym stopniu odpowiadają regulacjom dyrektywy 95/46/WE, co pozwala uznać polski materiał normatywny, wraz z prawie dwudziestoletnim dorobkiem orzeczniczym i doktrynalnym za badawczo interesujący punkt referencyjny, przydatny dla oceny odpowiedniości poziomu ochrony danych osobowych w państwie trzecim, jakim są Stany Zjednoczone.

W polskiej ustawie o ochronie danych osobowych zastosowano dychotomiczny podział państw świata na:

– państwa należące do Europejskiego Obszaru Gospodarczego (w jego skład wchodzą państwa członkowskie UE oraz Islandia, Lichtenstein

[5] *C. Kuner*, Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future (October 1, 2010). TILT Law, Technology Working Paper No. 016/2010; Tilburg Law School Research Paper No. 016/2010, s. 11, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483 (dostęp: 1.6.2017 r.).

[6] *C. Kuner*, Transborder Data Flows and Data Protection Privacy, Oxford 2013, s. 102.

[7] Zwraca na to uwagę *C. Kuner*, pisząc w tym kontekście o hybrydowej naturze regulacji dziedziny ochrony danych osobowych – *C. Kuner*, Transborder Data Flows, s. 20.

[8] *P. Carey*, Data Protection. A Practical Guide to UK and EU Law, Oxford 2009, s. 103.

[9] Dz.U. Nr 78, poz. 483 ze zm.

[10] T.j. Dz.U. z 2016 r., poz. 922.

i Norwegia), które – zgodnie z przyjętym domniemaniem adekwatności (*presumption of adequacy*)[11] spełniają europejskie standardy ochrony danych osobowych[12];
– państwa trzecie, do których zaliczane są wszystkie pozostałe państwa[13].

Podział ten zastosowano także w dyrektywie 95/46/WE, jak również w ogólnym rozporządzeniu o ochronie danych, które zastąpi polską ustawę o ochronie danych osobowych oraz dyrektywę 95/46/WE w dniu 25.5.2018 r. Trzeba zastrzec, że przyjęcie wskazanego rozporządzenia stanowi przejaw reformy regulacji ochrony danych osobowych w UE, aczkolwiek cele i zasady ochrony danych osobowych pozostają aktualne, a zmiany mają na celu zapewnienie jednolitości regulacji wewnątrz Unii Europejskiej[14].

Z perspektywy polskich uregulowań dziedziny ochrony danych osobowych przekazywanie danych osobowych do państw trzecich jest niedopuszczalne, chyba że zachodzą szczególne przesłanki legalizacyjne[15]. Z tego powodu, aby usprawnić obrót z wybranymi państwami nienależącymi do EOG, Komisja Europejska uznała, że państwa te zapewniają odpowiedni – z perspektywy standardów europejskich – poziom ochrony danych. Komisja Europejska wpisała na tę listę, zwykle w wyniku szczegółowych, kilkuletnich postępowań weryfi-

11 Zob. *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych. Komentarz, Kraków 2007, s. 655; *X. Konarski*, *G. Sibiga*, Zasady przekazywania danych osobowych do państwa trzeciego w prawie polskim i Unii Europejskiej, w: *G. Sibiga*, *X. Konarski* (red.), Ochrona danych osobowych. Aktualne problemy i nowe wyzwania Warszawa 2007, s. 88, jak również: *R.K. Baker*, Offshore It Outsourcing And The 8th Data Protection Principle – Legal And Regulatory Requirements – With Reference To Financial Services, International Journal of Law and Information Technology, Vol. 14, No. 1, Oxford, Spring 2006.

12 Szerzej piszę o tym aspekcie w: Die Übermittlung personenbezogener Daten aus Polen in die Drittländer (unter Berücksichtigung des spezifischen Datenverkehrs in die Vereinigten Staaten) – ausgewählte Rechtsfragen, w: *I. Lipowicz* (red.), Die Europaisierung der öffentlichen Verwaltung, Wien 2010, s. 58 i 59.

13 Zob. art. 7 pkt 7 polskiej ustawy o ochronie danych osobowych.

14 Zob. Explonatory Memorandum – Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD) (Text with EEA relevance), {SEC(2012) 72 final}, {SEC(2012) 73 final}, s. 3 i 5. Obszernie na temat europejskiej debaty w obliczu zmiany unijnej regulacji ochrony danych osobowych zob. zwłaszcza *I. Lipowicz*, Nowe wyzwania, s. 5 oraz *G. Szpor*, Kierunki zmian w ustawodawstwie dotyczącym ochrony danych osobowych, w: *A. Mednis* (red.), Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym, Warszawa 2013, s. 53 i n.

15 Zob. *P. Carey*, Data Protection, s. 103.

kacyjnych[16], takie państwa, jak: Andora, Argentyna, Australia, Kanada, Szwajcaria, Wyspy Owcze, Guernsey, Izrael, Wyspy Man i Jersey oraz Nową Zelandię, a w przeszłości Węgry (przed ich przystąpieniem do UE)[17].

Na owej „białej liście" Komisji Europejskiej nie ma Stanów Zjednoczonych, państwa, o którym *Joanna Braciak* pisze, że jest „ojczyzną prawa do prywatności"[18]. Zatem państwo, w którym narodziła się prywatność, z polskiej (i unijnej) perspektywy uchodzi za niedostatecznie chroniące tę wartość.

Nie oznacza to jednak, że w Stanach Zjednoczonych dziedzina ochrony danych osobowych nie jest poddana regulacji. Przeciwnie, amerykański system prawny cechuje mnogość, różnorodność, ale i fragmentaryczność normatywna omawianej materii; mówi się w tym kontekście o regulacji rozdrobnionej (*patchwork regulation*[19]).

Reakcja prawodawców po obu stronach Atlantyku na zachodzące zmiany otoczenia technologicznego i społecznego w dziedzinie ochrony danych osobowych przybiera różną postać, wywodzącą się z głębokich uwarunkowań historycznych, kulturowych i politycznych.

Prawodawca polski zatem, podobnie jak unijny, dąży do administracyjnoprawnego, powszechnego uregulowania badanej dziedziny, m.in. powołując wyspecjalizowany organ zajmujący się wyłącznie materią ochrony danych osobowych oraz koncentrując w miarę możności materiał normatywny w jednym akcie prawnym znajdującym swoje umocowanie w normie konstytucyjnej.

Inaczej czyni prawodawca amerykański, który wykazuje charakterystyczne podejście sektorowe (branżowe), przy jednoczesnym braku jednolitego aktu prawnego o charakterze generalnym, odpowiadającego swoim zakresem np. polskiej ustawie o ochronie danych osobowych[20] oraz braku organu

---

[16] *C. Kuner*, Transborder Data Flows, s. 65 i n.

[17] Zob. odpowiednio decyzje Komisja Europejskiej http://europa.eu.int/eur-lex/pl/dd/docs/2003/32003D0490-PL.doc (dostęp: 20.6.2003 r.); http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32003D0821:PL:HTML (dostęp: 21.11.2003 r.); http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32002D0002:PL:HTML (dostęp: 20.12.2001 r.); http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32000D0518:PL:HTML (dostęp: 26.7.2000 r.); http://europa.eu.int/eur-lex/pl/dd/docs/2004/32004D0411-PL.doc (dostęp: 28.4.2004 r.).

[18] *J. Braciak*, Prawo do prywatności, Warszawa 2004, s. 30.

[19] *C. Kuner*, Transborder Data Flows, s. 174; *A. Levin, M.J. Nicholson*, Privacy Law in the United States, the EU and Canada: The Allure of the middle Ground, University of Ottava Law, Technology Journal 2005 2:2 UOLTJ 357, s. 360.

[20] Zob. Dokument WP 12 Grupy Roboczej Art. 29: Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document: Transfers of personal

ochrony danych o kompetencjach zbliżonych czy identycznych z przyznanymi np. polskiemu Generalnemu Inspektorowi Ochrony Danych Osobowych[21].

Wymienione różnice systemowe skutkują odmiennym traktowaniem jednostki, która doznała naruszenia swoich danych osobowych mimo istnienia wspólnego systemu wartości – deklarowanego m.in. w obrębie NATO.

Nie ulega zarazem wątpliwości, że transatlantycki przepływ danych osobowych jest „koniecznym warunkiem rozwoju handlu międzynarodowego"[22]. Wobec konfliktowej sytuacji na przestrzeni lat wypracowywane były kompromisowe rozwiązania, mające zapewnić danym pochodzącym z UE minimum bezpieczeństwa w USA. Temu celowi służyło porozumienie wprowadzające program Safe Harbor[23], uchylony jednakże wyrokiem TSUE w dniu 6.10.2015 r. i zastąpiony od 12.7.2016 r. programem Privacy Shield[24]. Uchylenie porozumienia Safe Harbor dobrze ilustruje rozziew pomiędzy politycznymi intencjami a wdrażanymi rozwiązaniami prawnymi. We wspomnianym wyroku Trybunał stwierdził nieważność decyzji Komisji aprobującej program

data to third countries: Applying Articles 25 and 26 of the EU data protection directive, Adopted by the Working Party on 24 July 1998, DG XV D/5025/98.

21 Zob. też *J. Zimmermann*, Aksjomaty prawa administracyjnego, Warszawa 2013, s. 160 i n.

22 Zob. pkt 56 i 57 preambuły dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

23 Porozumienie Safe Harbor zostało zatwierdzone decyzją Komisji Europejskiej 2000/520/WE z 26.7.2000 r., Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance), Dz.Urz. WE L 215 z 28.8.2000 r., s. 7–47, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML (dostęp: 1.6.2017 r.). Wyrokiem z 6.10.2015 r. TSUE stwierdził nieważność powołanej wyżej decyzji Komisji (C-362/14). Szerzej na ten temat zob. *M. Krzysztofek*, Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, Warszawa 2016, s. 241 i n. oraz *C. Kuner*, Reality and Illusion in EU Data Transfer Regulation Post Schrems, Cambridge 2016, http://ssrn.com/abstract=2732346 (dostęp: 1.6.2017 r.).

24 Angielski tekst decyzji Komisji Europejskiej z 12.7.2016 r. (Commission Implementing Decission of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU – US Privacy Shield), C(2016) 4176 final, dostępny jest na stronie internetowej http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf. Szczegółowe zasady Privacy Shield opracowane przez Departament Handlu USA – http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf (dostęp: 1.6.2017 r.).

Safe Harbor[25], stanowiący w swoim założeniu najbardziej uniwersalny i systemowy instrument pozwalający na stosunkowo powszechne przekazywanie danych osobowych z UE do USA. Wyrok Trybunału wywołał nagły kryzys we wzajemnych, niełatwych relacjach.

Legalnemu przekazywaniu danych osobowych z UE do USA służą także kilkakrotnie modyfikowane porozumienia Passanger Name Record (odnoszące się do przekazywania amerykańskim służbom danych podróżnych)[26] czy porozumienia SWIFT (dotyczące transferów pieniężnych[27]). Wskazane rozwiązania cechuje jednak wąsko zarysowany cel, trudno zatem mówić o ich uniwersalnym czy generalnym charakterze.

Dodatkowo obraz komplikuje fakt, że unijna wizja ochrony danych osobowych, wyrażona zwłaszcza w dyrektywie 95/46/WE, staje się międzynarodowym standardem[28]. Obserwowany jest eksport europejskich rozwiązań do in-

---

25 Wyr. Trybunału (Wielka Izba) z 6.10.2015 r., *Maximillian Schrems v. Data Protection Commissioner*, C-362/14.

26 Porozumienie zostało opublikowane w Official Journal of the European Communities L 204 z 4.8.2007 r. (http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2007:204:SOM:EN:HTML). Dnia 3.11.2008 r. opublikowano w polskim Dzienniku Ustaw ustawę z 19.9.2008 r. o ratyfikacji umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Umowa PNR z 2007 r.), sporządzonej w Brukseli 23.7.2007 r. oraz w Waszyngtonie 26.7.2007 r. (Dz.U. Nr 196, poz. 1212). Na temat roli i celów stawianych porozumieniu 2007 PNR zob. także uzasadnienie powołanej ustawy http://orka.sejm.gov.pl/Druki6ka.nsf/0/F7A714E058DD28F5C12574810037057B/$file/720.pdf (dostęp: 1.6.2017 r.).

27 Porozumienie zostało zatwierdzone przez Parlament Europejski w dniu 8.6.2010 r. – zob. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2010-0279+0+DOC+PDF+V0//EN (dostęp: 1.6.2017 r.).

28 *B. Fischer*, Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich, Warszawa 2010, s. 153. Zob. też więcej *A. Monarcha-Matlak*, Proces europeizacji prawa administracyjnego jako prawna droga do Unii Europejskiej, w: *Z. Janku*, *Z. Leoński*, *M. Szewczyk*, *M. Waligórski*, *K. Wojtczak* (red.), Europeizacja polskiego prawa administracyjnego, Wrocław 2005, s. 56–58; *B. Marcinkowski*, Wpływ prawodawstwa unijnego na polską regulację ochrony danych osobowych, w: *I. Lipowicz* (red.), Europeizacja administracji publicznej, Warszawa 2008, s. 222 i powołane tam źródła. Zob. na ten temat *A. Mednis*, Ustawa o ochronie danych osobowych a zagraniczne regulacje w tym zakresie, w: *P. Fajgielski* (red.), Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia, Lublin 2008, s. 77 i n.; *B. Fischer*, *D. Karwala*, Transfer danych osobowych do państwa trzeciego (Wybrane zagadnienia), PiP 2007, z. 1, s. 100 oraz *D. Heisenberg*, Negotiating Privacy. The European Union, The United States, and Personal Data Protection, London 2005, s. 101. Na temat międzynarodowego znaczenia dyrektywy 95/46, w tym zwłaszcza jej oddziaływania na prawodawstwo w Stanach Zjednoczonych oraz Kanadzie, pisze *S. Princen*, EU Regulation and Transatlantic Trade, Haga 2002, s. 327 i 328.

nych krajów[29]. Stopniowe przyjmowanie europejskich standardów w dziedzinie ochrony danych osobowych dotyczy nawet takich krajów jak Japonia, która początkowo skłaniała się ku przyjęciu regulacji zbliżonej do północnoamerykańskich rozwiązań autocertyfikacyjnych, a także krajów, w których kultura *common law* nadal odgrywa znaczącą rolę (Australia, Kanada czy Nowa Zelandia)[30].

W tym kontekście można zatem mówić nawet o postępującej regulacyjnej izolacji Stanów Zjednoczonych, a problem transferu danych osobowych do USA pozostaje systemowo nierozwiązany[31]. Pogłębiający się w skali globalnej dualizm regulacji ochrony danych nie służy pewności obrotu i bezpieczeństwu danych oraz rodzi dodatkowo elementarne dylematy w zakresie prawa właściwego i forum władnego rozstrzygać spory w zakresie transatlantyckich transferów danych osobowych[32].

Niniejsza rozprawa poświęcona jest więc, przede wszystkim, próbie wyjaśnienia przyczyn amerykańskiej negacji unijnego, w tym polskiego, systemu ochrony danych osobowych, a także wskazania dróg umożliwiających osiągnięcie konwergencji pomiędzy systemami unijnymi – obrazowanymi przez pryzmat systemu polskiego – oraz federalnym systemem amerykańskim.

---

[29] Można mówić o efekcie kalifornijskim, tj. przenoszeniu surowych reguł na nowe obszary – zob. *C.J. Bennett*, *C.D. Raab*, The Governance of Privacy. Policy Instruments in Global Perspective, Cambridge, Massachusetts, London 2006, s. 114 i 269–276, wraz ze wskazanymi tam źródłami. Zob. też *A. Mednis*, Ustawa o ochronie danych osobowych, s. 77 i n.; *B. Fischer*, *D. Karwala*, Transfer danych osobowych do państwa trzeciego (Wybrane zagadnienia), PiP 2007, z. 1, s. 100 oraz *D. Heisenberg,* Negotiating Privacy. The European Union, The United States, and Personal Data Protection, s. 101. Na temat międzynarodowego znaczenia dyrektywy 95/46/WE, w tym zwłaszcza jej oddziaływania na prawodawstwo w Stanach Zjednoczonych oraz Kanadzie pisze także *S. Princen*, EU Regulation, s. 327 i 328. Na temat oceny tego zjawiska i jego skutków dla bezpieczeństwa danych zob. np. *P.M. Schwartz*, *J.R. Reidenberg*, Data Privacy Law, s. 205–206, 283 i 341–344; *C.J. Bennett*, Regulating Privacy. Data Protection and Public Policy in Europe and the United States, Ithaca–London 1992, s. 199; *S. Princen*, EU Regulation, s. 5–9 oraz powołane tam źródła.

[30] *C. Kuner* wskazuje także, że dyrektywa 95/46/WE wpłynęła na prawodawstwo takich państw, jak Albania, Bośnia i Hercegowina, Serbia i Szwajcaria, Argentyna, Kolumbia, Peru, Angola czy Maroko, zob. *C. Kuner*, Transborder Data Flows, s. 82.

[31] Dowodem tych starań jest ostateczne zwieńczenie w maju 2016 r. procesu negocjacji Umbrella Agreement (dotyczącego transatlantyckiej wymiany i retencji danych wykorzystywanych przez organy ścigania). Na temat pozycji negocjacyjnej USA w relacjach międzynarodowych zob. np. *P.K. Rosiak*, Stosunek USA do swobody handlu międzynarodowego, w: *C. Mik*, *M. Jeżewski* (red.), Swoboda handlu międzynarodowego w prawie międzynarodowym, Kraków–Warszawa 2013, s. 241.

[32] *C. Kuner*, Transborder Data Flows, s. 160–161 i 165.

Franciszek Longchamps objaśniał, że celem prac badawczych przedstawionych w opracowaniu „Współczesne kierunki w nauce prawa administracyjnego na zachodzie Europy" jest „zbadanie w sposób porównawczy i przedstawienie głównych kierunków, które dziś rysują się w nauce prawa administracyjnego w krajach Europy Zachodniej"[33]. Na tle tak przedstawionego celu dzieła *Longchampsa* zasadne zdaje się twierdzenie, że celem niniejszej rozprawy jest próba zarysowania kierunków dalszych badań umożliwiających osiągnięcie w przyszłości dynamicznej konwergencji i wypracowanie systemowych rozwiązań zapewniających odpowiedni poziom ochrony danych osobowych w USA.

Hipotezę pracy stanowi twierdzenie, że amerykański system prawa federalnego nie zapewnia z punktu widzenia prawa polskiego (jak również szerzej: prawa unijnego) odpowiedniego poziomu ochrony danych osobowych. Hipotezie towarzyszy stwierdzenie, że możliwe jest wypracowanie hybrydowych (niejednorodnych) rozwiązań prawnych, które łącząc m.in. elementy administracyjnoprawne, cywilnoprawne oraz z zakresu prawa międzynarodowego i ponadnarodowego, pozwolą osiągnąć odpowiedni poziom ochrony danych osobowych przekazywanych z Polski (i innych państw Unii Europejskiej) do Stanów Zjednoczonych. Należy jednak założyć ograniczoną uniwersalność i powszechność rzeczonych rozwiązań.

Analizie hipotezy posłuży odpowiedź na postawione niżej pytania badawcze:

1. Jaki jest stosunek zakresów terminów: „dane osobowe" (stosowanego w polskich aktach prawnych, orzecznictwie i piśmiennictwie) oraz „*privacy*" (typowego zwłaszcza dla tradycyjnego piśmiennictwa amerykańskiego) i czy zasadne jest afirmatywne twierdzenie dotyczące występowania systemu ochrony danych osobowych w USA?
2. Jakie – w razie ustalenia, że można mówić o efektywnej prawnej ochronie danych osobowych w USA – metody regulacji tej dziedziny przyjęto w Polsce, a jakie w Stanach Zjednoczonych?
3. Czy, w razie ustalenia, że zasadnie można mówić o prawnej ochronie danych osobowych w USA, możliwe jest wskazanie kluczowych wśród podstawowych zasad przetwarzania danych osobowych przyjętych w Polsce i przyjętych w Stanach Zjednoczonych oraz czy istnieją zasady akceptowane zarówno w systemie polskim, jak i federalnym USA?

[33] *F. Longchamps de Bérier*, w: *J. Boć*, *K. Nowacki* (red.), Współczesne kierunki w nauce prawa administracyjnego na zachodzie Europy, Wrocław 2001, s. 2.

4. Czy i w jakim zakresie polski wzorzec ochrony danych osobowych i skorelowany z nim wymóg oceny odpowiedniości poziomu ochrony danych osobowych w państwie trzecim (USA) można w zasadny sposób stosować w odniesieniu do federalnego systemu amerykańskiego, jak również – w razie stwierdzenia dopuszczalności poddania systemu amerykańskiego temu testowi – jaki będzie wynik badania?
5. Czy polska regulacja i doktryna zawiera elementy, które można uwzględnić, dążąc do osiągnięcia systemowej, transatlantyckiej konwergencji, zwłaszcza wobec przyjęcia przez Unię Europejską ogólnego rozporządzenia o ochronie danych?

Dążąc do zachowania możliwie uniwersalnego i ogólnego charakteru pracy, poza jej zakresem pozostawiono ważkie, choć wyspecjalizowane i cechujące się znacznymi odrębnościami zagadnienia wykorzystywania danych osobowych przez organy powołane do zapobiegania przestępstwom[34]. Podobnie, z konieczności dyktowanej objętością pracy, poza zakresem szczegółowej analizy pozostają szczególne regulacje dotyczące danych medycznych (danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym) i innych danych wrażliwych (zwanych sensytywnymi), ujawniających informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej oraz dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych oraz innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym)[35].

Wspominana dynamika przemian w dziedzinie wykorzystywania danych osobowych, jak i możliwości ich przetwarzania powodują stałą zmianę regulacji prawnych. Już na końcowym etapie prac badawczych przyjęte zostało ogólne rozporządzenie o ochronie danych z 27.4.2016 r. (mające zastosowanie od 25.5.2018 r.) oraz porozumienie pomiędzy UE a USA „Tarcza Prywatności" (Privacy Shield) z 12.7.2016 r. Z uwagi na fundamentalne znaczenie dla przedmiotu niniejszej pracy oba wskazane akty prawne zostały uwzględnione poniżej, przy czym moment ich formalnego przyjęcia wyznacza granice czasowe bezustannie ewoluującego przedmiotu analiz.

---

[34] Zagadnieniom tym poświęcone są m.in. dyrektywy: „policyjna" 2016/680 z 27.4.2016 r. (Dz.U. WE L z 2016 r., Nr 119) oraz PNR 2016/681 z 27.4.2016 r. (Dz.Urz. WE L z 2016 r., Nr 119, s. 132–149), a także porozumienie Umbrella Agreement, wynegocjowane pomiędzy UE a USA w 2015 r., http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (dostęp: 1.6.2017 r.).

[35] Zakres pojęcia danych wrażliwych wskazany zgodnie z normą art. 27 ust. 1 OchrDOU.