Wydział Prawa i Administracji
Uniwersytet Śląski w Katowicach

Wojciech Panek

Ochrona praw i wolności osób, których dane dotyczą w przypadku transferu danych osobowych z Unii Europejskiej do Chińskiej Republiki Ludowej

Rozprawa doktorska przygotowana pod kierunkiem
dr hab. Mariusza Jagielskiego, prof. UŚ
w dyscyplinie nauki prawne

Katowice 2024

SPIS TREŚCI

WYKAZ SKRÓTÓW

APEC – Wspólnota Gospodarcza Azji i Pacyfiku.

CAC – Guojia Hulianwang Xinxi Bangongshi (国家互联网信息办公室) [Chińska Administracja Cyberprzestrzeni].

Chiny – Chińska Republika Ludowa.

c.k.c. – Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Kodeks cywilny Chińskiej Republiki Ludowej] (tekst ogłoszony przez Ogólnochińskie Zgromadzenie Przedstawicieli Ludowych 28.05.2020, data wejścia w życie: 1.01.2021, tekst w wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

CSL – Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Ustawa o cyberbezpieczeństwie Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 07.11.2016, data wejścia w życie: 1.06.2017, tekst w wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

Dyrektywa 2016/680 – 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. UE. L. z 2016 r. Nr 119, str. 89 ze zm.).

Dyrektywa 95/46 – 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. UE. L. z 1995 r. Nr 281, str. 31 ze zm.).

DSL – Zhonghua Renmin Gongheguo shuju Anquan Fa (中华人民共和国数据安全法) [Ustawa o bezpieczeństwie danych Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 10.06.2021, data wejścia w życie: 1.09.2021, tekst w wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

ECtHR – Europejski Trybunał Praw Człowieka.

Europejska Konwencja Praw Człowieka – Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona

następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze. zm.).

Karta Praw Podstawowych – Karta praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 ze. zm.).

Konwencja nr 108 – Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 ze zm.).

MIIT – Zhonghua Renmin Gongheguo Gongye He Xinxi Hua Bu (中华人民共和国工业和信息化部)[Ministerstwo Przemysłu i Technologii Informacyjnych Chińskiej Republiki Ludowej].

MLPS – Multi-level protection system.

MPS – Gongan Bu (公安部) [Ministerstwo Bezpieczeństwa Publicznego].

NIL – Zhonghua Renmin Gongheguo Guojia Qingbao Fa (中华人民共和国国家情报法) [Ustawa o wywiadzie Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 27.04.2018, data wejścia w życie: 27.04.2018, tekst w wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

NSL – Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [Ustawa o bezpieczeństwie narodowym Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 1.07.2015, data wejścia w życie: 1.07.2015, tekst w wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

OECD – Organizacja Współpracy Gospodarczej i Rozwoju.

PIPL – Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Ustawa o ochronie danych osobowych Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 20.08.2021, data wejścia w życie: 1.11.2021, tekst w wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

RODO – 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze. zm.).

SNChRL – Zhonghua Renmin Gongheguo Zuigao Renmin Fayuan (中华人民共和国最高人民法院) [Sąd Najwyższy Chińskiej Republiki Ludowej].

Stały Komitet – Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui (全國人民代表大會常務委員會) [Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych].

TSUE – Trybunał Sprawiedliwości Unii Europejskiej.

TUE – Traktat o Unii Europejskiej (Dz. U. z 2004 r. Nr 90, poz. 864/30 ze. zm.).

Wytyczne CAC dotyczące transferów danych – Shuju Chujing Anquan Pinggu Banfa (数据出境安全评估办法) [Wytyczne oceny bezpieczeństwa transferu danych] (tekst ogłoszony przez Chińską Administrację Cyberprzestrzeni 7.07.2022, data wejścia w życie: 1.09.2022, tekst w wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

Wytyczne w sprawie ochrony danych osobowych OECD – Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r., zmieniona 11 lipca 2013 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami.

WSTĘP

1. Zarys problemu

Międzynarodowy transfer danych osobowych [1] to taka postać przetwarzania danych osobowych [2], która polega na przesłaniu (przekazaniu) danych osobowych z terytorium jednego państwa na terytorium innego państwa. Rozstrzygającym jest przy tym fakt fizycznej zmiany lokalizacji danych osobowych.

Współczesna gospodarka oparta jest o nieustanną wymianę wielorakich informacji (danych)[3]. Aby przedsięwzięcia gospodarcze mogły sprawnie działać, dane m.in. na temat kontrahentów, klientów, pracowników muszą krążyć. Przepływ danych umożliwia także uzyskanie przez przedsiębiorców dostępu do różnorakich rynków, jak i właściwe planowanie oraz zarządzanie produkcją czy łańcuchem dostaw [4]. Rola transferów danych, w tym danych osobowych, jest szczególnie widoczna w przypadku produktów i usług społeczeństwa informacyjnego (IT)[5]. Ich funkcjonowanie jest oparte o nieprzerwaną wymianę danych, także danych osobowych, najczęściej zdeponowanych na wielu serwerach zlokalizowanych w różnych częściach świata[6]. Stąd, dane, w tym

[1] W dalszej części pracy posługuje się skróconą wersją tego terminu, tj. transfer danych osobowych. Zamiennie używam także określenia: przekazywanie danych osobowych, przesył lub przepływ danych osobowych. Za każdym razem mam na myśli międzynarodowe transfery danych osobowych.

[2] Tak: P. Drobek: *Komentarz do art. 44*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, 2018; C. Kuner: *Komentarz do art. 44*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020, s. 762; wątpliwości w odniesieniu do kwalifikacji transferu danych osobowych jako czynności przetwarzania zgłaszają: U. Wuermeling, I. Oldani: *Regulation of International Data Transfers in Clouds: The Impact of the GDPR*. W: *Cloud Computing Law*. Red. C. Millard, Oxford University Press, wyd. 2, Oxford 2021, s. 22; P. Fajgielski: *Komentarz do rozporządzenia nr 2016/679 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)*, *art. 44.* W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.

[3] OECD: *Fostering Cross-Border Data Flows with Trust.* 2022. https://www.oecd.org/publications/fostering-cross-border-data-flows-with-trust-139b32ad-en.htm [dostęp: 10.10.2023], s. 8

[4] World Economic Forum: *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. 05.2020. https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf [dostęp: 11.10.2023], s. 8.

[5] *Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows*. 27.11.2013. https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF [dostęp: 7.10.2021], s. 2.

[6] Podobnie: U. Wuermeling, I. Oldani: *Regulation of International…,* s. 20; także – H.B. Bentzen, O.H. Kvammen, G. Ursin: *Maximizing the GDPR potential for data transfers: first in Europe.* „The Lancet Regional Health - Europe", 2023, nr 27, s. 1 – autorzy podkreślają, że w dobie pandemii Covid-19 wymiana danych miała szczególne znaczenia, czyniąc możliwym natychmiastowe rozpoczęcia badań naukowych w celu poszukiwania środków zaradczych.

także dane osobowe, są traktowane jako siła napędowa gospodarki[7], w konsekwencji czego ich globalne przepływy są nierozerwalnym elementem współczesnej rzeczywistości[8]. To z kolei powoduje, że relacje gospodarcze wywierają bezpośredni wpływ na problematykę prawnej regulacji transferów danych, w szczególności poprzez oczekiwanie, adresowane także w odniesieniu do danych osobowych, że transfery danych będą się odbywały w sposób nieprzerwany i swobodny[9].

Prawo Unii Europejskiej, w tym zwłaszcza RODO, przyjęło restrykcyjne podejście do transgranicznych przepływów danych osobowych. Owa restrykcyjność polega na ograniczeniu dopuszczalności transferów danych osobowych z terytorium Unii Europejskiej na terytorium państw trzecich, a więc poza Europejski Obszar Gospodarczy[10]. Aby transfer danych osobowych z Unii Europejskiej do jednego z państw trzecich był zgodny z RODO, musi wystąpić jedna z okoliczności wskazanych w rozdziale V RODO, przy czym, w myśl art. 44 RODO (…) „wszystkie przepisy niniejszego rozdziału [rozdziału V RODO – dod. aut.] należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu".

Spośród wielu kierunków przeznaczenia danych osobowych, istotne znaczenie ma kierunek chiński. Wszystko za sprawą obecności chińskich produktów i usług na

[7] D. Khan: *Data Flow Challenges to International Trade Law and the Global Economy*. „Indian Journal of Law and Legal Research", 2023, nr 5, str. 3 – dane są wręcz zrównywane z ropą naftową, stąd, zwłaszcza w literaturze popularnonaukowej, można spotkać się z określeniem: "dane to nowa ropa"; także H. Weiden, K. Takase: *Data Privacy in Europe and Its Reception under Japanese Law*. W: *Research Handbook on Information Law and Governance*. Red. S.K. Sandeen, C. Rademacher, A. Ohly. Edward Elgar Publishing, Cheltenham 2021, s. 265.

[8] M. Burri: *Introduction.* W: *Big Data and Global Trade Law*. Red. M. Burri. Cambridge University Press, Cambridge, Cambridge 2021, s. 4.

[9] O czym wspomina: E.D. McKeaver - E.D. McKeaver*: Is It Best Not to Regulate Transborder Data Flow*. „International Business Lawyer", 1984, nr 4, s. 159; także: World Economic Forum: *Data Free Flow*…, s. 9; W.G. Voss: *Cross-Border Data Flows, the GDPR, and Data Governance*. „Washington International Law Journal", 2020, nr 29, s. 516-517; N. Mishra, A.D. Mitchell, E. Sheargold,: *Restrictions on cross-border data transfers*. W: *Principles of International Trade and Investment Law*. Red. A.D. Mitchell, E. Sheargold. Edward Elgar Publishing, Cheltenham 2021; C. Kuner: *The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards*. „National Law Review of India", 2021, nr 1, s. 84; V. Zeno-Zencovich: *Free-Flow of Data. Is International Trade Law the Appropriate Answer?.* W: *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*. Red. F. Fabbrini, E. Celeste, J. Quinn, Hart Publishing, Oxford 2021.

[10] Za państwo trzecie uznaje się powszechnie państwo nienależące do Europejskiego Obszaru Gospodarczego – tak: P. Barta, P. Litwiński, M. Kawecki: *Komentarz do art. 44.* W: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. i swobodnym przepływem takich danych. Komentarz.* Red. P. Barta, P. Litwiński, M. Kawecki. C.H. Beck, Warszawa 2017, s. 629-630; B. Fischer: *Komentarz do art. 44 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentar*z. Red. M. Sakowska-Baryła. C. H. Beck, Warszawa 2018, s. 462; M. Krzysztofek: *Komentarz do art. 44 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C. H. Beck, Warszawa 2016, s. 225; por. także: P. Drobek: *Komentarz do art. 44*….

rynku europejskim. Chiny są znaczącym partnerem gospodarczym Unii Europejskiej. Według danych aktualnych na dzień składania niniejszej pracy do druku[11], Chiny to drugi, po USA, największy partner handlowy Unii Europejskiej.[12] O doniosłości współpracy gospodarczej między Państwem Środka a Unią Europejską świadczy m.in. fakt, że to Chiny były największym eksporterem towarów na terytorium Unii Europejskiej [13]. Powyższe oznacza, że chińskie produkty i usługi są powszechnie wykorzystywane przez mieszkańców Europy. Należy przy tym podkreślić, że obecnie udział Chin w rynku europejskim wiąże się z produktami i usługami związanymi z branżą IT[14] czy usługami e-commerce[15]. Wspólną cechą obu kategorii produktów i usług jest tak zdalne działanie, związane z lokalizacją infrastruktury technicznej poza terytorium Unii Europejskiej, jak i potrzeba dostępu do danych (informacji) o odpowiedniej ilości i jakości. To zaś czyni przekazywanie danych osobowych immanentną cechą współpracy gospodarczej Unii Europejskiej i Chin. Tym samym, dane osobowe użytkowników chińskich towarów lub usług, którzy znajdują się w Unii Europejskiej trafiają na terytorium Chin. Dopuszczalność takiego transferu w świetle art. 44-49 RODO nie jest już oczywista.

Powodem niejednoznacznego statusu transferów danych osobowych z Unii Europejskiej do Chin jest niejasny poziom ochrony danych osobowych w Chinach. W latach 2016–2021 w Chinach miała miejsce reforma prawa, której skutkiem było wdrożeniem do krajowego porządku prawnego nowych przepisów, które m.in. dotyczą zagadnienia ochrony danych osobowych. Ocenia się, że Chin wypracowały oryginalny

[11] Według informacji dostępnych na stronie internetowej Eurostat, aktualizacja danych ma nastąpić w lipcu 2024 r.

[12] *International Trade in Goods by Partner*. 06.2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_in_goods_by_partner [dostęp 24.11.2023].

[13] ibid.; por. także: A. Krstinovska: *For Chinese Companies, Better Access to the EU Single Market Leads through the Western Balkans*. 11.01.2024. https://chinaobservers.eu/for-chinese-companies-better-access-to-the-eu-single-market-leads-through-the-western-balkans/ [dostęp: 17.5.2024]; *Chinese companies see revenue growth in Europe: report*. 15.11.2023. https://english.news.cn/europe/20231115/3aad1c1399ef4054bf7865f505775852/c.html [dostęp; 17.5.2024]

[14] Por. EY Switzerland: *Chinese company takeovers in Europe fall to 12-year low – more investments in Switzerland.* 27.2.2024. https://www.ey.com/en_ch/news/2024/02/chinese-company-takeovers-in-europe-fall-to-12-year-low-more-investments-in-switzerland [dostęp: 17.5.2024]; S. Bu: *Chinese Smart Hardware Brands Flooding Into Europe: How to Divide the Spoils?*. 7.7.2023. https://equalocean.com/analysis/2023070719866 [dostęp: 17.5.2024].

[15] Por. F. Southey: *Alibaba on the 'continued desire' for European brands in China: 'Consumers are willing to pay for quality and provenance'*. 7.11.2023. https://www.foodnavigator.com/Article/2023/11/07/alibaba-on-the-continued-desire-for-european-brands-in-china-consumers-are-willing-to-pay-for-quality-and-provenance [dostęp: 17.5.2024]; por. także: C. Dawson: *Alibaba's Tmall Global takes European Brands into China*. 14.11.2023. https://channelx.world/2023/11/alibabas-tmall-global-takes-european-brands-into-china/ [dostęp: 17.05.2024] – autor wspomina również o otwarciu rynku chińskiego dla europejskich przedsiębiorców za pośrednictwem usług oferowanych przez Alibaba.

system ochrony danych osobowych, motywowany różnymi wartościami, nie tylko potrzebą należytej ochrony praw i wolności jednostki[16].

2. Potrzeba prowadzenia badań

Zakres zmian wprowadzonych w chińskim systemie prawnym poddaje pod wątpliwość wcześniejsze ustalenia w przedmiocie poziomu ochrony danych osobowych w Chinach. Publikacje dotyczące prawa chińskiego związanego z ochroną danych osobowych były nieliczne[17]. Najbardziej kompleksową publikacją[18] była publikacja autorstwa P. de Herta oraz V. Papakonstantinou, która ukazała się w 2015 r[19]. Z uwagi na reformę prawa chińskiego, nie odzwierciedla ona aktualnego stanu prawnego w Chinach[20].

Nowe przepisy prawa chińskiego znacząco zmieniły otoczenie prawne, jednakże, tak jak w przypadku pozostałych reform, z chińską specyfiką[21]. W przypadku prawa ochrony danych osobowych, przejawem chińskiej specyfiki jest wyłącznie instrumentalne znaczenie przepisów prawa[22]. Mają one służyć realizacji innych celów, przede wszystkim zapewnieniu szeroko pojętego bezpieczeństwa narodowego[23].

---

[16] L. Belli, D. Doneda: *Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence*. „International Data Privacy Law", 2022, nr 2, s. 9.

[17] Por. m.in. A. Boram Yang: *China in Global Trade: Proposed Data Protection Law and Encryption Standard Dispute*. „A journal of Law and Policy for the Information Society", 2008, nr 3. Część publikacji powstała również w trakcie reform prawa chińskiego, przez co nie uwzględniają wszystkich zmian wdrożonych przez chińskiego ustawodawcę – por. m.in.: B. Zhao, G.P. Mifsud Bonnici: *Protecting EU Citizens' Personal Data in China: A Reality or a Fantasy?*. „International Journal of Law and Information Technology", 2016, nr 126; J.-A. Lee: *Hacking into China's Cybersecurity Law*. „Wake Forest Law Review", 2018, nr 53.

[18] Autorzy nie ograniczyli się do omówienia tylko jednej z ustaw powiązanych z ochroną danych osobowych, ale przedstawili całokształt ówczesnej regulacji chińskiej, mając na względzie standardy ochrony danych osobowych wynikające z prawa Unii Europejskiej.

[19] Publikacja została stworzona na potrzeby Parlamentu Europejskiego – Sekretariatu Generalnego ds. Polityki Wewnętrznej, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) – por. P. de Hert, V. Papakonstantinou: *The data protection regime in China. In-depth analysis*. Parlament Europejski, Bruksela 2015.

[20] Pomija także nowe podejście do oczekiwanego poziomu ochrony danych osobowych w państwie trzecim, wykształcone w orzecznictwie Trybunały Sprawiedliwości Unii Europejskiej w latach 2015-2020.

[21] E. Pernot-Lepley: *China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU?*. „Penn State Journal of Law and International Affairs", 2020, nr 8, s. 53-54; B. Qu, C. Huo: *Privacy, National Security, and Internet Economy: An Explanation of China's Personal Information Protection Legislation*. „Frontiers of Law in China", 2020, nr 3, s. 364; D. Hanlin: *The System Position and Protection of Personal Information Right in General Provisions of the Civil Law*. „US-China Law Review", 2018, nr 3, s. 153; pośrednio: Y. Shao: *Personal Information Protection: China's Path Choice*. „US-China Law Review", 2021, nr 18, s. 236, 238.

[22] R. Berti: *Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union*. „European Journal of Privacy Law & Technologies", 2020, nr 34, s. 18.

[23] P. Cai, L. Chen: *Demystifying Data Law in China: A Unified Regime of Tomorrow*. „International Data Privacy Law", 2022, nr 5, s. 88-90; D. Hanlin: *The System Position*…, s. 153. W doktrynie podkreśla się, że przejawem znaczenia, bliżej nieokreślonego, bezpieczeństwa narodowego Chin jest rozmiar angażowanych środków finansowych – D. Gershgorn wyjaśnia, że w 2018 r. tzw. budżet na rozwój narzędzi inwigilacji jednego z miast chińskich dorównywał wielkością budżetowi na edukację – por. D. Gershgorn:

Przejawem działania motywowanego zapewnieniem bezpieczeństwa narodowego było narzucenie przedsiębiorcom zagranicznym obowiązku przechowywania danych, w tym danych osobowych, na terenie Chin, co stanowiło odpowiedź na informacje ujawnione przez E. Snowdena[24]. Z tego powodu, w ogólnym ujęciu, ochronę danych osobowych w Chinach łączy się bardziej z ochroną bezpieczeństwa narodowego niż z ochroną praw podstawowych (praw i wolności jednostki)[25].

Obok bezpieczeństwa narodowego Chin, nie bez znaczenia są również interesy gospodarcze oraz związana z tym potrzeba dalszego rozwoju technologicznego. W tym kontekście dane, także osobowe, są traktowane jako niezbędny zasób dla działalności biznesu[26]. Przepisy prawa ochrony danych osobowych nie mogą więc stanowić żadnej przeszkody dla przedsięwzięć gospodarczych [27], jakkolwiek ograniczając konkurencyjność chińskich przedsiębiorstw [28], zwłaszcza na rynku tzw. nowych technologii[29].

W świetle powyższego, prawną ochronę danych osobowych w Chinach traktuje się jako wyraz kompromisu[30], który można opisać jako ograniczanie praw jednostki niemalże w każdej sytuacji uzasadnionej potrzebą ochrony interesu publicznego, o którym była mowa powyżej[31]. Bez wątpienia, taka konstrukcja wykracza poza ramy akceptowalne przez przepisy RODO[32]. Dlatego też, weryfikacja aktualnego poziomu ochrony danych osobowych w Chinach jest zasadna.

China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space The program turns neighbors into agents of the surveillance state. 2.03.2021. https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015 [dostęp: 28.03.2023].

[24] por. J. Liu: *China's data localization*. „Chinese Journal of Communication", 2020, nr 1, s. 89.

[25] Tu na przykładzie ochrony danych wrażliwych – A. Geller: *How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective*. „GRUR International", 2020, nr 69, s. 1195.

[26] P. Cai, L. Chen: *Demystifying Data Law*…, s. 75.

[27] L. Belli, D. Doneda: *Data Protection in*…, s. 3; P. Cai, L. Chen: *Demystifying Data Law*…, s. 88; X. Duoye: *The Civil Code and the Private Law Protection of Personal Information*. „Tsinghua China Law Review", 2020, nr 13, s. 193; także: A. Boram Yang: *China in Global…*, s. 901, 906.

[28] B. Qu, C. Huo: *Privacy, National Security*…, s. 361-363.

[29] Podobnie: Y. Shao: *Personal Information Protection*…, s. 228, 235.

[30] R. Creemers: *China's Emerging Data Protection Framework*. „Journal of Cybersecurity", 2022, nr 1, s. 3.

[31] Por. X. Fei: *National Security Considerations in China's Trade Legislations: Offensive or Defensive?*. „US-China Law Review", 2022, nr 19, s. 189, 193.

[32] A. Geller: *How Comprehensive Is*…, 1198; także: B. Zhao, F. Yang: *Mapping the development of China's data protection law: Major actors, core values, and shifting power relations*. „Computer Law & Security Review", 2021, nr 40, s. 10; B. Zhao: *Connected Cars in China: Technology, Data Protection and Regulatory Responses*. W: *Grundrechtsschutz im Smart Car. DuD-Fachbeiträge*. Red. A. Roßnagel, G. Hornung. Springer Vieweg, Wiesbaden 2019, s. 14; J. Wang wyjaśnia, że powodem wątpliwej skuteczności zagranicznych orzeczeń w Chinach jest podejście władz chińskich do zasady wzajemności uznawania orzeczeń – J. Wang: *Dispute Settlement in the Belt and Road Initiative: Progress, Issues, and Future Research Agenda*. „The Chinese Journal of Comparative Law", 2020, nr 1, s. 13-14; także: J. Huang: *Reciprocal Recognition and Enforcement of Foreign Judgments in China: The Proposal of a Registration*

Istotnym zagadnieniem stają się zatem skutki, jakie poziom ochrony danych osobowych w Chinach wywiera na pozycję osób, których dane dotyczą w sytuacji przekazania ich danych osobowych na terytorium Chin [33]. Jak zauważają C. Docksey i H. Hijmans, mając na względzie m.in. problematykę dostępu organów państwa (także organów ściągania) do danych osobowych przekazywanych na terytorium państwa trzeciego, podmioty dokonujące owego przekazania same nie mogą wiele zdziałać [34]. Co więcej, pozycja podmiotów prywatnych w Chinach jest o tyle skomplikowana, że władze chińskie *de facto* dysponują nieograniczonymi uprawnieniami kontrolnymi, za pośrednictwem których mogą realizować aktualne cele natury politycznej[35].

W tej sytuacji pojawiły się pomysły, aby wszelkie zagrożenia dla praw i wolności osoby, której dane dotyczą wyeliminować poprzez zakaz transferów danych osobowych na terytorium Chin[36]. Takie kroki podjęły władze amerykańskie w związku ze sporem dotyczącym działalności ByteDance (operator aplikacji TikTok), a w szerszym ujęciu, w celu przeciwdziałania dostępowi władz chińskich do danych obywateli amerykańskich[37]. Władze USA podkreślają, że w istocie rzeczy takie podmioty jak ByteDance umożliwiają władzom chińskim wykorzystywać dane użytkowników zgodnie z ich celami[38]. Jako że te cele mogą zagrażać bezpieczeństwu narodowemu USA, zakaz

System. W: *Commercial Issues in Private International Law: A Common Law Perspective*. Red. M. Douglas, M. Keyes, A. Dickinson. Hart Publishing, Oxford 2019, s. 134-135.

[33] OECD: *Fostering Cross-Border Data*…, s. 8-9; por. także: M. Broersma: *Council Of Europe Warns Over Data Protection Rights*. 30.01.2023. *silicon.co.uk* LexisNexis, [dostęp: 22.09.2023] – autor wyjaśnia, że można wręcz mówić o wzroście świadomości jednostek w odniesieniu do konsekwencji transferu danych osobowych poza terytorium Unii Europejskiej.

[34] C. Docksey, H. Hijmans: *The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law*. „European Data Protection Law Review", 2019, nr 5, s. 311.

[35] Human Rights Watch: *Letter to House Committee on Energy and Commerce*. 16.03.2023. https://www.hrw.org/sites/default/files/media_2023/03/Letter%20to%20House%20Committee%20on%20TikTok%20-%20web.pdf [29.03.2023], s. 1 i n.

[36] Jednym z takich pomysłów jest wykorzystanie prawidłowej anonimizacji danych osobowych – na temat anonimizacji jako alternatywnej ścieżki dla przekazywania danych do państw trzecich - L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses for cross-border transfers of health data after Schrems II*. „Journal of Law and the Biosciences", 2021, nr 1, s. 9.

[37] Por. C. Zweifel-Keegan: *A new era of US privacy policy? National security restrictions on personal data transactions*. 4.03.2024. https://iapp.org/news/a/a-new-era-of-u-s-privacy-policy-national-security-restrictions-on-personal-data-transactions/ [dostęp: 20.05.2024]; C. Zweifel-Keegan: *A view from DC: US House ready to pass data broker bill*. 15.03.2024. https://iapp.org/news/a/a-view-from-dc-us-house-is-ready-to-pass-a-data-broker-bill/ [dostęp: 20.05.2024].

[38] The Committee on Energy and Commerce: *Experts Agree: ByteDance is Beholden to the CCP and Cannot Be Allowed to Exploit Americans' Data*. 7.03.2024. https://energycommerce.house.gov/posts/experts-agree-byte-dance-is-beholden-to-the-ccp-and-cannot-be-allowed-to-exploit-americans-data [dostęp: 20.05.2024].

transferu danych osobowych amerykańskich użytkowników chińskich aplikacji do Chin jest uzasadniony[39].

W mojej ocenie takie podejście jest całkowicie zrozumiałe i niekiedy może okazać się najlepszą gwarancją właściwej ochrony praw i wolności jednostki[40]. Jednakże, mając na względzie interesy podmiotów żywo zainteresowanych utrzymaniem relacji gospodarczych z Chinami oraz (oczekiwaną) swobodą przekazywania danych, w tym danych osobowych, do państw trzecich w każdych okolicznościach[41], nie da się całkowicie wyeliminować transferów danych osobowych do Chin. To właśnie tych transferów dotyczy moja rozprawa doktorska.

3. Pytania badawcze

Główne pytanie badawcze tej rozprawy doktorskiej jest następujące: w jaki sposób należycie zabezpieczyć prawa i wolności osób, których dane dotyczą, o których mowa w RODO, w sytuacji transferu ich danych osobowych z terytorium znajdującego się w Unii Europejskiej na terytorium Chin?

Główne pytanie badawcze opiera się na założeniu, że poziom intensywności współpracy gospodarczej Unii Europejskiej, a zarazem jej poszczególnych członków, z Chinami uniemożliwia całkowite wyeliminowanie transferów danych osobowych do Chin[42]. W tym względzie, inspiracją dla moich badań jest dorobek wypracowany w ramach współpracy USA i Unii Europejskiej, gdzie doniosłość współpracy gospodarczej oraz relacji politycznych przyczyniła się do wypracowania kompromisu i stworzenia mechanizmu swobodnego przekazywania danych osobowych, którego istotą jest próba zagwarantowania należytej ochrony praw i wolności osób, których dane dotyczą.

---

[39] Ibidem.

[40] Niemniej jednak oznacza to zwrot w kierunku wprowadzenia obowiązku lokalnego przechowywania danych, tzw. data localisation – tak: OECD: *Fostering Cross-Border Data*…, str. 30; por. także: L. Bertuzzi: *Is data localization coming to Europe?*. 23.8.2022. https://iapp.org/news/a/is-data-localization-coming-to-europe [dostęp: 24.05.2024] – autor sugeruje, że zainteresowanie obowiązkiem lokalnego przechowywania danych osobowych można dostrzec w działaniach władz Unii Europejskiej.

[41] Por. także: Allen & Overy: *Global policy makers take further steps to support data free flow with trust*. 19.05.2023. https://www.jdsupra.com/legalnews/global-policy-makers-take-further-steps-2406526/ [dostęp: 11.10.2023].

[42] Por. m.in.: The Diplomatic Service of the European Union: *EU-China Relations factsheet*. 7.12.2023. https://www.eeas.europa.eu/eeas/eu-china-relations-factsheet_en [dostęp: 20.05.2024]; C. Soong: *Expert opinions about EU-China relations in 2024*. 25.01.2024. https://merics.org/en/comment/expert-opinions-about-eu-china-relations-2024 [dostęp: 20.05.2024]; Q. Xijia, C. Qingrui: *China signs 18 deals with France to expand economic cooperation, opening up wider for France, Europe*. 7.05.2024. https://www.globaltimes.cn/page/202405/1311825.shtml [dostęp: 20.05.2024]; także: C. Kuner: *Reality and Illusion in EU Data Transfer Regulation Post Schrems*. „German Law Journal", 2017, nr 4, s. 884-885 – autor uważa, że obecnie można mówić o podtrzymywaniu mitu, jakoby prawo Unii Europejskiej, samoistnie, było w stanie urzeczywistnić swobodę transferu danych osobowych, połączoną ze skuteczną ochroną praw i wolności jednostek.

W celu wypracowania odpowiedzi na główne pytanie badawcze postawiłem następujące pytania pomocnicze:

(P.1) Czy kryteria oceny systemu prawnego państwa trzeciego wynikają z przepisów RODO?

(P.2) Czy, a jeśli tak to jakie, czynniki pozaprawne wpływają na interpretację i stosowanie kryteriów oceny systemu prawnego państwa trzeciego?

(P.3) Jaki poziom ochrony danych osobowych zapewniają przepisy prawa chińskiego, poddane analizie w oparciu o kryteria oceny systemu prawnego państwa trzeciego?

(P.4) Czy poziom ochrony danych osobowych, zapewniany przez przepisy chińskiego prawa ochrony danych osobowych, wyklucza uzyskanie przez Chiny decyzji w sprawie adekwatności w rozumieniu art. 45 ust. 1 RODO?

(P.5) Czy odpowiednie zabezpieczenia w rozumieniu art. 46 RODO lub odstępstwa, o których mowa w art. 49 RODO, stosowane w sytuacji transferu danych osobowych między Unią Europejską a Chinami, gwarantują ochronę praw i wolności osób, których dane dotyczą?

(P.6) Czy pomimo istnienia różnic w poziomie ochrony danych osobowych w Chinach i Unii Europejskiej, dla zapewniania należytej ochrony praw i wolności osób, których dane dotyczą, możliwe jest zawarcie porozumienia międzynarodowego między Unią Europejską a Chinami, na wzór porozumień zawieranych między Unią Europejską a USA, w celu regulacji przekazywania danych osobowych?

4. Struktura pracy

Rozprawa doktorska składa się ze wstępu, trzech rozdziałów oraz zakończenia.

We wstępie omawiam problem badawczy, pytania badawcze oraz metodologię przeprowadzonych badań.

Rozdział I dotyka problematyki oceny systemu prawnego państwa trzeciego. Celem tego rozdziału jest rekonstrukcja kryteriów oceny systemu prawnego ważnych z perspektywy przepisów RODO. W pierwszej kolejności omawiam kryteria oceny wykorzystywane podczas oceny systemu prawnego państwa trzeciego na podstawie przepisów Dyrektywy 95/46, w tym także w odniesieniu do oceny porozumień w sprawie transferów danych osobowych z Unii Europejskiej do USA. Następnie, przedstawiam kryteria oceny systemu prawnego państwa trzeciego, które wynikają z RODO. W ramach rozdziału I udzielam odpowiedź na pierwsze i drugie pytanie pomocnicze (P.1 oraz P.2).

W rozdziale II przeprowadzam ocenę systemu ochrony danych osobowych, który wynika z przepisów prawa chińskiego po reformie z lat 2016-2021. W oparciu

o kryteria oceny systemu prawnego państwa trzeciego, ustalone w rozdziale I, poddaję analizie przepisy prawa chińskiego powiązane z ochroną danych osobowych. Wyjaśniam także relacje jakie zachodzą pomiędzy poszczególnymi ustawami dotyczącymi ochrony danych osobowych w Chinach. W dalszej kolejności oceniam poziom ochrony danych osobowych zapewniany przez przepisy prawa chińskiego, mając na uwadze standard ochrony danych osobowych wynikający z przepisów prawa Unii Europejskiej, odpowiadając na trzecie i czwarte pytanie badawcze (P.3 i P.4).

Rozdział III składa się z dwóch części. Część pierwsza, w której udzielam odpowiedzi na pytanie piąte (P.5), skupia się na ocenie kompatybilności odpowiednich zabezpieczeń w rozumieniu art. 46 RODO lub odstępstw, o których mowa w art. 49 RODO dla transferów danych osobowych między Unią Europejską a Chinami. W związku tym, dokonuję przeglądu oraz analizy treści polityk prywatności wybranych podmiotów chińskich działających na terytorium Unii Europejskiej. Wyniki przeprowadzonej analizy zestawiam z poglądami doktryny.

Druga część rozdziału III jest poświęcona koncepcji porozumienia legalizującego przekazywanie danych osobowych do państw trzecich. Na przykładzie porozumień zawieranych między Unią Europejską a USA, omawiam m.in. przesłanki ich wykorzystania przez Komisję Europejska oraz wymagania treściowe, formułowane przez doktrynę. W dalszej części rozdziału III przedstawiam argumenty przemawiające za możliwością wykorzystania porozumienia legalizującego przekazywanie danych osobowych między Unią Europejską a Chinami, jak również formułuję pożądany zakres treściowy takiego porozumienia, mając na uwadze niedociągnięcia chińskiego systemu ochrony danych osobowych, wskazane w rozdziale II. Tym samym, udzielam odpowiedzi na pytanie szóste (P.6).

W zakończeniu udzielam odpowiedzi na główne pytanie badawcze w oparciu o wnioski sformułowane w rozdziałach I-III.

5. Metodologia badań

Badania opisane w tej rozprawie doktorskiej zostały przeprowadzone z wykorzystaniem metod dogmatycznej oraz komparatystycznej.

Metoda dogmatyczna posłużyła do przeprowadzenia analizy zgromadzonego materiału badawczego. Na materiał badawczy składały się akty prawa Unii Europejskiej, w szczególności RODO oraz prawa chińskiego, tj. m.in. CSL, DSL, c.k.c., PIPL. Analiza aktów prawnych została dokonana w świetle literatury i orzecznictwa.

Obok stanowisk przedstawicieli doktryny, zawartych w literaturze naukowej, analizie został poddany także dorobek europejskich organów ochrony danych osobowych, w szczególności wytyczne i opinie Europejskiej Rady Ochrony Danych Osobowych i Europejskiego Inspektora Danych Osobowych związane z problematyką transferów danych osobowych. Analizie zostały poddane także dokumenty związane z oceną systemu prawnego państwa trzeciego w ramach procedury wydawania decyzji w sprawie adekwatności, tj. decyzje w sprawie adekwatności wraz z dokumentacją towarzyszącą, opracowaną przez Europejską Radę Ochrony Danych Osobowych, Europejskiego Inspektora Danych Osobowych, Komisję Europejską oraz Parlament Europejski tak na etapie pierwotnej oceny systemu prawnego państwa trzeciego, jak i w ramach okresowych przeglądów funkcjonujących decyzji w sprawie adekwatności, w szczególności decyzji w sprawie adekwatności USA.

Orzecznictwo stanowiło orzecznictwo TSUE w sprawie transferów danych osobowych, zwłaszcza, decyzji w sprawie adekwatności USA.

Dla prawidłowej analizy przepisów prawa chińskiego istotne znaczenie miały spostrzeżenie doktryny, które legły u podstaw zidentyfikowaniu katalogu ustaw regulujących ochronę danych osobowych w Chinach po 2016 r. W odniesieniu do ustawodawstwa chińskiego, związanego z dostępem organów ścigania do danych osobowych, wybór właściwych przepisów ułatwiło opracowanie sporządzone na potrzeby Parlamentu Europejskiego[43]. Aktualnie obowiązujące teksty ustawodawstwa chińskiego zostały pozyskane z bazy danych uniwersytetu pekińskiego, do której miałem dostęp w okresie luty 2023 - luty 2024[44].

Dla uzyskania całościowego obrazu chińskiego porządku prawnego, analiza uwzględniała zarówno dorobek przedstawicieli doktryny afiliowanych przy zachodnich jak i przy chińskich ośrodkach badawczych. Pomocne okazały się również opracowania organizacji związanych z ochroną praw człowieka, jak również artykuły popularnonaukowe i artykuły z prasy, w szczególności na temat zakresu dostępu władz chińskich do danych osobowych.

Nadto, analizowany materiał badawczy stanowiły polityki prywatności wybranych podmiotów chińskich, oferujących swoje produkty i usługi na terytorium Unii Europejskiej tj. Xiaomi, Huawei, ZTE, Hisense, Haier, Oppo, TikTok, Aliexpress, Tencent, QQ, Baidu, WeChat oraz Weixin, będącej wersją Wechat działającą na

[43] J. Czarnocki, F. Giglio, E. Kun, M. Petik, S. Royer: *Government access to data in third countries. Final report*. Milieu Consulting SRL, European Data Protection Board, Bruksela 2021.
[44] https://www.pkulaw.com

terytorium Chin. Powodem wyboru właśnie tych podmiotów była ich popularności oraz rozmiar działalności prowadzonej na rynku europejskim[45].

Metoda komparatystyczna została wykorzystana do porównania chińskich przepisów prawa, stanowiących źródło ochrony danych osobowych w Chinach z przepisami prawa Unii Europejskiej. Na potrzeby tej oceny, uzupełniająco, uwzględniłem poglądy prezentowane przez przedstawicieli nauki amerykańskiej. Wyniki porównania obu systemów prawnych posłużyły do oceny chińskiego systemu ochrony danych osobowych na tle standardów prawa Unii Europejskiej, a zwłaszcza RODO.

Przedmiot badań opisanych w tej rozprawie doktorskiej spowodował, że zasadniczą rolę odgrywały źródła w języku angielskim, co tyczy się także literatury i prawodawstwa chińskiego. To właśnie językiem angielskim posługiwali się przedstawiciele doktryny, którzy omawiali zagadnienie ochrony danych osobowych w prawie chińskim. Z tego względu, na potrzeby badań wykorzystałem chińskie akty prawne w wersji dwujęzycznej, tj. zarówno w języku angielskim, jak i języku chińskim, które pozyskałem z bazy uniwersytetu pekińskiego[46]. Język chiński (mandaryński) stanowił język uzupełniający, którym posługiwałem się dla rozwiania wątpliwości interpretacyjnych przepisów prawa chińskiego[47].

Badania opisane w tej rozprawie doktorskiej są powiązane z projektem pt. „Przekazywanie danych osobowych pomiędzy Unią Europejską a Chińską Republiką Ludową. Aspekty prawne", który jest finansowany ze środków Narodowego Centrum Nauki w ramach konkursu Preludium-19[48].

Rozprawa uwzględnia stan prawny na 4 czerwca 2024 r.

---

[45] T. Alsop: *Most valuable technology brands worldwide 2023*. 7.03.2024. https://www.statista.com/statistics/267966/brand-values-of-the-most-valuable-technology-brands-in-the-world/ [dostęp: 17.05.2024]; L.L. Thomala: *Most valuable Chinese brands by Brand Finance 2023*. 19.01.2024. https://www.statista.com/statistics/259063/most-valuable-chinese-brands/ [dostęp: 17.05.2024]; A. Gburek: *Świat według chińczyków (raport)*. 5.02.2024. https://geekweek.interia.pl/raport-swiat-wedlug-chinczykow/news-tania-chinszczyzna-te-produkty-podbijaja-swiat-i-sa-dobrej-j,nId,7307968 [dostęp: 17.05.2024]; S. Bu: *Chinese Smart Hardware*…; L. Nan: *TikTok, Huawei, Lenovo lead Kantar's China top 50 global brands ranking*. 6.07.2023. https://jingdaily.com/posts/tiktok-huawei-lenovo-lead-kantars-china-top-50-global-brands-ranking [dostęp: 17.05.2024]; K. Kucharczyk: *Chiny podbijają rynek IT*. 3.10.2018. https://cyfrowa.rp.pl/it/art18011891-chiny-podbijaja-rynek-it [dostęp: 17.05.2024]; J. Qian, I. Chu, P. Kirby i in.: *Leading Chinese cross-border brands The Top 50*. [Dokument elektroniczny], KPMG, 2018, s. 8-10; C. Liu: *Chinese brands make a mark in Europe*. 6.03.2016. https://www.chinadaily.com.cn/kindle/2016-03/06/content_23758762.htm [dostęp: 17.05.2024].

[46] https://www.pkulaw.com

[47] Zapis bibliograficzny chińskich aktów prawnych odpowiada powszechnie stosowanym zasadom – por. P. Kossof: *Chinese legal research.* Carolina Academic Press, Durham, Karolina Północna 2014, s. 67 i n.

[48] Umowa nr UMO-2020/37/N/HS5/01799.

ROZDZIAŁ PIERWSZY
KRYTERIA OCENY SYSTEMU PRAWNEGO PAŃSTWA TRZECIEGO

1. Wprowadzenie

Transfer danych osobowych jest immanentnie związany ze zmianą terytorium, na którym znajdują się dane osobowe. Wraz ze zmianą fizycznego położenia danych osobowych zmienia się ich otoczenie prawne, gwarantujące pewien poziom ochrony danych osobowych, a zwłaszcza ochrony praw i wolności osoby, której dane dotyczą. Prawo Unii Europejskiej, a więc przede wszystkim RODO, wymaga, aby poziom ochrony danych osobowych zapewniany przez jego przepisy był co do zasady niezmienny. W pewnym uproszczeniu oznacza to, że przekazanie danych osobowych z państwa A do państwa B nie powinno negatywnie wpłynąć na pozycję jednostki i ochronę jej praw i wolności związanych z danymi osobowymi[49]. Co oczywiste, przedstawiony scenariusz dotyczy wyłącznie przekazywania danych osobowych z terytorium państwa członkowskiego Unii Europejskiej do państwa trzeciego, jako że transfery wewnątrzunijne korzystają z domniemania jednolitego poziomu ochrony danych osobowych[50].

Syntetyczny opis zasady przekazywania danych osobowych do państw trzecich, o którym mowa powyżej, znajduje obecnie pełne odzwierciedlenie w przepisach rozdziału V RODO, a zwłaszcza w jego art. 44. Zgodnie z treścią art. 44 RODO transfer danych osobowych do państwa trzeciego lub do organizacji międzynarodowej nie może powodować naruszenia stopnia ochrony osób fizycznych, który jest gwarantowany przepisami RODO. Tym samym, nie ma znaczenia wybór narzędzia legalizacji transferów danych osobowych, o których mowa w art. 45-49 RODO. Za każdym razem transfer danych osobowych do państwa trzeciego ma się odbywać tylko w takich warunkach, w których nie dojdzie do naruszenia minimalnego, oczekiwanego przez przepisy RODO poziomu ochrony danych osobowych. Można więc mówić o swego rodzaju zakazie przekazywania danych osobowych, który zostaje uchylony pod warunkiem ustalenia lub zapewnienia w państwie trzecim odpowiedniego poziomu

[49] P. Fajgielski: *Komentarz do rozporządzenia nr 2016/679 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)*, *art. 44*….
[50] Por. m.in. motyw 10 RODO.

ochrony danych osobowych [51] . Określenie co należy rozumieć pod pojęciem odpowiedniego poziomu ochrony danych osobowych w państwie trzecim i w jaki sposób należy go wyznaczyć jest więc kluczowe.

Przyjmuje się, że katalog środków legalizujących transfery danych ma postać hierarchiczną, tzn., że kolejność, środków legalizujących transfery danych w rozdziale V RODO nie jest przypadkowa, a odzwierciedla oczekiwaną hierarchię[52]. W pierwszej kolejności należy więc skorzystać z decyzji w sprawie adekwatności (jeśli została wydana dla danego państwa trzeciego), a dopiero następnie, gdy brak takiej decyzji, z jednego z odpowiednich zabezpieczeń, o których mowa w art. 46 RODO. Jedynie wyjątkowych przypadkach można rozważyć posłużenie się katalogiem odstępstw, o których mowa w art. 49 RODO.

Spośród wymienionych środków legalizujących transfery danych, tylko decyzja w sprawie adekwatności wiąże się z oceną poziomu ochrony danych osobowych w państwie trzecim. Jest to jedyne, oficjalne potwierdzenie poziomu ochrony danych osobowych w konkretnym państwie trzecim. Na podstawie przeprowadzonej oceny systemu prawnego państwa trzeciego, Komisja Europejska stwierdza, że zapewnia on adekwatny poziom ochrony danych osobowych. Dla administratorów danych osobowych i podmiotów przetwarzających oznacza to, że w ramach operacji przekazywania danych osobowych na terytorium takiego państwa (lub do takiej organizacji międzynarodowej) nie jest potrzebna dodatkowa weryfikacja poziomu ochrony danych osobowych.

Kryteria oceny związane z decyzją w sprawie adekwatności zawiera art. 45 ust. 2 RODO. Jednakże, zapoznając się ze stanowiskami przedstawicieli doktryny, jak również z treścią wydanych dotychczas decyzji w sprawie adekwatności pojawiają się wątpliwości, co do faktycznego zakresu i treści oceny systemu prawnego państwa trzeciego. Dość wskazać zróżnicowane poglądy doktryny na temat roli, jaką odgrywa podczas oceny systemu prawnego państwa trzeciego art. 45 ust. 2 RODO. S. Sharma, uważa, że posługiwanie się kryteriami, o których mowa w art. 45 ust. 2 RODO jest obligatoryjne[53]. Przeciwny pogląd prezentuje J. Wagner, dla którego RODO nie zawiera kryteriów pozwalających na ustalenie adekwatności poziomu ochrony danych osobowych w państwie trzecim[54].

[51] C. Kuner zauważa, że w przypadku standardu adekwatności mowa raczej o celu politycznym niż o zasadzie prawa ochrony danych osobowych - C. Kuner: *Developing an Adequate Legal Framework for International Data Transfers*. W: *Reinventing Data Protection?*. Red. S. Gutwirth, Y. Poullet, P. de Hert i in. Springer Science+Business Media B.V., [b.m.w.] 2009, s. 267.

[52] P. Drobek: *Komentarz do art. 44*…; C. Kuner: *Komentarz do art. 44*…, s. 764-765.

[53] S. Sharma: *Data Privacy and GDPR Handbook*. Wiley, Hoboken, New Jersey 2019, s. 162–63.

[54] J. Wagner: *The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection*?. „International Data Privacy Law", 2018, nr 8, s. 319.

J. Wagner uważa, że treść art. 45 RODO daje niewiele wskazówek w przedmiocie ustalenia czy państwo trzecie jest adekwatne, ponieważ treść przepisu stanowią wskazanie zakresu prawa i orzecznictwa potrzebnego do oceny oraz zakreślenie wymagań stawianych prawu państwa trzeciego[55]. Nie bez znaczenia jest również problematyka wpływu czynników pozaprawnych na ocenę systemu prawnego państwa trzeciego. Zdaniem C. Kunera, proces związany z wydawaniem decyzji w sprawie adekwatności, a więc także i ocena poziomu ochrony danych osobowych w państwie trzecim, nie jest wolny od wpływu okoliczności natury politycznej[56].

Celem rozdziału pierwszego rozprawy doktorskiej jest ustalenie jaki jest oczekiwany poziom ochrony danych osobowych w państwie trzecim oraz z wykorzystaniem jakich kryteriów należy dokonać oceny tego poziomu, a także weryfikacja wpływu czynników pozaprawnych na stosowanie tychże kryteriów. Tym samym, w rozdziale pierwszym zostanie udzielona odpowiedź na dwa pytania badawcze (P.1), „Czy kryteria oceny systemu prawnego państwa trzeciego wynikają z przepisów RODO?" oraz (P.2) „Czy, a jeśli tak to jakie, czynniki pozaprawne wpływają na interpretację i stosowanie kryteriów oceny systemu prawnego państwa trzeciego?".

2. Ocena poziomu ochrony danych osobowych w państwie trzecim na podstawie przepisów Dyrektywy 95/46

Analiza problematyki oceny systemu prawnego państwa trzeciego na podstawie RODO rozpoczyna się od okresu obowiązywania Dyrektywy 95/46. To właśnie w tym czasie została wypracowana praktyka oceny systemu prawnego państwa trzeciego, która wywarła przemożny wpływ na treść katalogu kryteriów wskazanych w art. 45 ust. 2 RODO[57]. Ponadto, decyzje w sprawie adekwatności wydane na podstawie przepisów Dyrektywy 95/46, mimo jej uchylenia i zastąpienia przez RODO, pozostały w mocy[58]. Ich treść odzwierciedla więc ewolucję oczekiwań Komisji Europejskiej względem systemów prawnych państw trzecich, jak również stanowi wskazówkę interpretacyjną dla wykładni art. 45 ust. 2 RODO. Z tego względu, w pierwszej kolejności zostaną omówione

[55] Ibidem, s. 321.
[56] C. Kuner: *Developing an Adequate*…, s. 267; podobnie m.in.: S. Sharma: *Data Privacy and*…, s. 164
[57] O czym szerzej będzie mowa w dalszej części tego rozdziału.
[58] Por. art. 45 ust. 9 RODO. 15 stycznia 2024 r. Komisja Europejska opublikowała raport z oceny funkcjonowania decyzji w sprawie adekwatności wydanych na podstawie przepisów Dyrektywy 95/46 (treści raportu zostanie omówiona w dalszej części tego rozdziału). Komisja Europejska potwierdziła, że Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Wyspa Man, Izrael, Jersey, Nowa Zelandia, Szwajcaria oraz Urugwaj zapewniają adekwatny poziom ochrony danych osobowych, w związku z czym decyzje pozostają w mocy.

kryteria oceny systemu prawnego państwa trzeciego, które były stosowana na podstawie Dyrektywy 95/46.

Dyrektywa 95/46 przewidywała, że zasadniczym i jedynym warunkiem, jaki musiało spełniać państwo trzecie, aby transfer danych osobowych na jego terytorium był dopuszczalny, było zapewnienie odpowiedniego poziomu ochrony danych osobowych. Ustalenie tego poziomu było zadaniem Komisji Europejskiej, w ramach procedury związanej z wydaniem decyzji w sprawie adekwatności. Co do zasady, Komisja Europejska miała dokonać analizy i oceny systemu prawnego państwa trzeciego z wykorzystaniem kryteriów wynikających z art. 25 ust. 2 Dyrektywy 95/46, tj. w oparciu o:

a) kryterium charakteru danych,
b) kryterium celu i czasu trwania operacji przetwarzania danych,
c) kryterium kraju pochodzenia danych i kraju ostatecznego przeznaczenia danych,
d) kryterium przepisów prawa państwa trzeciego,
e) kryterium przepisów zawodowych i środków bezpieczeństwa w państwie trzecim.

2.1. Ocena systemu prawnego państwa trzeciego w decyzjach w sprawie adekwatności wydanych na podstawie Dyrektywy 95/46

W okresie obowiązywania Dyrektywy 95/46 Komisja Europejska wydała jedenaście decyzji w sprawie adekwatności[59] oraz dwie decyzje w sprawie adekwatności związane z transferem danych do USA[60]. Procedura związana z wydaniem decyzji przez Komisję Europejską składała się z dwóch elementów: opinii Grupy Roboczej art. 29 oraz decyzji Komisji Europejskiej. O ile podstawą całej procedury były przepisy Dyrektywy 95/46, w tym przywołany art. 25, o tyle bezpośrednie stosowanie kryteriów wynikających z art. 25 ust. 2 nie miało miejsca. W opiniach wydawanych przez Grupę Roboczą art. 29 w związku z postępowaniem w sprawach decyzji[61], wyłącznym punktem odniesienia dla

[59] *Adequacy Decisions*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. [dostęp: 14.09.2021].
[60] Przy czym obie decyzje zostały unieważnione przez TSUE, o czym mowa w dalszej części tego rozdziału.
[61] Grupa Robocza art. 29: *Opinion No 5/99 on The Level of Protection of Personal Data in Switzerland*. 7.06.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp22_en.pdf [dostęp: 27.04.2021], s. 3; pośrednio: Grupa Robocza art. 29: *Opinion 6/99 Concerning The Level of Personal Data Protection in Hungary*. 7.09.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp24_en.pdf [dostęp: 12.05.2021], s. 3; Grupa Robocza art. 29: *Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act*. 26.01.2001. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf [dostęp: 27.04.2021], s. 3; Grupa Robocza art. 29: *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*. 26.01.2001. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp40_en.pdf [dostęp: 27.04.2021], s. 4–6; Grupa Robocza art. 29: *Opinion 4/2002 on the Level of Protection of Personal Data in Argentin*a. 3.10.2002.

oceny systemu prawnego państwa trzeciego były kryteria i wytyczne sformułowane w dokumencie WP12[62]. Pozornie, nieco inne kryteria znalazły zastosowanie opiniach Grupy Roboczej art. 29 dotyczących z przekazywaniem danych osobowych pasażerów poza terytorium UE[63]. Jednak także i tym przypadku, wymagania stawiane systemowi prawnemu państwa trzeciego przez Grupę Roboczej art. 29 odpowiadały kryteriom zawartym w dokumencie WP12[64].

W przypadku właściwych decyzji w sprawie adekwatności, wyjaśnienie sposobu w jaki ustalono poziom ochrony danych osobowych w państwie trzecim było lakoniczne. Uwagi Komisji Europejskiej ograniczały się do stwierdzenia, w jednym z punktów

---

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp63_en.pdf, [dostęp: 27.04.2021], s. 8; Grupa Robocza art. 29: *Opinion 5/2003 on the Level of Protection of Personal Data in Guernsey*. 13.06.2003. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp79_en.pdf [dostęp: 27.04.2021], s. 4; Grupa Robocza art. 29: *Opinion 6/2003 on the Level of Protection of Personal Data in the Isle of Man*. 21.11.2003. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp82_en.pdf [dostęp: 27.04.2021], s. 3; Grupa Robocza art. 29: *Opinion 8/2007 on the Level of Protection of Personal Data in Jersey*. 9.10.2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp141_en.pdf [dostęp: 4.05.2021], s. 3; Grupa Robocza art. 29: *Opinion 9/2007 on the Level of Protection of Personal Data in the Faroe Islands*. 9.10.2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp142_en.pdf [dostęp: 4.05.2021], s. 4; Grupa Robocza art. 29: *Opinion 6/2009 on the Level of Protection of Personal Data in Israel*. 1.12.2009. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf [dostęp: 4.0.2021], s. 2; Grupa Robocza art. 29: *Opinion 7/2009 on the Level of Protection of Personal Data in the Principality of Andorra*. 1.12.2009. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp166_en.pdf [dostęp: 4.05.2021], s. 2; Grupa Robocza art. 29: *Opinion 6/2010 on the Level of Protection of Personal Data in the Eastern Republic of Uruguay*. 12.10.2010. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf [dostęp: 4.05.2021], s. 2; Grupa Robocza art. 29: *Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand*. 4.04.2011. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf [dostęp: 4.05.2021], s. 2; Grupa Robocza art. 29: *Opinion 07/2012 on the Level of Protection of Personal Data in the Principality of Monaco*. 19.07.2012. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp198_en.pdf [dostęp: 26.05.2021], s. 3; Grupa Robocza art. 29: *Opinion 7/2014 on the Protection of Personal Data in Quebec*. 4.06.2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf [dostęp: 26.05.2021], s. 3.

[62] Grupa Robocza art. 29.: *Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU Data Protection Directive*. 24.07.1998. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf [dostęp: 7.09.2021], dalej: Dokument WP12 lub WP12.

[63] Grupa Robocza art. 29: *Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data*. 13.06.2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp78_en.pdf [dostęp: 12.05.2021], s. 3; Grupa Robocza art. 29: O*pinion 1/2005 on the Level of Protection Ensured in Canada for the Transmission of Passenger Name Record and Advance Passenger Information from Airlines*. 19.01.2005. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp103_en.pdf [dostęp: 17.05.2021], s. 3.

[64] Grupa Robocza art. 29: *Opinion 1/2004 on the Level of Protection Ensured in Australia for the Transmission of Passenger Name Record Data from Airlines*. 16.01.2004. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp85_en.pdf [dostęp: 12.05.2021], s. 5-12; Grupa Robocza art. 29: *Opinion 3/2004 on the Level of Protection Ensured in Canada for the Transmission of Passenger Name Records and Advanced Passenger Information from Airlines*. 11.02.2004. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp88_en.pdf [dostęp: 17.05.2021], s. 5-11.

preambuły każdej z decyzji, że w danym państwie trzecim funkcjonują podstawowe zasady ochrony danych osobowych, funkcjonują sposoby zapewnienia egzekwowalności tych zasad, w tym organy nadzoru oraz funkcjonują środki zaradcze na wypadek naruszenia tychże zasad[65]. Faktycznymi kryteriami oceny były więc:

1. zasady ochrony danych osobowych,
2. sposoby ich egzekwowania,
3. istnienie organu nadzoru oraz
4. dostępność środków zaradczych, z których jednostka może skorzystać w razie naruszenia zasad ochrony danych osobowych.

Komisja Europejska nie uzasadniała jednak, dlaczego zastosowała wspomniane kryteria, zbieżne z kryteriami, o których mowa w Dokumencie WP12 a nie kryteria wynikające z art. 25 ust. 2 Dyrektywy 95/46. Komisja Europejska dysponowała więc swobodą w zakresie doboru kryteriów oceny systemu prawnego państwa trzeciego.

---

[65] Decyzja Komisji z dnia 26 lipca 2000 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Szwajcarii (Dz. U. UE. L. z 2000 r. Nr 215, str. 1 ze. zm., dalej: Decyzja w sprawie adekwatności Szwajcarii) pkt 10; Decyzja Komisji z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych (Dz. U. UE. L. z 2002 r. Nr 2, str. 13 ze zm., dalej: Decyzja w sprawie adekwatności Kanady) pkt 9; Decyzja Komisji z dnia 30 czerwca 2003 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Argentynie (Dz. U. UE. L. z 2003 r. Nr 168, str. 19 ze zm., dalej: Decyzja w sprawie adekwatności Argentyny) pkt 14; Decyzja Komisji z dnia 21 listopada 2003 r. w sprawie właściwej ochrony danych osobowych w Guernsey (Dz. U. UE. L. z 2003 r. Nr 308, str. 27 ze zm., dalej: Decyzja w sprawie adekwatności Guernsey) pkt 9; Decyzja Komisji z dnia 28 kwietnia 2004 r. w sprawie odpowiedniej ochrony danych osobowych na wyspie Man (Dz. U. UE. L. z 2004 r. Nr 151, str. 51 ze zm., dalej: Decyzja w sprawie adekwatności wyspy Man) pkt 8; Decyzja Komisji z dnia 8 maja 2008 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony danych osobowych na Jersey (Dz. U. UE. L. z 2008 r. Nr 138, str. 21 ze zm., dalej: Decyzja w sprawie adekwatności Jersey) pkt 9; Decyzja Komisji z dnia 5 marca 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony na podstawie ustawy Wysp Owczych w sprawie ochrony danych osobowych (Dz. U. UE. L. z 2010 r. Nr 58, str. 17 ze zm., dalej: Decyzja w sprawie adekwatności Wysp Owczych) pkt 7; Decyzja Komisji z dnia 19 października 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Andorze (Dz. U. UE. L. z 2010 r. Nr 277, str. 27 ze zm., dalej: Decyzja w sprawie adekwatności Andory) pkt 10; Decyzja Komisji z dnia 31 stycznia 2011 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Państwie Izrael w odniesieniu do zautomatyzowanego przetwarzania danych osobowych (Dz. U. UE. L. z 2011 r. Nr 27, str. 39 ze zm., dalej: Decyzja w sprawie adekwatności Izraela) pkt 9-10; Decyzja wykonawcza Komisji z dnia 21 sierpnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych przez Wschodnią Republikę Urugwaju w odniesieniu do zautomatyzowanego przetwarzania danych osobowych (Dz. U. UE. L. z 2012 r. Nr 227, str. 11 ze zm., dalej: Decyzja w sprawie adekwatności Urugwaju) pkt 9-10; Decyzja wykonawcza Komisji z dnia 19 grudnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Nowej Zelandii (Dz. U. UE. L. z 2013 r. Nr 28, str. 12 ze zm., dalej: Decyzja w sprawie adekwatności Nowej Zelandii) pkt 10-11; wydaje się, że także Decyzja Komisji z dnia 6 września 2005 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Imiennym Rejestrze Pasażerów linii lotniczych, przekazanym do Agencji Służb Granicznych Kanady (Dz. U. UE. L. z 2006 r. Nr 91, str. 49 ze zm., dalej: Decyzja w sprawie adekwatności Kanady - dane pasażerów) pkt 3; pkt 15-22.

Przejawem owej swobody było również posługiwanie się dodatkowym kryterium, kryterium zobowiązań międzynarodowych państwa trzeciego. Ani art. 25 ust. 2 Dyrektywy 95/46, ani Dokument WP12 nie wymieniały tego kryterium jako jednego z elementów oceny systemu prawnego państwa trzeciego. Natomiast w wybranych decyzjach w sprawie adekwatności Komisja Europejska wskazywała na istnienie różnych zobowiązań międzynarodowych państwa trzeciego, również tych bezpośrednio związanych z ochroną danych osobowych. W przypadku Szwajcarii, Guernsey, Wyspy Man, Jersey oraz Andory, w jednym z punktów decyzji w sprawie adekwatności pojawiała się wzmianka o tym, że dane państwo trzecie jest stroną Konwencji nr 108 Rady Europy. Natomiast w decyzji w sprawie adekwatności dotyczącej Kanady pojawiła się wzmianka o członkostwie Kanady w OECD. Z kolei dla Urugwaju funkcję zobowiązania międzynarodowego pełniła Amerykańska Konwencja Praw Człowieka. W odniesieniu do pozostałych czterech państw trzecich, wobec których Komisja Europejska wydała decyzje w sprawie adekwatności, pominięto weryfikację zobowiązań międzynarodowych państwa trzeciego.

2.2. Kryteria oceny systemu prawnego państwa trzeciego w wytycznych Grupy Roboczej art. 29

Wytyczne Grupy Roboczej art. 29 w sprawie oceny systemu prawnego państwa trzeciego, zawarte w Dokumencie WP12, odgrywały szczególną rolę na etapie oceny systemu prawnego państwa trzeciego. Wstępne założenia dotyczące treści kryteriów zawartych w jego treści znalazły się w pierwszym dokumencie dotyczącym transferów danych osobowych, WP4[66]. Grupa Robocza art. 29 przedstawiła w nim koncepcję minimalnych wymagań, których spełnienie było jednoznaczne z zapewnieniem odpowiedniego poziomu ochrony danych osobowych w państwie trzecim. Uznano, że tym, co powinno wskazywać zakres oceny powinno być ryzyko z jakim związany jest transfer danych[67]. Kryteriami, które należało brać pod uwagę dla ustalenia minimalnego, odpowiedniego poziom ochrony danych osobowych w państwie trzecim były podstawowe zasady ochrony danych osobowych wraz z odpowiednimi środkami ich egzekwowania[68]. Na podstawowe zasady ochrony danych osobowych składały się:

i) „Zasada ograniczenia celu przetwarzania,

[66] Grupa Robocza art. 29: *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*. 26.06.1997. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf [dostęp: 7.09.2021], dalej: Dokument WP4 lub WP4.
[67] Ibidem, s. 5–6.
[68] Ibidem.

ii) Zasada proporcjonalności i odpowiedniości danych,
iii) Zasada przejrzystości,
iv) Zasada bezpieczeństwa,
v) Prawo dostępu do danych, na które składa się m.in. prawo do sprostowania; prawo do wyrażenia sprzeciwu,
vi) Zasada ograniczenia dalszego transferu danych"[69].

Zasady podlegały uzupełnieniu o dodatkowe zasady, właściwe dla szczególnych typów przetwarzania danych, w szczególności zasady dotyczące przetwarzania danych sensytywnych, marketingu bezpośredniego czy automatycznego podejmowania decyzji[70]. Grupa Robocza art. 29 zwracała także uwagę na konieczność uwzględniania w ocenie rzeczywistej praktyki postępowania[71].

Dokument WP12 podtrzymał stanowisko wyrażone w Dokumencie WP4, w tym w zakresie kryterium ryzyka jako podstawowego wyznacznika oceny[72], kryteriów minimalnego odpowiedniego poziomu ochrony danych osobowych, czy doniosłości praktyki dla przeprowadzanej oceny[73]. Tak jak w Dokumencie WP4, tak i w Dokumencie WP12 Grupa Robocza art. 29 sugerowała, ażeby ocena egzekwowalności prawa była przeprowadzana z uwzględnieniem celu (przedmiotu) systemu ochrony danych osobowych, tak aby było możliwe odnalezienie w prawie państwa trzeciego odpowiednich środków proceduralnych[74]. Grupa Robocza art. 29 podkreślała, że podczas oceny należy także uwzględnić tzw. samoregulację (*soft law*) dotyczącą ochrony danych osobowych, która funkcjonuje w poszczególnych branżach[75]. Wyjaśniono, że ocena samoregulacji powinna być przeprowadzona w taki sam sposób, w jaki ocenia się przepisy prawa, a zatem z zamiarem odnalezienia w treści samoregulacji podstawowych zasad ochrony danych osobowych oraz oceny samoregulacji w praktyce, tj. poprzez weryfikację czy jest przestrzegana, czy jest pomocna dla podmiotów danych, w tym czy zapewnia odpowiednie środki zaradcze[76]. W Dokumencie WP12 poszczególne kryteria zostały dodatkowo doprecyzowane przez katalog przykładowych pytań, których

[69] Ibidem s. 6.
[70] Ibidem.
[71] Ibidem, s. 5.
[72] Dokument WP12, s. 27.
[73] Ibidem, s. 5–6.
[74] Ibidem, s. 7.
[75] Ibidem, s. 9.
[76] Ibidem, s. 11.

wykorzystanie miało wykazać przestrzeganie przez państwo trzecie każdego z kryteriów[77].

Proponowane przez Grupę Roboczą art. 29 zakres i treść oceny systemu prawnego państwa trzeciego, wynikające z Dokumentów WP4 i WP12, nawiązują do poglądów wyrażonych przez organy Komisji Europejskiej w wydanym w 1998 r. Raporcie Wprowadzającym[78] oraz Metodologii Oceny[79].

W Raporcie Wprowadzającym autorzy dostrzegali generalną cechę wpisaną w art. 25 Dyrektywy 95/46 jaką była otwartość i zdolność dostosowania do różnych warunków[80]. Przejawem przytoczonych cech był otwarty katalog kryteriów, które należało uwzględnić podczas oceny systemu prawnego państwa trzeciego, brak definicji adekwatności czy podejście wpadkowe (*case-by-case*)[81]. Zawężeniu oceny miała służyć identyfikacja ryzyk związanych z transferem, zaś samą ocenę traktowano jako poszukiwanie w systemie prawnym państwa trzeciego właściwego środka zaradczego[82]. Za taki środek uznano przede wszystkim podstawowe zasady ochrony danych wraz ze środkami, które zapewnią ich skuteczność[83]. Zdaniem autorów podstawowe zasady to: zasada udziału jednostki (principle of individual participation), zasada celu końcowego (principle of end objective), zasada jakości (principle of quality) oraz zasada proporcjonalności (principle of proportionality)[84]. Pierwsza z zasad sprowadzała się do uzyskania przez jednostkę informacji na temat swojej osoby, które znajdują się u podmiotu przetwarzającego oraz możności sprawowania władzy nad tymi informacjami, co niejako wpływało na zdolność wykonywania pozostałych zasad[85]. Druga zasada (celu końcowego) miała wiązać z poszanowaniem celu przetwarzania danych osobowych, tak aby dane były przetwarzane wyłącznie w sposób pozwalający na osiągnięcie celu określonego przez podmiot pozyskujący dane[86]. Pozostałe dwie zasady były ściśle

[77] Ibidem, s.11–13.
[78] M.-H. Boulanger, H. Burkert, B. Havelange i in.: *Preparation of a Methodology for Evaluating the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data. Annex to the Annual Report 1998 (XV D/5047/98) of the Working Party Established by Article 29 of Directive 95/46/*EC. 1998. https://ec.europa.eu/justice/article-29/documentation/annual-report/files/1998/wp14_en.pdf., [dostęp: 6.09.2021], dalej: Raport Wprowadzający.
[79] C.D. Raab, C.J. Bennet, R.M. Gellman i in*.: Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Tran*. 1998. https://op.europa.eu/en/publication-detail/-/publication/fd67e466-699b-4491-af96-2f3169a92c4d [dostęp: 6.09.2021], dalej: Metodologia Oceny.
[80] Raport Wprowadzający, s. 4–5.
[81] Ibidem, s. 4.
[82] Ibidem, s. 7–9; 22.
[83] Ibidem, s. 9.
[84] Ibidem, s. 10.
[85] Ibidem, s. 10;11.
[86] Ibidem, s.10.

związane z zasadą celu końcowego[87]. Stąd dla autorów Raportu Wprowadzającego twierdzenie o istnieniu dwóch najważniejszych zasad ochrony danych było zasadne[88]. W przypadku środków zapewniających skuteczne poszanowanie zasad ochrony danych, istnienie katalogu kryteriów miało drugorzędne znaczenie. Najważniejszym było przeznaczenie tych środków, czyli zapewnienie przestrzegania zasad[89]. Do jego realizacji miały się przyczyniać sankcje odstraszające przed naruszaniem zasad ochrony danych, jak również dostęp osoby, której dane dotyczą do sądowego organu, uprawnionego do wydawania egzekwowalnych rozstrzygnięć[90]. Natomiast badanie systemu prawnego państwa trzeciego powinno rozpoczynać poszukiwanie źródła (umocowania) ochrony danych osobowych, przy czym mogło to być także źródło pozaustawowa, a następnie ustalenie sposobów zapewniających kontrolę nad przestrzeganiem zasad ochrony danych oraz środków zaradczych na wypadek naruszenia tychże zasad[91]. Z ostatnich dwóch elementów badania wynikała konieczność istnienia odpowiednich środków bezpieczeństwa, jak również organu nadzorczego[92]. Autorzy podkreślali jednak, że chodzi tu o taki organ nadzorczy, który jest niezależny, m.in. poprzez odpowiednią procedurę powołania, dostępny dla podmiotów danych, z czym związane jest propagowanie zasad ochrony danych osobowych, pomoc jednostkom oraz czuwanie nad przestrzeganiem owych zasad[93]. Spośród dodatkowych wymagań, jakie powinno spełniać państwo trzecie zwrócono uwagę na koniczność regulacji zagadnienia dalszych transferów danych[94].

Metodologia Oceny powtarzała część spośród uwag zawartych w Raporcie Wprowadzającym. Za szczególnie istotne kryterium autorzy uznali funkcjonowanie przepisów (i powiązanych z nimi rozwiązań) w praktyce, która wespół z teorią miała obrazować rzeczywisty poziom ochrony danych w państwie trzecim[95]. Zasady ochrony danych osobowych uznano za ważne, ale przez brak hierarchii kryteriów oceny, to całościowe spojrzenie na badany przypadek (*casum ad casum)* przedstawi istniejący

[87] Ibidem, s. 11;18.
[88] Podobnie: ibidem, s.12; pozostałe zasady są postrzegane przez autorów jako wynikające z dwóch podstawowych zasad, tak: zasady prawa dostępu do danych czy prawa sprzeciwu - s. 19.
[89] Raport Wprowadzający, s.10.
[90] Ibidem, s.25–26.
[91] Ibidem, s.13–14.
[92] Ibidem, s. 19.
[93] Ibidem, s. 20–21.
[94] Ibidem, s. 21.
[95] Metodologia Oceny s. 200.

stan rzeczy[96]. W związku z tym, przeprowadzając ocenę należy wziąć pod uwagę także różnice kulturowe[97].

W świetle powyższego, od początku stosowania art. 25 ust. 2 Dyrektywy 95/46, jego wykładnia zakładała przyznanie Komisji Europejskiej swobody w ocenie systemu prawnego państwa trzeciego, dla której jedynym ograniczeniem była konieczność odnalezienia w badanym państwie trzecim zasad ochrony danych oraz środków ich egzekwowania.

3. Przekazywanie danych osobowych między Unią Europejską a USA w okresie obowiązywania Dyrektywy 95/46

Osobny punkt rozdziału został przeznaczony na omówienie regulacji transferów danych osobowych między Unią Europejską a USA. Spośród wszystkich badanych systemów prawnych państw trzecich, przypadek USA okazał się najbardziej skomplikowany, a zarazem wywarł największy wpływ na aktualne podejście do przekazywania danych osobowych do państw trzecich. Poszczególne zagadnienia dotyczące relacji Unia Europejska-USA w sprawie transferu danych osobowych znalazły odzwierciedlenie w dyskusji doktryny, dlatego moje rozważania skupiają się wyłącznie na kwestii oceny systemu prawnego państwa trzeciego. Dla tematu niniejszej pracy szczególnie ważną jest kwestia wpływu, jaki kazus USA wywarł na postrzeganie oceny systemu prawnego państwa trzeciego, a przede wszystkim na elementy systemu prawnego państwa trzeciego, które należy ocenić.

3.1. Decyzja w sprawie adekwatności porozumienia Safe Harbor i jej unieważnienie

Pierwsza decyzja w sprawie adekwatności dotycząca USA została wydana w 2000 r. i była związana z porozumieniem Safe Harbor[98]. Zakres oceny dokonywanej przez Komisję Europejską oraz Grupę Roboczą art. 29 obejmował postanowienia przywołanego porozumienia a nie bezpośrednio systemu prawnego USA. Przedmiot oceny był pierwszym odstępstwem od dotychczasowej praktyki Komisji Europejskiej. Sama ocena nie wyróżniała się na tle pozostałych przypadków. W opiniach Grupy Roboczej art. 29 dotyczących poziomu ochrony danych osobowych w USA w związku

[96] Ibidem, s. 202.
[97] Ibidem.
[98] Decyzja 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. UE. L. z 2000 r. Nr 215, str. 7, ze zm., dalej: Porozumienie Safe Harbor).

z porozumieniem Safe Harbor zasygnalizowano konieczność praktycznego spojrzenia na przypadek USA[99]. Odnosząc się do organu nadzorczego, w tym do kwestii braku jurysdykcji organów europejskich na terytorium USA, podkreślono, że istnienie skutecznego mechanizmu egzekwowalności praw jest kluczowym elementem oceny [100]. W pozostałym zakresie opiniowanie oparto o Dokument WP12[101]. Również w treści decyzji w sprawie adekwatności Komisja Europejska wskazywała na zapewnienie przez porozumienie Safe Harbor tych elementów oceny, na które wskazywał Dokument WP12.

Momentem przełomowym dla omawianego zagadnienia okazała się pierwsza sprawa zainicjowana przez M. Schremsa. Autor skargi, skierowanej do jednego z europejskich organów nadzorczych, zwrócił uwagę organów Unii Europejskiej i opinii publicznej na problemy w systemie prawnym USA, które, jego zdaniem, wpływały na poziom ochrony danych osobowych zapewniany przez porozumienie Safe Harbor. M. Schrems zainicjował w ten sposób szereg dyskusji, które przez lata toczyły się w dokumentach i opiniach organów Unii Europejskiej.

Spośród wielu sformułowanych wniosków, część dotyczyła oceny systemu prawnego państwa trzeciego. W wyjaśnieniach kierowanych do Parlamentu Europejskiego z 2013 r., Komisja Europejska zwracała uwagę na zagrożenia wynikające z dostępu organów państwowych USA do danych, które należą do podmiotów prywatnych świadczących usługi[102]. Na tle owych zagrożeń, Komisja Europejska pośrednio odniosła się do samych kryteriów oceny. Według Komisji Europejskiej, tym co szczególnie przekłada się na odpowiedni poziom ochrony danych osobowych jest respektowanie zasady proporcjonalności, ograniczony okres przechowywania danych oraz egzekwowalne prawa osób, których dane dotyczą[103]. W przypadku tych ostatnich, Komisja Europejska zaznaczała, że jednym z praw przyznanych jednostce powinien być dostęp do sądowej procedury dotyczącej naprawienia naruszeń praw, wolnej od

---

[99] Grupa Robocza art. 29: *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions between the European Commission and the United States Government*. 26.01.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf [dostęp: 7.10.2021], s. 2.

[100] Grupa Robocza art. 29: *Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" Issued by the US Department of Commerce on 19th April 1999*. 3.03.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp19_en.pdf [dostęp: 7.10.2021], s. 3.

[101] Grupa Robocza art. 29: *Opinion 4/2000 on the Level of Protection Provided by the "Safe Harbor Principles"*. 16.05.2000. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf [dostęp: 12.05.2021], s. 2.

[102] *Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows…,* s. 3.

[103] Ibidem, s. 8.

zróżnicowanego traktowanie obywateli i nie-obywateli państwa trzeciego[104]. W kolejnym komunikacie adresowanym do Parlamentu Europejskiego, Komisja Europejska przedstawiła uchybienia mechanizmu samocertyfikacji, na którym opierało się porozumienie Safe Harbor, a przede wszystkim trudności z weryfikacją czy certyfikowane podmioty rzeczywiście przestrzegają zasady wynikające z porozumienia Safe Harbor[105]. Ponownie dostrzeżoną poważną wadą systemu prawnego USA było nierówne traktowanie obywateli i nie-obywateli USA w ramach postępowań sądowych[106]. Do obu komunikatów Komisji Europejskiej odniósł się Europejski Inspektor Ochrony Danych Osobowych. W swojej opinii zwrócił uwagę na słabości związane z regulacją dalszego przekazywania danych osobowych[107], a także, dostęp organów państwowych USA do danych[108]. Europejski Inspektor Ochrony Danych Osobowych dostrzegał potrzebę istnienia organu nadzoru, którego zadania i skuteczne uprawnienia byłyby związane zarówno z przestrzeganiem zasad ochrony danych osobowych, jak i ochroną przed nieuzasadnionym dostępem organów państwowych do danych na etapie ich pozyskiwania i dalszego przetwarzania[109].

Zagadnienie zgodnego z prawem dostępu organów państwowych do danych osobowych na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego [110] oraz odpowiednich zabezpieczeń służących przestrzeganiu zasad ochrony danych osobowych zostało następnie rozwinięte w opiniach Grupy Roboczej art. 29[111] w zakresie, który wykracza poza temat tej rozprawy. Niemniej jednak, na potrzeby dalszych rozważań, przyjmuję, że wytyczne Grupy Roboczej art. 29 w sprawie dostępu organów

---

[104] Ibidem, s. 8–9.

[105] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*. 27.11.2013. https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.05/DOC_1&format=PDF [dostęp: 7.10.2021], s. 5-9.

[106] Ibidem, s. 17.

[107] Europejski Inspektor Ochrony Danych Osbowych: *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU"*. 20.02.2014. https://edps.europa.eu/sites/default/files/publication/14-02-20_eu_us_rebuliding_trust_en.pdf [dostęp: 7.10.2021], pkt 30.

[108] Ibidem, m.in. pkt 19, pkt 34, pkt 52, pkt 74.

[109] Ibidem, pkt 75-76.

[110] W dalszej części pracy będę się posługiwał zamiennie określeniami: dostęp organów do danych; dostęp organów państwa do danych osobowych, dostęp organów ścigania do danych

[111] Por. Grupa Robocza art. 29: *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes*. 10.04.2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf [dostęp: 7.10.2021]; Grupa Robocza art. 29: *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes*. 5.12.2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf [dostęp: 7.10.2021].

państwa do danych osobowych stanowią źródło kryterium oceny systemu prawa państwa trzeciego w tym zakresie.

Sprawa zainicjowana przez M. Schremsa znalazła swój finał w TSUE. Oprócz tez zawartych w orzeczeniu kończącym sprawę, dla przedmiotu tej rozprawy przydatne są także uwagi zawarte w opinii Rzecznika Generalnego Y. Bota. W toku postępowania przed TSUE, Rzecznik Generalny Y. Bot skupił się na dwóch zagadnieniach. Pierwsze zagadnienie to wymagania stawiane organowi nadzorczemu. Istnienie organu nadzorczego jest z perspektywy wymagań Unii Europejskiej kluczowym elementem systemu prawnego ochrony danych osobowych[112]. Zasadniczą cechą organu nadzorczego powinna być niezależność[113]. Aby podmiot pełnił rolę organu nadzorczego należy przyznać mu odpowiedni zakres działania, który nie jest ograniczony wyłącznie do sprawowania pieczy nad szeroko pojętymi zagadnieniami ochrony konkurencji i praw konsumentów[114]. Drugie zagadnienie to ocena systemu prawnego państwa trzeciego. W ocenie Rzecznika, decyzja w sprawie adekwatności i powiązana z nią ocena muszą odpowiadać rzeczywistości, przez co ponowna ocena systemu prawnego przez właściwe organy Unii Europejskiej powinna następować za każdym razem, gdy pojawią się uzasadnione wątpliwości co do aktualnego poziomu ochrony[115]. Nie oznacza to, że państwo trzecie zwolnione jest z jakichkolwiek działań, ponieważ jego obowiązkiem jest nieustanne zapewnienie takiego poziomu ochrony danych osobowych, który będzie zgodny ze standardami prawa Unii Europejskiej [116]. Ocena systemu prawnego państwa trzeciego sprowadza się do wykorzystania dwóch kluczowych kryteriów: kryterium zasad ochrony danych oraz kryterium środków, dzięki którym zasady są stosowane i przestrzegane[117]. Za sprawą środków zapewniających przestrzeganie zasad osoba, której dane dotyczą powinna mieć możliwość sądowej kontroli postępowania z danymi osobowymi, także gdy dane przetwarzają podmioty publiczne[118]. W przypadku dodatkowych, pozasądowych postępowań, w tym alternatywnych sposobów rozwiązywania sporów, konieczne jest ustalenie do jakich spraw znajdą zastosowanie, a zwłaszcza czy pozasądowe postępowania obejmują spory z udziałem podmiotów

[112] Y. Bot: *Opinion Of Advocate General Bot Case C-362/14 Maximillian Schrems v Data Protection Commissioner (Request for a Preliminary Ruling from the High Court (Ireland))*. 23.09.2015. ECLI:EU:C:2015:627, pkt 145.
[113] Ibidem, m.in. pkt 67-68.
[114] Ibidem, pkt 205.
[115] Ibidem, pkt 135, pkt 137, pkt 146.
[116] Ibidem, pkt 147.
[117] Ibidem, pkt 143, w oparciu o Dokument WP12.
[118] Ibidem, m.in. pkt 158, pkt 165.

publicznych[119]. Poza powyższymi zagadnieniami Rzecznik w swojej opinii niejako sformułował dodatkowe kryterium, wzorzec kontroli, w postaci Karty Praw Podstawowych. Według Rzecznika Bota wykorzystanie Karty Praw Podstawowych może polegać na interpretacji uprawnień organu nadzorczego w świetle art. 8 ust. 3 Karty Praw Podstawowych [120]. Jednocześnie, Karta Praw Podstawowych, a szczególnie art. 7,8, 47 i 52 są źródłem standardów, jakie powinno spełniać prawo państwa trzeciego w zakresie dostępu organów państwa do danych osobowych[121].

Wyrok TSUE, nazywany powszechnie wyrokiem w sprawie Schrems I [122], potwierdził dotychczasowe rozważania organów Unii Europejskiej. Trybunał wyjaśnił, że cecha niezależności organu nadzorczego to gwarancja efektywnej kontroli przestrzegania przepisów ochrony danych osobowych, a zarazem to wsparcie osoby, której dane dotyczą, ponieważ tylko niezależnie sprawowany nadzór może stać na straży równowagi interesów podmiotów danych i uczestników obrotu tymi danymi. Przejawem niezależności jest uprawnienie organu nadzorczego do weryfikacji przekazywania danych osobowych do państwa trzeciego, które jest objęte właściwą decyzją Komisji Europejskiej[123]. Odnosząc się do oceny systemu prawnego państwa trzeciego, TSUE podkreślał, że katalog kryteriów oceny jest otwarty, przez co ocena powinna uwzględniać całokształt okoliczności [124]. Nie oznacza to jednak dowolności w przeprowadzeniu oceny[125]. Spojrzenie na system prawny państwa trzeciego to poszukiwanie efektywnej ochrony danych osobowych osiąganej niekoniecznie przy wykorzystaniu tych samych sposób, które są obecne w prawie Unii Europejskiej [126]. Ważne, aby rozwiązania przyjęte w systemie prawnym państwa trzeciego stanowiły element rzeczywistej praktyki postępowania [127]. W konsekwencji, aby ocenić system prawny państwa trzeciego konieczne jest wykorzystanie dwóch kryteriów: kryterium zasad ochrony danych osobowych (zwłaszcza treści zasad) oraz kryterium sposobów zapewniających przestrzeganie tych zasada w praktyce[128]. Drugie kryterium wymaga zbadania wyjątków, które wyłączają stosowanie zasad, a także zbadania środków ochrony, z których może

[119] Ibidem, pkt 204, pkt 206.
[120] Ibidem, pkt 79; także pkt 94.
[121] Ibidem, pkt 170, pkt 174, pkt 177, pkt 181, pkt 200.
[122] Wyrok TSUE z 6.10.2015 r., C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (dalej: Wyrok Schrems I lub Sprawa Schrems I), pkt 41, pkt 42.
[123] Ibidem, pkt 53, pkt 54, pkt 56, pkt 57, pkt 66.
[124] Ibidem, pkt 70.
[125] Ibidem, pkt 78.
[126] Ibidem, pkt 74.
[127] Ibidem, pkt 71 i 73.
[128] Ibidem, pkt 75.

skorzystać jednostka na wypadek naruszenia tychże zasad [129]. Zdaniem TSUE uzasadnieniem badania właśnie tych elementów systemu prawnego państwa trzeciego są standardy płynące z Karty Praw Podstawowych [130].

3.2. Tarcza Prywatności jako nowe porozumienie w sprawie transferów danych do USA

Unieważnienie decyzji w sprawie adekwatności porozumienia Safe Harbor rozpoczęło prace nad nowym rozwiązaniem dla przekazywania danych osobowych z Unii Europejskiej do USA. Dyskusja na temat Tarczy Prywatności [131] i jej uchwalenia dostarcza wielu uwag w przedmiocie kryteriów oceny systemu prawnego państwa trzeciego.

Opiniując projekt Tarczy Prywatności, Europejski Inspektor Ochrony Danych Osobowych zauważył, że o ile ocena powinna dotyczyć elementów kluczowych z perspektywy prawa UE, o tyle spośród całokształtu okoliczności szczególnie doniosłe są niezależny organ nadzorczy oraz środki ochrony prawnej przyznane jednostce na wypadek naruszenia jej praw[132]. W przypadku kryterium organu nadzorczego ważne jest zarówno wyposażenie organu w odpowiednie uprawnienia, jak również istnienie gwarancji zapewniających respektowanie decyzji organu nadzorczego przez inne podmioty[133]. Odnośnie do kryterium środków ochrony prawnej Europejski Inspektor Ochrony Danych Osobowych zauważył, że jednostka może mieć trudności w rozeznaniu się w obcym systemie prawnym, stąd potrzebna jest jasna i zrozumiała informacja na temat środków, które przysługują jednostce[134]. Traktowanie nie-obywateli i obywateli państwa trzeciego korzystających z przyznanych środków nie może być zróżnicowane[135]. Poza powyższymi kryteriami podczas oceny nie bez znaczenia są odpowiednie reguły przetwarzania danych osobowych, szczególnie te odpowiadające m.in. zasadom celowości, minimalizacji, automatycznego podejmowania decyzji, a także możliwe wyjątki wyłączające zastosowanie zasad[136].

---

[129] Ibidem, pkt 82-83; pkt 86-89.
[130] Ibidem, pkt 91-95.
[131] 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 (Dz. U. UE. L. z 2016 r. Nr 207, str. 1, dalej: Decyzja w sprawie adekwatności Tarczy Prywatności).
[132] Europejski Inspektor Ochrony Danych Osbowych: *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*. 30.05.2016. https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf [dostęp: 12.10.2021], s. 6.
[133] Ibidem, s. 8.
[134] Ibidem, s.11.
[135] Ibidem, s. 8.
[136] Ibidem, s. 10–11.

Ocena projektu Tarczy Prywatności autorstwa Grupy Roboczej art. 29 została sformułowana w inny sposób. Grupa Robocza art. 29 uznała za zasadnicze kryterium oceny prawa i wolności osób, których dane dotyczą, wynikające z Karty Praw Podstawowych i Europejskiej Konwencji Praw Człowieka[137]. Z związku z tym, pojawiła się konieczność uwzględnienia w ocenie także kryterium weryfikującego uzasadnienie ograniczeń dla praw i wolności osób, których dane dotyczą [138]. Tak określone, podstawowe kryterium przełożyło się na dalsze, szczegółowe kryteria. Grupa Robocza art. 29 wykorzystała przede wszystkim kryterium zasad ochrony danych, na które składały się: zasada ochrony danych wrażliwych[139] i danych medycznych[140], zasada retencji danych[141], zasada automatycznego podejmowania decyzji[142], zasada celowości[143], zasada dalszego transferu danych, zasada dostępu do danych i jakości danych[144], zasada proporcjonalności[145], zasada przetwarzania danych związanych z zatrudnieniem[146]. Dodatkowo, kryterium oceny były wyłączenia zastosowanie zasad ochrony danych osobowych [147], czy zagadnienie podziału obowiązków wynikających z Tarczy Prywatności pomiędzy administratorem a podmiotem przetwarzającym dane na zalecenie administratora[148]. Nadto, ważne było ustalenie czy postanowienia Tarczy Prywatności są jasnei przejrzyste dla odbiorcy [149]. W przypadku kryterium środków ochrony prawnej przyznanych jednostce, Grupa Robocza art. 29 uwzględniła aspekt finansowy dostępu do profesjonalnej pomocy prawnej[150] oraz problem ograniczenia dostępu do niektórych środków ochrony prawnej dla nie-obywateli USA[151]. Kryterium organu nadzorczego obejmowało badanie uprawnień organów pełniących funkcje nadzorcze, w tym ich uprawnienia do przeprowadzania kontroli w miejscu przetwarzania danych, jak również badanie praktyki funkcjonowania organów, z uwzględnieniem możliwości egzekwowania w USA orzeczeń zapadłych przed organami nadzorczymi znajdującymi

[137]Grupa Robocza art. 29: *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision*. 12.04.2016. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [dostęp: 12.10.2021], s. 10.
[138] Ibidem, s.11.
[139] Ibidem, s. 14.
[140] Ibidem, s. 32.
[141] Ibidem, s.17.
[142] Ibidem, s. 18.
[143] Ibidem, s. 20, 24.
[144] Ibidem, s. 25–26.
[145] Ibidem, s.23.
[146] Ibidem, s.31.
[147] Ibidem, s.17, 22, 25.
[148] Ibidem, s. 16.
[149] Ibidem, s. 12–13.
[150] Ibidem, s. 28.
[151] Ibidem, s.43.

się w Unii Europejskiej[152]. Ocena Grupy Roboczej art. 29 dotyczyła także zagadnienia dostępu organów państwa, w tym organów wywiadowczych do danych osobowych[153]. W tym względzie na szczególną uwagę zasługiwało stosowanie zasad dostępu do danych osobowych w praktyce postępowania organów państwa[154]. Na tle problematyki dostępu organów państwa, w tym organów wywiadowczych, do danych osobowych Grupa Robocza art. 29 dokładniej objaśniła treść kryterium organu nadzorczego, na które składa się zakres działania organu nadzorczego[155], zasady dostępu do organu nadzorczego, w tym zagadnienie istnienia interesu prawnego osoby zwracającej się do organu, niezależność organu nadzorczego oraz dwojakie uprawnienia organu nadzorczego: uprawnienia śledcze oraz uprawnienia pozwalające na korygowanie dostrzeżonych uchybień[156].

Swoje uwagi do projektu Tarczy Prywatności przedstawił także Parlament Europejski. W rezolucji wyjaśniono, że przepisy prawa państwa trzeciego regulujące ograniczenie praw osób, których dane dotyczą powinny odpowiadać standardom jakie wynikają z Karty Praw Podstawowych[157]. Dostateczną podstawą dla dokonywanej oceny systemu prawnego państwa trzeciego nie mogą być wyłącznie zapewnienia państwa trzeciego[158]. Co się tyczy organu nadzorczego, ważna jest jego niezależność i odpowiednie kompetencje[159].

Tarcza Prywatności, podobnie jak porozumienie Safe Harbor, została przyjęta w formie decyzji w sprawie adekwatności[160]. Tak jak w przypadku Safe Harbor, przedmiotem oceny Komisji Europejskiej stało się porozumienie, czyli Tarcza Prywatności. Dodatkowo, w związku z zastosowaniem kryterium oceny dostępu organów państwa do danych osobowych, Komisja Europejska uwzględniła w ocenie także odnośne prawodawstwo federalne USA. Kryteria oceny, wskazane w treści decyzji w sprawie adekwatności Tarczy Prywatności, były zbieżne z elementami oceny, które wynikały z opinii Grupy Roboczej art. 29 w sprawie Tarczy Prywatności. Co do zasady, nadal wiodącą rolę odgrywały kryteria oceny zawarte w Dokumencie WP12. Tym co wyróżniło decyzję w sprawie adekwatności Tarczy Prywatności była dokładność i obszerność opisu

[152] Ibidem, s.31.
[153] Ibidem, s. 33–56.
[154] Ibidem, s.36.
[155] Ibidem, s.48–50.
[156] Ibidem, s.47.
[157] *European Parliament Resolution of 26 May 2016 on Transatlantic Data Flows*. 26.05.2016, https://www.europarl.europa.eu/doceo/document/TA-8-2016-0233_EN.pdf [dostęp: 19.10.2021], pkt 4.
[158] Ibidem, pkt 7.
[159] Ibidem, pkt 8.
[160] Decyzja w sprawie adekwatności Tarczy Prywatności, pkt 13 - adekwatność dotyczy Tarczy Prywatności.

elementów systemu prawnego USA, w tym Tarczy Prywatności, które odpowiadały poszczególnym kryteriom oceny.

Decyzje w sprawie adekwatności dotyczące innych państw trzecich były kilkustronicowymi dokumentami, w których Komisja Europejska lakonicznie opisywała badany system prawny, z wyraźnym potwierdzeniem, że w tym systemie identyfikuje kryteria oceny, o których mowa w Dokumencie WP12. W preambułach do poszczególnych decyzji w sprawie adekwatności państw trzecich znajdowały się punkty, poświęcone każdemu z kryteriów oceny systemu prawnego państwa trzeciego z Dokumentu WP12, wraz z wyraźnym, aczkolwiek zwięzłym wyjaśnieniem Komisji Europejskiej, że w badanym systemie prawnym państwa trzeciego są rozwiązania, które czynią zadość określonemu kryterium. I tak w odniesieniu do zasad ochrony danych osobowych, wymieniano wszystkie zasady obecne w systemie prawnym państwa trzeciego, wraz z przywołaniem ich podstawy prawnej. Taki sam schemat stosowano do opisu pozostałych kryteriów.

Tymczasem, licząca 112 stron decyzja w sprawie adekwatności Tarczy Prywatności dokładnie opisywała niemalże wszystkie przepisy prawa lub postanowienia Tarczy Prywatności realizujące zastosowane kryteria. Uznanie adekwatności było związane przede wszystkim z zasadami ochrony danych osobowych, które znalazły się w Tarczy Prywatności[161]. Każda z zasad ochrony danych osobowych została omówiona z osobna. Oprócz przywołania podstawy prawnej, opis zawierał wyjaśnienie jak zasada jest rozumiana w praktyce amerykańskiej i jakie mogą być tego konsekwencje. Określono także podstawowy podmiot odpowiedzialny za działanie i przestrzeganie Tarczy Prywatności[162], wraz z jego uprawnieniami[163]. Omówiono środki ochrony prawnej przyznane podmiotom danych, w tym sposoby umożliwiające ich wykonanie[164]. Odnosząc się do zagadnienia dostępu organów państwa, w tym organów wywiadowczych do danych osobowych, Komisja Europejska wskazała na właściwe ustawodawstwo USA stworzone w tym celu, a zwłaszcza zasady regulujące dostęp do danych i ich przetwarzanie[165]. W zakresie środków mających zapewnić przestrzeganie określonych zasad dostępu do danych opisano organy sprawujące nadzór, z uwzględnieniem procedury ich powołania oraz przyznanych uprawnień[166]. W opisie organów nadzorczych

[161] Ibidem, pkt 19-27.
[162] Ibidem, pkt 18, ale Departament Handlu nie został *expressis verbis* uznany za organ nadzorczy.
[163] Ibidem, pkt 33-37.
[164] Ibidem, pkt 39-41, pkt 43-63.
[165] Ibidem, pkt 69-70, pkt 72-76, pkt 78, pkt 80, pkt 82-83, pkt 86-87.
[166] Ibidem, pkt 92-99, pkt 100-109.

uwzględniono także nowo powołany organ mający sprawować nadzór nad przetwarzaniem danych w celach wywiadowczych[167]. W tym zakresie opisano również środki prawne przyznane osobom, których dane dotyczą na wypadek naruszenia zasad przetwarzania danych przez organy państwa, ze wskazaniem możliwych do wykorzystania podstaw prawnych[168].

Tym samym, ubocznym skutkiem wydania decyzji w sprawie adekwatności Tarczy Prywatności była modyfikacja wzorca decyzji w sprawie adekwatności stosowanego przez Komisję Europejską. Wyprzedzając kolejne punkty rozdziału, decyzję w sprawie adekwatności Tarczy Prywatności można poczytywać jako zapowiedź zmiany w podejściu Komisji Europejskiej do treści decyzji w sprawie adekwatności. Wydana na podstawie art. 25 Dyrektywy 95.46, decyzja w sprawie adekwatności Tarczy Prywatności w zakresie treści i struktury odpowiada decyzjom w sprawie adekwatności wydanym na podstawie art. 45 RODO.

Na etapie funkcjonowania decyzja w sprawie adekwatności Tarczy Prywatności podlegała corocznej ocenie. Podczas pierwszej oceny, w 2017 r., w swojej opinii Grupa Robocza art. 29 podkreślała konieczność stosowania jasnego przekazu w komunikacji z podmiotami danych[169]. Co się tyczyło sprawowania nadzoru nad przestrzeganiem przepisów, nie powinna go cechować ograniczona aktywność właściwych podmiotów[170]. W przypadku dostępu organów państwa do danych osobowych, w tym organów wywiadowczych, zasadniczym problemem była pozorność części z wprowadzonych ograniczeń, jak również pozorność niektórych uprawnień przyznanych osobom, których dane dotyczą, w tym dostępu do organu nadzorczego[171]. Komisja Europejska w swoim raporcie związanym z pierwszą oceną decyzji w sprawie adekwatności Tarczy Prywatności odniosła się do praktyki obejmującej wdrożenie odpowiednich zasad ochrony danych osobowych oraz do kwestii nadzoru[172]. Sama ocena Komisji Europejskiej przyjęła dwutorową postać, obejmując osobno przetwarzanie danych osobowych przez podmioty prywatne oraz przez organy państwa, w tym organy

[167] Ibidem, pkt 116-117, pkt 119-122.
[168] Ibidem, pkt 111-115, pkt 125-127, pkt 130, pkt 132-134.
[169] Grupa Robocza art. 29: *EU – U.S. Privacy Shield – First Annual Joint Review*. 28.10.2017. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782 [dostęp: 12.10.2021], s. 7-8.
[170] Ibidem, s. 10–12.
[171] Ibidem, s. 14–16, 20.
[172] *Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU–U.S. Privacy Shield*. 18.10.2017. https://ec.europa.eu/info/sites/default/files/report_on_the_first_annual_review_of_the_eu-us_privacy_shield_2017.pdf [dostęp: 19.10.2021] s. 3.

wywiadowcze[173]. Szczególną uwagę przyciągnęła potrzeba faktycznych, skutecznych działań organu nadzorczego[174].

Podczas drugiej oceny decyzji w sprawie adekwatności Tarczy Prywatności, przeprowadzonej w 2018 r., dla Europejskiej Rady Ochrony Danych Osobowych ponownie ważna była przejrzystość informacji kierowanych do osób, których dane dotyczą[175]. Sporo uwagi poświęcono funkcjonowaniu nadzoru w praktyce, w tym w zakresie fałszywych zapewnień administratorów i podmiotów przetwarzających o przestrzeganiu zasad ochrony danych osobowych[176]. Rozważania Europejskiej Rady Ochrony Danych Osobowych dotyczyły także kwestii rzeczywistego działania i dostępu osób, których dane dotyczą do środków ochrony prawnej w sytuacji dostępu organów państwa, w tym organów wywiadowczych, do danych osobowych[177]. Europejska Rada Ochrony Danych Osobowych zwróciła uwagę także na brak w systemie prawnym USA regulacji w zakresie profilowania[178].

Do oceny decyzji w sprawie adekwatności Tarczy Prywatności włączył się również Parlament Europejski. W swojej rezolucji, skupił się na problemach związanych z organizacją organu nadzorczego powołanego na potrzeby nadzoru nad dostępem organów państwa, w tym organów wywiadowczych, do danych osobowych poprzez brak odpowiedniej liczby członków organu, jak również na zagadnieniu niezależności organu

---

[173] *Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 18.10.2017. http://webcache.googleusercontent.com/search?q=cache:8suwjp581o0J:ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D47799+&cd=2&hl=pl&ct=clnk&gl=pl&client=safari [dostęp: 19.10.2021], s. 3. Podczas drugiej oceny, Komisja Europejska podtrzymała dwutorowe spojrzenie - *Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 19.12.2018. https://ec.europa.eu/info/sites/default/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf [dostęp: 19.10.2021], s. 2; *Commission Staff Working Document Accompanying the Document Report From the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 19.12.2018. https://ec.europa.eu/info/sites/default/files/staff_working_document_-_second_annual_review.pdf [dostęp: 19.10.2021], s. 4.

[174] *Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*…, s. 3–5; *Commission Staff Working Document Accompanying the Document Report From the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*…, s. 4-8.

[175] Europejska Rada Ochrony Danych Osobowych: *EU - U.S. Privacy Shield - Second Annual Joint Review*. 22.01.2019. https://edpb.europa.eu/sites/default/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf [dostęp: 19.10.2021], pkt 44-45.

[176] Ibidem, pkt 54, pkt 56-65.

[177] Ibidem, pkt 78, pkt 81, pkt 83, pkt 86, pkt 95, pkt 101, pkt 103.

[178] Ibidem, pkt 68-77.

nadzorczego[179]. Odnosząc się do wykonywania uprawnień nadzorczych, podkreślono potrzebę przeprowadzania kontroli administratorów i podmiotów przetwarzających z urzędu[180]. Mając na uwadze środki ochrony prawnej przyznane osobom, których dane dotyczą niezwykle istotny jest jasny przekaz[181]. Obejmuje to także regulację dostępu organów państwa, w tym organów wywiadowczych do danych osobowych, ponieważ niejasność sformułowań zawartych przepisach może wywoływać wiele negatywnych skutków[182]. Parlament Europejski wyjaśnił, że dla właściwej ochrony danych osobowych ważne jest funkcjonowanie regulacji dotyczącej profilowania i automatycznego podejmowania decyzji[183]. Spostrzeżenia poczynione w rezolucji skłoniły Parlament Europejski do uznania, że Tarcza Prywatności nie zapewnia odpowiedniego poziomu ochrony danych osobowych[184].

W ramach trzeciej i ostatniej oceny, która miała miejsce w 2019 r., Komisja Europejska również stosowała dwutorowe podejście (podział na podmioty prywatne i publiczne), przy czym dla obu grup podmiotów to praktyka funkcjonowania ochrony danych osobowych była najważniejsza[185]. Dotyczyło to także podmiotu sprawującego nadzór, którego działania powinny obejmować kontrole przeprowadzane w odpowiedni sposób, nie ograniczając się tylko do weryfikacji kwestii formalnych[186]. Prawidłowe funkcjonowanie nadzoru obejmuje również zagadnienia dostępu organów państwa, w tym organów wywiadowczych do danych osobowych[187]. W przeciwieństwie do pozostałych raportów, tym razem Komisja Europejska nie odniosła się do zagadnienia ochrony danych pracowników oraz automatycznego podejmowania decyzji, które zostały poruszone jedynie w dokumencie towarzszącym raportowi[188].

---

[179] *European Parliament Resolution on the Adequacy of the Protection Afforded by the EU- US Privacy Shield*. 5.07.2018. https://www.europarl.europa.eu/doceo/document/B-8-2018-0305_EN.pdf [dostęp: 19.10.2021], pkt 4-7.
[180] Ibidem, pkt 9.
[181] Ibidem, pkt 11.
[182] Ibidem, pkt 20-22, pkt 24-27.
[183] Ibidem, pkt 16.
[184] Ibidem, pkt 34.
[185] *Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 23.10.2019. https://ec.europa.eu/info/sites/default/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf [dostęp: 19.10.2021], s. 3.
[186] Ibidem, 5.
[187] Ibidem, 7.
[188] *Commission Staff Working Document Accompanying the Document Report From the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 23.10.2019. https://ec.europa.eu/info/sites/default/files/staff_working_document_-_third_annual_review.pdf [dostęp: 19.10.2021], s. 5.

Tak jak dla porozumienia Safe Harbor, tak i dla decyzji w sprawie adekwatności Tarczy Prywatności, momentem kluczowym okazała się sprawa zawisła w TSUE. Ponownie, działania TSUE, a w konsekwencji unieważnienie decyzji w sprawie adekwatności, zostały zainicjowane wskutek złożenia skargi przez M. Schremsa.

3.3. Unieważnienie decyzji w sprawie adekwatności Tarczy Prywatności – sprawa Schrems II

Rzecznik Generalny Ø. Saugmandsgaard w opinii towarzyszącej postępowaniu przed TSUE zaznaczył, że zapewnienie odpowiedniego poziomu ochrony danych osobowych to samodzielne zadanie państwa trzeciego[189]. Zdaniem Ø. Saugmandsgaarda ocena systemu prawnego państwa trzeciego sprowadza się do badania dwóch elementów: zasad ochrony danych osobowych oraz środków zapewniających ich przestrzeganie[190]. Nie bez znaczenia jest praktyka postępowania[191]. O ile praktyka jest momentami szczególnie doniosła, o tyle nie może stanowić wyłącznego umocowania dla środków chroniących przed naruszeniami, przy jednoczesnym braku podstawy prawnej[192]. W przypadku przetwarzania danych osobowych przez organy państwowe w związku z zapewnieniem bezpieczeństwa narodowego**,** Rzecznik Generalny Ø. Saugmandsgaard sugeruje ocenę poszukującą odpowiednich zabezpieczeń dla osób, których dane dotyczą. Minimalne zabezpieczenia określa w tej sytuacji Europejska Konwencja Praw Człowieka i Karta Praw Podstawowych[193]. Dlatego też, ocena powinna obejmować uprawnienia organu nadzorczego w zakresie sprawowania nadzoru także w sytuacji, gdy dane są dopiero przesyłane, a więc nie trafiły jeszcze na terytorium państwa trzeciego[194]. To z kolei powoduje, że ocena musi uwzględniać tzw. metadane dotyczące przemieszczania się właściwych danych[195]. Jednocześnie, Rzecznik Generalny Ø. Saugmandsgaard dostrzega związek między prawem dostępu do danych, rozumianym także w zakresie informacji o przetwarzaniu danych przez konkretny podmiot, a możliwością realizacji środków ochrony prawnej[196]. Doniosłym elementem ochrony jednostki jest uprawnienie organu nadzorczego do wydawania decyzji, których

[189] Ø. Saugmandsgaard: *Opinion of Advocate General Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, Interveners:The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance, Inc., Digitaleurope*. 19.12.2019. ECLI:EU:C:2019:1145, pkt 119.
[190] Ibidem, pkt 135.
[191] Ibidem, pkt 202.
[192] Ibidem, pkt 266-267, pkt 270-271.
[193] Ibidem, pkt 207, pkt 209, pkt 229.
[194] Ibidem, pkt 236.
[195] Ibidem, pkt 257-262.
[196] Ibidem, pkt 319-320, pkt 326-327.

respektowanie i wykonanie przez pozostałe podmiotu jest obowiązkowe [197]. Ø. Saugmandsgaard uważa, że wymóg minimalności nie jest ograniczony do przetwarzania danych na potrzeby bezpieczeństwa narodowego, ale dotyczy oceny jako takiej, ponieważ występujące różnice kulturowe czy tradycje prawne mogły wpłynąć na odmienne ukształtowanie badanego systemu prawnego, co jednak nie przekreśla możliwości odnalezienia treści ochrony danych osobowych[198].

W wyroku w sprawie Schrems II TSUE podkreślił wymóg istnienia w państwie trzecim ochrony danych osobowych odpowiadającej rzeczywistej praktyce[199]. Za kryteria oceny systemu prawnego jednoznacznie uznano art. 7, 8 i 47 KPP[200]. Zdaniem TSUE, badając sytuację prawną osób, których dane dotyczą w obcym systemie prawnym należy zwrócić uwagę na możliwość realizacji przyznanych środków ochrony prawnej, w tym dostępu do organu nadzorczego[201]. Realizacja środków ochrony prawnej może się odbyć nie tylko przez dostęp do postepowania sądowego, ale także przez dostęp do niezależnego, wyposażonego w skuteczne uprawnienia organu nadzorczego[202].

4. Ocena poziomu ochrony danych osobowych w państwie trzecim na podstawie przepisów RODO

Jednym ze skutków wejścia w życie RODO była zmiana kryteriów oceny systemu prawnego państwa trzeciego. Katalog kryteriów, o którym była mowa w art. 25 ust. 2 Dyrektywy 95/46 został zastąpiony przez art. 45 ust. 2 RODO. Według przywołanego przepisu, na potrzeby oceny systemu prawnego państwa trzeciego Komisja Europejska powinna uwzględnić co najmniej:

a) „praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub

[197] Ibidem, pkt 338.
[198] Ibidem, pkt 249.
[199] Wyrok TSUE z 16.07.2020 r., C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559 (dalej: Wyrok Schrems II lub Sprawa Schrems II), pkt 94, pkt 126, pkt 162.
[200] Ibidem, pkt 169, pkt 186.
[201] Ibidem, pkt 180-181, pkt 192.
[202] Ibidem, pkt 194-196.

w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia;

b) istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub w stosunku do organizacji międzynarodowej, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym posiadające odpowiednie uprawnienia do egzekwowania przestrzegania przepisów – pomagać i doradzać osobom, których dane dotyczą, w toku wykonywania przysługujących im praw, a także współpracować z organami nadzorczymi państw członkowskich;

c) międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne obowiązki wynikające z prawnie wiążących konwencji lub instrumentów oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych".

Zestawiając oba katalogi kryteriów można dostrzec, że katalog z art. 45 ust. 2 RODO w porównaniu z jego odpowiednikiem zawartym w art. 25 ust. 2 Dyrektywy 95/46 jest bardziej rozbudowany i szczegółowy. Jednocześnie, treść kryteriów oceny systemu prawnego państwa trzeciego w RODO wskazuje na konkretne zagadnienia związane z ochroną praw podstawowych oraz ochroną danych osobowych w państwie trzecim. Bezsprzecznie, katalog kryteriów, o którym mowa w art. 45 ust. 2 RODO nawiązuje do katalogu kryteriów wynikającego z Dokumentu WP12. Tym samym, za sprawą RODO kryteria oceny systemu prawnego, które były faktycznie stosowane w okresie obowiązywania Dyrektywy 95/46, a wynikały wyłącznie z Dokumenty WP12, zyskały właściwe umocowanie.

4.1. Ocena systemu prawnego państwa trzeciego w decyzjach w sprawie adekwatności wydane na podstawie RODO

W stosunkowo krótkim okresie obowiązywania RODO[203], Komisja Europejska wydała cztery decyzje w sprawie adekwatności, tj.: w sprawie Japonii[204], w sprawie

[203] O czym była mowa wyżej, w ponad dwudziestoletnim okresie obowiązywania Dyrektywy 95/46 zostało wydanych 13 decyzji w sprawie adekwatności.

[204] Decyzja wykonawcza Komisji (UE) 2019/419 z dnia 23 stycznia 2019 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Japonię na mocy ustawy o ochronie informacji osobowych (Dz. U. UE. L. z 2019 r. nr 76, str. 1, dalej: Decyzja w sprawie adekwatności Japonii).

Zjednoczonego Królestwa [205], w sprawie Korei Południowej [206] oraz w sprawie adekwatności Ram Ochrony Prywatności (DPF)[207].

Procedura związana z wydaniem decyzji w sprawie adekwatności na podstawie RODO, składa się z opinii Europejskiej Rady Ochrony Danych Osobowych oraz właściwej decyzji Komisji Europejskiej [208]. Natomiast, nowym elementem procedury jest stanowisko Parlamentu Europejskiego przyjmowane w formie rezolucji.

W swoich opiniach Europejska Rada Ochrony Danych Osobowych utrzymała dotychczasową praktykę, przeprowadzając ocenę z wykorzystaniem kryteriów zawartych w wytyczanych swojego autorstwa, Dokumencie WP254[209]. Pozornie, tylko w jednym przypadku Europejska Rada Ochrony Danych Osobowych dokonała oceny w nieco inny sposób. Był to przypadek oceny Zjednoczonego Królestwa, w związku z procedurą wyjścia tego państwa z Unii Europejskiej. Mimo deklarowania, że Zjednoczone Królestwo to były kraj członkowski Unii Europejskiej, którego system prawny musiał uwzględniać prawo Unii Europejskiej [210], zasadniczym punktem odniesienia dla Europejskiej Rady Ochrony Danych Osobowych był Dokument WP254, wspierany przez dodatkowe kryteria w postaci art. 7, 8 i 47 Katy Praw Podstawowych oraz art. 8 Europejskiej Konwencji Praw Człowieka[211].

---

[205] Decyzja wykonawcza Komisji (UE) 2021/1772 z dnia 28 czerwca 2021 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo (Dz. U. UE. L. z 2021 r. Nr 360, str. 1 ze zm., dalej: Decyzja w sprawie adekwatności Zjednoczonego Królestwa).

[206] Decyzja wykonawcza Komisji (UE) 2022/254 z dnia 17 grudnia 2021 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 stwierdzająca odpowiedni stopień ochrony danych osobowych przez Republikę Korei na mocy ustawy o ochronie danych osobowych (Dz. U. UE. L. z 2022 r. Nr 44, str. 1, dalej: Decyzja w sprawie adekwatności Korei Południowej).

[207] Decyzja wykonawcza Komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE-USA (Dz. U. UE. L. z 2023 r. Nr 231, str. 118, dalej: Decyzja w sprawie adekwatności Ram Ochrony Prywatności).

[208] Podobnie jak procedura związana z wydaniem decyzji w sprawie adekwatności przeprowadzana na podstawie przepisów Dyrektywy 95/46.

[209] Europejska Rada Ochrony Danych Osobowych: *Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan*'. 5.12.2018. https://edpb.europa.eu/sites/default/files/files/file1/2018-12-05-opinion_2018-28_art.70_japan_adequacy_en.pdf [dostęp: 26.05.2021], pkt 7; Europejska Rada Ochrony Danych Osobowych: *Opinion 32/2021 Regarding the European Commission Draft Implementing Decision Pursuant to Regulation (EU) 2016/679 on the Adequate Protection of Personal Data in the Republic of Korea Version 1.0*. 24.09.2021, https://edpb.europa.eu/system/files/2021-09/edpb_opinion322021_republicofkoreaadequacy_en.pdf [dostęp: 21.10.2021], pkt 4, pkt 34.

[210] Europejska Rada Ochrony Danych Osobowych: *Opinion 14/2021 Regarding the European Commission Draft Implementing Decision Pursuant to Regulation (EU) 2016/679 on the Adequate Protection of Personal Data in the United Kingdom*. 13.04.2021, https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf [dostęp: 26.05.2021], pkt 45.

[211] Ibidem, pkt 46.

Rezolucje Parlamentu Europejskiego, co do zasady, treściowo odpowiadają opiniom Europejskiej Rady Ochrony Danych Osobowych. Parlament Europejski odnosi się więc do zidentyfikowanych w systemie prawnym państwa trzeciego podstawowych definicji, czy ogólnie do zasad ochrony danych osobowych i środków zapewniających ich egzekwowanie[212]. Jednocześnie, Parlament Europejski wskazuje te kryteria oceny systemu prawnego państwa trzeciego stosowane przez Europejską Radę Ochrony Danych Osobowych, które w jego ocenie wymagają badanym państwie trzecim szczególnej uwagi[213].

W przypadku decyzji w sprawie adekwatności, zmianie ulegało jej uzasadnienie. Uzasadnienie stało się bardziej wyczerpujące w porównaniu z decyzjami wydanymi na podstawie Dyrektywy 95/46. Komisja Europejska, wyjaśniając wyniki przeprowadzonej oceny systemu prawnego państwa trzeciego, omawia aparaturę pojęciową, zasady ochrony danych osobowych i prawa osób, których dane dotyczą, ze wskazaniem podstawy prawnej oraz sposobów postrzegania tych zasad lub praw w badanym państwie trzecim. Omawiany jest także funkcjonujący nadzór, a zwłaszcza organ nadzorczy, jak również środki ochrony prawnej przyznanych jednostce[214]. Osobna część każdej z decyzji przeznaczona jest na opis dotyczący przetwarzania danych przez organy państwa w zakresie zapewnienia bezpieczeństwa narodowego[215]. W zakresie tego kryterium treściowo wyróżnia się decyzja w sprawie adekwatności Zjednoczonego Królestwa z uwagi na szczegółowości ustaleń na temat przetwarzania danych organy państwa w związku z zapewnienie bezpieczeństwa narodowego[216].

W świetle powyższego, Komisja Europejska zasadniczo stosuje kryteria wskazane w art. 45 ust. 2 RODO, wzbogacone o kryteria, o których mowa w Dokumencie WP254. Wciąż jednak Komisja Europejska dysponuje swobodą wyboru kryteriów oceny systemu prawnego. Mimo, że art. 45 ust. 2 RODO wprost wskazuje na konieczność uwzględnienia co najmniej wszystkich kryteriów, które wymienia, Komisja Europejska w praktyce stosowana jest odmienna interpretacja. W żadnej z decyzji w sprawie adekwatności wydanej na podstawie RODO nie znalazło się omówienie kryterium

[212] *European Parliament Resolution of 13 December 2018 on the Adequacy of the Protection of Personal Data Afforded by Japan*. 13.12.2018. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0529_EN.pdf pkt O-T [dostęp: 31.05.2021] pkt 8.
[213] Ibidem, pkt 12, pkt 14-15, pkt 17-18, pkt 20-22.
[214] Decyzja w sprawie adekwatności Japonii, pkt 17-112; Decyzja w sprawie adekwatności Zjednoczonego Królestwa, pkt 20-111; Decyzja w sprawie adekwatności Korei Południowej, pkt 14-138.
[215] Decyzja w sprawie adekwatności Japonii, pkt 114-170; Decyzja w sprawie adekwatności Zjednoczonego Królestwa, pkt 112 - 272; Decyzja w sprawie adekwatności Korei Południowej, pkt 139 - 208.
[216] Decyzja w sprawie adekwatności Zjednoczonego Królestwa, pkt 134-174, pkt 176-272.

ochrony praw człowieka i rządów prawa, na które wskazuje art. 45 ust. 2 lit. a RODO. Z kolei kryterium międzynarodowych zobowiązań państwa trzeciego, wynikające z art. 45 ust. 2 lit. a RODO znalazło swój wyraz tylko w decyzji w sprawie Zjednoczonego Królestwa. Komisja Europejska wskazała wówczas na fakt ratyfikacji przez Zjednoczone Królestwo Konwencji nr 108. W obu sytuacjach, Komisja Europejska nie wyjaśniła w treści decyzji co było powodem pominięcia jednego lub obu kryteriów.

Ocena Komisji Europejskiej wyrażona w treści decyzji w sprawie adekwatności pozostaje bliższa kryteriom stosowanym przez Europejską Radę Ochrony Danych Osobowych. Tym samym, nadal podstawowe znaczenie dla oceny systemu prawnego państwa trzeciego należy przypisać dokumentowi Europejskiej Rady Ochrony Danych Osobowych, aktualnie Dokumentowi WP254.

4.2. Rola wytycznych Europejskiej Rady Ochrony Danych Osobowych

Dokument WP254[217] to nowa wersja Dokumentu WP12. Tak jak Dokument WP12, Dokument WP254 został oparty na dwóch podstawowych kryteriach oceny, które można określić jako kryterium treści zasad ochrony danych osobowych oraz kryterium sposobów zapewnienia ich zastosowania w praktyce[218].

Na kryteria proponowane przez Europejską Radę Ochrony Danych Osobowych w dokumencie WP254 składają się:

(1) kryterium odpowiedniej aparatury pojęciowej, obejmujące pojęcia danych osobowych, przetwarzania danych, administratora, podmiotu przetwarzającego na zlecenie administratora (procesora), odbiorcy danych oraz danych wrażliwych[219].

(2) kryterium podstawowych zasad ochrony danych osobowych, na które składają się zasady:
   (a) przetwarzania danych zgodnie z prawem,
   (b) ograniczonego celu przetwarzania,
   (c) jakości i proporcjonalności danych,
   (d) retencji danych,
   (e) bezpieczeństwa danych (w tym ich poufności),
   (f) przejrzystości,

[217] Europejska Rada Ochrony Danych Osobowych: *Adequacy Referential WP 254*. 28.11.2017. https://webcache.googleusercontent.com/search?q=cache:qz03vIIbQwsJ:https://ec.europa.eu/newsroom/article29/redirection/document/57550+&cd=2&hl=pl&ct=clnk&gl=pl&client=safari [dostęp: 26.10.2021], dalej: Dokument WP254 lub WP254.
[218] Ibidem, s. 3.
[219] Ibidem, s. 5.

(g) prawa dostępu do danych i ich modyfikacji, prawa do usunięcia danych i sprzeciwu wobec przetwarzania,
(h) dalszego transferu danych,
(i) dodatkowe zasady: przetwarzania specjalnych kategorii danych, przetwarzania danych na potrzeby marketingu, przetwarzania danych na potrzeby profilowania i automatycznego podejmowania decyzji[220].

(3) kryterium zapewnienia przestrzegania zasad i ich egzekwowania, w ramach którego wyróżniono:
(a) organ nadzorczy o odpowiednich kompetencjach,
(b) ogólny dobry poziom ochrony danych osobowych wynikający ze świadomego postępowania administratorów danych,
(c) rozliczalność administratorów
(d) środki ochrony prawnej przyznane osobie, której dane dotyczą, umożliwiające wykorzystanie jej praw i podjęcie działań zaradczych na wypadek naruszenia zasad ochrony danych osobowych[221].

(4) kryterium dotyczące zagadnienia przetwarzania danych przez organy państwowe w celu zapewnienia bezpieczeństwa narodowego, odnoszące się do wytycznych Europejskiej Rady Ochrony Danych Osobowych w tym zakresie[222], przy czym Europejska Rada Ochrony Danych Osobowych wyjaśnia, że kryterium to obejmuje zrozumiałą, precyzyjną podstawę prawną przetwarzania danych, wykazanie konieczności i proporcjonalności dostępu do danych, nadzór oraz skuteczne środki ochrony prawnej przyznane osobom, których dane dotyczą[223].

Przywołane powyżej kryteria nawiązują do kryteriów, o których wspominał Dokument WP12. Jednakże, kryteria oceny wynikające z Dokumentu WP254 są bardziej rozbudowane i szczegółowe. Za sprawą Dokumentu WP254 nieodłącznym elementem oceny systemu prawnego państwa trzeciego stało kryterium przetwarzania danych przez organy państwowe, a więc kryterium wynikające z wyroków w sprawach Schrems I oraz Schrems II. Nadto, elementem oceny stała się także siatka pojęciowa, związana z zagadnieniami ochrony danych osobowych. Niektóre z kryteriów, czyli kryterium zasad

[220] Ibidem, s. 5–7.
[221] Ibidem, s. 7–8.
[222] Zob. Grupa Robocza art. 29: *Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection through Surveillance Measures When Transferring Personal Data (European Essential Guarantees)*. 13.04.2016. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf [dostęp: 26.10.2021], dalej: Dokument WP237 lub WP237.
[223] Dokument WP254, s. 9.

oraz kryterium zapewnienia ich przestrzegania, bezpośrednio nawiązują do kryteriów oceny, o których mowa w art. 45 ust. 2 RODO. Europejska Radę Ochrony Danych Osobowych nie zdecydowała się jednak na implementację wszystkich kryteriów oceny państwa trzeciego, na które wskazuje art. 45 ust. 2 RODO.

Pobocznie, należy zauważyć, że kombinacja teorii, treści przepisów i praktyki stanowiła punkt wyjścia także dla oceny systemu prawnego, którą Europejska Rada Ochrony Danych Osobowych przeprowadza na zasadach określonych w Dyrektywie 2016/680[224].

4.3. Przekazywanie danych osobowych między Unią Europejską a USA w okresie obowiązywania RODO – nowe porozumienie

Unieważnienie decyzji w sprawie adekwatności Tarczy Prywatności spowodowało, że transfery danych osobowych z Unii Europejskiej do USA stały się dopuszczalne pod warunkiem zastosowania jednego z odpowiednich zabezpieczeń, o których mowa w art. 46 RODO lub jednego z odstępstw wskazanych w art. 49 RODO. Niedogodności z tym związane, w tym rosnące koszty działalności, a zwłaszcza obsługi prawnej oraz ograniczony zakres zastosowania art. 46 i 49 RODO[225] przyczyniły się do intensyfikacji prac organów europejskich nad wypracowaniem kolejnego mechanizmu przekazywania danych osobowych między Unią Europejską a USA. W swojej rezolucji z 20 maja 2021 Parlament Europejski wezwał Komisję Europejską do podjęcia działań zmierzających do wypracowania nowego rozwiązania, które stanie się podstawą prawną dla swobodnych transferów danych osobowych między Unią Europejską a USA[226]. O ile przywołana rezolucja skupiała się na potrzebie wypracowania nowego rozwiązania dla transferów danych osobowych między Unią Europejską a USA, o tyle Parlament Europejski przedstawił swoje zapatrywania w przedmiocie kryteriów wykorzystywanych na potrzeby oceny. Zdaniem Parlamentu Europejskiego, „(…) Komisja [Europejska – dod. aut.] nie powinna schodzić poniżej tych kryteriów przy ocenie, czy dane państwo trzecie kwalifikuje się do decyzji stwierdzającej odpowiedni stopień ochrony”[227]. Tym samym, Parlament Europejski uważa, że z Dokumentu WP254 oraz jego

---

[224] Europejska Rada Ochrony Danych Osobowych: *Recommendations 01/2021 on the Adequacy Referential under the Law Enforcement Directive*. 2.02.2021. https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf [dostęp: 26.05.2021], pkt 5, pkt 14, pkt 25.

[225] *European Parliament Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework*. 11.05.2023. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html [dostęp: 8.04.2024], pkt 11.

[226] *European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 — Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (‘Schrems II’), Case C-311/18 (2020/2789(RSP))*. 20.05.2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0256 [dostęp: 16.02.2024], pkt 27-28.

[227] Ibidem, pkt 33.

odpowiednika wydanego na tle przepisów Dyrektywy 2016/680, wynika minimalny, niezbędny zakres oceny systemu prawnego państwa trzeciego[228].

Współpraca Komisji Europejskiej z przedstawicielami władz USA doprowadziła do wynegocjowania nowego porozumienia, Ram Ochrony Prywatności, które stały się podstawą dla wydania nowej decyzji w sprawie adekwatności.

Przedstawiony przez Komisję Europejską projekt decyzji w sprawie adekwatności Ram Ochrony Prywatności, tak jak w przypadku każdego innego państwa trzeciego, został poddany opiniowaniu Europejskiej Rady Ochrony Danych Osobowych. W opinii podkreślono, że motywacją dla ponownego posłużenia się modelem porozumienia w sprawie ochrony danych osobowych były relacje gospodarcze między Unią Europejską a USA oraz potrzeba zapewniania poziomu ochrony danych osobowych satysfakcjonującego z perspektywy standardów Unii Europejskiej [229]. Zdaniem Europejskiej Rady Ochrony Danych Osobowych treść zasad funkcjonowania Ram Ochrony Prywatności jest identyczna z zasadami funkcjonowania Tarczy Prywatności [230]. Z tego względu, Europejska Rada Ochrony Danych Osobowych zdecydowała się na pominięcie rozważań dotyczących zasad funkcjonowania Ram Ochrony Prywatności, które odpowiadają zasadom funkcjonowania Tarczy Prywatności, a swoje rozważania ograniczyć tylko do niektórych, wybranych elementów. Tak, jak w przypadku pozostałych decyzji w sprawie adekwatności wydanych na podstawie RODO, zasadniczym punktem odniesienia dla Europejskiej Rady Ochrony Danych Osobowych był Dokument WP254, wspierany przez dodatkowe kryteria w postaci art. 7,8 i 47 Karty Praw Podstawowych oraz art. 8 Europejskiej Konwencji Praw Człowieka[231]. Co istotne, w treści opinii Europejska Rady Ochrony Danych Osobowych posługiwała się dodatkowo kryterium międzynarodowych zobowiązań państwa trzeciego, tj. kryterium wynikającym wyłącznie z art. 45 ust. 2 RODO[232]. Europejska Rada Ochrony Danych Osobowych omówiła zobowiązania międzynarodowe USA, podkreślając fakt członkostwa USA w OECD i stosowania wytycznych OECD w sprawie ochrony danych osobowych, członkostwa w APEC oraz uczestnictwa jako państwo – obserwator w pracach komitetu konsultacyjnego Rady Europy w sprawie Konwencji nr 108.

[228] Ibidem.
[229] Europejska Rada Ochrony Danych Osobowych*: Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework*. 28.02.2023. https://www.edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [dostęp: 16.02.2024] pkt 6.
[230] Ibidem, pkt 12.
[231] Ibidem, pkt 14.
[232] Ibidem, pkt 22-26.

Ocena Ram Ochrony Prywatności przeprowadzona przez Europejską Radę Ochrony Danych Osobowych dotyczyła również jasności i przejrzystości DPF dla odbiorcy, w tym w zakresie wykorzystywanej terminologii[233]. Zgodnie z deklaracją, Europejska Rada Ochrony Danych Osobowych w dalszej części opinii omówiła wybrane zagadnienia. Do tej grupy zaliczają się:

1. siatka pojęciowa[234];
2. zasada celowości[235];
3. prawo dostępu do danych i ich modyfikacji, prawa do usunięcia danych i sprzeciwu wobec przetwarzania[236];
4. zasada dalszego transferu danych[237];
5. zasada przetwarzania danych na potrzeby profilowania i automatycznego podejmowania decyzji[238];
6. zagadnienia związane z zapewnieniem przestrzegania zasad Ram Ochrony Prywatności i ich egzekwowania, w szczególności wykorzystania modelu certyfikacji[239];
7. zagadnienia związane z ochroną prawną przyznaną osobie, której dane dotyczą[240];
8. problematyka przetwarzania danych osobowych przez organy państwowe, w tym w celu zapewnienia bezpieczeństwa narodowego[241].

Do projektu decyzji w sprawie adekwatności Ram Ochrony Prywatności odniósł się także Parlament Europejski. W rezolucji podkreślono, że względy natury politycznej lub relacje handlowe nie mogą być przeciwwagą dla ochrony prawa do prywatności i prawa do ochrony danych osobowych[242]. Następnie, szczegółowo omówiono zagadnienia funkcjonowania Ram Ochrony Prywatności w odniesieniu do dostępu organów państwa do danych osobowych[243]. W ocenie Parlamentu Europejskiego aktualnym pozostaje problem braku równego dostępu obywateli i nie-obywateli USA do środków ochrony prawnej w związku z przetwarzaniem danych osobowych przez organy państwa,

[233] Ibidem, pkt 36-39.
[234] Ibidem, pkt 40-41.
[235] Ibidem, pkt 42-43.
[236] Ibidem, pkt 44-54.
[237] Ibidem, pkt 55-59.
[238] Ibidem, pkt 60-65.
[239] Ibidem, pkt 66-70.
[240] Ibidem, pkt 71-79.
[241] Ibidem, pkt 80-241.
[242] *European Parliament Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework*…, pkt 1.
[243] Ibidem, pkt 2-9.

a zwłaszcza organy wywiadowcze[244]. Jednocześnie, Parlament Europejski zarzucał Komisji Europejskiej nienależyte uregulowaniu środków ochrony prawnej, dostępnych dla jednostki w kontaktach z podmiotami niepaństwowymi, gdzie zasadniczym problemem jest przyznanie tym podmiotom znacznej swobody w wyborze i implementacji tychże środków[245]. Parlament Europejski, komentując umocowanie Ram Ochrony Prywatności, zwrócił uwagę na fakt, że stanowią one rozporządzenie wykonawcze prezydenta USA, które w każdej chwili, bez zgody Kongresu USA lub notyfikacji organów Europejskich, może zostać uchylone lub zmienione[246]. Nadto, obawy Parlamentu Europejskiego wzbudza potencjalna niemożność monitorowania implementacji Ram Ochrony Prywatności do porządku prawnego USA, ponieważ procedury Sądu Ochrony Kontroli Danych (ustanowionego przez Ramy Ochrony Prywatności) są niejasne[247]. W związku z tym, wytknięto Komisji Europejskiej pobłażliwość w stosunku do USA, której przejawem ma być oparcie decyzji w sprawie adekwatności na rozporządzeniu wykonawczym prezydenta USA o wątpliwej stabilności, a także brak daty końcowej obowiązywania decyzji w sprawie adekwatności[248], która zmusiłaby Komisję Europejską do przeprowadzenia kolejnej, całościowej oceny[249]. Dodatkowo, Parlament Europejski poparł uwagi zgłaszane pod adresem Ram Ochrony Prywatności przez Europejską Radę Ochrony Danych Osobowych[250]. Mając na uwadze powyższe spostrzeżenia, Parlament Europejski uznał, że poziom ochrony danych osobowy zapewniany przez Ramy Ochrony Prywatności nie odpowiada standardom oczekiwanym przez prawo Unii Europejskiej[251] i wezwał Komisję Europejską do podjęcia dalszych negocjacji z USA celem wypracowania właściwego porozumienia[252].

Decyzja w sprawie adekwatności Ram Ochrony Prywatności została wydana przez Komisję Europejską 10 lipca 2023 r. Treść i konstrukcja decyzji są identyczne z treścią i konstrukcją decyzjami w sprawie adekwatności Tarczy Prywatności. Komisja Europejska zastosowała kryteria oceny wynikające z Dokumentu WP254 i omówiła każdy z elementów Ram Ochrony Prywatności, który realizuje poszczególne kryterium. Zgadzam się z uwagami Parlamentu Europejskiego i Europejskiej Rady Ochrony Danych

[244] Ibidem, pkt 6.
[245] Ibidem, pkt 10.
[246] Ibidem, pkt 12.
[247] Ibidem, pkt J.
[248] Datę końcową zawiera decyzja w sprawie adekwatności Zjednoczonego Królestwa.
[249] *European Parliament Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework* …, pkt 12.
[250] Ibidem, pkt 13.
[251] Ibidem, pkt 17-19.
[252] Ibidem, pkt 20.

Osobowych o trudności w odbiorze tej części decyzji. Komisja Europejska zamiast przytoczyć poszczególne postanowienia Ram Ochrony Prywatności, powiązane z opisywanym kryterium, zdecydowała się na zawarcie jedynie właściwych odesłań do tychże postanowień[253]. Przedmiotem oceny Komisji Europejskiej były Ramy Ochrony Prywatności, jak również przepisy prawa w zakresie regulacji dostępu organów państwa do danych osobowych. Podobnie jak w przypadku opinii Europejskiej Rady Ochrony Danych Osobowych i rezolucji Parlamentu Europejskiego opis realizacji tego kryterium oceny zdominował treść decyzji w sprawie adekwatności.

W treści decyzji w sprawie adekwatności Ram Ochrony Prywatności Komisja Europejska nie odniosła się jednak ani do kryterium ochrony praw człowieka i rządów prawa (art. 45 ust. 2 lit. a RODO) ani do kryterium międzynarodowych zobowiązań państwa trzeciego (art. 45 ust. 2 lit. c RODO)[254].

5. Ocena poziomu ochrony danych osobowych w państwie trzecich w spostrzeżeniach przedstawicieli doktryny

Problematyka oceny systemu prawnego państwa trzeciego znajduje odzwierciedlenie w rozważaniach doktryny. Mimo zmiany przepisów regulujących ochronę danych osobowych w Unii Europejskiej, poglądy wypracowane pod rządami Dyrektywy 95/46 uległy dalszemu rozwinięciu. W związku z tym, rozważania doktryny zostaną przedstawione z zastosowaniem podziału tematycznego a nie chronologicznego.

Rozważania doktryny obejmują pożądany kształt oceny systemu prawnego. W ocenie P. Bluma konieczne jest przeprowadzenie całościowej oceny, uwzględniającej także kulturę prawną[255]. Podobnego zdania jest S.L. Duque Carvahlo, dla której ocena powinna obejmować całokształt sytemu prawnego państwa trzeciego, ale nie chodzi tu o dokładną kopię systemu Unii Europejskiej, a właśnie o całościową ocenę[256]. P.M. Schwartz za punkt wyjścia uznaje uwzględnienie kontekstu w jakim znajduje się regulacja ochrony danych osobowych w państwie trzecim[257]. Sądzę, że powyższe postulaty można potraktować jako swego podstawę czy motyw przewodni, którym należy się kierować przeprowadzając każdą ocenę. Innymi słowy, całościowa ocena, w której

[253] Ramy Ochrony Prywatności są jednym z załączników decyzji w sprawie adekwatności Ram Ochrony Prywatności

[254] Mimo, że opis spełnienia przez USA kryterium zobowiązań międzynarodowych państwa trzeciego przedstawiła Europejska Rada Ochrony Danych Osobowych w swoje opinii.

[255] P. Blume: *EU Adequacy Decisions: The Proposed New Possibilities*. „International Data Privacy Law" , 2015, nr 1, s. 37.

[256] S.L. Duque de Carvalho: *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108*. „European Data Protection Law Review (EDPL)", 2019, nr 1, s. 58.

[257] P.M. Schwartz: *The EU-U.S. privacy collision: a turn to institutions and procedures*. „Harvard Law Review", 2013, nr 126, s. 1973.

bierze się pod rozwagę zarówno kontekst jak i tło kulturowe to fundament prawidłowo przeprowadzanej oceny systemu prawnego państwa trzeciego. Potwierdzeniem takiego stanowiska są prezentowane poniżej spostrzeżenia doktryny odnośnie do stosowanych, jak i rekomendowanych kryteriów oceny.

Wątkiem pobocznym rozważań doktryny są poglądy na temat wytycznych Grupy Roboczej art. 29, a zwłaszcza Dokumentu WP12. P. Blume traktuje Dokument WP12 jako Dyrektywę 95/46 w pigułce, który odpowiada ścisłemu rozumieniu adekwatności[258]. Według V. Ledhonvirty stosowanie Dokumentu WP12 podyktowane jest brakiem możliwości bezpośredniego stosowania przepisów prawa Unii Europejskiej w stosunku do państw trzecich[259]. Nieco inaczej Dokument WP12 postrzega A.B. Makulilo, według którego kryteria wynikające z Dokumentów WP4 i WP12 wykraczają poza wymagania wynikające z przepisów Dyrektywy 95/46[260]. J. Wagner dostrzega, że w opiniach Grupy Roboczej art. 29 brakuje wyjaśnień na temat sposobu przeprowadzenia oceny, ponieważ same opinie wskazują tylko na Dokument WP12 i jego kryteria[261].

Przedstawiciele doktryny omawiają również stosowane, jak i proponowane kryteria oceny systemu prawnego państwa trzeciego, niekiedy ujmowanym przez pryzmat rozumienia adekwatności. W skrajnie odmienny sposób postrzegane są kryteria zawarte w przepisach prawa ochrony danych osobowych Unii Europejskiej, a szczególnie w RODO. S. Sharma[262], podobnie jak C. Kuner i L. Wittershagen[263] uważa, że ocena systemu prawnego państwa trzeciego, dokonywana przez Komisję Europejską jest determinowana przez art. 45 ust. 2 RODO, którego kryteria muszą być uwzględnione podczas oceny. Przeciwny pogląd głosi J. Wagner[264]. W podobny sposób wypowiada się S. Slokenberga wraz z zespołem, dla której ocena systemu prawnego państwa trzeciego dokonywana jest z użyciem trzech zasadniczych kryteriów: kryterium rządów prawa, kryterium istnienia organu nadzorczego oraz kryterium zobowiązań międzynarodowych, zwłaszcza w przedmiocie ochrony danych osobowych, przy czym przepisy prawa Unii Europejskiej nie wskazują, jak przeprowadzić ocenę i kiedy uznać, że dane kryterium

[258] P. Blume: *Transborder Data Flow: Is There a Solution in Sight*. „International Journal of Law and Information Technology", 2000, nr 1, s. 69.
[259] V. Lehdonvirta: *European Union Data Protection Directive: Adequacy of Data Protection in Singapore*. „Singapore Journal of Legal Studies ", 2004, nr 2, s. 521.
[260] A.B. Makulilo: *Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?*. „International Data Privacy Law ", 2013, nr 1, s. 49.
[261] J. Wagner: *The Transfer of…*, s. 325.
[262] S. Sharma, *Data Privacy and…*, s. 162–63.
[263] C. Kuner: *The Path to…*, s. 69, 80; L. Wittershagen: *Transfer of Personal Data to Third Countries under the European Data Protection Laws*. W: *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. Red. L. Wittershagen. De Gruyter, Berlin – Boston 2023, s. 59.
[264] J. Wagner: *The Transfer of…*, s. 319.

zostało spełnione[265]. C. Kuner podkreśla jednak, że art. 45 ust. 2 RODO to otwarty katalog kryteriów[266]. Tym samym, jak twierdzi P. Fajgielski[267], z art. 45 ust. 2 RODO wynika jedynie minimalny zakres oceny państwa trzeciego. Można więc przyjąć, że charakter otwartego katalogu kryteriów z art. 45 ust. 2 RODO pozwala na stosowanie dodatkowych kryteriów oceny[268].

Nawiązując do poglądów o otwartym katalogu kryteriów oceny systemu prawnego, część spośród przedstawicieli doktryny wprost formułuje własne kryteria lub proponuje ich zestaw. A. Zinser wyjaśnia, że katalog kryteriów oceny systemu prawnego państwa trzeciego jest otwarty, a jednym z dodatkowych kryteriów, które powinno się uwzględnić przy ocenie jest czas trwania planowanego przetwarzania danych osobowych[269]. Autor zaproponował swoją listę kryteriów, na którą składają się:

1) zgodność przetwarzania z przepisami prawa,
2) istnienie szczególnego reżimu dla danych wrażliwych,
3) istnienie praw podmiotów danych,
4) bezpieczeństwo przetwarzania danych oraz istnienie środków nadzoru i mechanizmów egzekwowania prawa[270].

Zdaniem A. Zinsera z pojęcia rządów prawa wynika konieczność uwzględnienia w ocenie całokształtu przepisów obowiązujących w danych państwie, które mogą wpływać na poziom ochrony danych osobowych[271]. Natomiast sam fakt członkostwa danego państwa w takiej organizacji międzynarodowej jak Rada Europy czy OECD nie jest tożsamy z istnieniem odpowiedniej regulacji ochrony danych osobowych, choć ratyfikacja Konwencji nr 108 pozwala domniemywać o adekwatnym poziomie ochrony danych[272]. Busch dostrzega dwa zasadnicze kryteria: regulację ochrony danych osobowych

---

[265] S. Slokenberga, J. Reichel, R. Niringiye i in.: *EU Data Transfer Rules and African Legal Realities: Is Data Exchange for Biobank Research Realistic?*. „International Data Privacy Law", 2019, nr 1. str. 35.
[266] C. Kuner: *Komentarz do art. 45*…, s. 788.
[267] P. Fajgielski: *Komentarz do rozporządzenia nr 2016/679 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), art. 45.* W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.
[268] Szerzej na temat problematyki wykorzystywania dodatkowych kryteriów oceny systemu prawnego państwa trzeciego w dalszej części tego rozdziału.
[269] A. Zinser: *International Data Transfer out of The European Union: The Adequate Level of Data Protection According to Article 25 of The European Data Protection Directive*. „The John Marshall Journal of Information Technology & Privacy Law", 2003, nr 4. s. 551–552.
[270] A. Zinser: *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*. „Tulane Journal of Technology and Intellectual Property", 2004, nr 6, s. 176; także A. Zinser: *International Data Transfer…*, s. 559.
[271] A. Zinser: *International Data Transfer…*, s. 553.
[272] Ibidem, s. 553–554.

za pomocą odpowiedniej ustawy oraz istnienie organu nadzorczego, ponieważ to te kryteria niejako przesądzają o uznaniu adekwatności ochrony danych osobowych zapewnianej przez system prawny państwa trzeciego[273]. A.B. Makulilo zauważa, że ocena powinna prowadzić do ustalenia rzeczywistego poziomu ochrony danych osobowych[274]. W związku z tym, szczególnie ważnym elementem analizy jest praktyka[275]. A.B. Makulilo sugeruje, że ocena systemu prawnego państwa trzeciego powinna składać się z dwóch elementów, na które wskazuje Dokument WP12 tj. poszukiwania podstawowych zasad ochrony danych osobowych oraz środków zapewniających ich przestrzeganie[276]. R.H. Weber uważa, że badanie systemu prawnego państwa trzeciego powinno dotyczyć przepisów, w tym samoregulacji, nadzoru, odpowiedzialności za naruszenia ochrony danych i właściwych sankcji[277]. Autor jest zdania, że rozumienie kryteriów powinno być wolne od wpływów (naleciałości) wynikających z krajowych systemów prawnych, a jako punkt odniesienia należy traktować podstawowe rozumienie zakorzenione powszechnie w międzynarodowej doktrynie ochrony praw człowieka[278]. Katalog kryteriów R.H. Webera obejmuje wykorzystanie:

1) kryterium rodzaju danych, oparte o założenie, że im bardziej dane są wrażliwe tym intensywniejsza powinna być ich ochrona;
2) kryterium celu przetwarzania danych, gdzie interes administratora przekłada się na poziom zapewnianej ochrony;
3) kryterium retencji danych rozumiane jako odpowiedni okres, ponieważ zarówno za krótki, jak i za długi okres przetwarzania danych niesie za sobą ujemne skutki dla podmiotów danych i administratora[279].

C. Wolf proponuje spoglądanie na system prawny państwa trzeciego z uwzględnieniem Fair Information Practice Principles, które w jego ocenie są podstawą systemu ochrony danych osobowych, w tym także systemów Unii Europejskiej i USA, które różni sposób implementacji owych zasad do systemów prawnych[280]. Zdaniem autora sięganie do

[273] A. Busch*: The Regulation of Transborder Data Traffic: Disputes across the Atlantic*. „Security and Human Rights", 2012, nr 4, s. 318–319.
[274] A. B. Makulilo: *Data Protection Regimes*…, s. 43.
[275] Ibidem, s. 47.
[276] Ibidem, s. 44–46.
[277] R.H. Weber: *Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives*. „International Data Privacy Law", 2013, nr 2, s. 124.
[278] Ibidem.
[279] Ibidem.
[280] J. Wolf: *Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*. „Washington University Journal of Law & Policy ", 2013, nr 43, s. 229–230.

dotychczasowych decyzji Komisji Europejskiej jest dobrym uzupełnieniem w zakresie kryteriów stosowanych przy ocenie, a zarazem wymagań jakie stawia się państwu trzeciemu[281]. C. Wolf podkreśla, że bazując na przeprowadzonych ocenach, w tym opiniach Grupy Roboczej art. 29, można dostrzec tendencję do pomijania treści regulacji, na rzecz formy systemu ochrony danych w państwie trzecim[282]. P.M. Schwartz uznaje trzy zasady ochrony danych osobowych za priorytetowe dla Unii Europejskiej, a tym samym kluczowe dla oceny: zasadę minimalizacji danych, zasadę jakość danych oraz prawo dostępu do danych[283]. B. Marcinkowski wyjaśnia, że związek ochrony danych osobowych z rządami prawa i demokratycznym społeczeństwem jako kryterium oceny przejawia się we wpływie, jaki wywiera ochrona informacji na gwarantowaną jednostce wolność[284]. Autor dostrzega konieczność poszukiwania zagrożeń dla ochrony danych osobowych zarówno wśród podmiotów prywatnych, jak i publicznych[285]. Jednocześnie ostrzega przed ograniczeniem oceny wyłącznie do przepisów prawa, z pominięciem orzecznictwa, ponieważ taka analiza nie dostarczy rzeczywistego obrazu systemu prawnego państwa trzeciego[286]. G. Maldoff i O. Tene, w oparciu o kazus USA, wskazują wyłącznie na dwa zasadnicze elementy-kryteria, które przesądzają o adekwatności, jakimi są prawo w zakresie ochrony danych osobowych (o ogólnym zakresie zastosowania) oraz istnienie organu nadzorczego[287]. M. Tzanou uważa, że ocena adekwatności sprowadza się także do dwóch kryteriów, jakimi są treść przepisów ochrony danych osobowych oraz praktyka stworzona w celu respektowania przepisów[288]. J. Stoddart, B. Chan i Y. Joly sprowadzają ocenę systemu prawnego państwa trzeciego wyłącznie do poszukiwania w tym państwie odpowiednich zasad ochrony danych osobowych, na które składają się zasady: ograniczenia celu przetwarzania, przejrzystości, jakości danych, proporcjonalności, bezpieczeństwa, dostępu do danych, sprostowania danych[289]. Samo przeprowadzenie oceny, jako ścisłe poszukiwanie w systemie prawnym państwa trzeciego jednego rozwiązania, kompleksowej regulacji ochrony danych

[281] Ibidem, s. 238.
[282] Ibidem, s., 256.
[283] P.M. Schwartz: *The EU-U.S*…., s. 1976.
[284] B. Marcinkowski*: Privacy Paradox(Es): In Search of a Transatlantic Data Protection Standard*. „Ohio State Law Journal ", 2013, nr 6, s. 1170–1171.
[285] Ibidem, s. 1171.
[286] Ibidem, s. 1183.
[287] G. Maldoff, O. Tene: *Essential Equivalence and European Adequacy after Schrems: The Canadian Example*. „Wisconsin International Law Journal", 2016, nr 2, s. 222–223.
[288] M. Tzanou: *European Union Regulation of Transatlantic Data Transfers and Online Surveillance*. „Human Rights Law Review ", 2017, nr 3, s. 547, 552.
[289] J. Stoddart, B. Chan, Y. Joly: *The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research*. „Journal of Law, Medicine and Ethics", 2016, nr 1, s. 144.

osobowych, to poważne zagrożenie[290]. Podobnego zdania jest C. Kuner, który przestrzega przed formalistycznym, sztywnym podejściem do oceny, ponieważ standard określony przez TSUE w sprawie Schrems I bynajmniej nie wymaga dokładnie takiej samej ochrony, ale zapewnienia wysokiego poziomu ochrony danych osobowych wynikającego z Karty Praw Podstawowych[291]. Według Komisji Europejskiej ocena to poszukiwanie w jako takim systemie prawnym państwa trzeciego istoty praw osoby, której dane dotyczą, wdrożonych w życie, a także sposobów egzekwowania tychże praw wraz z nadzorem[292]. A.D. Murray, przeprowadzając zwięzłą ocenę systemu prawnego Zjednoczonego Królestwa, wykorzystuje kryterium:

1) wyposażonego we właściwe kompetencje organu nadzorczego,
2) kryterium międzynarodowych zobowiązań w postaci przynależności do Europejskiej Konwencji Ochrony Praw Człowieka,
3) kryterium praw ochrony danych funkcjonujących w systemie prawnym, kryterium środków ochrony prawnej przyznanych jednostce, w tym środków administracyjnych i sądowych, które są skuteczne w praktyce[293].

Na tle art. 45 RODO, wespół z orzecznictwem TSUE, J. Wagner uznaje za szczególnie ważną praktykę postępowania w państwie trzecim[294]. Wskazówką dla interpretacji RODO może być Konwencja nr 108, ponieważ RODO to akt wdrażający Konwencję nr 108[295]. Przypisywanie szczególnej roli zasadom ochrony danych osobowych jest wspólne dla RODO, Konwencji nr 108 i OECD[296]. J. Wagner dostrzega jednak różnicę między podstawowymi zasadami, a ich rozumieniem według Grupy Roboczej art. 29, która sprowadza się do szerszego katalogu zasad, obejmującego dodatkowo kryterium aparatu pojęciowego oraz zasady dalszego transferu[297]. Zasada dalszego transferu ma chronić przed omijaniem wysokiego poziomu ochrony danych osobowych i wynikających z niego ograniczeń poprzez przekazanie danych do kolejnego kraju[298]. O ile kryterium środków ochrony prawnej trzeba odczytywać mając na względzie jego związek z prawem międzynarodowym, o tyle kryterium to nie może pomijać uprawnień,

---

[290] Ibidem, s. 150–151.
[291] C. Kuner*: Reality and Illusion…,* s. 902, 917.
[292] *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*. 10.01.2017. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN [dostęp: 2.11.2021] s. 6-7.
[293] A.D. Murray: *Data Transfers between the EU and UK Post Brexit?*. „International Data Privacy Law", 2017, nr 3, s. 156.
[294] J. Wagner: *The Transfer of…*, s.323.
[295] Ibidem, s. 327.
[296] Ibidem, s. 329.
[297] Ibidem.
[298] Ibidem, s. 330.

które zostały wprowadzone przez RODO[299]. S.L. Duque Carvahlo odnosząc się do koncepcji ekwiwalentności poziomu ochrony danych osobowych w państwie trzecim, uznaje, że na ocenę systemu prawnego państwa trzeciego składają się zasady ochrony danych osobowych wraz ze środkami ich egzekwowania, zaś zasadniczym celem ekwiwalentności jest ochrona praw fundamentalnych[300]. Według S.L. Duque Carvahlo, spośród kryteriów oceny trudno ustalić, które odpowiadają istocie rzeczy, z pewnością jednak nie wszystkie zasady zawarte w RODO muszą funkcjonować w systemie prawnym państwa trzeciego[301]. W ujęciu S. Sharmy ocena skupia się na poszukiwaniu w obcym systemie prawnym sposobów zapewniających ochronę osoby, której dane dotyczą[302]. Dla C.M.J. Ryngaerta i N.A.N.M van Eijka podczas oceny szczególną rolę odgrywają dwa kryteria: kryterium niezależnego organu nadzorczego oraz kryterium przejrzystości[303]. I. Ntouvas podsumowuje kryteria zawarte w art. 45 ust. 2 lit. a RODO jako wymagające skutecznej, generalnej regulacji ochrony danych osobowych, egzekwowalnych praw osoby, której dane dotyczą oraz środków ochrony prawnej, administracyjnych i sądowych, na wypadek naruszenia ochrony danych osobowych[304]. Z kolei B.A. Gur dostrzega w RODO trzy podstawowe kryteria: kryterium całokształtu systemu prawnego państwa trzeciego, kryterium skutecznego organu nadzorczego i kryterium międzynarodowych zobowiązań[305]. Ponieważ szczególnie ważną cechą organu nadzorczego jest niezależność, wskazówkami co do rozumienia niezależności należy poszukiwać w art. 52 i 53 RODO[306]. W dyskursie na temat kryteriów pojawia się niejako wątek poboczny, który sprowadza się do pytania o rolę samoregulacji podczas przeprowadzanej oceny. P.M. Schwartz powołując się na brzmienie Dyrektywy 95/46 sugeruje uwzględnianie w ocenie praktyki postępowania podmiotów profesjonalnych w państwie trzecim, w tym także samoregulacji, którą można postrzegać jako czynnik wywołujący pozytywny wpływ na poziom ochrony danych osobowych w sektorze prywatnym[307]. A. White uważa, że w niektórych przypadkach samoregulacja, wespół

[299] Ibidem, s. 333, 335.
[300] S. L. Duque de Carvalho: *Key GDPR Elements*…, s. 55.
[301] Ibidem s. 59–61.
[302] S. Sharma, *Data Privacy and…*, s. 164.
[303] C.M.J. Ryngaert, N.A.N.M. van Eijk: *International Cooperation by (European) Security and Intelligence Services: Reviewing the Creation of a Joint Database in Light of Data Protection Guarantees*. „International Data Privacy Law", 2019, nr 1, s. 72.
[304] I. Ntouvas: *Exporting Personal Data to EU-Based International Organizations under the GDPR*. „International Data Privacy Law", 2019, nr 4, s. 275.
[305] B.A. Gur: *The Normative Power of the EU: A Case Study of Data Protection Laws of Turkey*. „International Data Privacy Law", 2020, nr 4, s. 11.
[306] Ibidem, s. 14.
[307] P. M. Schwartz: *European Data Protection Law and Restrictions on International Data Flows*. „Iowa Law Review ", 1995, nr 3, s. 485, 492.

z legislacją, pozwala nawet uznać system prawny państwa trzeciego za adekwatny[308]. W podobny sposób wypowiada się A. Hughes, która wyraża aprobatę dla uznawania za adekwatne systemów prawnych, w których podstawą ochrony danych osobowych jest regulacja sektorowa czy samoregulacja[309]. S.R. Salbu zaznacza jednak, że samoregulacja, a tym samym jej ocena, nie może być pozostawiona bez właściwego nadzoru, ponieważ zagrożeniem płynącym z samoregulacji jest utrudnienie w egzekwowaniu przestrzegania zasad określonych przez dany podmiot, a tym samym zapewnianej ochrony[310]. A. Zinser argumentuje uwzględnienie w ocenie samoregulacji ze względu na jej popularność i funkcjonalnością[311]. Samoregulacja w ujęciu A. Zinsera wiąże się z rozproszoną regulacją, która nie jest rzadkim problem, a dodatkową komplikacją może być federalna struktura państwa czy regulacja ochrony danych osobowych albo tylko w sektorze publicznym albo tylko w sektorze prywatnym[312]. Nie stanowi to przeszkody dla postrzegania samoregulacji jako doprecyzowania ogólnie sformułowanych przepisów prawa[313]. P.M. Schwartz wyjaśnia, że problemem wynikającym z regulacji sektorowej jest niejednolita ochrona, ponieważ źródłem zróżnicowania jest podmiot przetwarzający dane i różne regulacje, którymi jest objęty ze względu na przedmiot swojej działalności[314]. W przypadku samoregulacji oraz regulacji sektorowych zasadnicza trudność, zdaniem P. Blume'a, to ustalenie rzeczywistego poziomu ochrony danych osobowych jaki zapewnia samoregulacja[315]. Z kolei największą wadą samoregulacji jest właśnie egzekwowalność przyznawanych uprawnień i nadzór nad ich przestrzeganiem, które to kryteria są podstawą ochrony danych osobowych w Unii Europejskiej[316]. V. Ledhonvirta także proponuje uwzględnienie samoregulacji w ocenie, jednak nie oznacza to, że samoregulacja automatycznie spełni wymagania stawiane przez Dokument WP12[317]. Według A. Deighton ochrona za pomocą samoregulacji powinna być sprzężona

[308] A. White: *Control of Transborder Data Flow: Reactions to the European Data Protection Directive*. „International Journal of Law and Information Technology", 1997, nr 2, s. 241.
[309] A. Hughes: *A Question of Adequacy - The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (CTH)*. „University of New South Wales Law Journal", 2001, nr 1, s. 271.
[310] S. R. Salbu: *The European Union Data Privacy Directive and International Relations*. „Vanderbilt Journal of Transnational Law", 2002, nr 2, s. 682.
[311] A. Zinser: *International Data Transfer…,* s. 554.
[312] A. Zinser: *European Data Protection…,* s. 176.
[313] A. Zinser: *International Data Transfer…,* s 554.
[314] P.M. Schwartz: *The EU-U.S….,* s. 1974–75.
[315] P. Blume: *EU Adequacy Decisions*…, s. 38.
[316] P. Blume: *Transborder Data Flow*…, s. 78.
[317] V. Lehdonvirta: *European Union Data*…, s. 522.

z nadzorem nad ich przestrzeganiem, szczególnie w zakresie wykrywania naruszeń zasad ochrony danych osobowych[318].

Zarówno pogląd o obowiązku stosowania kryteriów oceny systemu prawnego wynikających z art. 45 ust. 2 RODO, jak i pogląd uznający katalog kryteriów zawarty w RODO za otwarty nie są sprzeczne i zasługują na aprobatę. W pełni zgadzam się z C. Kunerem, że należy unikać sztywnego podejścia do oceny. Spośród proponowanych przez doktrynę kryteriów w większości prezentowane katalogi są zbieżne i dotykają tych samych zagadnień, między innymi kryterium zasad ochrony danych osobowych oraz kryterium nadzoru. Sądzę, że te dwa kryteria można uznać za minimalny, niezbędny katalog kryteriów. Do takiego stanowiska prowadzi w pierwszej kolejności treść art. 45 ust. 2 RODO, w którym jako elementy poddawane badaniu wymieniono zarówno zasady ochrony danych, jak i nadzór, w tym poprzez organ nadzorczy. Nie bez znaczenia jest także praktyka stosowana podczas wszystkich dotychczasowych ocen, jak również ściśle powiązane z praktyką Dokumentów WP12 i WP254. Spoglądając na treści decyzji w sprawie adekwatności wydanych na podstawie Dyrektywy 95/46 okazuje się, że to właśnie duet zasady-nadzór stanowiły główny przedmiot oceny. Powodem takiego stanu rzeczy jest stosowanie Dokumentu WP12, którego katalog kryteriów stanowią zasady ochrony danych osób wraz z szeroko pojętym nadzorem. Podobnym schemat postępowania jest wykorzystywany podczas oceny systemu prawnego państwa trzeciego na podstawie RODO i stosowanego do tej oceny dokumentu WP254. Zbyt daleko idącym jest postulat S.L. Duque Carvahlo, która dopuszcza brak istnienia w systemie prawnym państwa trzeciego niektórych spośród zasad ochrony danych osobowych zawartych w RODO. Przyjęcie takiego stanowiska z jednej strony pozwalałoby na kwestionowania istnienia wszystkich zasad. Z drugiej strony doktryna dość zgodnie wskazuje podstawowe zasady, których odnalezienie w systemie prawnym państwa trzeciego jest konieczne, a które to zasady są w większości zbieżne z katalogiem zasad wynikających z RODO. Jako drugorzędne uznaję kryteria dotyczące źródła uregulowania zasad ochrony danych osobowych, ponieważ stosując całościową ocenę systemu prawnego może się okazać, że samoregulacja jest doskonałym rozwiązaniem, gwarantującym skuteczną ochronę dla podmiotów danych. Mimo że przedstawiciele doktryny nie odnieśli się do roli jaką spełnia samoregulacja w zakresie nadzoru, można uznać, że samo umocowanie nadzoru, w tym powołanie organu nadzorczego, jak i podstawowe i jego uprawnienia powinny

[318] A. Deighton: *The EU-US Privacy Shield - Is It Strong Enough?*. „Privacy & Data Protection ", 2016, nr 4, s. 8.

znaleźć się w regulacji ustawowej. Jako podstawowe uprawnienia postrzegam te uprawnienia, które pozwalają organowi nadzorczemu na skuteczne działanie i wykonywanie swoich zadań. Uważam, że poprzez samoregulację możliwe jest jedynie doposażenie organu nadzorczego w pewne dodatkowe uprawnienia.

W nawiązaniu do problematyki kryteriów oceny systemu prawnego państwa trzeciego, doktryna zwraca uwagę na rolę Karty Praw Podstawowych w ocenie oraz powiązanej z tym kontroli dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego do danych osobowych przekazanych na terytorium państwa trzeciego. G. Maldoff i O. Tene wyjaśniają, że za sprawą wyroku w sprawie Schrems I Karta Praw Podstawowych stała się samodzielnym kryterium oceny, zwłaszcza w zakresie dostępu organów ścigania do danych osobowych, zaś wsparciem dla Karty Praw Podstawowych jest Europejska Konwencja Ochrony Praw Człowieka i orzecznictwo ECtHR z uwagi na powiązania między przywołanymi aktami prawnymi[319]. W ocenie C. Kunera wymaganie poziomu ochrony danych osobowych wynikającego z Karty Praw Podstawowych jest przejawem zmiany podejścia do transferów danych osobowych ku bardziej restrykcyjnemu w porównaniu z dotychczasowym podejściem, którego źródłem była sprawa Lindquist[320]. O tym samym problemie wspomina O. Lynsky, wyjaśniając, że Karty Praw Podstawowych jest źródłem rygorystycznego podejścia do wymaganego poziomu ochrony danych osobowych, co jednak niekoniecznie pozostaje w zgodzie z celem ochrony danych osobowych w postaci wyrównania pozycji podmiotu danych względem administratora [321]. A.D. Murray uznaje Kartę Praw Podstawowych za istotne kryterium, ponieważ jest ona źródłem prawa do ochrony danych osobowych, przy czym wsparciem i dodatkową ochroną jest także Europejska Konwencja Ochrony Praw Człowieka, której wdrożenie może osłabiać braki dostrzegalne na gruncie stosowania Karty Praw Podstawowych [322]. S. Slokenberga wraz z zespołem stoją na stanowisku, że wykorzystanie Karty Praw Podstawowych podczas oceny państwa trzeciego jest konieczne dla prawidłowej interpretacji przepisów RODO, ponieważ transfer danych nie może osłabić ochrony praw wynikających z Karty Praw Podstawowych [323]. Do związku Karty Praw Podstawowych i Europejskiej Konwencji Ochrony Praw Człowieka odnosi się także J. Bourgeois

[319] G. Maldoff, O. Tene: *Essential Equivalence and*…, s. 238–240.
[320] C. Kuner: *Reality and Illusion*…, s. 893, 895.
[321] O. Lynskey: *Delivering Data Protection: The next Chapter.* „German Law Journal", 2020, nr 1, s. 81–82.
[322] A.D. Murray: *Data Transfers between...,* s. 151–52.
[323] S. Slokenberga, J. Rachel, R. Niringiye i in.: *EU Data Transfer…*, s. 35.

z zespołem, którzy w orzecznictwie ECtHR dostrzegają wsparcie w stosowaniu kryterium dostępu organów ścigania do danych osobowych[324]. Wykorzystanie orzecznictwa ECtHR wraz z wskazówkami zawartymi w wyroku Schrems I pozwala autorom sformułować kryteria oceny dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego, a którymi są:

1. kryterium konkretnej podstawy prawnej,
2. kryterium ograniczonego zasięgu dostępu do danych,
3. kryterium nadzoru,
4. kryterium środków prawnych przyznanych osobie, której dane dotyczą na wypadek naruszenia ochrony danych osobowych w związku z dostępem do danych[325].

Samo kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego jest według Komisji Europejskiej obowiązkowym kryterium[326]. Także G. Maldoff i O. Tene uznają badanie zagadnienia dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego za istotne kryterium, którego pominięcie powinno spotkać się z dezaprobatą[327]. Autorzy zalecają jednak ostrożne posługiwanie się wspomnianym kryterium, ponieważ prawo państw członkowskich Unii Europejskiej niekoniecznie odpowiada standardom, jakie wynikają z prawa Unii Europejskiej[328]. Zdaniem C. Kunera stosowanie Karty Praw Podstawowych jako kryterium oceny pozwala na posługiwanie się szczegółowym kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego[329]. W związku ze stawianym w doktrynie zarzutem o niedociągnięciach w krajowych porządkach prawnych członków Unii Europejskiej w zakresie omawianego dostępu do danych, które to niedociągnięcia miałyby uniemożliwiać ocenę państwa trzeciego w tym zakresie, C. Kuner nie zgadza się z takim uzasadnieniem, ponieważ naruszenia praw podstawowych w państwie trzecim w żaden sposób nie mogą być usprawiedliwione przez braki dostrzegane w państwach członkowskich Unii Europejskiej[330]. J. Wagner dopatruje się w kryterium dostępu

[324] J. Bourgeois, C.F. Kerry, W.R.M. Long i in.: *Essentially Equivalent. A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States*. Sidley, Austin 2019, s. 19, 23, 26.
[325] Ibidem, s. 26–27.
[326] C*ommunication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*…, s. 6.
[327] G. Maldoff, O. Tene: *Essential Equivalence and…,* s. 211, 220, 281.
[328] Ibidem, s. 230–31.
[329] C. Kuner: *Reality and Illusion*…, s. 896–97.
[330] Ibidem, s. 899.

organów ścigania do danych wyrazu połączenia RODO z orzecznictwem TSUE i ECtHR[331]. W ocenie A. Chandera kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego jest tak istotne, że może uzasadniać konieczność powtórzenia oceny w stosunku do państw uznanych uprzednio za adekwatne[332]. Jednocześnie autor zauważa, że niektóre państwa członkowskie Unii Europejskiej mogą nie odpowiadać wymaganiom płynącym ze standardu dostępu organów ścigania do danych osobowych, co z kolei może skutkować negatywną oceną państw członkowskich przez te państwa trzecie, które wdrożyły model ochrony danych osobowych oparty na modelu Unii Europejskiej[333]. Treść kryterium oceny dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego, według A. Matoo i J.P. Meltzera, to przede wszystkim dwa kryteria: kryterium dostępu zgodnego z prawem oraz kryterium praw osoby, której dane dotyczą na wypadek naruszenia ochrony danych, przy czym w obu wypadkach punktem odniesienia dla oceny jest zgodność z RODO[334]. W ujęciu S.L. Duque de Carvalho istotę wymagań w zakresie dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego oddaje wspomniany Dokument WP237[335].
Podzielam pogląd uznający badanie dostępu organów państwa trzeciego do danych za obowiązkowy element oceny. Zgadzam się z C. Kunerem, że podstawą prawną, dla odpowiedniej interpretacji przepisów RODO, pozwalającą na zastosowanie tego kryterium, jest Karta Praw Podstawowych, przy czym podobnie jak O. Lynsky uważam, że nie należy zapominać o celu ochrony danych osobowych. Jednocześnie w pełni aprobuję stanowisko C. Kunera, dla którego usprawiedliwieniem braków w państwie trzecim nie może być argument z braków występujące w porządkach prawnych państw członkowskich Unii Europejskiej.

Osobny wątek dyskusji doktryny dotyczy najpoważniejszych wad oceny systemu prawnego państwa trzeciego w ramach procesu wydawania decyzji w sprawie adekwatności, jak również decyzji w sprawie adekwatności jako takiej.
Pierwsza wada związana jest z zarzucanym nierównym traktowanie państw trzecich. J. Wolf zauważa, że wyniki ocen przeprowadzonych przez Komisję Europejską, mimo

[331] J. Wagner: *The Transfer of…*, s. 332.
[332] A. Chander: *Is Data Localization a Solution for Schrems II?*. „Journal of International Economic Law", 2020, nr 3, s. 4-5.
[333] Ibidem, s. 13.
[334] A. Mattoo, J.P. Meltzer: *International Data Flows and Privacy: The Conflict and Its Resolution*. „Journal of International Economic Law", 2018, nr 4, s. 776.
[335] S.L. Duque de Carvalho: *Key GDPR Elements…*, s. 60–61.

identycznych problemów dostrzeganych w badanych państwach trzecich, pociągały za sobą dwie, skrajne reakcje[336]. Na zróżnicowane traktowanie zbliżonych przypadków, a tym samym brak równego, jednolitego traktowania wskazują także J. Stodart, B.Chan i Y. Joly[337]. W oparciu o niejednolite podejście Komisji Europejskiej, bazując na przeprowadzonych przez nią ocenach, C. Kuner poddał pod wątpliwość konieczność uwzględniania w ocenie zasady dalszego przekazywania danych osobowych, której brak nie koniecznie powodował negatywną ocenę[338]. Na brak restrykcyjnego podejścia do kryterium podstawowych zasad ochrony danych osobowych zwraca uwagę także A. Hughes, powołując się na przypadek Australii, gdzie dostrzeżone wady w regulacji ochrony danych osobowych pracowników nie zostały wytknięte przez Grupę Roboczą art. 29[339]. Autorka podkreśla jednak, że takie odstępstwo to swego rodzaju nadzwyczajne złagodzenie rygorów dotyczącego konkretnego przypadku, a jego uzasadnieniem może być uwzględnienie specyfiki badanego systemu[340].

Druga wada to stosowanie dodatkowych kryteriów oceny. J. Stodart, B.Chan i Y. Joly wyjaśniają, że mimo stosowania Dokumentu WP12, podczas oceny używa się także innych kryteriów o wątpliwej doniosłości, jak krótki czas obowiązywania regulacji ochrony danych osobowych, położenie geograficzne państwa trzeciego, które powoduje, że niewiele danych osobowych jest przesyłanych do danego kraju[341]. Także J. Wolf dostrzega dodatkowe, faktycznie stosowane kryteria w postaci kryterium wielkości państwa trzeciego i intensywności jego współpracy z Unią Europejską[342]. Z kolei C. Kuner zwraca uwagę na problem wpływu polityki na przeprowadzaną ocenę[343]. W ocenie P. Blume'a oczywistym jest wpływ polityki na ostateczną decyzję w sprawie adekwatności[344]. S. Sharma wymienia dodatkowe kryteria wykorzystywane przez Komisję Europejską i w postaci politycznych relacji czy rozmiarów współpracy państwa trzeciego z Unią Europejską[345]. Za potwierdzenie uwag doktryny o stosowaniu dodatkowych kryteriów oceny można uznać stanowisko Komisji Europejskiej, która w jednym ze swoich dokumentów przedstawiła czynniki, które decydują o rozpoczęciu procedury oceny systemu prawnego państwa trzeciego. Za takie czynniki uznano:

---

[336] J. Wolf: *Delusions of Adequacy*…, s. 240–241.
[337] J. Stoddart, B. Chan, Y. Joly: *The European Union's*…, s. 146–49.
[338] C. Kuner: *Developing an Adequate*…, s. 266–267.
[339] A. Hughes: *A Question of*…, s. 273, 275.
[340] Ibidem, s. 275.
[341] J. Stoddart, B. Chan, Y. Joly: *The European Union's*…, s. 150.
[342] J. Wolf: *Delusions of Adequacy*…, s. 239.
[343] C. Kuner: *Developing an Adequate*…, s. 265.
[344] P. Blume: *Transborder Data Flow*…, s. 69.
[345] S. Sharma: *Data Privacy and…,* s. 164.

1. relacje handlowe,
2. nasilenie przepływów danych osobowych, w tym z uwagi na więzy kulturowe,
3. wiodącą rolę państwa trzeciego w ochronie danych osobowych,
4. szeroko pojęte relacje polityczne i współpracę[346].

J. Bourgois wraz z zespołem, w opozycji do poglądów o możliwości stosowania dodatkowych kryteriów oceny, postulują, żeby tym co przesądza o ocenie systemu prawnego państwa trzeciego były fakty, a samo podejście do państw trzecich było wolne od arbitralności i nierównego traktowania[347]. Konsekwencją oparcia oceny o fakty jest wymóg, aby zarówno pozytywna, jak i negatywna ocena wyjaśniały, dlaczego dany kraj uzyskał taką a nie inną ocenę[348]. Pośrednio problemu dodatkowych kryteriów dotyka także wpływu zapewnień państwa trzeciego. G. Maldoff i O. Tene zwracają uwagę na wątpliwą skuteczność zapewnień składanych przez państwo trzecie, choć nie wykluczają ich przydatności[349]. A. Deighton również dostrzega słabość polegania na zapewnieniach państwa trzeciego. Jednakże, ujmuje zapewnienia państwa trzeciego jako przejaw zobowiązań międzynarodowych, o których mowa w art. 45 RODO[350].

Trzecia wada to skromny zasób informacji na temat przebiegu oceny, przez co państwa trzecie nie są świadome czego się od nich oczekuje[351]. Zdaniem C. Kunera dla samej oceny niekorzystnym jest brak jawności i transparentności stosowanych przez Komisję Europejską wewnętrznych wytycznych[352]. Zarzut C. Kunera jest jak najbardziej trafny. Przejawem przytoczonego problemu są decyzje w sprawie adekwatności wydawane na podstawie Dyrektywy 95/46, w których trudno mówić o bezpośrednim stosowaniu kryteriów wynikających z art. 25 ust. 2 Dyrektywy 95/46[353].

Za wadę decyzji w sprawie adekwatności doktryna uznaje także jej wątpliwą stabilność, wynikającą z obowiązku aktualizacji oceny systemu prawnego państwa trzeciego, a która może prowadzić do zawieszenia lub uchylenia decyzji w sprawie adekwatności[354].

---

[346] *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*…, s. 8.
[347] J. Bourgeois, C.F. Kerry, W.R.M. Long: *Essentially Equivalent. A*…, s. 29–30, 32.
[348] Ibidem, s. 29.
[349] G. Maldoff, O. Tene: *Essential Equivalence and*…, s. 238.
[350] A. Deighton: *The EU-US*…, s. 9.
[351] C. Kuner: *Developing an Adequate*…, s. 268.
[352] C. Kuner: *Reality and Illusion*…, s. 900–901.
[353] O czym była mowa w pkt 2.1 tego rozdziału.
[354] P. Breitbarth: *A Risk-Based Approach to International Data Transfers*. „European Data Protection Law Review", 2021, nr 4 s. 542; JD Supra: *New EU-U.S. Data Privacy Framework Legalizes Personal Data Transfers from the EU to US.* 1.08.2023. Newstex Blogs LexisNexis [dostęp: 23.09.2023]; *The Fight against the EU_s New Data Deal_ Will Google_ Facebook and Amazon Be Allowed to Send Personal Information of Users to the US? The EU's Agreeement Is Wobbing*. 17.07.2023, Die Welt (English) LexisNexis [dostęp: 22.09.2023].

Uważam, że taki zarzut jest chybiony. Jak słusznie zauważa L. Wittershagen, ocena w sprawie adekwatności ukierunkowana na przedstawienie wyników odpowiadających rzeczywistemu poziomowi ochrony danych osobowych w państwie trzecim [355]. Tym samym, brak obowiązku okresowego przeglądu i, w razie potrzeby, aktualizacji decyzji w sprawie adekwatności prowadziłby do sytuacji, w której poziom ochrony danych osobowych w państwie trzecim tylko pozornie odpowiadałby standardowi adekwatności.

Wadą decyzji w sprawie adekwatności ma być również jej niewielka praktyczna doniosłość. Jak dotąd, Komisja Europejska wydała 15 decyzji w sprawie adekwatności. Oznacza to, że tylko 15 państw trzecich jest objęte korzyściami płynącymi z korzystania z decyzji w sprawie adekwatności, a więc tylko ok. 10% światowej regulacji ochrony danych osobowych, pomijając państwa członkowskie UE[356]. W przypadku pozostałych państw trzecich poziom ochrony danych osobowych wymaga każdorazowej oceny przez administratora lub podmiot przetwarzający. Braku decyzji w sprawie adekwatności nie należy jednak utożsamiać z faktycznym brakiem adekwatności [357]. Faktycznym, ponieważ ocena przeprowadzona przez administratora lub podmiot przetwarzający mogą wskazywać, że rzeczywisty poziom ochrony danych w badanym państwie trzecim nie jest daleki od standardu adekwatności[358]. Uwzględniwszy poboczny, ale niemniej istotny, zarzut czasochłonności procedury związanej z wydawaniem decyzji w sprawie adekwatności[359], można uznać, że staje się ona narzędziem o niewielkiej, praktycznej doniosłości.

W pełni podzielam wątpliwości podnoszone przez doktrynę w odniesieniu do wykorzystania dodatkowych kryteriów oceny o zabarwieniu politycznym. Ich stosowanie jest poważnym problemem, który potęguje zarzut nieuzasadnionego zróżnicowanego traktowania poszczególnych państw. Potwierdza także, że w ramach oceny systemu prawnego państwa trzeciego, Komisja Europejska uwzględnia także czynniki pozaprawne. Niemniej jednak, za dobre rozwiązanie uznaję posłużenie się dodatkowymi

---

[355] L. Wittershagen: *Transfer of Personal…,* s. 69.
[356] Podobnie: A. Chander, P.M. Schwartz: *Privacy and/or Trade*. „University of Chicago Law Review", 2023, nr 1 s. 74.
[357] M. Krzysztofek: *Komentarz do art. 45 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C. H. Beck, Warszawa 2016, s. 234; P. Drobek: *Komentarz do art. 45 RODO*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2018; B. Fischer: *Komentarz do art. 45 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Red. M. Sakowska-Baryła. C. H. Beck, Warszawa 2018, s. 468.
[358] B. Fischer: *Komentarz do art. 45 RODO…,* s. 468.
[359] S. Slokenberga, J. Rachel, R. Niringiye i in.: *EU Data Transfer*…, s. 36.

kryteriami oceny w celu pogłębionej analizy systemu prawnego państwa trzeciego, zwłaszcza dla dokładniejszego rozeznania sytuacji jednostki. Rację ma J. Bourgois z zespołem, twierdząc, że podstawą oceny powinny być fakty. W związku z tym zgadzam się z G. Maldoff i O. Tene oraz A. Deighton, którzy kwestionują rolę zapewnień państw trzecich, choć podobnie jak przywołani autorzy dostrzegam potencjalne korzyści płynące z korzystania zapewnień.

W świetle przedstawionych powyżej poglądów doktryny, w tym zwłaszcza poglądów dotyczących charakteru katalogu kryteriów oceny, o którym mowa w art. 45 ust. 2 RODO oraz roli kryterium ochrony praw człowieka i poszanowania rządów prawa, zwracam uwagę na dodatkowy problem. Jak już wspominałem w pkt 2.1 oraz 4.1 tego rozdziału, treść żadnej z decyzji w sprawie adekwatności nie zawiera odniesienia do kryterium rządów prawa i ochrony praw człowieka, zaś kryterium współpracy międzynarodowej jest stosowane wybiórczo.

Kryterium rządów prawa i ochrony praw człowieka jest uznawane za istotny element oceny systemu prawnego państwa trzeciego[360]. Uzasadnieniem takiego stanowiska jest fakt, że brak poszanowania praw człowieka i respektowania standardu rządów prawa wyklucza w przedbiegach państwo trzecie z ubiegania się o przyznanie decyzji w sprawie adekwatności[361]. Stąd kryterium rządów prawa i ochrony praw człowieka powinno być pierwszym z punktów oceny systemu prawnego państwa trzeciego[362]. Motyw 104 preambuły RODO wyjaśnia, że „zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, Komisja powinna w swojej ocenie państwa trzeciego lub terytorium lub określonego sektora w państwie trzecim wziąć pod uwagę sposób, w jaki dane państwo trzecie przestrzega praworządności, dostępu do wymiaru sprawiedliwości oraz międzynarodowych norm i standardów ochrony praw człowieka, jego prawo ogólne i sektorowe, w tym ustawodawstwo dotyczące bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i porządku publicznego, a także prawo karne.” Z kolei punktem odniesienia dla oczekiwanego standardu rządów prawa powinno być rozumienie pojęcia rządów prawa zawarte

[360] P. Drobek: *Komentarz do art. 45 RODO…*; G. Greenleaf: *NGO Involvement in the Evaluation and Follow-Up Mechanisms for Data Protection Convention 108+ (Submission to the Consultative Committee of Data Protection Convention 108 by the Australian Privacy Foundation (APF).* „University of New South Wales Law Research Series ", 2019, nr 19, s. 3; L. Wittershagen: *Transfer of Personal…*, s. 60.
[361] L. Drechsler, I. Kamara: *Essential equivalence as a benchmark for international data transfers after Schrems II*. W: *Research Handbook on EU Data Protection Law*. Red. E. Kosta, R. Leenes, I. Kamara. Edward Elgar Publishing, Cheltenham 2022, s. 341.
[362] P. Drobek: *Komentarz do art. 45 RODO…*, ; L. Drechsler, I. Kamara: *Essential equivalence as…,* s. 332.

w jednym z komunikatów Komisji Europejskiej[363]. J. Wagner w zakresie rozumienia kryteriów rządów prawa z art. 45 ust. 2 lit. a RODO odsyła do wykształconego w prawie Unii Europejskiej podejścia, związanego ze stosowaniem TUE oraz kryteriów kopenhaskich[364]. Zdaniem J. Wagnera, kryterium rządów prawa sprowadza się do istnienia „zasady zgodności z prawem, zasady pewności prawa, zakazu podejmowania arbitralnych decyzji, funkcjonowania niezależnego i skutecznego nadzoru sądowego oraz równości prawa"[365]. Niemniej jednak, według J. Wagnera za kryterium ochrony praw człowieka kryje się poszanowanie praw człowieka wynikających z Karty Praw Podstawowych i Europejskiej Konwencji Praw Człowieka, na co wprost wskazuje TUE[366]. Natomiast, w odniesieniu do kryterium współpracy międzynarodowej państwa trzeciego, w motywie 105 RODO wskazano, że „poza zobowiązaniami międzynarodowymi państwa trzeciego lub organizacji międzynarodowej, Komisja powinna brać pod uwagę obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, w szczególności w odniesieniu do ochrony danych osobowych, a także realizację takich obowiązków. W szczególności powinna wziąć pod uwagę przystąpienie państwa trzeciego do konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych."

Uważam, że obecną praktykę Komisji Europejskiej w zakresie stosowania kryterium ochrony praw człowieka i rządów prawa, jak również kryterium międzynarodowych zobowiązań państwa trzeciego można uznać za naruszenie art. 45 ust. 2 RODO. Katalog kryteriów, o którym mowa w art. 45 ust. 2 RODO jest postrzegany jako przepis określający minimalną treść oceny systemu prawnego państwa trzeciego. Należałoby więc oczekiwać od Komisji Europejskiej, że treść decyzji w sprawie adekwatności będzie poruszała te wszystkie zagadnienia, na które wprost wskazuje art. 45 ust. 2 RODO. Obecne podejście Komisji Europejskiej jedynie potwierdza zarzut braku jednoznaczności standardu adekwatności, a zarazem potęguje zarzut braku transparentności procedury i towarzyszącej jej oceny państwa trzeciego[367]. Co więcej, pominięcie wspomnianych

[363] L. Wittershagen: *Transfer of Personal…, s.* 59; mowa o: *Communication from the Commission to the European Parliament and the Council A New EU Framework to Strengthen the Rule of Law*. 11.03.2014. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0158 [dostęp: 13.10.2023].
[364] J. Wagner: *The Transfer of…*, s. 322 "(…) principles of legality, of legal certainity, of the prohibition of executive arbitrariness, of independent nad effective judical review and of equality before the law".
[365] Ibidem, s. 322.
[366] Ibidem.
[367] C. Kuner: *Komentarz do art. 45*…, s. 785; C. Kuner: *The Path to*…, s. 82; C. Pauletto: *Options towards a Global Standard for the Protection of Individuals with Regard to the Processing of Personal Data*. „Computer Law & Security Review ", 2021, nr 40, s. 14.

kryteriów oceny systemu prawnego państwa trzeciego można poczytywać za przejaw wpływu czynników pozaprawnych na przeprowadzaną ocenę[368].

Mając na względzie wątpliwości co do rozumienia standardu adekwatności zgadzam się z tymi przedstawicielami doktryny, którzy uważają, że obecnie trudno jednoznacznie wskazać czym jest wymagana przez przepisy RODO adekwatność[369]. Uważam, że zarzut niejednoznaczności standardu adekwatności jest konsekwencją rozbieżności między faktycznym zakresem oceny systemu prawnego państwa trzeciego, a zakresem wynikającym z art. 45 ust. 2 RODO. Co oczywiste, decyzja w sprawie adekwatności może być przyznana wyłącznie państwu, które będzie spełniało wszystkie kryteria oceny, o których mowa w art. 45 ust. 2 RODO, a zarazem, w myśl poglądów TSUE, poziom ochrony danych osobowych zapewniany przez to państwo będzie równoważny z poziomem ochrony danych osobowych w Unii Europejskiej. Jednakże, treść decyzji w sprawie adekwatności wydanych na podstawie RODO potwierdza, że dla uzyskania przez państwo trzecie pozytywnego wyniku oceny nie jest niezbędne spełnienie wszystkich kryteriów wskazanych w art. 45 ust. 2 RODO. Wydane dotychczas decyzje w sprawie adekwatności kładły nacisk na niektóre elementy systemu prawnego państwa trzeciego, a więc na istnienie egzekwowalnych zasad ochrony danych osobowych, praw przyznanych jednostce (wraz z odpowiednimi środkami pozwalającymi na reakcję na naruszenie jej danych osobowych), niezależnego i kompetentnego organu nadzoru, a także istnienie ograniczeń w dostępie organów ścigania do danych osobowych. Przywołane, faktyczne kryteria oceny pokrywały się z katalogiem kryteriów zawartym w art. 45 ust. 2 RODO, ale tylko częściowo. W tym stanie rzeczy można uznać, że Komisja Europejska przeprowadza ocenę systemu prawnego państwa trzeciego w minimalnym, dopuszczalnym zakresie, wyznaczanym przez kryteria oceny Dokumentu WP254. Rację ma więc Parlament Europejski, który w swojej rezolucji stwierdza, że Dokument WP254 określa niezbędny, minimalny zakres

[368]Podobnie: A. Hughes: *A Question of*…, s. 275, która wspomina o zróżnicowanym podejściu do wad dostrzeganych w systemach prawnych badanych państw trzecich..

[369] C. Kuner *Komentarz do art. 45*…, s. 788–789 ; Z. Gulczyńska: *A certain standard of protection for international transfers of personal data under the GDPR*. „International Data Privacy Law", 2021, nr 4, s. 3, 4; G. Greenleaf: *Global Data Privacy Laws 2021: Uncertain Paths for International Standards*. „Privacy Laws & Business International Report", 2021, nr 169, s. 1; [brak danych autora] *National Security Law — Surveillance — Court of Justice of the European Union invalidates the EU-U.S. Privacy Shield. — Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020)*. „Harvard Law Review", 2021, nr 134, s. 1567, 1571, 1574; D. Erdos: *The UK and the EU Personal Data Framework after Brexit: A New Trade and Cooperation Partnership Grounded in Council of Europe Convention 108+?*. „Computer Law & Security Review", 2022, nr 44, s. 9; L. Wittershagen: *Transfer of Personal*…, s. 68; A. Chander, P.M. Schwartz: *European Data Protection*…, s. 72.

oceny[370]. W ten sposób, ocenione zostaję tylko te elementy systemu prawnego państwa trzeciego, co do których możliwe będzie uznanie, że w mniejszym lub większym stopniu, gwarantują poziom ochrony danych osobowych równoważny z poziomem ochrony danych osobowych w Unii Europejskiej. To z kolei oznacza, że standard adekwatności, przyjmuje dwie postaci. Pierwsza postać to standard adekwatności powiązany z kryteriami oceny systemu prawnego państwa trzeciego, o których mowa w Dokumencie WP254. O tej postaci standardu adekwatności można mówić jako o minimalnym standardzie adekwatności. Druga postać to standard adekwatności, dla którego wyznacznikiem jest art. 45 ust. 2 RODO. Wówczas, przedmiotem oceny systemu prawnego państwa trzeciego są wszystkie elementy, na które wskazują kryteria oceny zawarte w przywołanym przepisie.

Uważam, że przedstawione powyżej dwojakie rozumienie standardu adekwatności jest bezpośrednią konsekwencją wpływu czynników pozaprawnych na ocenę systemu prawnego państwa trzeciego, a więc także na stosowane kryteria oceny i ich wykładnię. Rację ma więc A. Hughes, która zauważa, że te same wady prawa ochrony danych osobowych w państwie A nie spotykają się z taką samą reakcją w przypadku oceny systemu prawnego państwa B[371]. Również C. Wolf dostrzega niekonsekwencję Komisji Europejskiej, przywołując przypadek Argentyny i Burkina Faso, gdzie identyczne niedociągnięcia w systemach prawnych obu państw były przeszkodą dla przyznania decyzji w sprawie adekwatności wyłącznie Burkina Faso[372]. Podobnie S. Sharma, zdaniem której tak relacje polityczne czy rozmiar współpracy gospodarczej państwa trzeciego z Unią Europejską są uwzględniane przez Komisję Europejską na etapie oceny systemu prawnego państwa trzeciego, modyfikując tę ocenę[373].

6. Rekonstrukcja kryteriów oceny systemu prawnego państwa trzeciego wynikających z przepisów RODO, dorobku orzecznictwa i doktryny

Zaprezentowany w pkt 2 – 5 rozdziału przegląd katalog kryteriów oceny systemu prawnego państwa trzeciego wynikających z art. 45 ust. 2 RODO, praktyki Komisji Europejskiej oraz innych organów Unii Europejskiej zaangażowanych w proces

[370] *European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 — Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP))*…, pkt 33.

[371] A. Hughes: *A Question of*…, s. 275 - "Thus a shortcoming in one country need not be automatically acceptable in another.".

[372] C. Wolf: *Delusions of Adequacy…*, s. 240-241.

[373] S. Sharma: *Data Privacy and…,* s. 164.

wydawania decyzji w sprawie adekwatności, rozważań doktryny pozwala na rekonstrukcję następującego katalogu kryteriów:

1) Kryterium podstawowych zasad ochrony danych osobowych,
2) Kryterium egzekwowalności podstawowych zasad ochrony danych osobowych,
3) Kryterium kompetentnego, niezależnego organu nadzorczego,
4) Kryterium środków prawnych przyznanych osobie, której dane dotyczą na wypadek naruszenia ochrony danych osobowych, obejmujący środki administracyjne i sądowe,
5) Kryterium dostępu do danych osobowych przekazanych na terytorium państwa trzeciego przez organy państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego.

Katalog kryteriów oceny systemu prawnego państwa trzeciego wynikający z RODO, wsparty przez praktykę postępowania Komisji Europejskiej, jak również poglądy doktryny jednogłośnie wskazuje na konieczność weryfikacji systemu prawnego państwa trzeciego w zakresie istniejących zasad ochrony danych osobowych. Sam katalog zasad nie jest jednak jednolity, przez co konieczne jest wyjaśnienie co na potrzeby tej rozprawy doktorskiej składa się na podstawowe zasady ochrony danych. Biorąc pod uwagę zasady przytaczane przez doktrynę, jak również zasady wykorzystywane przez Komisję Europejską w decyzjach w sprawie adekwatności katalog podstawowych zasad ochrony danych osobowych jest zbudowany z zasad, o których mowa w Dokumencie WP254, tj.:

1) Zasady przetwarzania danych zgodnie z prawem,
2) Zasady ograniczonego celu przetwarzania,
3) Zasady jakości i proporcjonalności danych,
4) Zasady retencji danych,
5) Zasady bezpieczeństwa danych (w tym ich poufności),
6) Zasady przejrzystości,
7) Zasady prawa dostępu do danych i ich modyfikacji, prawa do usunięcia danych i sprzeciwu wobec przetwarzania,
8) Zasady dalszego transferu danych,
9) Zasady przetwarzania specjalnych kategorii danych,
10) Zasady przetwarzania danych na potrzeby marketingu,
11) Zasady przetwarzania danych na potrzeby profilowania i automatycznego podejmowania decyzji.

Powyższy zestaw zasad odpowiada zasadom wzmiankowanym w treści decyzji w sprawie adekwatności, w tym zwłaszcza decyzji wydanych na podstawie RODO. Jednocześnie, swoją treścią zasady, o których mowa w Dokumencie WP254 odpowiadają treści zasad powszechnie przytaczanych przez przedstawicieli doktryny[374].

Ochrona danych osobowych w państwie trzecim ma być elementem rzeczywistej praktyki. Organy ochrony danych osobowych oraz TSUE uznają rzeczywiste i skuteczne przestrzeganie zasad oraz przeciwdziałanie ich naruszeniom za wyraz rzeczywistego poziomu ochrony danych osobowych w państwie trzecim. Dlatego też kolejnym kryterium oceny systemu prawnego państwa trzeciego na potrzeby tej rozprawy doktorskiej jest kryterium egzekwowalności podstawowych zasad ochrony danych osobowych oraz kryterium środków prawnych przyznanych osobie, której dane dotyczą na wypadek naruszenia ochrony danych osobowych. Oba kryteria nakierowane są na przedstawienie uprawnień osoby, której dane dotyczą w zakresie wykonywania praw przyznanych przez zasady ochrony danych osobowych państwa trzeciego, jak również uprawnień, za pomocą których osoba, której dane dotyczą może przeciwdziałać na drodze sądowej i administracyjnej naruszeniom jej praw dotyczących ochrony danych osobowych, w tym praw wynikających z zasad ochrony danych osobowych.

Sprawy Schrems I i Schrems II przypomniały o roli, jaką odgrywa w systemie prawnym państwa trzeciego organ nadzorczy. Spostrzeżenia TSUE zawarte w wyrokach w sprawie Schrems I i Schrems II korespondują z rozważaniami doktryny oraz uwagami Grupy Roboczej art. 29, o których mowa w Raporcie Wprowadzającym i Metodologii Oceny. Tym samym ocena systemu prawnego państwa trzeciego nie może odbyć się bez oceny organu nadzorczego w zakresie przyznanych uprawnień oraz pozycji ustrojowej, gwarantującej jego niezależność. Kryterium organu nadzorczego przenika się również z kryterium egzekwowalności zasad ochrony danych osobowych i kryterium środków prawnych przyznanych osobie, której dane dotyczą na wypadek naruszenia ochrony danych osobowych, dla których to kryteriów istnienie skutecznie działającego organu nadzorczego przekłada się na zakres dostępnych uprawnień.

Ostatnie kryterium jest bezpośrednią konsekwencją przypadku USA. TSUE wespół z niektórymi przedstawicielami doktryny, uznają kryterium dostępu do danych osobowych przekazanych na terytorium państwa trzeciego przez organy państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego za

[374] Można mówić o uwzględnieniu w dokumentach Grupy Roboczej art..29 katalogu zasad przytaczanych przez doktrynę - podobnie: H.P. Lowry: *Transborder Data Flow: Public and Private International Law Aspects*. „Houston Journal of International Law", 1984, nr 2, s. 159–74.

obowiązkowy element każdej oceny systemu prawnego państwa trzeciego. Zgadzam się z tym stanowiskiem. O doniosłości tego kryterium świadczy także treść raportu Komisji Europejskiej z przeglądu decyzji w sprawie adekwatności wydanych na podstawie Dyrektywy 95/46[375]. To właśnie realizacja kryterium dostępu do danych osobowych przekazanych na terytorium państwa trzeciego przez organy państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego była zasadniczym elementem zwięzłego opisu poszczególnych systemów prawnych państw trzecich objętych decyzjami w sprawie adekwatności[376]. Z uwagi na przedmiot tej rozprawy doktorskiej, zastosowanie kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego do danych osobowych przekazanych na terytorium państwa trzeciego będzie obejmowało wyłącznie elementy, na które wskazuje Europejska Rada Ochrony Danych Osobowych w Dokumencie WP254[377], tj.:

1) Kryterium zrozumiałej, precyzyjnej podstawy prawną przetwarzania danych,
2) Kryterium wykazania konieczności i proporcjonalności dostępu do danych,
3) Kryterium nadzoru,
4) Kryterium skutecznych środki ochrony prawnej przyznane osobom, których dane dotyczą.

Oprócz kryteriów o charakterze prawnym, w ramach oceny systemu prawnego uwzględniane są także czynniki pozaprawne, które można podsumować jako wpływ relacji politycznych i współpracy gospodarczej. Za Komisją Europejską owe szczegółowe dodatkowe czynniki to:

1) relacje handlowe z państwem trzecim,
2) nasilenie przepływów danych osobowych, w tym z uwagi na więzy kulturowe,
3) wiodąca rola państwa trzeciego w ochronie danych osobowych,
4) szeroko pojęte relacje polityczne i współpraca[378].

---

[375] *Report from the Commission to the European Parliament and the Council on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) of Directive 95/46/EC.* 15.01.2024. https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf [dostęp: 17.01.2024].

[376] Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Wyspa Man, Izrael, Jersey, Nowa Zelandia, Szwajcaria i Urugwaj

[377] Dokument WP254, s. 9.

[378] *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*…, s. 8.

7. Wnioski

Przedstawione w rozdziale I rozważania nasuwają wniosek, że ocena systemu prawnego państwa trzeciego jest przeprowadzana w sposób, który nie wynika bezpośrednio z przepisów prawa ochrony danych osobowych. Właściwe przepisy, odpowiednio Dyrektywy 95/46 oraz RODO, dotyczące wydania decyzji w sprawie adekwatności stanowiły podstawę dla przeprowadzenia oceny systemu prawnego państwa trzeciego. Szczegółowa analiza treści decyzji w sprawie adekwatności, wsparta przez spostrzeżenia doktryny i organów Unii Europejskiej zaangażowanych w procedurę wydawania decyzji w sprawie adekwatności wykazuje, że co do zasady stosowanie przepisów odpowiednio Dyrektywy 95/46 oraz RODO miało wyłącznie pośredni charakter.

Treści decyzji w sprawie adekwatności, jak również opinii Grupy Roboczej art. 29, wydanych w okresie obowiązywania Dyrektywy 95/46 potwierdzają, że nie wykorzystywano kryteriów oceny wynikających z artykułu 25 ust. 2 Dyrektywy 95/46. Wówczas, wyłączną podstawą oceny był Dokument WP12 i kryteria zeń wynikające. Dyrektywa 95/46 nie była całkowicie pominięta podczas oceny, ale służyła jedynie jako punkt odniesienia dla oceny, źródło stawianych wymagań czy wreszcie wskazówka interpretacyjna. Do takiego wniosku prowadzą zarówno wyjaśnienia zawarte w samym Dokumencie WP12, jak również znaczenie dokumentu WP12 przypisywane przez doktrynę. Był to więc szczególny przejaw pominięcia konkretnego przepisu Dyrektywy 95/46, art. 25 ust. 2, na rzecz uwzględnienia kryteriów odpowiadających standardom wynikającym z całej Dyrektywy 95/46. Tym samym, art. 25 Dyrektywy 95/46 można postrzegać jako formalną podstawę przeprowadzenia oceny, której kształt determinował Dokument WP12.

Pozornie inaczej można postrzegać ocenę systemów prawnych państw trzecich przeprowadzoną na podstawie RODO. Katalog kryteriów zawarty w art. 45 ust. 2 RODO zawiera w sobie kryteria oceny, o których mowa w Dokumencie WP254. Ponownie, praktyka Komisji Europejskiej, odzwierciedlona przez treść decyzji w sprawie adekwatności, potwierdza, że ocena przeprowadzana jest wyłącznie z zastosowaniem kryteriów, o których mowa w Dokumencie WP254. Tym samym, istotne dla oceny systemu prawnego państwa trzeciego jest istnienie egzekwowalnych zasad ochrony danych osobowych, praw przyznanych jednostce (wraz z odpowiednimi środkami pozwalającymi na reakcję na naruszenie jej danych osobowych), niezależnego i kompetentnego organu nadzoru, a także istnienie ograniczeń w dostępie organów

państwa do danych osobowych. Zdaniem Parlamentu Europejskiego to właśnie Dokument WP254 określa minimalny zakres oceny systemu prawnego państwa trzeciego. Pozostałe kryteria oceny, zawarte wyłącznie w art. 45 ust. 2 RODO nie znajdują odzwierciedlenia w dotychczas przeprowadzanych ocenach. Tym samym, pierwszy wniosek sprowadza się do uznania, że wykorzystywane podczas oceny systemu prawnego państwa trzeciego kryteria są związane z katalogami kryteriów zawartymi w przepisach prawa, ale nie oznaczają ich dosłownego stosowania.

Wykorzystywane kryteria oceny systemu prawnego państwa trzeciego wynikają bezpośrednio nie tylko z przepisów prawa, ale również z orzecznictwa TSUE. Sprawy dotyczące przekazywania danych do USA, a więc sprawy Schrems I i Schrems II spowodowały, że zagadnienie przetwarzania danych, w tym dostępu organów państwa do danych stało się przedmiotem wzmożonej dyskusji, a zarazem, niejako automatycznie, jednym z obowiązkowych kryteriów oceny.

Nadto, orzecznictwo TSUE podkreśliło znaczenie kryterium organu nadzorczego jako jednego z kluczowych elementów systemu ochrony danych osobowych, a tym samym przedmiotu oceny. O ile rozważania na ten temat stanowią kontynuację dotychczasowych poglądów doktryny i wymagań stawianych organowi nadzorczemu m.in. przez Europejską Radę Ochrony Danych Osobowych, o tyle przypadek USA można postrzegać jako ujednolicenie kryterium organu nadzorczego.

Stanowisko doktryny w odniesieniu do oceny systemu prawnego państwa trzeciego jest, co do zasady, zgodne. W poglądach doktryny można dostrzec katalogi kryteriów zbliżone, czy wręcz bazujące na Dokumentach WP12 oraz WP254. Podobnie jak orzecznictwo, doktryna zwraca uwagę na problem niejednolitego traktowania obywateli i nie obywateli państwa trzeciego. W mojej ocenie zbyt restrykcyjne podejście do tego kryterium nie jest wskazane, ponieważ nie jest możliwe dokładne i jednoznaczne poznanie sytuacji jednostki niebędącej obywatelem w systemie prawnym państwa trzeciego. G. Maldoff i O. Tene wyjaśniają, że nawet na przykładzie Kanady nie jest do końca jasne na jaką ochronę rzeczywiście może liczyć obcokrajowiec[379].

Zarówno doktryna, jak i orzecznictwo uznają za konieczne stosowanie Karty Praw Podstawowych podczas oceny. Z przedstawionych wyjaśnień nie wynika jednak czy Karta Praw Podstawowych miałaby stanowić samodzielne kryterium. W oparciu o prezentowane poglądy można stwierdzić, że chodzi o pośrednie stosowanie. W takim ujęciu Karta Praw Podstawowych jest samoistnym źródłem stawianych

[379] G. Maldoff, O. Tene: *Essential Equivalence and…*,s. 254, 278–281.

wymagań, które, po zastosowaniu odpowiednich zabiegów interpretacyjnych, bezpośrednio wynikają z RODO. Z tego względu, podczas oceny systemu prawnego państwa trzeciego Karta Praw Podstawowych przejawia się jako konkretne kryterium, kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego do danych.

Mając na uwadze powyższe, na pytanie pierwsze (P.1), należy odpowiedzieć twierdząco, jako że kryteria oceny systemu prawnego państwa trzeciego wynikają z przepisów RODO. Na ich interpretację wpływa dorobek doktryny i orzecznictwa. Ocena systemu prawnego państwa trzeciego jest przeprowadzana za pomocą kryteriów, które wynikają zarówno z przepisów RODO, wytycznych Europejskiej Rady Ochrony Danych Osobowych w postaci dokumentu WP254, a także orzecznictwa TSUE wspieranych przez doktrynę.

Ocena systemu prawnego państwa trzeciego nie ogranicza się jednak wyłącznie do stosowania kryteriów o charakterze prawnym, tj. wynikających z treści przepisów prawa. Zarówno stanowisko doktryny, w tym organów Unii Europejskiej potwierdza, że Komisja Europejska uwzględnia podczas oceny czynniki pozaprawne, na które składają się relacje polityczne i gospodarcze państwa trzeciego z Unią Europejską. Ich uszczegółowieniem są czynniki, o których wspomina Komisja Europejska w swoim komunikacie kierowanym do Parlamentu Europejskiego. Są to:

1) relacje handlowe z państwem trzecim,
2) nasilenie przepływów danych osobowych, w tym z uwagi na więzy kulturowe,
3) wiodąca rola państwa trzeciego w ochronie danych osobowych,
4) szeroko pojęte relacje polityczne i współpraca[380].

To właśnie te czynniki wyznaczają rzeczywiste podejście Komisji Europejskiej do badanego państwa trzeciego, determinując surowość z jaką Komisja Europejska zastosuje poszczególne kryteria oceny systemu prawnego państwa trzeciego, a więc czy zaakceptuje pewne wady systemu prawnego państwa trzeciego czy nie. Taki mechanizm działania Komisji Europejskiej znajduje bezpośrednie potwierdzenie w przypadku USA, a także Australii, gdzie niedoskonałości dostrzeżone w obu badanych systemach prawnych spotkały się z odmiennymi reakcjami Komisji Europejskiej.

W związku z tym, również pytanie drugie (P.2) wymaga odpowiedzi twierdzącej – czynniki pozaprawne w postaci relacji politycznych i gospodarczych z Unią Europejską

[380] *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*…, s. 8.

wpływają na interpretację i stosowanie kryteriów oceny systemu prawnego państwa trzeciego.

Przeprowadzone badania i przedstawione wnioski pozwalają na stworzenie następującego katalogu kryteriów oceny systemu prawnego państwa trzeciego:

1) Kryterium podstawowych zasad ochrony danych osobowych,
2) Kryterium egzekwowalności podstawowych zasad ochrony danych osobowych,
3) Kryterium kompetentnego, niezależnego organu nadzorczego,
4) Kryterium środków prawnych przyznanych osobie, której dane dotyczą na wypadek naruszenia ochrony danych osobowych, obejmujący środki administracyjne i sądowe,
5) Kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego do danych osobowych przekazanych na terytorium państwa trzeciego.

Przedstawione kryteria oceny posłużą do analizy systemu prawnego Chin.

ROZDZIAŁ DRUGI POZIOM OCHRONY DANYCH OSOBOWYCH W CHINACH USTALONY W OPARCIU KRYTERIA OCENY SYSTEMU PRAWNEGO PAŃSTWA TRZECIEGO

1. Wprowadzenie

Rekonstrukcja kryteriów oceny systemu prawnego państwa trzeciego pozwala przejść do następnej części badań, poświęconej problematyce poziomu ochrony danych osobowych w Chinach. W ramach rozdziału drugiego udzielę odpowiedzi dwa pytania pomocnicze: pytanie trzecie (P.3) „Jaki poziom ochrony danych osobowych zapewniając przepisy prawa chińskiego, poddane analizie w oparciu o kryteria oceny systemu prawnego państwa trzeciego" oraz pytanie czwarte (P.4), „Czy poziom ochrony danych osobowych. zapewniany przez przepisy chińskiego prawa ochrony danych osobowych, wyklucza uzyskanie przez Chiny decyzji w sprawie adekwatności w rozumieniu art. 45 ust. 1 RODO".

W celu odpowiedzi na przywołane pytania pomocnicze, w rozdziale drugim poddaję analizie przepisy prawa, które regulują ochronę danych osobowych w Chinach. Rozdział został podzielony na części odpowiadające poszczególnym kryteriom oceny systemu prawnego państwa trzeciego, tj.:

1) Kryterium podstawowych zasad ochrony danych osobowych,
2) Kryterium egzekwowalności podstawowych zasad ochrony danych osobowych,
3) Kryterium kompetentnego, niezależnego organu nadzorczego,
4) Kryterium środków prawnych przyznanych osobie, której dane dotyczą na wypadek naruszenia ochrony danych osobowych, obejmujący środki administracyjne i sądowe,
5) Kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego do danych osobowych przekazanych na terytorium państwa trzeciego.

Dodatkowo, w pkt 2 rozdziału została omówiona siatka pojęciowa stosowana przez ustawodawcę chińskiego.

1.1. Krajobraz chińskiego prawa ochrony danych osobowych po reformie z lat 2016 - 2021 r.

Przez lata ochrona danych osobowych i ochrona prywatności w Chinach przybierały specyficzną formę. Przejawem owej specyfiki była fragmentaryczna

i rozproszona regulacja. Na potrzeby niniejszej pracy wystarczy stwierdzić, że pewna postać prawnej ochrony danych osobowych w Chinach do 2016 roku wynikała z kilkudziesięciu różnych aktów prawnych należących do różnych gałęzi prawa[381]. Znaczącą rolę odgrywały także poglądy SNChRL oraz decyzje Stałego Komitetu[382]. Jednakże w praktyce takie ujęcie wywoływało szereg wątpliwości wśród przedstawicieli doktryny.

Dążenie do dominacji Chin w sieci, będące nowym kierunkiem w polityce chińskiej[383], uznaje się za jedną z przyczyn, daleko idącej zmiany w prawnym systemie ochrony danych osobowych w Chinach. Przełomowym momentem zmian było uchwalenie w 2016 roku CSL, ustawy będącej podstawowym aktem prawnym regulującym zagadnienie cyberbezpieczeństwa, a także pierwszym aktem prawnym takiej rangi, który w zaawansowany sposób regulował ochronę danych osobowych. O ile wejście w życie CSL nie wyeliminowało z chińskiego systemu prawnego rozproszonej regulacji ochrony danych osobowych (wynikającej z pozostałych aktów prawnych), o tyle CSL jest uznawane za pierwszy chiński akt prawny, który ogólnie i do pewnego stopnia, kompleksowo reguluje zagadnienie ochrony danych osobowych. Biorąc pod uwagę dalsze reformy władz chińskich CSL można uznać za początek ery kompleksowej i jednolitej regulacji ochrony danych osobowych w Chinach, której zwieńczeniem było uchwalenie PIPL.

Nie oznacza to, że chiński system ochrony danych osobowych w obecnym kształcie jest wolny od rozproszenia. Przeciwnie. Jedną z konsekwencji reform prawa chińskiego, która miała miejsce w latach 2017-2021 jest uzupełnienie systemu prawnego o kilka dodatkowych ustaw, które zostały skonstruowane w taki sposób, że każda z nich wiąże się z ochroną danych osobowych. W związku z tym, zanim przejdę do analizy chińskich przepisów prawa z pomocą kryteriów ustalonych w rozdziale I, wyjaśnię relacje zachodzące między poszczególnymi ustawami związanymi z ochroną danych osobowych, dążąc do wskazania ich zakresu zastosowania oraz konsekwencji jakie wynikają z wzajemnych relacji między przepisami.

---

[381] B. Zhao, G.P. Mifsud Bonnici: *Protecting EU Citizens'…*, s. 32; Z. Hanhua: *Consumer Data Protection in China*. W: *Consumer Data Protection in Brazil, China and Germany. A Comparative Study.* Red. R. Metz, J. Binding, P. Haifeng i in. Göttingen University Press, Göttingen 2016, s. 37; A. Qi, G. Shao, W. Zheng: *Assessing China's Cybersecurity Law*. „Computer Law & Security Review: The International Journal of Technology Law and Practice", 2018, nr 6, s. 1342; R. Berti: *Data Protection Law…,* s. 48–49; E. Pernot-Leplay: *China's Approach on*…, s. 65–81; X. Duoye: *The Civil Code*…, s. 187, 188.

[382] m.in. Z. Hanhua: *Consumer Data Protection*…, s. 43.

[383] G. Austin: *Cybersecurity in China. The Next Wave.* Springer, Cham 2018, s. 5–11.

1.2. Ustawy związane z ochroną danych osobowych w Chinach

Przyjmując kolejność chronologiczną, pierwszą z ustaw powiązanych z ochroną danych osobowych jest CSL. Celem ustawy, zgodnie z art. 1 CSL, jest ochrona cyberbezpieczeństwa. O ile art. 1 CSL oprócz ochrony cyberbezpieczeństwa wymienia inne cele, to biorąc pod uwagę ich sformułowanie, jak również całokształt regulacji, można uznać, że są to cele wspierające zasadniczy cel, czyli cyberbezpieczeństwo[384]. Tak określony cel koresponduje z zakresem zastosowania przepisów, którym zgodnie z art. 2 CSL, jest tworzenie i korzystanie z sieci oraz powiązane z nimi nadzór i zarządzanie cyberbezpieczeństwem[385].

W treść CSL zostały wkomponowane przepisy dotyczące ochrony danych osobowych. Rozdział IV CSL, w artykułach 40-50, reguluje takie zagadnienia, jak m.in. dopuszczalne podstawy przetwarzania danych, zasady przetwarzania danych oraz podstawowe wymagania w zakresie bezpieczeństwa danych. Zakres regulacji rozdziału IV CSL spowodował, że w krótkim czasie po wejściu w życie CSL niektórzy przedstawiciele doktryny twierdzili, że rozdział IV CSL stanowi ogólną regulację ochrony danych osobowych w Chinach[386]. Podejmując się obrony tego stanowiska można argumentować, że przepisy rozdziału IV CSL, a zwłaszcza przepisy określających obowiązki operatora sieci dotyczących ochrony danych osobowych[387], zostały sformułowane na tyle ogólnie, że mogłyby dotyczyć przetwarzania danych osobowych w każdych warunkach. Z czasem, tak daleko idące twierdzenie zaczęło tracić na znaczeniu. W doktrynie pojawiły się głosy, że CSL z racji jej ograniczonego zasięgu nie jest ogólną regulacją ochrony danych osobowych, przywołując przykład przetwarzania danych w sposób analogowy, które pozostaje poza regulacją CSL[388]. Ponadto, wskazywano, że CSL nie ogranicza się wyłącznie do ochrony danych osobowych, ale dotyczy także innych danych, w tym danych niewykazujących związku z osobą fizyczną[389]. Wyjaśniano także, że zmiany regulacyjne obejmujące ochronę danych osobowych to w zasadzie tylko pozytywny skutek uboczny działań chińskich polityków[390]. Uzasadnienia takiego stanowiska można

[384] podobnie J.-A. Lee: *Hacking into China's*…, s. 65.
[385] wyłącznie na terytorium Chin.
[386] A. Qi, G. Shao, W. Zheng: *Assessing China's Cybersecurity*…, s. 7.
[387] m.in. Art. 41-45, 47, 49 CSL.
[388] S. Wang Han, A.B. Munir: *Information Security Technology – Personal Information Security Specification: China's Version of the GDPR?*. „European Data Protection Law Review", 2018, nr 4, s. 535.
[389] R. Berti: *Data Protection Law…*, s. 39–40.
[390] R. Vecellio Segate: *Litigating Trade Secrets in China: An Imminent Pivot to Cybersecurity?*. „Journal of Intellectual Property Law & Practice", 2020, nr 15, s. 649, 650.

się dopatrywać w tym, że to sprawowanie władzy (i kontroli) nad siecią[391] pozostaje zasadniczym przedmiotem zainteresowania chińskiego ustawodawcy, czego przejawem miało być takie a nie inne sformułowanie katalogu celów CSL[392]. Jednocześnie, coraz częściej podkreślano, że w CSL pierwszoplanową rolę odgrywa bezpieczeństwo sieci[393]. Niemniej jednak wciąż to CSL stanowi kamień milowy w rozwoju chińskiej ochrony danych osobowych[394].

Drugą ustawą jest chiński kodeks cywilny z 2020 r. Jak każda tego rodzaju regulacja, c.k.c. ma na celu ochronę praw i interesów stron stosunków cywilnoprawnych[395]. Zgodnie z art. 2 c.k.c., regulacją kodeksową są objęte stosunki cywilnoprawne osób fizycznych i osób prawnych, które co do zasady, są związane z działaniami na terenie Chin[396]. W treści c.k.c. znalazły się także przepisy regulujące problematykę ochrony danych osobowych. W księdze pierwszej, rozdziale V, zatytułowanym dobra osobiste[397], za pośrednictwem art. 111 c.k.c. wprowadzono prawną ochronę danych osobowych osoby fizycznej oraz omówiono jej podstawowe konsekwencje [398]. Z kolei w księdze IV regulującej ochronę dóbr osobistych, w artykułach 1034 – 1039 c.k.c., zawarto szczegółowe przepisy, obejmujące m.in. podstawy i zasady przetwarzania danych, prawa osób których dane dotyczą czy zasady wyłącznie odpowiedzialności cywilnej za przetwarzanie danych osobowych [399]. Analizując zakres zastosowania kodeksowych przepisów o ochronie danych osobowych doktryna podkreśla, że c.k.c. to regulacja należąca do prawa prywatnego [400]. Samo znaczenie c.k.c. dla chińskiego systemu prawnego jest o tyle doniosłe, że jego treść w zakresie ochrony danych osobowych spowodowała, że definicje i zasady, dotychczas

[391] Określane niekiedy mianem suwerenności sieci.
[392] Z. Xinbao: *China's Strategy for International Cooperation on Cyberspace*. „Chinese Journal of International Law", 2017, nr 16, s. 377, 379–380.
[393] A. Qi, G. Shao, W. Zheng: *Assessing China's Cybersecurity*…, s.3; J. Quinn: *A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law*. „Science and Technology Law Review", 2018, nr 20, s. 407; X. Fei: *National Security Considerations in China's Trade Legislations: Offensive or Defensive?*. „US-China Law Review", 2022, nr 19, s. 186, 189.
[394] E. Pernot-Leplay: *China's Approach on*…, s. 71.
[395] Zgodnie z art. 1 c.k.c., który określa cel regulacji.
[396] Por. Art. 12 c.k.c.
[397] Według angielskiego tłumaczenia to *civil rights*, jednak z uwagi na przedmiot rozdziału V zasadnym jest tłumaczenie tytułu rozdziału V jako dobra osobiste.
[398] O czym będzie mowa dalej.
[399] O czym będzie mowa dalej.
[400] R. Y. Gao: *Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era*. „Tsinghua China Law Review", 2020, nr 13, s. 182; X. Duoye: *The Civil Code*…, s. 196; W. Guangping: *Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction*. „China Legal Science", 2021, nr 9, s. 144.

o niewiążącym charakterze stały się prawem powszechnie obowiązującym [401]. Dodatkowo, ochrona danych osobowych zapewniana przez c.k.c. jest uznawana za ogólną podstawę dla bardziej szczegółowych rozwiązań i bardziej szczegółowych przepisów[402].

Omawiając regulację ochrony danych osobowych w Chinach nie sposób pominąć DSL. Obowiązujące od 1 września 2021 r. DSL reguluje przetwarzanie wszelkich rodzajów danych. Szeroki zakres zastosowania wynika z celu ustawy, jakim jest ustandaryzowanie przetwarzania danych[403], a także z szerokiej definicji danych, za które uznawane są wszelkie informacje w jakiejkolwiek formie[404]. Omawiając DSL, doktryna podkreśla silny związek ustawy z ochroną bezpieczeństwa narodowego, co jednocześnie stanowi łącznik między CSL a DSL[405].

Ostatnią ustawą związaną z ochroną danych osobowych jest PIPL, która weszła w życie 1 października 2021 r. PIPL w art. 2 przyznaje osobom fizycznym prawną ochronę danych osobowych[406]. Zakres zastosowania ustawy, zawarty w art. 3 PIPL obejmuje czynności przetwarzania na wszelkich danych osobowych, którą są, co do zasady, wykonywane na terenie Chin[407]. PIPL ogranicza się więc wyłącznie do ochrony danych osobowych, a więc danych związanych z osobą fizyczną, w przeciwieństwie do DSL, który obejmuje wszelkie dane[408]. Jednocześnie, wskazuje się, że PIPL jest także silnie powiązane z cyberbezpiezczeństwem[409]. Zdaniem przedstawicieli doktryny PIPL stanowi pierwsze całościowe ujęcie problematyki ochrony danych osobowych w chińskim porządku prawnym[410].

---

[401] R. Berti: *Data Protection Law*…, s. 51; R. Y. Gao: *Personal Information Protection*…, s. 174; X. Duoye: *The Civil Code*…, s. 188; W. Guangping: *Challenges and Responses*…, s. 141–142; Y. Shao: *Personal Information Protection: China's Path Choice*. „US-China Law Review", 2021, nr 18, s. 239.
[402] R.Y. Gao: *Personal Information Protection*…, s. 181–182; Y. Shao: *Personal Information Protection*…, s. 239.
[403] Art. 1 DSL
[404] Art. 3 DSL
[405] W. Guangping: *Challenges and Responses*…, s. 146; P. Cai, L. Chen: *Demystifying Data Law*…, s. 90.
[406] Art. 2 PIPL zawiera odwołanie do Konstytucji ChRL. Taką konstrukcję można rozpatrywać jako próbę wyinterpretowania prawa do ochrony danych osobowych z przepisów chińskiej konstytucji. Przyjmując takie stanowisko za prawidłowe, należałoby stwierdzić, że prawo do ochrony danych osobowych wynika z prawa do prywatności. Zdaniem przedstawicieli doktryny Konstytucja ChRL zawiera w swoich przepisach ochronę prywatności. Tym samym, art. 2 PIPL, uznany za przejaw tzw. pośredniczącej roli ustawy, mógłby być uznany za wprowadzenie jednego z przejawów konstytucyjnej ochrony prywatności do chińskiego porządku prawnego.
[407] Art. 3 PIPL zawiera listę wyjątkowych sytuacji, w których PIPL znajdzie zastosowanie także poza granicami Chin.
[408] P. Cai, L. Chen: *Demystifying Data Law*…, s. 78.
[409] por. H. Dorwart: *Chinese Data Protection in Transition: A Look at Enforceability of Rights and the Role of Courts*. W: *Data Protection and Privacy. In Transitional Times.* Red. H. Matsumi, D. Hallinan, D. Dimitrova i in. Bloomsbury Publishing, Londyn 2023.
[410] C. Yan Wang: *Governing Data Markets in China: From Competition Litigation and Government Regulation to Legislative Ordering*. „George Mason International Law Journal", 2022, nr 1, s. 39.

1.3. Zasady stosowania przepisów o ochronie danych osobowych

Przedstawiony powyżej syntetyczny opis podstawowych cech chińskich aktów prawnych związanych z ochroną danych osobowych stanowi potwierdzenie utrzymującego się w chińskim porządku prawnym rozproszenia regulacyjnego. Należy mieć także na uwadze fakt, że źródłem pogłębiania się rozproszenia regulacyjnego, a tym samym partykularyzmów, jest dodatkowo działalność prawotwórcza organów lokalnych[411], których przepisy są niekiedy adresowane wyłącznie do wydzielonych stref ekonomicznych[412]. Cechą wspólną wszystkich wymienionych ustaw jest to, że zostały sformułowane w taki sposób, że każda z nich, choćby potencjalnie, może znaleźć zastosowanie do każdego przypadku kategoryzowanego jako zagadnienie ochrony danych osobowych.

Dążąc do usystematyzowania relacji zachodzących między CSL, c.k.c., DSL i PIPL na potrzeby dalszych prac, rozważę dwa możliwe scenariusze. Pierwszy z nich to odnalezienie w chińskim porządku prawnym jednej ustawy, która będzie pełniła rolę ustawy ogólnej, która, co do zasady, będzie stosowana (scenariusz „ustawa ogólna – ustawy szczególne"). Pozostałe ustawy będą wówczas stanowiły przepisy szczególne, uchylając w niektórych przypadkach zastosowanie ustawy ogólnej[413].

Drugi scenariusz polega na uznaniu, że w chińskim porządku prawnym, w zakresie prawa ochrony danych osobowych mamy do czynienia ze jednoczesnym stosowaniem przepisów różnych (scenariusz „jednoczesnego stosowania kilku ustaw"). Tym samym, wszystkie ustawy będą miały swego rodzaju ogólny charakter, zaś konkretny przypadek będzie determinował wybór ustawy, która znajdzie zastosowanie.

1.3.1. Ustawa ogólna – ustawy szczególne

Scenariusz „ustawa ogólna – ustawy szczególne" stanowi rzadko wykorzystywaną metodę wykładni chińskich przepisów o ochronie danych osobowych. Nieliczni przedstawiciele doktryny uznają CSL za ustawę o generalnym zasięgu[414],

---

[411] G. Zheng: *Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China*. „Computer Law & Security Review", 2021, nr 43, s. 6; T. Giladi Shtub, M.S. Gal: *The Competitive Effects of China's Legal Data Regime*. „Journal of Competition Law and Economics", 2022, nr 4; Y-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI and the IoT: The Privacy Concerns of Smart Speaker Users and the Personal Information Protection Law in China*. „Telecommunications Policy", 2022, nr 46, s. 8.

[412] I. Calzada: *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*. „Smart Cities", 2022, nr 5, s. 1141.

[413] Stosując zasadę *legi speciali derogat legi generali*.

[414] Z. Yuexin: *Cyber Protection of Personal Information in a Multi-Layered System*. „Tsinghua China Law Review", 2019, nr 12, s. 167, 169; Y. Shao: *Personal Information Protection*…, s. 239; A. Tiwari: *The*

czy ustawę będącą *legi speciali*[415]. Powodem takiego stanu rzecz są liczne wątpliwości zgłaszane przez doktrynę odnośnie do kwalifikacji poszczególnych ustaw, w tym zwłaszcza CSL, a w konsekwencji, zgody co do tego, która z ustaw ma charakter ogólny. Największe wątpliwości doktryny budzą związki poszczególnych ustaw z bezpieczeństwem sieci, czy spoglądając szerzej, bezpieczeństwem narodowym. Wskazuje się, że CSL reguluje przede wszystkim zagadnienie bezpieczeństwa sieci, które jest silnie związane z bezpieczeństwem narodowym[416]. To z kolei prowadzi do wniosku, że CSL nie jest samodzielną, zupełną regulacją ochrony danych osobowych[417], zwłaszcza, że w ten sposób ochrona interesów jednostki traci na znaczeniu i nie stanowi pierwszorzędnego przedmiotu regulacji[418].

W podobny sposób można mówić o DSL, która również jest uznawana za przejaw regulacji bezpieczeństwa narodowego, nie ochrony danych osobowych jako takiej[419]. DSL i CSL różnią się jednak, zwłaszcza w zakresie odpowiedniego klasyfikowania danych i odpowiedniej ochrony uprzednio sklasyfikowanych danych, które to zagadnienia są szczególnym przedmiotem zainteresowania DSL[420]. W tym względzie, na aprobatę zasługuje stanowisko, zgodnie z którym DSL eksponuje przede wszystkim interesy zbiorowe[421].

W przypadku PIPL sprawa nie jest już oczywista. Niektórzy autorzy uznają ustawę za rozwinięcie przepisów CSL[422] lub zarazem i DSL[423]. Taka koncepcja może być uzasadniona tym, że PIPL oraz DSL są uzupełnieniem CSL, ponieważ nie ograniczają się do środowiska sieciowego[424]. Nie stoi to jednak na przeszkodzie, aby postrzegać PIPL

Comparison between Indian Personnel and PRC New Civil Code, Cyber Laws, and Privacy. „Jus Corpus Law Journal", 2022, nr 2, s. 368, 377.

[415] por. C. You: *Half a Loaf Is Better than None: The New Data Protection Regime for China's Platform Economy*. „Computer Law & Security Review", 2022, nr 45.

[416] Z. Xinbao: *China's Strategy for*…, s. 381; J.-A. Lee: *Hacking into China's*…, s. 63, 65; C. Si: *Research on Data*…, s. 266–267; X. Fei: *National Security Considerations*…, s. 193; P. Cai, L. Chen: *Demystifying Data Law*…, s. 91; L. Belli, D. Doneda: *Data Protection in*…, s. 23.

[417] G. Greenleaf, S. Livingston: *China's New Cybersecurity Law – Also a Data Privacy Law?*. „Privacy Laws & Business International Report", 2016, nr 19, s. 1, 2; Y. Feng: *The Future of*…, s. 62, 71; L. Yu, B. Ahl: *China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform*. „Hong Kong Law Journal", 2021, nr 51, s. 290; R. Creemers: *China's Emerging Data…,* s. 9; C. You: *Half a Loaf*…, s. 9.

[418] L. Jia, L. Ruan: *Going Global: Comparing Chinese Mobile Applications' Data and User Privacy Governance at Home and Abroad*. „Internet Policy Review", 2020, nr 9, s. 3.

[419] R. Creemers: *China's Emerging Data*…, s. 2.

[420] Y.-L.Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 8.

[421] R. Creemers: *China's Emerging Data*…, s. 16, 19.

[422] Ibidem, s. 13; Y.-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 12.

[423] C. You: *Half a Loaf*…, s. 3

[424] Q A. Qi, G. Shao, W. Zheng: *Assessing China's Cybersecurity*…, s. 4, 5; X. Duoye: *The Civil Code*…, s. 191; P. Cai, L. Chen: *Demystifying Data Law*…, s. 77; M. Clausius: *The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes*. „Washington University Global Studies Law Review", 2022, nr 21 s. 279, 281.

jako ustawę związaną z bezpieczeństwem sieci[425], czy wręcz ustawę głównie powiązaną bezpieczeństwem sieci, podobnie jak CSL i DSL[426].

Na tle powyższego dyskursu nie bez znaczenia jest także rola jaką odgrywa w chińskim systemie prawnym c.k.c. Przyjmuje się, że c.k.c. został oparty o model zastosowany w CSL, z zastrzeżeniem, że c.k.c. ma szerszy zasięg zastosowania[427]. Szerszy zasięg zastosowania c.k.c. można rozpatrywać jako następstwo wyższego stopnia ogólności przepisów c.k.c. w porównaniu z przepisami CSL czy prawa konsumenckiego[428]. Nadto, sam c.k.c. jest uznawany za ustawę, która usystematyzowała zagadnienia związane z ochroną danych osobowych[429]. Chen stoi na stanowisku, że c.k.c. pełni wręcz funkcję ustawy implementującej przepisy konstytucyjne, które nie mogą być wprost stosowane przez sądy chińskie[430]. W związku z tym, zdaniem L. Zhanga, to właśnie przepisy c.k.c. stanowią podstawę prawną, w oparciu o którą została uchwalona PIPL[431]. Zarówno c.k.c., jak i PIPL są więc postrzegane jako ustawy zawierające ogólne przepisy dotyczące ochrony danych osobowych, a tym samym ustawy o szerokim zakresie zastosowania. Jednakże, ewentualne, wzajemne powiązania między c.k.c. a PIPL budzą poważne wątpliwości i są uznawane za niejasne[432].

1.3.2. Jednoczesne stosowanie kilku ustaw

W oparciu o przedstawione powyżej uwagi można stwierdzić, że doktryna skłania się ku scenariuszowi jednoczesnego stosowania kilku ustaw. Przyjmuje się, że CSL, DSL i PIPL mają pewne wspólne podłoże, do którego zalicza się regulacje przepływów danych oraz ochronę przed naruszeniem bezpieczeństwa danych osobowych[433]. Co oczywiste, wspólne podłoże nie oznacza braku jakichkolwiek różnic[434]. W oparciu o istnienie wspólnego podłoża CSL, DSL i PIPL, spośród całokształtu regulacji dotyczących ochrony danych osobowych, to właśnie te ustawy są uznawane za ustawy znajdujące zastosowanie do każdego przypadku przetwarzania danych, ponieważ w swojej treści zawierają generalne, uniwersalne zasady, które można określić mianem rdzenia

[425] por. H. Dorwart: *Chinese Data Protection*…..
[426] C. You: *Half a Loaf*…, s. 24; Y.-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 12.
[427] X. Duoye: *The Civil Code*…, s. 191.
[428] R. Y. Gao: *Personal Information Protection*…, s. 183.
[429] Y. Shao: *Personal Information Protection*…, s. 229, 237.
[430] L. Chen: *Continuity and Change: Some Reflections on the Chinese Civil Code*. „Asia Pacific Law Review", 2021, nr 2, s. 294.
[431] L. Zhang: *"Personal Information of Privacy Nature" under Chinese Civil Code*. „Computer Law & Security Review", 2021, nr 43, s. 4.
[432] X. Duoye: *The Civil Code*…, s. 199; P. Cai, L. Chen: *Demystifying Data Law*…, s. 90–91.
[433] L. Belli, D. Doneda: *Data Protection in*…, s. 82, 86, 87.
[434] Podobnie: L. Belli, D. Doneda: *Data Protection* in…, s. 84; 88; 91; W. Guangping: *Challenges and Responses*…, s. 145.

treściowego[435]. Oprócz ustaw będących rdzeniem, mogą pojawić się sytuacje, kiedy także stosowane będą przepisy dotyczące sektorowych zagadnień, jak choćby prawo konsumenckie; takie przepisy sektorowe cechuje różny stopień szczegółowości, jednakże z natury rzeczy znajdą zastosowanie tylko do przypadków zaliczających się do danego sektora[436]. Tak rozumiany scenariusz jednoczesnego stosowania kilku ustaw nie wyjaśnia jednak, które przepisy należy zastosować. Ułatwieniem ustalenia właściwego przepisu ustawy ma być poleganie na kontekście faktycznym danego przypadku, który zawsze powinien decydować o wyborze przepisu, który ostatecznie znajdzie zastosowanie[437].

1.4. Jednoczesne stosowanie kilku ustaw jako model zasadniczy

Biorąc pod uwagę specyfikę chińskiego systemu prawnego oraz dotychczas prezentowane poglądy doktryny, uważam, że najbardziej odpowiednim jest scenariusz jednoczesnego stosowania kilku ustaw. W oparciu o teksty CSL, c.k.c., DSL i PIPL nie sposób jednoznacznie przypisać tylko jednej z ustaw funkcji ustawy o podstawnym znaczeniu, która będzie bezwzględnie stosowana do każdego przypadku powiązanego z ochroną danych osobowych. Bez wątpienia, przepisy DSL nie będą aż tak istotne. Ich zakresy zastosowania nie pokrywają się całkowicie[438]. Rację ma R. Creemers, dla którego DSL i PIPL przenikają się do pewnego stopnia, ale ich odmienne cele, w tym zwłaszcza przedmiot regulacji DSL, jakim są dane jako takie, powoduje, osłabienie tej relacji[439]. W ten sposób, DSL można postrzegać jako swego rodzaju ułatwienie realizacji obowiązków w zakresie bezpieczeństwa danych[440]. Jak wyjaśnia W. Chaskes, prawdopodobnie naruszenie DSL będzie skutkowało uznaniem, że doszło także do naruszenia PIPL[441]. Dodatkowo DSL, obok PIPL ma być przejawem wzmocnienia kontroli państwa nad dopuszczalnością przekazywania danych osobowych do państw trzecich[442].

Akceptując pogląd o istnieniu rdzenia treściowego, skłaniam się ku uznaniu CSL za ustawę sektorową a nie jedną z ustaw zawierających taki rdzeń. Jak już była o tym mowa, CSL jest powiązane z zagadnieniem bezpieczeństwa danych. Jednocześnie, CSL

---

[435] L. Belli, D. Doneda: *Data Protection* in…, s. 78.
[436] Ibid.
[437] P. Cai, L. Chen: *Demystifying Data Law*…, s. 79.
[438] Ibid, s. 87;
[439] R. Creemers: *China's Emerging Data*…, s. 3.
[440] X. Li: *Information Privacy Protection in the New Chinese Civil Code: Priority or Replacement?*. „Frontiers of Law in China ", 2020, nr 15, s. 337; także: J. Chen, J. Sun: *Understanding the Chinese Data Security Law*. „International Cybersecurity Law Review", 2021, nr 2, s. 218.
[441] W. Chaskes: *The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet*. „Washington and Lee Law Review", 2022, nr 79, s. 1205.
[442] Podobnie: C. Yan Wang: *Governing Data Markets*…, s. 42.

ogranicza się wyłącznie do środowiska sieciowego. Te cechy powodują, że CSL bliżej do kategorii sektorowych regulacji ochrony danych osobowych[443]. Ponadto, na co zwracają uwagę niektórzy autorzy, CSL zasadniczo jest powoływana jako ustawa towarzysząca innymi przepisom a nie jako samodzielna podstawa prawna[444]. Natomiast, jak słusznie zauważa G. Grenleaf, uzasadnieniem szczególnego traktowania CSL przez doktrynę jest fakt, że w chwili wejścia w życie zawierała w sobie przepisy dotyczące ochrony danych osobowych o najszerszym jak dotąd zakresie zastosowania, a zarazem wprowadzające niektóre brakujące elementy właściwe prawu ochrony danych osobowych[445].

Miejsce CSL pośród ustaw zawierających rdzeń treściowy powinien zająć c.k.c.[446]. Za zbyt daleko idące uznaję stanowisko, zgodnie z którym c.k.c. jest jedyną ustawą regulującą ochronę danych osobowych o odpowiednim stopniu ogólności, a zarazem szerokim zakresie zastosowania[447]. To właśnie c.k.c. wraz z PIPL są uznawane za ustawy będące źródłem prywatnoprawnej ochrony danych osobowych, funkcjonującej obok publicznoprawnej ochrony realizowanej przez przepisy prawa karnego[448]. Niemniej jednak, nie można zapominać, że PIPL zasadniczo odrywa się od ujęcia prywatności, typowej dla chińskiego prawa cywilnego[449], o której szerzej będzie mowa w dalszej części rozdziału.

W niniejszej pracy przyjmuję wiec scenariusz jednoczesnego stosowania kilku ustaw związanych z ochroną danych osobowych w Chinach. Pomimo ewolucji poglądów doktryny, jest to scenariusz odzwierciedlający stanowisko dominujące[450]. W dalszej części pracy poddam analizie przepisy CSL, c.k.c., DSL oraz PIPL, które zbiorczo określam jako chińskie prawo ochrony danych osobowych. Już w tym miejscu można

---

[443] Podobnie: E. Pernot-Leplay: *China's Approach on*… s. 79, 82. Autor wyjaśnia, że z treści CSL nie wynika cecha całościowej regulacji ochrony danych osobowych, w szczególności zgodnie z podejściem Unii Europejskiej. Zdaniem autora to wytyczne władz chińskich (tzw. standard), opublikowane w 2018 r., w większym stopniu odpowiadają standardom wynikającym z prawa Unii Europejskiej.

[444] G. Pyo: *An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts*. „Columbia Journal of Transnational Law", 2021, nr 1, s. 263.

[445] G. Greenleaf: *China Issues a Comprehensive Draft Data Privacy Law*. „Privacy Laws & Business International Report", 2020, nr 168, s. 6.

[446] X. Duoye: *The Civil Code*…, s. 195 - zdaniem autora to c.k.c. znajduje zastosowanie do każdego przetwarzania danych osobowych a nie CSL.

[447] Tak: R.Y. Gao: *Personal Information Protection*…, s. 184.

[448] Y. Shao: *Personal Information Protection*…, s. 241.

[449] R. Creemers: *China's Emerging Data*…, s. 6.

[450] G. Greenleaf: *China Issues a*…, s. 12; H. Dorwart: *Platform Regulation from the Bottom up: Judicial Redress in the United States and China*. „Policy & Internet", 2021, nr 14, s. 379; W. Chaskes: *The Three Laws*…, s. 1173; H. Xing, *Government Data Sharing and Personal Information Protection*. „Administrative Law Research", 2023, nr 2, s. 72; Q. Zhou: *Whose Data Is It Anyway? An Empirical Analysis of Online Contracting for Personal Information in China.* „Asia Pacific Law Review", 2023, nr 31, s. 74.

zaznaczyć, że skomplikowane zasady stosowania przepisów o ochronie danych osobowych będą miał wpływ na ocenę egzekwowalności i praktycznego zastosowania chińskiego prawa ochrony danych osobowych. Zdaniem doktryny, ustalenie w praktyce ustawy, której przepisy znajdą zastosowanie do konkretnego przypadku jest bardzo trudne[451].

2. Siatka pojęciowa wykorzystywana w chińskim prawie ochrony danych osobowych

Jak już była o tym mowa w pierwszym rozdziale, siatka pojęciowa stanowi pierwsze z kryteriów oceny systemu prawnego państwa trzeciego, o których mowa w Dokumencie WP254. Dlatego też, dalszą analizę chińskiego prawa ochrony danych osobowych poprzedza omówienia najważniejszych pojęć wykorzystywanych w tychże przepisach.

2.1. Dane osobowe (informacje osobowe)

Ustawodawca chiński zdecydował się zdefiniować dane osobowe jako informacje osobowe (personal information). Przyjęta konstrukcja, o czym mowa dalej, zasadniczo odpowiada pojęciu danych osobowych, które jest stosowane przez europejską naukę ochrony danych osobowych. Definicja danych (jako takich) znajduje się w DSL i obejmuje swoim zakresem wszelkie informacje, w dowolnej formie, w tym formie elektronicznej. Tym samym, chińskie przepisy prawa ochrony danych, w tym danych osobowych jednoznacznie kwalifikują dane jako nośnik informacji.

Definicja informacji osobowych wynika z trzech ustaw: CSL, c.k.c. oraz PIPL. Co do zasady, wyznacznikiem przynależności informacji do kategorii informacji osobowych jest zdolność do identyfikacji osoby fizycznej. Identyfikacja może nastąpić bezpośrednio w oparciu o informacje osobowe lub wraz z innymi informacjami. Dla ułatwienia określenia charakteru konkretnej informacji, definicje informacji osobowych w CSL i c.k.c. zawierają w swojej treści otwarte katalogi czynników identyfikujących osobę fizyczną, wśród których znalazły się m.in. imię i nazwisko czy data urodzenia. Greenleaf i Livingston uważają, że katalog czynników identyfikacyjnych w CSL jest wyjątkowy, ponieważ za informacje osobowe uznaje informacje biometryczne, co w chwili uchwalenia przepisów CSL stanowiło pierwsze potwierdzenie osobowego charakteru takich informacji[452]. Nadto, spośród informacji osobowych, definicja wynikająca z PIPL wyłącza informacje, które zostały poddane anonimizacji.

[451] X. Duoye: *The Civil Code*…, s. 191; P. Cai, L. Chen: *Demystifying Data Law*…, s. 92.
[452] G. Greenleaf, S. Livingston: *China's New Cybersecurity*…, s. 3.

Wszystkie trzy definicje dopuszczają utrwalenie informacji w dowolnej formie, a zwłaszcza w formie elektronicznej.

W świetle powyższego, zastosowana definicja informacji osobowych zasadniczo nie odbiega od definicji danych osobowych, o której mowa w art. 4 RODO. Wyjątkiem jest podejście do informacji uprzednio zanonimizowanych, które *expressis verbis* nie stanowią danych osobowych w rozumieniu PIPL (o czym szerzej będzie mowa dalej).

W dalszym toku rozważań będę posługiwał się zamiennie terminem dane osobowe lub informacje osobowe.

2.2. Dane wrażliwe i dane prywatne (informacje wrażliwe i informacje prywatne)

Oprócz informacji osobowych, chińskie prawo ochrony danych osobowych wyróżnia dwie dodatkowe kategorie informacji, informacje wrażliwe oraz informacje prywatne.

O informacjach wrażliwych, będących odpowiednikiem danych wrażliwych w RODO, stanowi wyłącznie PIPL. Zgodnie z art. 28 zdanie 1 PIPL informacja osobowa staje się informacją wrażliwą, jeśli dojdzie do uznania, że jej wyciek lub niezgodne z prawem wykorzystanie może w stanowić naruszenie godności osoby, której dane dotyczą, poważną szkodę dla jej bezpieczeństwa osobistego lub majątku. W ten sposób, informacje wrażliwe obejmuje znacznie szerszy katalog informacji w porównaniu z RODO, ponieważ informacją wrażliwą potencjalnie może być każda informacja osobowa. Praktyka wskazuje, że okolicznością powodującą uznanie informacji za informację wrażliwą jest jej wysoka podatność na nielegalne pozyskanie, a następnie na jej wykorzystanie do kradzieży czy oszustwa[453]. Na szerszy zasięg ochrony informacji wrażliwych wskazuje także analiza otwartego katalogu danych wrażliwych, będącego częścią definicji zawartej w PIPL, gdzie oprócz informacji o cechach biometrycznych, informacji o stanie zdrowia czy informacji o przekonaniach religijnych, które to informacje zostały sklasyfikowane przez RODO jako dane wrażliwe, za informacje wrażliwe uznano również informacje o finansach, informacje dotyczące osób poniżej 14 roku życia czy indywidualne informacje lokalizacyjne. Zdaniem A. Geller przedstawione podejście do danych wrażliwych jest konsekwencją bliższego związku regulacji z problematyką bezpieczeństwa informacji i sieci[454]. Bez wątpienia,

[453] F. Feng, X. Wang, T. Chen: *Analysis of the Attributes of Rights to Inferred Information and China's Choice of Legal Regulation*. „Computer Law & Security Review", 2021, nr 41, s. 8.
[454] A. Geller: *How Comprehensive is*… s. 1191, 1195.

przynajmniej teoretycznie, wykorzystana definicja informacji wrażliwych jest przejawem wzmocnienia ochrony jednostki.

Ochronny charakter wyróżnia także informacje prywatne. Informacje prywatne wiążą się z przenikaniem przepisów c.k.c. o ochronie prywatności i o ochronie danych osobowych. Artykuł 1034 zdanie 3 c.k.c. w ramach informacji osobowych dodatkowo wyróżnia informacje prywatne. Skutkiem przynależności do kategorii informacji prywatnych jest odrębna ochrona, co do zasady realizowana w oparciu o przepisy o ochronie prywatności, a dopiero w braku takich przepisów, w oparciu o przepisy o ochronie danych osobowych. Mimo tak daleko idących konsekwencji, w c.k.c. zabrakło definicji informacji prywatnych, których aktualne pojmowanie jest wyłącznym wynikiem rozważań doktryny i praktyki orzeczniczej. L. Zhang za kryteria pozwalające ocenić, czy w konkretnym przypadku mamy do czynienia z informacją prywatną uznaje trzy czynniki: osobowy charakter informacji, prywatność rozumiana jako oczekiwany stopień poufności konkretnej informacji, oraz brak związku takiej informacji z interesem publicznym [455] . Jednocześnie wyjaśnia, że przenikanie się informacji prywatnych i informacji wrażliwych jest o tyle nieuniknione, że trudno wyobrazić sobie informację wrażliwą, która nie zostałaby uznana za informacje prywatną. L. Zhang przytacza również przykłady wynikające praktyki orzeczniczej, gdzie za informacje prywatne uznano m.in. informacje dotyczące finansów czy dokumentu tożsamości (np. kopia takiego dokumentu). W podobny sposób informacje prywatne definiuje X. Li, który precyzuje, że prywatny charakter informacji to brak jej związku z interesem publicznym, zaś poufność w tym wypadku powinna być rozumiana jako brak chęci ujawnienia takich informacji na rzecz osób trzecich[456]. Subiektywne zapatrywanie jednostki będzie więc wpływało na kwalifikację informacji jako informacji prywatnej, przy czym nie można pominąć obiektywizowanego spojrzenia opinii publicznej. X. Li jako przykład informacji prywatnych podaje m.in. DNA, dane medyczne, informacje finansowe czy informacje na temat treści przeglądanych w Internecie.

Jak zauważa L. Zhang, problematyka odrębnej ochrony informacji osobowych prywatnych jest konstrukcją, która nie występuje w innych porządkach prawnych[457], stąd uchwycenie jej istoty może być trudne, zwłaszcza dla podmiotów spoza Chin. Sądzę, że

[455] L. Zhang: *"Personal Information of*…, s. 2, 5–6, 11.
[456] X. Li: *Information Privacy Protection*…, s. 322, 332.
[457] L. Zhang: *"Personal Information of*…, s. 5.

zbyt śmiałym uproszczeniem jest twierdzenie o braku jakiejkolwiek wartości użytkowej informacji prywatnej[458].

2.3. Przetwarzanie danych osobowych

Definicja przetwarzania danych osobowych jest wyjątkowa. PIPL i c.k.c. tylko pośrednio definiują przetwarzanie danych osobowych. Definicje przybrały postać otwartych katalogów czynności, które można streścić jako operacje na danych osobowych, począwszy od ich zebrania, przetwarzanie *sensu stricto* (a więc m.in. przechowywanie, wykorzystywanie, ujawnianie), aż po usunięcie danych. Oba katalogi można więc traktować jako egzemplifikacje cyklu życia danych osobowych przetwarzanych przez administratora, co powoduje, że faktycznie każda operacja na danych osobowych będzie stanowiła ich przetwarzanie w rozumieniu PIPL i c.k.c. Taka interpretacja pozwala uznać, że definicja przetwarzania danych osobowych w prawie chińskim jest zgodna z definicją wynikającą z RODO.

2.4. Administrator danych osobowych

Administrator danych osobowych został zdefiniowany wyłącznie w PIPL. Administratorem danych może być organizacja lub jednostka. Podobnie jak ma to miejsce w RODO, wyznacznikiem sprawowania funkcji administratora danych osobowych jest podejmowanie decyzji o celach i sposobach ich przetwarzania Jeśli cele i sposoby przetwarzania danych osobowych określa więcej niż jeden podmiot, wówczas dochodzi do sytuacji współadministrowania, przy czym zgodnie z art. 20 zdanie pierwsze PIPL konieczne jest uzgodnienie wzajemnych praw i obowiązków administratorów danych osobowych. Takie rozwiązanie również odpowiada przepisom RODO.

Tym, co wyróżnia przepisy RODO na tle przepisów prawa chińskiego jest ich zastosowanie do organów państwowych. Oczywistym jest, że w ramach wykonywania władzy publicznej i powiązanych z tym obowiązków niektóre podmioty państwo mogą pełnić funkcję administratora danych osobowych. Jednakże doktryna prezentuje niejednolite stanowisko. Dla części autorów PIPL, choćby teoretycznie, może znaleźć zastosowanie do przetwarzania danych osobowych przez organy państwa [459] . Oznaczałoby to, że za administratora mogą być uznane także organy państwowe. Jest to jednak zbyt śmiała interpretacja, jako że sami zwolennicy takiego rozumienia

[458] Tak S. Cui, P. Qi: *The Legal Construction of Personal Information Protection and Privacy under the Chinese Civil Code.* „Computer Law & Security Review", 2021, nr 41, s. 16.
[459] G. Greenleaf: *China's Completed Personal Information Protection Law: Rights Plus Cyber-Security*. „Privacy Laws & Business International Report", nr 20, s. 2; R. Creemers: *China's Emerging Data*…, s. 14; C. You: *Half a Loaf*…, s. 19; Q. Zhou: *Whose Data Is*…, s. 90.

przepisów PIPL wyrażają obawę co do faktycznego podejścia do przestrzegania PIPL przez władze państwowe. W identyczny sposób wypowiadają się ci autorzy, którzy głoszą tezę o braku zastosowania PIPL do organów państwa[460]. Nadto, to właśnie wątpliwe podejście do organów państwa, które wynika z przepisów PIPL jest uznawane za zasadniczą wadę ustawy[461]. Przedstawione rozumienie definicji administratora wspierają uwagi doktryny zgłaszane na tle zakresu pojęcia operator sieci, o którym stanowi CSL[462]. Definicja operatora sieci w CSL jest na tyle pojemna, że nie można wykluczyć, że za operatora sieci zostanie uznany operator sieci wewnętrznej, a więc sieci działającej w ramach struktury danego podmiotu[463]. Mimo tego, część autorów uważa, że CSL w ogóle nie będzie stosowane do organów państwa, kwalifikujących się jako operatorzy sieci[464], lub znajdzie zastosowanie warunkowo, w związku z przekazywaniem informacji publicznych za pomocą stron internetowych, które prowadzą te organy[465], lub wyłącznie teoretycznie[466].

W świetle powyższego, można stwierdzić, że administratorem danych osobowych mogą być tzw. podmioty niepubliczne, zaś przypisanie roli administratora danych osobowych organom władzy jest obarczone poważnym ryzykiem niepowodzenia, co niewątpliwie odróżnia przepisy chińskiego prawa ochrony danych osobowych od RODO.

2.5. Podmiot przetwarzający

Przepisy chińskiego prawa ochrony danych osobowych zasadniczo nie zawierają definicji podmiotu przetwarzającego dane na zlecenie lub w imieniu administratora. PIPL ogranicza się w tym względzie do wskazania przesłanek powołania takiego podmiotu przez administratora, którym zgodnie z art. 21 PIPL ma być zawarcie umowy regulującej prawa i obowiązki administratora oraz podmiotu przetwarzającego, w tym cele powierzonego przetwarzania, kategorie danych, metody przetwarzania, okres, na który powierzono przetwarzanie, stosowane zabezpieczenia Co do zasady, podmiot

[460] por. L. Zheng: *"Personal Information of*…, s. 7.
[461] por. R. Creemers: *China's Emerging Data*…, s. 19.
[462] Zgodnie z art. 76 pkt 3 CLS operatorem sieci jest właściciel lub zarządca sieci, lub dostawca usług sieciowych.
[463] G. Greenleaf, S. Livingston: *PRC's New Data Export Rules: "Adequacy with Chinese Characteristics"?*. „Privacy Laws & Business International Report", 2017, nr 147. s. 7.
[464] Y-J. Chen, C-F. Lin, H-W. Liu: *"Rule of Trust": The Power and Perils of China's Social Credit Megaproject*. „Columbia Journal of Asian Law", 2018, nr 1, s. 27; Y. Duan: *Balancing the Free Flow of Information and Personal Data Protection*. 3.04.2019. https://ssrn.com/abstract=3484713 [dostęp: 26.04.2023], s. 11–12.
[465] L. Yu, B. Ahl: *China's Evolving Data*…s. 292.
[466] G. Greenleaf, S. Livingston:*China's New Cybersecurity*…, s. 3.

przetwarzający powinien postępować zgodnie z zawartą umową i nie może wykraczać poza zakres przetwarzania, który wynika z jej treści.

2.6. Automatyczne podejmowanie decyzji

Automatyczne podejmowanie decyzji w rozumieniu PIPL opiera się na następujących przesłankach:

1) Analiza i ocena jednostki w zakresie jej zwyczajów, hobby, statusu finansowego lub kredytowego, kondycji zdrowotnej.
2) Proces jest zautomatyzowany i realizuje go program komputerowy.
3) Zwieńczeniem procesu jest wydanie decyzji w oparciu o przeprowadzoną analizę i ocenę jednostki.

Zaistnienie wymienionych przesłanek oznacza, że dochodzi do automatycznego podejmowania decyzji.

Sposób, w jaki zredagowano przywołaną definicję może wywoływać wątpliwości co do zakresu czynności kwalifikowanych jako automatyczne podejmowanie decyzji. Porównując definicję PIPL z definicją profilowania zawartą w RODO, a także definicją automatycznego podejmowania decyzji, o której mowa w art. 22 RODO, dostrzegamy, że każda RODO dotyczy każdej postaci automatycznego podejmowania decyzji, w szczególności bez względu na przedmiot oceny jednostki i jej zachowań.

2.7. Anonimizacja danych

PIPL definiuje dwie szczególne postaci przetwarzania danych osobowych, które prowadzą do pozbawienia informacji jej charakteru osobowego. Deidentyfikacja prowadzi do uniemożliwienia identyfikacji osoby, której dane dotyczą bez pozyskania dodatkowych informacji. Innymi słowy, informacja osobowa staje się informacją o osobie możliwej do zidentyfikowania, pod warunkiem, że dostępu do dodatkowych informacji. Natomiast anonimizacja prowadzi do trwałego pozbawienia informacji osobowej zdolności identyfikacji osoby fizycznej. Oznacza to, że anonimizacja danych *de facto* skutkuje brakiem możliwości ponowne identyfikacji osoby fizycznej, nawet przy wykorzystaniu dodatkowych informacji. Co istotne, zarówno deidentyfikacja, jak i anonimizacja mogą być przeprowadzone z wykorzystaniem dowolnych czynności przetwarzania, które doprowadzą do zamierzonego efektu. Już w tym miejscu warto zauważyć, że skutki jakie pociąga za sobą zastosowanie deidentyfikacji są niejasne. Zdaniem G. Greenleafa i S. Livingstona, na tle CSL nie wiadomo czy dane poddane takiemu zabiegowi tracą przymiot informacji osobowej, a także czy w stosunku do nich

wciąż należy przestrzegać niektórych obowiązków, w tym zwłaszcza tych dotyczących bezpieczeństwa danych[467].

2.8. Naruszenie bezpieczeństwa danych

W chińskich przepisach ochrony danych osobowych nie zdecydowano się na definicję naruszenia bezpieczeństwa danych osobowych, tak jak ma to miejsce w RODO. Można jedynie mówić o swego rodzaju wskazówce interpretacyjnej, która wynika z PIPL. W artykule 57 zdanie pierwsze PIPL omówiono działania, jakie powinien podjąć administrator danych osobowych w razie zaistnienia sytuacji, które zbiorczo można określić jako naruszenie danych osobowych. Do tych sytuacji zaliczają się potencjalne lub rzeczywiste wycieki danych, zniekształcenia danych, utraty danych. To właśnie ten katalog sytuacji można traktować jako podstawowy wyznacznik naruszenia bezpieczeństwa danych osobowych w rozumieniu PIPL.

3. Kryterium pierwsze: podstawowe zasady ochrony danych osobowych

3.1. Uwagi wstępne

Podstawowe zasady ochrony danych osobowych to pierwsze zasadnicze kryterium oceny adekwatności systemu prawnego państwa trzeciego. Zasady ochrony danych osobowych zostały zawarte w przepisach CSL, c.k.c. i PIPL. Również DSL zawiera podstawowe zasady, którymi należy się kierować podczas przetwarzania wszelkich kategorii danych, nie tylko danych osobowych

3.2. Zasada zgodności z prawem

Naczelną zasadą przetwarzania danych osobowych jest zgodność prawem[468]. Takie ujęcie roli zasady legalności znajduje odzwierciedlenie w przepisach CSL, c.k.c., DSL oraz PIPL, w których zostały zawarte różne wersje omawianej zasady.

Cechą wspólną chińskiego prawa ochrony danych osobowych jest traktowanie legalności jako punktu wyjścia, centralnej zasady przetwarzania danych osobowych, która niejako jest budulcem dla pozostałych zasad, a także faktycznym gwarantem ich przestrzegania. Można więc mówić o zasadzie zgodności z prawem w szerszym i węższym ujęciu.

Szersze ujęcie zasady legalności oznacza konieczność przetwarzania danych osobowych w takich sposób, aby podejmowane czynności były zgodne z prawem, w tym także z przepisami administracyjnymi. Innymi słowy, cały cykl życia danych osobowych

[467] G. Greenleaf, S. Livingston: *China's New Cybersecurity*…, s. 5.
[468] W dalszej części pracy zasada zgodności z prawem jest nazywana także jako zasada legalności.

przetwarzanych przez administratora powinien odpowiadać standardom określonym przez prawo. Taka, minimalna treść zasady zgodności z prawem wynika z przepisów CSL, c.k.c., DSL i PIPL. Jednocześnie, niektóre ustawy nie ograniczają zasady zgodności z prawem wyłącznie do konieczności przestrzegania przepisów prawa. Zasada legalności w CSL łączy się z obowiązkiem przestrzegania umów zawartych z osobami, których dane dotyczą. Na uzgodnienia jakie poczyniły między sobą stron umowy wskazuje także art. 1035 pkt 4 c.k.c. Z kolei w DSL, obok przepisów prawa, art. 8 wymienia m.in. etykę biznesu, etykę zawodową, czy unikanie zagrożenia dla interesu publicznego oraz szkody dla praw i interesów jednostek i organizacji. W przypadku c.k.c. zasada legalności została dodatkowo ujęta w formie katalogu czynności przetwarzania, których nie można nielegalnie wykonywać. Do wyliczonych czynności należą nielegalne zbieranie, wykorzystywanie, przetwarzanie, przesyłanie, sprzedaż, kupno, udostępnienie i publikacja danych osobowych. Nadto, c.k.c. z wymogiem legalności jednoznacznie wiąże obowiązek zapewnienia bezpieczeństwa danych, jak również, na co wprost wskazuje art. 1035 c.k.c., przestrzeganie zasad publicznego przetwarzania danych. Zwłaszcza ten ostatni element kodeksowej zasady zgodności z prawem może budzić wątpliwości, mając na uwadze stanowisko, zgodnie z którym przepisy c.k.c. dotyczące danych osobowych nie znajdą zastosowania do relacji państwo-jednostka[469].

Węższe ujęcie zasady zgodności z prawem dotyczy podstaw przetwarzania danych osobowych, o których mowa poniżej.

3.2.1. Podstawy przetwarzania danych osobowych

Podstawy przetwarzania danych osobowych określają przepisy CSL, c.k.c. oraz PIPL. Z oczywistych względów, DSL nie zawiera katalogu podstaw przetwarzania, oczekując jedynie, w myśl art. 32 DSL, implementacji właściwych i zgodnych z prawem metod pozyskiwania danych oraz przestrzegania zakazu stosowania nielegalnych metod pozyskiwania danych, zwłaszcza ich kradzieży.

3.2.1.1. Zgoda jako podstawa przetwarzania danych osobowych

Cechą charakterystyczną chińskiego systemu ochrony danych osobowych jest podejście do zgody jako podstawy przetwarzania danych osobowych, które zdaniem doktryny polega na jej nadmiernym wykorzystywaniu[470].

[469] L. Yu, B. Ahl: *China's Evolving Data*… s. 293.
[470] L. Yu, B. Ahl: *China's Evolving Data*… s. 296–298; C. Wang, J. Zhang, N. Lassi i in.: *Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective*. „Healthcare", 2022, nr 10, s. 12; Y.-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 9–10; por. także:

Co do zasady, zgoda stanowi wyłączną podstawę przetwarzania danych osobowych na podstawie CSL oraz c.k.c. Różnica pomiędzy dwoma ustawami sprowadza się do możliwości zastosowania innych podstaw przetwarzania danych osobowych, którą dopuszcza c.k.c., dla którego zgoda osoby której dane dotyczą lub jej opiekuna prawnego znajdą zastosowanie dopiero, gdy brak przepisów szczególnych. Nie bez znaczenia jest fakt, że podstawa przetwarzania danych osobowych w c.k.c. odgrywa szczególną rolę także jako jedna z okoliczności wyłączających cywilną odpowiedzialność administratora[471].

Natomiast dla CSL zgoda to jedyna możliwa do zastosowania podstawa przetwarzania danych osobowych, której pominięcie zasadniczo ograniczono do jednej sytuacji. Obowiązek pozyskania zgody osoby, której dane dotyczą na udostępnienie jej danych uchyla jedynie nieodwracalna utrata identyfikowalności danych, wynikająca z czynności przetwarzania danych. Innymi słowy, zgoda na udostępnienie danych nie będzie konieczna, jeśli dane zostały przetworzone w taki sposób, że na ich podstawie nie jest już możliwa identyfikacja konkretnej osoby. Należy jednak zwrócić uwagę na lakoniczność CSL, a także c.k.c. w opisie zgody jako takiej. O ile w przypadku c.k.c. można bronić poglądu o zastosowaniu ogólnych przepisów kodeksowych, o tyle CSL w ogóle nie określiła podstawowych parametrów zgody, w tym zwłaszcza w kontekście warunków jej wyrażenia oraz cech dobrowolności i świadomości. Bez wątpienia, zgoda jako przesłanka przetwarzania danych osobowych w CSL jawi się jako niejasna[472].

Do pewnego stopnia PIPL przejęła opisaną powyżej konstrukcje zastosowaną w CSL i c.k.c. Mimo uwzględnienia w przepisach PIPL katalogu różnych podstaw przetwarzania danych osobowych, to wciąż zgoda jest najważniejszą z nich. Tym, co wyróżnia zgodę w PIPL, jest jej subsydiarny charakter. Artykuł 13 zdanie ostatnie PIPL wskazuje, że konieczność pozyskiwania zgody zostaje uchylona wyłącznie w sytuacji, gdy znajdzie zastosowanie jedna z pięciu szczególnych podstaw przetwarzania danych. Oznacza to, że administrator powinien najpierw skorzystać z jednej ze szczególnych podstaw przetwarzania danych, a dopiero w ostateczności sięgnąć po zgodę, a więc zamiast a nie obok innych podstaw przetwarzania[473].

B. Hu, Y-L. Liu, W. Yan: *Should I Scan My Face? The Influence of Perceived Value and Trust on Chinese Users' Intention to Use Facial Recognition Payment*. „Telematics and Informatics", 2023, nr 78.

[471] Zgodnie z art. 1036 pkt 1 c.k.c. wśród okoliczności wyłączających odpowiedzialność cywilną administratora znajdują się działania, które mieszczą się w zakresie uzgodnionym z osobą, której dane dotyczą lub jej opiekunem.

[472] L. Trakman, R. Walters, B. Zeller: *Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience*. „Information & Communications Technology Law", 2020, nr 2, s. 234.

[473] G. Greenleaf: *China's Completed Personal*…, s. 1.

Taka konstrukcja to wyraz spójności przepisów PIPL i c.k.c. Ponadto, PIPL określa minimalne standardy dotyczące samej zgody. Forma udzielenia zgody jest zasadniczo obojętna, chyba, że przepisy szczególne wskazują na konieczność udzielenia zgody w formie pisemnej. W taki sam sposób uregulowano zakres udzielanej zgody, ograniczając wyraźną zgodę tylko do przypadków, na które wprost wskazuje przepis prawa lub przepis administracyjny. Z przepisów PIPL wynika, że do pozyskania odrębnej zgody na przetwarzanie danych dojdzie w sytuacji, gdy administrator:

1) będzie chciał ujawnić przetwarzane dane[474];
2) będzie chciał udostępnić dane innemu administratorowi[475];
3) w sytuacji wykorzystywania wizerunku jednostki do celów innych niż zapewnienie bezpieczeństwa publicznego[476];
4) będzie przetwarzał dane wrażliwe[477];
5) będzie przekazywał dane osobowe poza terytorium Chin[478].

Natomiast ponowne pozyskanie zgody będzie konieczne, jeśli administrator, któremu udostępniono dane będzie chciał zmienić cel lub sposoby przetwarzania danych[479]. Odrębnie potraktowano sytuację, gdy przetwarzanie danych ujawnionych przez jednostkę wywiera znaczny wpływ na jej prawa i wolności. Wówczas administrator jest zobowiązany do pozyskania zwykłej zgody [480]. Aby zgoda została udzielona w prawidłowy sposób, osoba, której dane dotyczą musi być odpowiednio poinformowana, zaś jej oświadczenie musi być dobrowolne i wyraźne. W związku z tym, każda zmiana celu lub metod przetwarzania, jak również zmiana kategorii danych powoduje konieczność ponownego pozyskania zgody jednostki. Warunek dobrowolności udzielenia zgody znalazł rozwinięcie w art. 15 i 16 PIPL. Co do zasady, PIPL zakazuje odmowy dostarczenia produktu lub świadczenia usług tylko dlatego, że jednostka nie udzieliła zgody lub ją wycofała. Wyjątkiem jest sytuacja, w której przetwarzanie danych osobowych jest niezbędne dla dostarczenia produktu lub świadczenia usługi. Nadto, osoba, której dane dotyczą ma prawo do wycofania udzielonej zgody, które zostało skorelowane z obowiązkiem administratora, polegającym na stworzeniu

[474] Art. 25 PIPL.
[475] Art. 23 PIPL.
[476] Art. 26 PIPL.
[477] Art. 28 PIPL.
[478] Art. 39 PIPL.
[479] Art. 23 PIPL.
[480] Art. 27 PIPL.

przystępnej procedurę obsługi takich żądań. Wycofanie zgody zasadniczo nie wpływa na ważność i skuteczność przetwarzania danych osobowych wykonanego na tej podstawie.

Na tle powyższego opisu zgody jako przesłanki legalizującej przetwarzanie danych osobowych można stwierdzić, że dopiero PIPL wprowadziło do chińskiego systemu prawnego standard w zakresie zgody porównywalny ze standardami RODO, ale nie identyczny. Najważniejszym odstępstwem jest uznawanie zgody za ostatecznej, możliwej do zastosowania podstawy prawnej przetwarzania danych osobowych, co pozostaje w oczywistej sprzeczności z podejściem europejskim. Podobnie można scharakteryzować zbyt częste wykorzystywanie zgody, do czego wprost zachęcają przepisy, a zwłaszcza CSL. Takie postępowanie coraz częściej spotyka się z negatywnymi komentarzami opinii publicznej, kwestionującej m.in. dobrowolność wyrażanych zgód[481]. Jednocześnie, w ocenie niektórych autorów wciąż aktualne pozostają zarzuty co do niejasności przepisów związanych ze zgodą, które rozciągają się również na PIPL[482].

3.2.1.2. Szczególne podstawy przetwarzania danych osobowych

PIPL poszerza katalog możliwych do wykorzystania podstaw przetwarzania danych osobowych. Zdaniem G. Greenleaf'a katalog, o którym mowa w PIPL to wyraz europeizacji chińskich przepisów[483].

Katalog szczególnych podstaw przetwarzania danych osobowych, o których mowa w art. 13 PIPL otwiera podstawa związana z zawarciem lub wykonaniem umowy, której stroną jest osoba, której dane dotyczą. Przepis jednoznacznie wymaga, aby przetwarzanie danych osobowych było niezbędne dla zawarcia umowy lub jej wykonania, co można postrzegać jako jedną z emanacji zasady minimalizacji. Drugą szczególną podstawą jest wypełnienie obowiązków nałożonych przez prawo. Sposób sformułowania przepisu pozwala stwierdzić, że chodzi o wszelkie sytuacje, w których przepisy prawa zobowiązują do przetwarzania danych osobowych. Wyjątkowo potraktowano jedynie przepisy dotyczące prawa pracy. PIPL wprost wskazuje na sytuację, w której przetwarzanie danych osobowych jest konieczne dla zarządzania zasobami ludzkimi zgodnie z przepisami prawa pracy oraz postanowieniami zbiorowych porozumień. Nadto, art. 13 PIPL zawiera także ogólne odwołanie do tych wszystkich szczególnych sytuacji, które są traktowane przez przepisy prawa lub przepisy administracyjne jako

[481] Y.-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 10.
[482] C. You: *Half a Loaf*…, s. 12.
[483] G. Greenleaf: *China Issues a*…, s. 7.

podstawy przetwarzania danych osobowych. Trzecia szczególna podstawa uprawnia do przetwarzania danych w związku z zaistnieniem pewnych wydarzeń. W przepisie mowa o konieczności przetwarzania danych w reakcji na nagłe wydarzenia dotyczące zdrowia publicznego lub w związku z ochroną życia, zdrowia lub bezpieczeństwa dobytku osoby fizycznej w sytuacji zagrożenia. Czwarta szczególna podstawa jest związana z szeroko pojętym dostępem do informacji. Uprawnia do przetwarzanie uzasadnionego zakresu danych, które są konieczne do dostarczania informacji, sprawowania nadzoru przez opinię publiczną lub wykonywania innych, podobnych działań podejmowanych dla interesu ogółu. Piąta podstawa szczególna wiąże się z danymi udostępnionymi przez osobę, której dane dotyczą. Co do zasady, fakt upublicznienia danych staje się podstawą do ich przetwarzania w uzasadnionym zakresie. O upublicznieniu danych będzie mowa, jeśli dokona tego osoba, której dane dotyczą lub też jej dane zostaną legalnie upublicznione w inny sposób.

Porównując katalog podstaw przetwarzania danych osobowych zawarty w PIPL i w RODO, można dostrzec, że oba katalogi różnią się. Przede wszystkim, w PIPL zabrakło podstawy przetwarzania danych osobowych do celów wynikających z prawnie uzasadnionego interesu administratora [484] . Zamiast tego stosunkowo szczegółowo opisano podstawy prawne związane z realizacją obowiązków nałożonych przez przepisy prawa, czy realizacją zadań publicznych, w tym w razie zaistnienia nagłych zdarzeń. Co więcej, PIPL uznaje upublicznienie danych osobowych za samoistną podstawę przetwarzania danych osobowych przez inne podmioty, co także nie odpowiada podejściu, które wynika z RODO.

3.2.2. Podstawy przetwarzania danych wrażliwych

Wyjątkowy charakter danych wrażliwych powoduje, że tak, jak w przypadku RODO, tak i w przepisach PIPL, dane wrażliwe zyskały odrębną podstawę ich przetwarzania, z tym, że zgodnie z art. 29 PIPL może być nią wyłącznie odrębna zgoda jednostki. Przyjęte rozwiązanie znacznie różni się od podejścia do przetwarzania danych wrażliwych w RODO, którego katalog możliwych do wykorzystania podstaw przetwarzania jest znacznie szerszy[485]. Ponadto, wykorzystanie zgody jako wyłącznej podstawy przetwarzania danych wrażliwych budzi wątpliwości co do możliwość jej faktycznego nadużywania, czy wręcz pozbawienia jednostki prawa do podjęcia dobrowolnej i świadomej decyzji.

[484] G. Greenleaf: *China's Completed Personal*…, s. 1.
[485] C. Wang, J. Zhang, N. Lassi i in.: *Privacy Protection in*…, s. 9.

Wymagania formalne zgody pozostały takie same, jak w przypadku zgody pozyskiwanej na przetwarzanie zwykłych danych. Nadal pozyskanie zgody w formie pisemnej jest niezbędne tylko wtedy, gdy przepisy szczególne na to wskazują. Natomiast przetwarzając dane wrażliwe osób poniżej 14 roku życia administrator, zgodnie z art. 31 ust. 1 PIPL, jest zobowiązany do pozyskania zgody rodzica lub prawnego opiekuna małoletniego. Nadto, art. 31 ust. 2 PIPL wymaga, aby przetwarzanie danych wrażliwych małoletnich poniżej 14 roku życia było regulowane odrębnymi zasadami, które ma w tym celu stworzyć administrator.

W porównaniu z przepisami RODO, podstawy przetwarzania danych wrażliwych w przepisach chińskiego prawa ochrony danych osobowych są znacznie ograniczone. Ponownie, zarzut nadmiernego posługiwania się zgodą jako przesłanką przetwarzania danych osobowych w Chinach pozostaje aktualny.

3.2.3. Przetwarzanie danych przez organy państwa

Jak już była o tym mowa, zastosowanie przepisów poszczególnych ustaw składających się na prawną ochronę danych osobowych w Chinach w stosunku do organów państwa budzi uzasadnione wątpliwości. Niemniej jednak, art. 33 PIPL został tak sformułowany, że rozszerza zakres zastosowania przepisów PIPL na organy państwa. Przywołany przepis oznacza, że chociażby formalnie, obowiązki związane z przetwarzaniem danych osobowych, o których mowa w PIPL dotyczą także organów państwowych, a na podstawie art. 37 PIPL także podmiotów uprawnionych do wykonywania zadań publicznych. Tak śmiała teza nie spotyka się jednak z oczekiwanym entuzjazmem doktryny. O ile niektórzy autorzy uznają stosowanie PIPL w stosunku do organów państwa za oczywistość[486], o tyle częściej można spotkać się twierdzeniem o możliwości zastosowania tylko niektórych obowiązków [487], czy odczytywania zastosowania PIPL jako konieczności przestrzegania zasady minimalizmu, którą w przypadku państwa wyznaczają wykonywania zadania i obowiązki publiczne[488]. Mając na uwadze całościowe podejście przepisów prawa chińskiego do organów państwa, w tym także w związku z dostępem do danych (o czym będzie mowa w dalszej części tego rozdziału), ostrożnościowe podejście do możliwości stosowania przepisów PIPL w stosunku do organów państwa jest zasadne. To z kolei oznacza, że po

[486] Podobnie: H. Xing: *Government Data Sharing*…, s. 72.
[487] Por. Y. Yin: *Conflict and Balance Between Private Information Protection and Public Interests Against the Background of Normalization of Epidemic Prevention and Control.* „Hebei Law Science", 2023, nr 41 - autor wskazuje na obowiazki związane z bezpieczeństwem danych, w tym ich poufnością.
[488] Q. Zhou: *Whose Data Is*…, s. 90.

raz kolejny, przepisy prawa chińskiego różnią się w porównaniu ze standardami wynikającymi z RODO.

3.3. Zasada przejrzystości

Przejrzystość, określana też jako transparentność przetwarzania danych osobowych, można postrzegać jako jedną z gwarancji zgodnego z prawem postępowania z danymi osobowymi. W chińskich przepisach ochrony danych osobowych, o zasadzie przejrzystości wspomina CSL i PIPL.

CSL wprowadza wymóg publikacji informacji na temat zasad pozyskiwania danych oraz ich przetwarzania. Przekazywane informacje powinny także wskazywać cel przetwarzania danych oraz powiązany z nim zakres danych oraz sposoby ich przetwarzania. Nadto jako przejaw zasady przejrzystości można odczytywać obowiązki związane zaistnieniem wycieku, zniszczenia lub utraty danych. Wówczas operator sieci powinien poinformować osoby, których dane dotyczą oraz odpowiednie organy o zdarzeniu. W takim ujęciu, przepisy CSL wprowadzają swego rodzaju postać obowiązku informacyjnego.

W porównaniu z CSL, przepisy związane z zasadą w przejrzystości w PIPL są bardziej rozbudowane. Artykuł 17 PIPL nakłada na administratora obowiązek odpowiedniego poinformowania podmiotu danych zanim dojdzie do przetwarzania jego danych. W tym celu, administrator, w jasny i przystępny sposób, ma przedstawić prawdziwe i wyczerpujące informacje na temat przetwarzania danych. Katalog informacji, które należy przekazać podmiotom danych obejmuje nazwę i dane kontaktowe administratora, kategorie przetwarzanych danych, cel i metody przetwarzania danych, wskazanie okresu retencji danych, sposoby, za pomocą których jednostka może wykonywać prawa przyznane jej przez PIPL. Wskazany katalog stanowi minimalną treść klauzuli informacyjnej, która może być poszerzona o dodatkowe informacje wynikające z przepisów szczególnych lub przepisów administracyjnych. Artykuł 17 zdanie trzecie PIPL umożliwia administratorowi zawarcie klauzuli informacyjnej w polityce ochrony danych osobowych[489]. Aby móc skorzystać z tej ścieżki spełnienia obowiązku informacyjnego, polityka musi być upubliczniona w taki sposób, który umożliwi podmiotom danych zapoznanie się z jej treścią oraz zachowanie (pobranie) jej egzemplarza.

[489] Art. 17 zdanie trzecie PIPL posługuje się terminem „reguły przetwarzania danych osobowych", jednak nic nie stoi na przeszkodzie, aby przyjąć, że chodzi o politykę ochrony danych osobowych lub inny podobny dokument.

Jeśli dojdzie do jakichkolwiek zmian w zakresie informacji zawartych w klauzuli informacyjnej konieczne jest powiadomienie osoby, której dane dotyczą. Jako szczególny przypadek zmian potraktowano zmiany podmiotowe po stronie administratora danych. Zgodnie z art. 22 PIPL, w razie fuzji, przejęcia, połączenia, rozwiązania, ogłoszenia upadłości lub innych podobnych zdarzeń zmieniających sytuację administratora, dotychczasowy administrator powinien przekazać dane nowemu administratorowi, jednocześnie informując osobę, której dane dotyczą, o nazwie i danych kontaktowych nowego administratora. Co do zasady, nowy administrator staje się podmiotem tych samych obowiązków, które spoczywały na dotychczasowym administratorze. Tym samym, jeśli nowy administrator zmieni cel lub metody przetwarzania danych osobowych, to zgodnie z art. 22 PIPL jest zobowiązany do poinformowania podmiotu danych o zaistniałych zmianach.

Opisanej powyżej zmiany podmiotowej nie należy utożsamiać z sytuacją, w której dochodzi do udostępnienia danych innemu administratorowi. W takiej sytuacji aktualizuje się odrębny obowiązek informacyjny, o którym mowa w art. 23 PIPL. Osobę, której dane dotyczą należy poinformować o nazwie i danych kontaktowych administratora-odbiorcy danych oraz o kategorii danych, celu i sposobach ich przetwarzania.

PIPL przewiduje także odstępstwa od realizacji ogólnego obowiązku informacyjnego, zgodnie z art. 18. Najdalej idące odstępstwo to rezygnacja z wypełnienia obowiązku informacyjnego. Do takiej sytuacji dojdzie, jeśli przepisy prawa lub przepisy administracyjne nakazują zachowanie poufności przetwarzania danych osobowych lub uznają spełnienie obowiązku informacyjnego za zbędne.

Kolejne odstępstwo od ogólnego obowiązku informacyjnego jest związane z sytuacjami, w których z uwagi na potrzebę ratowania życia lub zdrowia ludzkiego lub bezpieczeństwa ich mienia, wypełnienie obowiązku informacyjnego w odpowiednim czasie jest niemożliwe. Wówczas, administrator może niezwłocznie rozpocząć przetwarzanie danych, natomiast po ustaniu stanu zagrożenia dla wymienionych wartości, powinien dopełnić obowiązku informacyjnego.

Dodatkowo, przepisy PIPL regulujące przetwarzanie danych wrażliwych nakazują poszerzenie katalogu informacji przekazywanych jednostce. Zgodnie z art. 30 PIPL, podmiot danych powinna dodatkowo uzyskać informacje, dlaczego przetwarzanie jego danych wrażliwych jest konieczne oraz w jaki sposób to przetwarzanie wpływa na jej

prawa i wolności. Co istotnie, obowiązek przekazania dodatkowych informacji może być wyłączone przez inne przepisy PIPL.

Szczególnym przejawem zasady przejrzystości są również przepisy PIPL poświęcone automatycznemu podejmowaniu decyzji. W myśl art. 24 zdanie pierwsze PIPL każdy proces decyzyjny powinien być transparentny, natomiast rezultat automatycznego procesu podejmowania decyzji ma odpowiadać cechom sprawiedliwości i uczciwości. Za zakazane postępowanie uznano nieuzasadnione, zróżnicowane traktowanie osób znajdujących się w ramach stosunków handlowych, w tym zwłaszcza w zakresie różnicowania cen. Art. 24 zdanie trzecie PIPL wprowadza rozróżnienie na zwykłe automatyczne podejmowanie decyzji i jego kwalifikowaną postać. O kwalifikowanej postaci automatycznego podejmowania decyzji będzie mowa, gdy podjęta decyzja wywiera znaczny wpływ na prawa i wolności jednostki. Wówczas, jednostka może domagać się dodatkowych wyjaśnień, a także ma prawo do sprzeciwu wobec podejmowania decyzji wyłącznie za pomocą automatycznego procesu. Nadto, art. 24 zdanie drugie PIPL wprowadza dodatkowe obowiązki dla podmiotów dostarczających wiadomości lub reklamujących sprzedaż z wykorzystaniem metod *push* powiązanych z automatycznym podejmowaniem decyzji. Dodatkowe obowiązki polegają na wprowadzeniu do programu funkcji, w ramach której treść nie będzie kierowana do jednostek o konkretnych cechach lub na umożliwieniu jednostce sprzeciwienia się wobec kierowania do niej takich treści.

Analizując przedstawiony powyżej opis zasady przejrzystości w przepisach chińskiego prawa ochrony danych osobowych można odnieść wrażenie o znacznym zbliżeniu chińskiej ochrony danych osobowych do standardów europejskich. W szczególności, zdaniem G. Greenleafa przepisy dotyczące automatycznego podejmowania zasadniczo nie odbiegają od rozwiązań przyjętych w RODO [490]. Niestety, praktyka postępowania administratorów danych osobowych przedstawia mniej optymistyczny obraz. W ramach badań nad zawartością stron internetowych oferujących sprzedaż domowych testów DNA, które przeprowadzono po wejściu w życie CSL autorzy wykazali, że 46 spośród 83 weryfikowanych stron w ogóle nie zawierało odnośnika (linku) do polityki prywatności lub innego, podobnego dokumentu [491]. Jednocześnie, jakość informacji przekazywanych w politykach prywatności była wątpliwa. Mimo oczywistego związku przetwarzania danych osobowych zawartych

[490] G. Greenleaf: *China's Completed Personal*…, s. 2.
[491] L. Du, M. Wang: *Genetic Privacy and Data Protection: A Review of Chinese Direct-to-Consumer Genetic Test Services*. „Frontiers of Law in China", 2020, nr 11, s. 4.

w testach DNA z danymi wrażliwymi, tylko 29 polityk prywatności zawierało rozróżnienie na dane zwykłe i dane wrażliwe[492]. Nadto, tylko na czterech stronach internetowych znalazło się jednoznaczne określenie przepisów, których przestrzega administrator, przy czym tylko dwa razy wskazano na CSL[493]. Problem dotyczy także tzw. popularnych serwisów internetowych. Wciąż nie wszystkie serwisy dokonały publikacji polityk prywatności, a nadto blisko ¾ serwisów nie postępuje zgodnie z deklarowanymi w nich zasadami, w tym zwłaszcza w odniesieniu do oświadczeń w sprawie przechowywania danych oraz ich przekazywania innym podmiotom[494]. To z kolei skutkuje naruszeniami danych osobowych, w tym niechcianym profilowaniem jednostek[495]. Nie dziwi więc fakt, że w ocenie chińskiego społeczeństwa wśród zagrożeń dla prywatności znalazły się właśnie brak informacji na temat przetwarzania danych osobowych oraz powiązany z tym brak odpowiedniej polityki prywatności[496]. Oczywistą komplikacją rzeczywistej realizacji zasady przejrzystości są także zasady dostępu organów państwa do danych osobowych, o czym będzie mowa w dalszej części tego rozdziału.

Tym samym, podobieństwo zasady przejrzystości w chińskich przepisach ochrony danych osobowych do standardu europejskiego ogranicza się wyłącznie do podobieństwa formalnego.

3.4. Zasada ograniczenia celu przetwarzania oraz minimalizacja

Zasady celowości i minimalizacji są na tyle blisko powiązane, że ich wspólny opis jest uzasadniony. Obie zasady znajdują umocowanie w przepisach CSL, c.k.c., PIPL, a także DSL. Ponownie, DSL w art. 32 zawiera ogólny nakaz, aby podmioty przetwarzające dane stosowały cele oraz zakresy pozyskiwanych danych, jeśli te zostały określone przez przepisy prawa, w tym regulacje administracyjne. Więcej szczegółów zawarto w pozostałych ustawach chińskiego prawa ochrony danych osobowych.

W ujęciu kodeksowym zasada celowości wymaga wskazania konkretnego celu, dla którego dane są pozyskiwane i przetwarzane. Jednocześnie, przestrzegając zasady

---

[492] Ibid, s. 5.
[493] Ibid, s. 6.
[494] X. Lin, H. Liu, Z. Li i in.: *Privacy Protection of China's Top Websites: A Multi-Layer Privacy Measurement via Network Behaviours and Privacy Policies*. „Computers & Security", 2022, nr 114, s. 18.
[495] Y.-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 10 - autorzy powołują przykład faktycznego przekazania danych osobowych jednego z autorów na rzecz podmiotu trzeciego, bez jego wiedzy lub zgody. Po skorzystaniu z głośnia elektronicznego wyposażonego w asystenta w celu wyszukania nieruchomości na sprzedaż w jego okolicy, po kilku godzinach od wyszukania do jednego z autorów zadzwonił agent nieruchomości.
[496] X. Chen, Y. Zhang: *The Construct of Information Privacy Concerns in the Chinese Cultural Setting.* „Nankai Business Review International", 2021, nr 12, s. 47–48.

minimalizacji administrator ma ograniczyć przetwarzanie tylko do danych koniecznych, a zarazem powinien powstrzymać się od zbędnych czynności przetwarzania. Konstrukcja zasady celowości w c.k.c. jest o tyle wyjątkowa, że skutkiem jej przestrzegania może być wyłączenie odpowiedzialności cywilnej administratora, o której była mowa. Niemniej jednak, odpowiedzialność zostanie wyłączona tylko w takim zakresie przetwarzania, który został uzgodniony z osobą, której dane dotyczą.

Przepisy CSL prezentują standardowy opis zasad celowości i minimalizacji. Określenie celu przetwarzania danych osobowych jest obowiązkiem administratora. Pozyskiwane dane muszą być ściśle związane z jego konkretnymi, legalnymi potrzebami. Zgodnie z art. 41 CSL zakazane jest pozyskiwanie danych, które nie są niezbędne dla świadczenia usług zapewnianych przez administratora. Jednocześnie, cel to determinanta zakresu pozyskiwanych danych, a także sposobów ich przetwarzania. W ocenie G. Greenleafa, tak ogólne i nieostre sformułowania wykorzystane do opisu zasady minimalizacji powodują, że jej praktyczna skuteczność jest wątpliwa[497]. Innymi słowy, można mówić o łagodniejszej wersji minimalizacji[498].

Dotychczasowy schemat zasad celowości i minimalizacji powtarza również PIPL, gdzie celowość to oznacza istnienie konkretnego i uzasadnionego celu przetwarzania danych, zaś cel ma bezpośrednio determinować czynności przetwarzania, które mają być podjęte. PIPL wprowadza jednak dodatkowe obowiązki związane z przestrzeganiem zasady celowości. Zasadniczo każda zmiana celu oznacza konieczność poinformowania podmiotu danych, jak również, pozyskania jego zgody na przetwarzanie danych w zmienionym celu[499]. Również zasada minimalizacji została dookreślona za pomocą trzech podstawowych wymagań. Po pierwsze, spośród dostępnych czynności przetwarzania danych, administrator ma wybrać takie metody, których ingerencja w prawa i wolności osoby, której dane dotyczą będzie najmniejsza. Po drugie, zasada minimalizacji pozostaje w związku z zasadą celowości i nakazuje, aby przetwarzano wyłącznie takie dane, które są niezbędne dla realizacji celu przetwarzania. Po trzecie, z zasady minimalizacji wynika zakaz pozyskiwania danych nadmiarowych.

Za dodatkowy przejaw realizacji zasad celowości i minimalizacji można uznać wynikając z PIPL standard retencji danych osobowych, o którym mowa w art. 19. Brak konkretnego

[497] G. Greenleaf: *China Issues a*…, s. 8.
[498] G. Greenleaf, S. Livingston: *China's New Cybersecurity*…, s. 4.
[499] Por. art. 23 PIPL. Brak obowiązku pozyskania zgody w sytuacjach zmian podmiotowych po stronie administratora, o których mowa w art. 22 PIPL, należy traktować jako wyjątek od ogólnie przyjętej zasady zawartej w art. 23 PIPL. Art. 23 PIPL obejmuje wszelkie sytuacje udostępnienia danych innemu administratorowi, zaś art. 22 PIPL ogranicza się do ściśle wymienionych przypadków.

okresu retencji danych zastąpioną ogólną dyrektywą nakazująca ograniczenie czasu przetwarzania danych osobowych do najkrótszego możliwego okresu, niezbędnego dla realizacji celu przetwarzania danych osobowych.

Zasady celowości i minimalizacji są bliskie europejskiemu wzorcowi. Co istotne, to w zasadzie minimalizacji w PIPL można dopatrywać się emanacji podejścia opartego na ryzyku, w tym sensie, że to właśnie zasada minimalizacji zapewnia, aby metody, którymi posłuży się administrator będą ingerowały w prawa i wolności jednostki w najmniejszym stopniu. Zastanawiając się nad motywami, którymi kierował się ustawodawca niewątpliwie zbliżając chińskie przepisy ochrony danych osobowych, a zwłaszcza PIPL do standardu wynikającego z RODO, można wskazać na zmianę jaka zaszła w społeczeństwie chińskim. Obecnie, coraz częściej chińscy użytkownicy zwracają uwagę na poziom ochrony danych osobowych z jakim wiąże się korzystanie przez nich z danej usługi[500], a wręcz oczekują takiej ochrony[501], nawet jeśli będzie się to wiązało z koniecznością zapłaty za korzystanie z usługi[502]. Jednocześnie, przykład analizy stron internetowych oferujących udzielanie pożyczek osobom fizycznym potwierdza, że ograniczenie przetwarzania danych do danych niezbędnych jest możliwe[503]. Zatrważający jest jednak fakt, że takie oczekiwania nie adresowane do organów państw przewarzających dane osobowe[504].

3.5. Zasada prawidłowości danych

Dbałość o jakość przetwarzanych danych osobowych, która stanowi sens zasady prawidłowości danych osobowych, wynika wyłącznie z przepisów PIPL. W CSL odnalezienie zasady prawidłowości danych wymaga zastosowania odpowiednich zabiegów interpretacyjnych. G. Greenleaf i S. Livingston sugerują, że w praktyce, namiastką zasady prawidłowości danych będzie wykorzystanie przez jednostkę przysługujących jej praw do żądania poprawienia danych lub ich usunięcia[505]. Nie jest to jednak zasada prawidłowości danych, skoro *de facto* będzie stanowiła wyłączne uprawnienie jednostki, przy jednoczesnym braku obowiązki aktywnego, prewencyjnego

[500] H. Roberts: *Informational Privacy with Chinese Characteristics*. W: *Digital Ethics Lab Yearbook 2021.* Red. J. Mökander, M. Ziosi, Springer, Cham 2022, s. 5–6; B. Zhao, Y. Feng: *Mapping the Development*…, s.10; por. także: B. Hu, Y-L. Liu, W. Yan: *Should I Scan*….
[501] Y.-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 11.
[502] Y. Tang, L. Wang: *How Chinese Web Users Value Their Personal Information: An Empirical Study on WeChat Users*. „Psychology Research and Behavior Management", 2021, nr 14, s. 996.
[503] Q. Zhou: *Whose Data Is*…, s. 83 - autor wyjaśnia, że w przypadku takich stron internetowych, zakres pozyskiwanych danych zasdniczo obejmował dane niezbędne dla świadczenia usługi, zaś dane nadmiarowe, jak np. dane biometryczne czy dane o lokalizacji, były rzadziej pozyskiwane.
[504] B. Zhao, F. Feng: *Mapping the development*…, s. 14; H. Roberts: *Informational Privacy with*…, s. 5–6.
[505] G. Greenleaf, S. Livingston: *China's New Cybersecurity*…, s. 5.

działania administratora danych osobowych zanim takie żądanie zostanie do niego skierowane.

O zasadzie prawidłowości danych, odpowiadającej rozumieniu, które wynika z RODO wspomina jednak art. 8 PIPL. Stanowi on źródło obowiązku administratora, który ma polegać na dbałości o jakość danych, w tym ich kompletność i aktualności. Nadrzędnym celem ma być uchronienie osoby, której dotyczą przed niekorzystnymi skutkami dla jej praw lub wolności, wynikających z przetwarzania danych niekompletnych czy nieaktualnych.

3.6. Zasada integralności i poufności danych

Integralność i poufność danych służą zarówno realizacji zasady prawidłowości, jak również wiążą się z zasadą bezpieczeństwa danych O obu tych aspektach można mówić w przepisach chińskiego prawa ochrony danych osobowych, przy czym to właśnie zapewnienie bezpieczeństwa danych będzie skutkowało dochowaniem ich integralności i poufności.

DSL zawiera ogólne wytyczne, które odzwierciedla podejście oparte na ryzyku. Art. 29 DSL nakazuje, aby procesowi przetwarzania każdych danych towarzyszył wzmożony monitoring ryzyka, sprzężony z odpowiednimi środkami zaradczymi pozwalającymi na natychmiastowa mitygację zidentyfikowanych ryzyk dla bezpieczeństwa danych. Jednocześnie system zarządzania ryzykiem powinien przewidywać odpowiednie postępowanie na wypadek naruszenia bezpieczeństwa danych, m.in. wykonanie obowiązków notyfikacyjnych w stosunku do odpowiednich władz oraz podmiotów danych. DSL przewiduje również kwalifikowaną postać zarządzania ryzykiem, dedykowaną ważnym danym.

O poufności danych wyraźnie stanowi art. 1038 zdanie pierwsze c.k.c., zakazując administratorowi danych naruszenia ich poufności W oczywisty sposób wiąże się to jednak z koniecznością zapewnienia bezpieczeństwa danych osobowych. Zabronionym jest jakiekolwiek rozpowszechnianie lub ujawnianie innym osobom danych przetwarzanych lub przechowywanych przez administratora. Z zakazu wyłączone są tylko takie dane, które po przetworzeniu nie pozwalają na identyfikację osoby fizycznej, a cechy identyfikowalności nie da się przywrócić. Nadto, sama osoba, której dane dotyczą może wyrazić zgodę na rozpowszechnienie lub ujawnienie jej danych.

W CSL zagadnienie bezpieczeństwa danych zyskało rozbudowaną regulację. Artykuł 21 CSL, który wymaga od operatorów sieci, aby realizowali swoje obowiązki w zakresie bezpieczeństwa sieci zgodnie z przyjętym na szczeblu krajowym

wielopoziomowym systemem ochrony bezpieczeństwa sieci [506]. Ogólna zasada bezpieczeństwa zostaje poddana modyfikacjom w odniesieniu do operatorów sieci związanych z infrastrukturą krytyczną, w tym krytyczną infrastrukturą informatyczną[507] oraz z przetwarzaniem danych osobowych, dla którego art. 42 CSL określa konkretne obowiązki operatora sieci (administratora) związane z bezpieczeństwem danych [508]. Operator sieci (administrator) jest zobowiązany do wdrożenia odpowiednich zabezpieczeń, w tym zabezpieczeń technicznych w celu zapewnienia bezpieczeństwa danych, które przetwarza. W szczególności, zabezpieczenia mają chronić przed wyciekiem, zniszczeniem lub utratą danych. Poza działaniami prewencyjnymi, art. 42 zdanie drugie CSL wskazuje postępowanie jakie należy podjąć w razie zaistnienia zdarzenia skutkującego wyciekiem, zniszczeniem lub utratą danych[509].

Artykuł 9 PIPL jednoznacznie wskazuje na administratora jako na podmiot odpowiedzialny za przetwarzanie danych osobowych. Oznacza to, że jest obowiązany do wdrożenia odpowiednich środków, które zapewnią bezpieczeństwo przetwarzanym danym osobowym. Bezpieczeństwo danych PIPL wiąże się za sprawą art. 51 z ich uchronieniem przed wyciekiem, nieuprawnionymi zmianami czy utratą.

Rozwiązania w zakresie zapewnienia bezpieczeństwa danych, w tym ich integralności i poufności przyjęte w DSL, c.k.c., CSL i PIPL są zbieżne. Potwierdzają jak istotne znaczenie ma dla chińskiego ustawodawcy przede wszystkim bezpieczeństwo

---

[506] MLPS.

[507] Zgodnie z art. 31 CSL infrastrukturę krytyczną stanowią publiczne usługi komunikacyjno-informacyjne, szeroko rozumiane: przemysł energetyczny, zaopatrzenie w wodę, działalność związana z finansami, działalność służby cywilnej, *e-government*. Nadto, za krytyczną infrastrukturę informatyczną (informacyjną) mogą być uznane takie przedsięwzięcia, dla których zniszczenie, utrata funkcjonalności lub wyciek danych mogą poważnie zagrozić bezpieczeństwu narodowemu, dobrobytowi narodowemu, źródłom utrzymania jednostek lub interesowi publicznemu.
Katalog obowiązków operatorów krytycznej infrastruktury informatycznej, w szczególności w zakresie zabezpieczeń, na podstawie art. 31 CSL został dookreślony w formie rozporządzenia, które weszło w życie 1 września 2021 r. - Zhonghua renmin gongheguo guowuyuan ling (中华人民共和国国务院令) [Rozporządzenie Rady Państwa Chińskiej Republiki Ludowej]. 30.07.2021. http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?mc_cid=da5881cf31&mc_eid=a268621911 [dostęp: 3.06.2024].
Jednocześnie, art. 31 CSL zdanie drugie nakłada na państwo obowiązek zachęcania tych wszystkich operatorów sieci, którzy nie kwalifikują się jako operatorzy sieci infrastruktury krytycznej do dobrowolnego stosowania przepisów i systemu ochrony infrastruktury krytycznej.

[508] Z bezpieczeństwem danych osobowych można wiązać także obowiązki, o których mowa w art. 46 – 48 CSL, które bezpośrednio dotyczą takich zagadnień jak odpowiedzialność za strony internetowe i ich treść, dbałość o jakość informacji publikowanych i przesyłanych przez użytkowników sieci (w tym postępowanie z informacjami, których publikacja lub przesył są niezgodne z prawem), dbałość o jakość oprogramowania (w tym zakaz umieszczania w aplikacji lub oprogramowaniu informacji, których publikacja lub przesył są niezgodne z prawem).

[509] Takie same działania należy podjąć, jeśli zaistnienie zdarzenia mogło mieć miejsce. Może przy tym chodzić o te sytuacje, gdy brak jest całkowitej pewności co do wystąpienia zdarzenia, ale zarazem stopień prawdopodobieństwa jego wystąpienia jest na tyle wysoki, że konieczna jest reakcja.

sieci i danych, w tym danych osobowych. Mimo że celem przepisów DSL, CSL i PIPL niekoniecznie jest ochrona jednostki przed zagrożeniami związanymi z naruszeniami danych osobowych, oczekiwany, wysoki poziom bezpieczeństwa można rozpatrywać jako korzystny dla jednostki skutek uboczny działań władz chińskich. Bez wątpienia, sposób sformułowania odnośnych przepisów c.k.c. jest bliższy podejściu europejskiemu. Niemniej jednak, całkowity obraz jaki wyłania się z przepisów chińskiego prawa ochrony danych osobowych potwierdza, że to właśnie podejście do jednostki w ramach zapewnienia bezpieczeństwa danych odróżnia chińskie przepisy ochrony danych osobowych od RODO.

3.7. Zasada rozliczalności

Zasada rozliczalności nie została sformułowana w chińskich przepisach ochrony danych w sposób jednoznaczny. Zdaniem G. Greenleaf'a, w przypadku PIPL, interpretacja art. 51, 53 i 54 pozwala osiągnąć ten sam efekt, jak gdyby zasadę rozliczalności implementowano jak w RODO[510]. Nadto, o swego rodzaju postaci zasady rozliczalności można także mówić jako o skutku przestrzegania pozostałych zasady wynikających z PIPL, a w szczególności zasady przejrzystości. Pośrednio, na taki kierunek interpretacyjny wskazuje art. 7 PIPL, który obliguje administratora do ujawnienia reguł, jakimi kieruje się przetwarzając dane osobowe, a także celu przetwarzania, zakresu danych i metod przetwarzania. Jednocześnie, w podobny sposób o zasadzie rozliczalności stanowi c.k.c., dla którego rozliczalność sprowadza się do konieczności wskazania celu przetwarzania danych, zakresu oraz sposobów przetwarzania danych. Wciąż, tak rozumiana rozliczalność będzie wiązała się z wykazaniem przestrzegania tylko części zasad i obowiązków ochrony danych osobowych, co nie odpowiada modelowi wynikającemu z RODO.

3.8. Zasada transferów danych osobowych

O zasadzie transferów danych osobowych wspominają przepisy CSL, DSL i PIPL. Tak jak dotychczas, DSL zawiera ogólne wymagania, nakazując, za pośrednictwem art. 31 DSL, stosowanie przepisów o transferach zlokalizowanych w CSL[511]. Mimo takiej

[510] G. Greenleaf: *China Issues a*…, s. 10.

[511] Art. 31 DSL wyróżnia dwie sytuacje: ważnych danych wytworzonych lub pozyskanych przez administratora będącego operatorem infrastruktury krytycznej działającego na terenie Chin oraz ważnych danych wytworzonych lub pozyskanych przez innych administratorów. W przypadku operatora infrastruktury krytycznej, art. 31 DSL odsyła wprost do przepisów CSL w zakresie oceny dopuszczalności transferów; w pozostałych przypadkach art. 31 DSL wyjaśnia, że odpowiednie wytyczne w zakresie oceny dopuszczalności transferów zostaną opracowane przez organy państwa.

konstrukcji przepisów DSL, zdaniem Chen i Sun to właśnie DSL wraz z PIPL przedstawiają całkowity obraz regulacji transferów danych w Chinach[512].

W CSL prawodawca chiński zdecydował się na umieszczenie art. 37, związanego z transferami danych, pośród przepisów rozdziału III sekcja 2 CSL, który jest dedykowany wymaganiom stawianym operatorom infrastruktury krytycznej. W związku z tym, obowiązki wynikające z art. 37 CSL, dotyczące ochrony danych osobowych, będą obejmowały wyłącznie administratorów, którym jednocześnie przypisuje się status operatora infrastruktury krytycznej. Jak już wspomniałem podczas omawiania definicji administratora danych, S. Livingston i G. Greenleaf podkreślają, że zakres pojęcia operator sieci jest bardzo nieostry. To z kolei oznacza, że wskazanie podmiotów, co do których te przepisy CSL, choćby potencjalnie, nie znajdą zastosowania jest utrudnione[513], co przy treści zasady transferów w CSL budzi uzasadnione obawy. Zasadniczo zabroniono jakichkolwiek transferów ważnych danych oraz danych osobowych poza terytorium Chin, jeśli te dane zostały pozyskane lub wytworzone w ramach czynności przetwarzania realizowanych w Chinach. Tym samym, takie dane powinny być przetwarzane wyłącznie na terytorium Chin. Rygorystyczny zakaz może być uchylony tylko, jeśli powodem transferu danych poza Chiny są realia rynku i prowadzonej działalności biznesowej a sam transfer danych jest rzeczywiście konieczny. Wówczas operator infrastruktury krytycznej (administrator) jest zobowiązany do postępowania zgodnie z wytycznymi opracowanymi przez organy państwa, której omawiam w dalszej części niniejszego rozdziału.

Restrykcyjne podejście do przekazywania danych osobowych poza terytorium Chin zostało wkomponowane także w PIPL. Artykuł 38 PIPL uprawnia administratora do przekazania danych osobowych poza terytorium Chin tylko gdy jest to niezbędne oraz została spełniona jedna z przesłanek dopuszczalności transferu. Przywołany przepis wymienia cztery takie przesłanki. Pierwszą z nich jest ocena bezpieczeństwa transferu, przeprowadzona przez właściwy państwowy departament cyberbezpieczeństwa i informatyzacji. Druga przesłanka to certyfikacja ochrony danych osobowych, przyznana przez podmiot uprawniony przez właściwy państwowy departament cyberbezpieczeństwa i informatyzacji. Trzecia przesłanka dopuszczalności transferu danych to zawarcie umowy, z wykorzystaniem wzoru stworzonego przez państwowy departament cyberbezpieczeństwa i informatyzacji, z podmiotem przyjmującym dane

[512] J. Chen, J. Sun: *Understanding the Chinese*…, s. 214.
[513] G. Greenleaf, S. Livingston: *PRC's New Data*…, s. 3–4.

w państwie trzecim, regulującej prawa i obowiązki obu stron. Czwarta przesłanka zawiera odesłanie do innych warunków, które wynikają z przepisów prawa, w tym przepisów administracyjnych i przepisów tworzonych przez państwowy departament cyberbezpieczeństwa i informatyzacji. Ponadto, zgodnie z art. 38 zdanie trzecie PIPL, jeśli umowa międzynarodowa, której stroną są Chiny zawiera własne przepisy zezwalające na transfer danych, to takie przepisy mogą znaleźć zastosowanie. Oprócz powyższych wymagań, art. 38 PIPL nakłada na administratora obowiązek wprowadzenia takich rozwiązań, które zagwarantują zgodność przetwarzania danych osobowych przez podmiot przyjmujący dane poza granicami Chin ze standardami wynikającymi z PIPL.

Przedstawienie zupełnego obrazu zasady transferów danych osobowych wymaga omówienia wytycznych CAC dotyczących transferów danych. Przywołany dokument jest związany ze wszystkimi przepisami chińskiego prawa ochrony danych osobowych, które regulują przekazywanie danych osobowych poza terytorium Chin[514], stanowiąc wykonanie delegacji ustawowej zawartej w CSL i PIPL. Zakres zastosowania wytycznych CAC dotyczących transferów danych obejmuje więc przekazywanie poza terytorium Chin ważnych danych lub danych osobowych, które zostały zebrane lub wytworzone w ramach operacji przetwarzania wykonywanych na terytorium chińskim.
Ocena bezpieczeństwa, o której mowa w wytycznych CAC dotyczących transferów danych to połączenie uprzedniej oceny ze stałym nadzorem, z jednoczesnym wykorzystaniem samooceny ryzyka i oceny bezpieczeństwa. Ocena bezpieczeństwa ma bowiem zapobiegać ryzykom związanym z bezpieczeństwem transferu oraz zapewniać zorganizowany, zgodny z prawem, wolny przepływ danych.
Wytyczne CAC dotyczące transferów danych zawierają własne przesłanki zastosowania. Administrator danych przekazujący dane poza terytorium Chin jest obowiązany do wystąpienia do krajowego organu cyberbezpieczeństwa i informatyzacji, za pośrednictwem lokalnych organów, o przeprowadzenie oceny bezpieczeństwa, jeśli zostanie spełniona jedna z przesłanek, o których mowa w art. 4 wytycznych CAC dotyczących transferów danych. Wśród okoliczności aktualizujących powyższy obowiązek wymienia się przekazywanie za granicę ważnych danych, przekazywanie za granicę danych osobowych przetwarzanych przez operatora krytycznej infrastruktury, administratora danych przetwarzającego dane ponad miliona ludzi, przekazywanie za granicę danych osobowych przez administratora danych, jeśli od 1 stycznia poprzedniego

[514] W szczególności z CSL, DSL i PIPL – por. art. 1 wytycznych CAC dotyczących transferów danych.

roku przekazał za granicę dane osobowe 100.000 ludzi lub dane wrażliwe 10.000 ludzi. Nadto, obowiązek przeprowadzenie oceny bezpieczeństwa może pojawić się w innych okolicznościach, które krajowy organy cyberbezpieczeństwa i informatyzacji uznaje za wymagające przeprowadzenia oceny.

Procedura przeprowadzenia oceny bezpieczeństwa składa się z kilku etapów. Samoocena ryzyka poprzedza wystąpienie przez administratora do właściwego organu o przeprowadzenie oceny bezpieczeństwa transferu. Artykuł 5 wytycznych CAC dotyczących transferów danych, w otwartym katalogu, określa minimalną treść samooceny ryzyka. Na treść samooceny ryzyka składa się ocena przetwarzania danych przez stronę przyjmującą dane oraz ocena czynności transferu danych w zakresie ogólnych zasad przetwarzania danych[515]. Samoocena ryzyka powinna zawierać także opis skali, rozmiarów, kategorii i stopnia wrażliwości przesyłanych danych; opis ryzyk dla bezpieczeństwa narodowego, interesu publicznego oraz praw i interesów osób, których dane dotyczą i organizacji, jakimi obarczony jest transfer danych; opis obowiązków strony przyjmującej dane, w tym z odniesieniem do możliwości zapewnienia bezpieczeństwa transferowanych danych poprzez odpowiednie zarządzanie i środki techniczne; opis różnych zidentyfikowanych ryzyk, które mogą pojawić się na etapie przekazywania danych i po ich przekazaniu, z jednoczesnym zapewnieniem, że transfer nie wpłynie na środki służące ochronie praw i interesów osób, których dane dotyczą. W samoocenie ryzyka należy uwzględnić również opis umowy lub innego wiążącego instrumentu prawnego, regulującego w pełni prawa i obowiązki w zakresie bezpieczeństwa danych, jeśli taka umowa lub instrument ma zostać zawarty ze stroną przyjmującą dane. Powyższy kształt samooceny ryzyka przypomina wynikającą z orzecznictwa TSUE ocenę w ramach dopuszczalności transferu danych[516].

W zakresie umowy lub innego instrumentu prawnego, zawieranego pomiędzy administratorem a stroną przyjmującą dane, art. 9 wytycznych CAC dotyczących transferów danych wyznacza ich minimalną treść. Oprócz podstawowych informacji na temat m.in. celu transferu, zakresu danych, wykorzystywanych sposobów przetwarzania, limitów w zakresie lokalizacji danych i czasu przetwarzania, postępowania jakie należy wdrożyć w sytuacji gdy upłynął czas przetwarzania danych lub zaistniało inne podobne zdarzenie, czy ograniczeń transferu danych do innego podmiotu, umowa lub inny

[515] Art. 5 pkt 1 wytycznych CAC dotyczących transferów danych tylko przykładowo wskazuje na legalność, konieczność, celowość, zakres czy metodę przetwarzania danych jako kryteria, które administrator ma wykorzystać.

[516] Zwaną również transfer impact assessment – TIA.

instrument prawny powinny określać środki zapewniające bezpieczeństwo danych na wypadek nieprzewidzianych zdarzeń, w tym zmiany w systemie prawnym lub systemie cyberbezpieczeństwa obowiązujących na terenie państwa trzeciego, w którym znajduje się podmiot przyjmujący dane, wpływającej na poziom bezpieczeństwa danych. W umowie lub innym instrumencie prawnym należy określić zasady odpowiedzialności za naruszenie wprowadzonych zasad ochrony danych, w tym odpowiednie środki naprawcze i procedury rozwiązywania sporów, a także określić zasady postępowania na wypadek materializacji ryzyka dla bezpieczeństwa danych, zapewniające jednostkom możliwość realizacji ich praw.

Właściwa ocena bezpieczeństwa, zgodnie z art. 8 wytycznych CAC dotyczących transferów danych, sprowadza się do oceny ryzyka dla bezpieczeństwa narodowego, interesu publicznego oraz praw i interesów osób, których dane dotyczą i organizacji z jakim wiąże się transfer danych. Co do zasady, treść oceny bezpieczeństwa odpowiada treści samooceny ryzyka przeprowadzanej przez administratora, a nadto zawiera m.in. opis systemu prawnego państwa, na terytorium którego znajduje się strona przyjmująca dane. Opis obejmuje wpływ tamtejszego prawodawstwa i poziomu cyberbezpieczeństwa na bezpieczeństwo danych, jak również opis odpowiedniości poziomu ochrony danych osobowych w tym państwie w zestawieniu z wymaganiami wynikającymi z prawa chińskiego. Wytyczne CAC dotyczących transferów danych regulują procedurę związaną z przeprowadzeniem oceny bezpieczeństwa, w tym wskazują terminy na przeprowadzenie oceny, organy właściwe do przeprowadzenia oceny, okres ważności pozytywnej oceny, jak również określają procedurę odwoławczą i przesłanki konieczności przeprowadzenia ponownej oceny.

Regulacja przekazywania danych osobowych do państw trzecich stanowi szczególny przedmiot zainteresowania ustawodawcy chińskiego. Doktryna uznaje przepisy poświęcone transferom danych osobowych za emanację ochrony bezpieczeństwa narodowego, a więc wartości, która legła u podstaw wdrożenia przepisów dotyczących bezpieczeństwa sieci i danych, w tym danych osobowych[517]. J. Liu uważa, że ochrona bezpieczeństwa narodowego jest zasadniczym motorem napędowym strategii chińskiej dotyczącej sieci (i kontroli nad nią), który wyprzedza potrzebę cyberbezpieczeństwa, ochrony danych jako takich, a także ochronę danych osobowych[518]. W konsekwencji, J. Chen i S. Sun wskazują na przenikanie się przepisów

[517] C. Wang, J. Zhang, N. Lassi i in.: *Privacy Protection in*…, s. 13.
[518] J. Liu: *China's Data Localization*…, s. 84, 86, 90.

DSL i NSL[519]. Jednocześnie, I. Calzada uznaje PIPL za całkowicie powiązane z koncepcją suwerenności sieci, której zasięg za pośrednictwem PIPL zostaje rozszerzony[520]. Teza I. Calzady koresponduje ze stanowiskiem S. Livingstona i G. Greenleafa, dla których przepisy prawa chińskiego to połączenie ochrony jednostki, wartości typowej dla podejścia europejskiego, z koncepcją suwerenności sieci[521]. W tym względzie, ograniczenia w transferze danych osobowych wynikające z przepisów chińskiego prawa ochrony danych osobowych realizują funkcję prewencyjną, o której wspomina G. Zheng[522]. W pewnym stopniu zbliżają się więc do przepisów RODO, ale nie są podobne. Jak wskazuje J. Liu, ograniczenia transferów danych pozwalają na ochronę nie tylko przed niewłaściwym postępowaniem z danymi przez podmioty prywatne, ale chronią także przed potencjalnym, wrogim działaniem zewnętrznych służb, którego celem jest chiński porządek polityczny[523]. Co więcej, autoryzacja transferów, o której mowa w PIPL jest w ocenie G. Greenleafa uzależniona od dyskrecjonalnej oceny przeprowadzanej przez CAC[524]. Dodatkowo, autor wskazuje, że wykorzystywane kryteria nie są obiektywne, a strony zainteresowaniem uzyskaniem aprobaty transferu nie mają możliwości skonfrontowania decyzji organu przed sądem[525]. Pozorne podobieństwo przepisów PIPL do mechanizmu oceny adekwatności rozwiewa także G. Zheng, który podkreśla, że w przypadku PIPL ocena dotyczy każdego przypadku transferu a nie państwa trzeciego[526]. Niemniej jednak, umowy, o których wspomina art. 38 PIPL są oceniane przez G. Greenleafa jako odpowiednik standardowych klauzul umownych, o których mowa w RODO[527].

4. Kryterium drugie: egzekwowalności zasad ochrony danych osobowych

4.1. Uwagi wstępne

Kryterium egzekwowalności zasad ochrony danych osobowych[528] odgrywa szczególną rolę podczas każdej oceny systemu prawnego państwa trzeciego. Jak już wspominałem w rozdziale I, egzekwowalność jest blisko związana z rzeczywistym poziomem ochrony danych osobowych w państwie trzecim, ponieważ za sprawą

[519] J. Chen, J. Sun: *Understanding the Chinese*…, s. 217.
[520] I. Calzada: *Citizens' Data Privacy*…, s. 1132.
[521] G. Greenleaf, S. Livingston: *PRC's New Data*…, s. 1.
[522] G. Zheng: *Trilemma and Tripartition*…, s. 4.
[523] J. Liu: *China's data localization*…, s. 90–91.
[524] G. Greenleaf: *China Issues a*…, s. 12.
[525] G. Greenleaf: *China's Completed Personal*…, s. 4.
[526] G. Zheng: *Trilemma and Tripartition*…, s. 8.
[527] G. Greenleaf: *China's Completed Personal*…, s. 4.
[528] Dalej będę się posługiwać zamiennie terminami egzekwowalność lub egzekwowalność zasad ochrony danych osobowych.

odpowiednich narzędzi teoretyczne, niekiedy ogólne zasady ochrony danych osobowych ulegają konkretyzacji.

O egzekwowalności zasad ochrony danych osobowych można mówić w trzech aspektach. Pierwszy z nich dotyczy konkretnych obowiązków administratora. W przypadku chińskiego prawa ochrony danych osobowych zasadnym jest osobne omówienie obowiązków administratora z zastosowaniem podziału na sektor publiczny i prywatny, mając na uwadze podejście prawodawcy chińskiego do organów państwa przetwarzających dane osobowe. Drugi aspekt egzekwowalności zasad ochrony danych osobowych to prawa przyznane jednostce, za pośrednictwem których może realizować uprawnienia przyznane bezpośrednio w poszczególnych zasadach ochrony danych osobowych. Ostatni, trzeci aspekt wiąże się z sankcjami za nieprzestrzeganie przepisów ochrony danych osobowych.

4.2. Egzekwowalność zasad ochrony danych osobowych – obowiązki administratora w sektorze prywatnym

Podmioty sektora prywatnego, o czym była już mowa, należą do tej grupy podmiotów, które są zasadniczym adresatem obowiązków wynikających z przepisów chińskiego prawa ochrony danych osobowych. W każdej z ustaw, konkretne obowiązki administratora wiążą z zapewnieniem właściwego bezpieczeństwa danych osobowych.

W DSL również przyjęto taki model. Jedynie z artykuł 34 DSL wynika ogólny obowiązek polegający na konieczności pozyskania odpowiednich zezwoleń, jeśli takie zezwolenia na przetwarzanie danych zostały przewidziane przez przepisy prawa. Natomiast artykuł 27 DSL nakłada na administratora danych obowiązek wdrożenia odpowiednich mechanizmów zarządzania, zapewniających bezpieczeństwo danych. Dodatkowo, jeśli dane są przetwarzane z wykorzystaniem Internetu [529], obowiązki administratora w zakresie bezpieczeństwa danych powinny odpowiadać zasadom wynikającym z obowiązującego MLPS. W ten sposób przepisy DSL jednocześnie egzekwują omawianą zasadę bezpieczeństwa danych w CSL, gdzie MLPS stanowi podstawowy wyznacznik działań operatora sieci (administratora). Jednocześnie, art. 33 DSL, adresowany do podmiotów zaangażowanych w usługi pośrednictwa w transakcjach danych wymaga podjęcia dodatkowych działań. Chodzi o to, aby takie podmioty, w ramach świadczonych usług, wymagały od kontrahentów, którzy dostarczają im dane wykazywania pochodzenia danych, a także przeprowadzania weryfikacji tożsamości obu stron transakcji. Niezbędne jest również zachowanie dowodów transakcji, jaki

[529] Lub innej, podobnej, sieci informacyjnej.

i dowodów przeprowadzonej weryfikacji. W takim ujęciu, można mówić o przejawie egzekwowalności zasady rozliczalności, która *de iure* nie wynika z przepisów DSL.
W przypadku przetwarzania ważnych danych[530] art. 27 DSL dodatkowo nakazuje wdrożenie jasnego podziału obowiązków związanych z bezpieczeństwem danych, tj. obowiązków w zakresie zapewnienia bezpieczeństwa danych oraz obowiązków w zakresie nadzoru nad tym bezpieczeństwem. Sprawowanie nadzoru należy powierzyć osoby powołanej wyłącznie w tym celu. W związku z przyjętym podejściem opartym na ryzyku, administratorzy przetwarzający ważne dane, na podstawie art. 30 DSL, mają przeprowadzać okresowe oceny ryzyka[531]. Podsumowaniem okresowej oceny ryzyka ma być sporządzenie raportu, przekazywanego właściwym organom odpowiedzialnym za nadzór[532].

Zasadniczym obowiązkiem administratora w c.k.c. jest również zapewnienia bezpieczeństwa danych. Swego rodzaju wytyczne w tym zakresie zawiera art. 1038 zdanie drugie c.k.c. Przywołany przepis nakazuje administratorowi wdrożenie odpowiednich środków technicznych i innych rozwiązań służących zapewnieniu bezpieczeństwa danych, które przetwarza i przechowuje. Przyjęte rozwiązania mają chronić dane przed wyciekiem, ujawnieniem lub utratą danych. Jeśli dojdzie do zdarzenia naruszającego którykolwiek z wymienionych atrybutów danych, lub zaistnienie zdarzenia jest prawdopodobne, administrator powinien podjąć w rozsądnym czasie odpowiednie środki zaradcze, a nadto powiadomić osobę, której dane dotyczą[533] i złożyć raport na ręce właściwego organu nadzoru.

Obowiązki administratora w CSL koncentrują się na bezpieczeństwie, przy czym w większości poruszają problematykę bezpieczeństwa sieci, co jednak pośrednio wiąże się z ochroną przetwarzanych danych. Postępując zgodnie z MLPS, operator sieci ma zapewnić, aby była ona wolna od ingerencji, nieuprawnionego dostępu, wycieków i kradzieży danych oraz ich fałszerstwa. W tym celu operator sieci powinien skorzystać ze środków bezpieczeństwa, do których zaliczono stworzenie wewnątrzorganizacyjnego systemu zarządzania bezpieczeństwem sieci, w ramach którego należy wyznaczyć osobę odpowiedzialną za zarządzania bezpieczeństwem sieci, wdrożyć odpowiednie zabezpieczenia techniczne (chroniące przed wirusami, atakami oraz pozostałymi

[530] W rozumieniu DSL.
[531] Art. 30 zdanie drugie DSL określa minimalną treść raportu z oceny ryzyka.
[532] DSL nie wskazuje o jaki konkretnie organ nadzorczy chodzi, ograniczając się wyłącznie do stwierdzenia, że ma to być właściwy organ. Szerzej na ten temat w części rozdziału poświęconej organom nadzorczym.
[533] Art. 1038 zdanie drugie c.k.c. wymaga jedynie, aby powiadomienie zostało dokonane zgodnie z przepisami prawa.

działaniami zagrażającymi bezpieczeństwu sieci), wdrożenie odpowiednich rozwiązań technicznych służących monitorowaniu i archiwizowaniu sprawności sieci oraz naruszeń bezpieczeństwa sieci [534] . Nadto, operator sieci powinien wdrożyć dodatkowe zabezpieczenia jak m.in. kategoryzacja danych, szyfrowania, sporządzania kopii zapasowych.

Osobno potraktowano operatorów sieci związanych z infrastrukturą krytyczną, w tym krytyczną infrastrukturą informatyczną [535] . Spośród wszystkich dodatkowych obowiązków operatorów sieci związanych z infrastrukturą krytyczną, pierwszoplanową rolę odgrywają dwa przepisy. Pierwszy z nich to art. 37 CSL, związany z dopuszczalnością transferów danych, o którym mowa w części niniejszego rozdziału poświęconej zasadzie transferów danych osobowych. Drugi to art. 34 CSL, który stanowi rozwinięcie obowiązków wynikających z art. 21 CSL, czyli obowiązków w zakresie bezpieczeństwa sieci. Artykuł 34 CSL wymaga od operatorów sieci związanych z infrastrukturą krytyczną, aby uzupełnili środki stosowane na podstawie art. 21 CSL o dodatkowe rozwiązania wynikające z przepisów prawa lub przepisów administracyjnych, a także, ażeby powołano odrębny, wyspecjalizowany dział zarządzania bezpieczeństwem, kierowany przez oddelegowaną do tego celu osobę, którego zadaniem ma być m.in. weryfikacja bezpieczeństwa otoczenia osób piastujących krytyczne stanowiska, okresowe szkolenie pracowników z zakresu cyberbezpieczeństwa, połączone z oceną ich umiejętności, tworzenie kopii zapasowych ważnych systemów i baz danych czy opracowanie i wdrożenie planów reagowania na zagrożenia dla bezpieczeństwa sieci wraz z okresowymi szkoleniami. Operator sieci związany z infrastrukturą krytyczną nie może się jednak poprzestać na wdrożeniu środków, o których mowa powyżej, ponieważ jest obowiązany do przeprowadzania okresowych przeglądów bezpieczeństwa sieci i ryzyk z tym związanych. Artykuł 38 CSL wymaga, aby taki przegląd był przeprowadzany co najmniej raz w roku. Operator sieci może przeprowadzić przegląd samodzielnie lub z wykorzystaniem usług wykwalifikowanych podmiotów – organizacji bezpieczeństwa sieci. Raport z przeglądu powinien zawierać

[534] W ramach tego obowiązku, art. 21 CSL wprost nakazuje operatorowi sieci przechowywanie danych logowania do sieci co najmniej przez 6 miesięcy.

[535] O czym była już mowa, zgodnie z art. 31 CSL infrastrukturę krytyczną stanowią publiczne usługi komunikacyjno-informacyjne, szeroko ujęte: przemysł energetyczny, zaopatrzenie w wodę, działalność związana z finansami, działalność służby cywilnej, *e-government*. Nadto, za krytyczną infrastrukturę informatyczną (informacyjną) mogą być uznane takie przedsięwzięcia, w których zniszczenie, utrata funkcjonalności lub wyciek danych mogą poważnie zagrozić bezpieczeństwu narodowemu, dobrobytowi narodowemu, źródłom utrzymania jednostek lub interesowi publicznemu.

.

omówienie zastanej sytuacji wraz ze wskazaniem planowanych modyfikacji wykrytych niedociągnięć. Opracowany raport należy przekazać organowi nadzoru właściwemu dla bezpieczeństwa infrastruktury krytycznej.

Operatorzy sieci są także zobowiązani do wdrożenia planów reakcji na naruszenie bezpieczeństwa sieci. Zgodnie z art. 25 CSL nadrzędnym celem takich planów jest niezwłoczna reakcja na ryzyka dla bezpieczeństwa sieci, a w szczególności na podatności sieci, ataki wirusowe i inne ataki na sieć. Jednocześnie, art. 25 CSL określa podstawowy scenariusz postępowania na wypadek wystąpienia naruszenia bezpieczeństwa sieci. W takiej sytuacji, operator sieci powinien, postępując zgodnie z przyjętym planem, niezwłocznie zareagować na naruszenie, podjąć środki naprawcze odpowiednie do powstałego naruszenia oraz zaraportować zdarzenie do właściwego organu.

W przypadku przetwarzania danych osobowych, przedstawione wyżej obowiązki ulegają nieznacznej modyfikacji, przy czym operator sieci (administrator) powinien postępować zgodnie z art. 42 CSL. Wdrożone zabezpieczenia mają w szczególności, chronić przed wyciekiem, zniszczeniem lub utratą danych. Poza działaniami prewencyjnymi, art. 42 zdanie drugie CSL wskazuje postępowanie jakie należy podjąć w razie zaistnienia zdarzenia skutkującego wyciekiem, zniszczeniem lub utratą danych [536]. Wówczas operator sieci (administrator) powinien niezwłocznie wdrożyć odpowiednie działania naprawcze. Dodatkowo, operator sieci (administrator) jest zobowiązany do poinformowania osób, których dane dotyczą oraz złożenia stosownego raportu właściwemu organowi nadzoru.

PIPL ujmuje obowiązki administratora dwojako. Konkretyzując zasadę legalności, art. 10 PIPL w sposób ogólny zakazuje nielegalnego przetwarzania danych osobowych oraz angażowania się w przetwarzanie, które może zagrażać bezpieczeństwu narodowemu lub interesowi publicznemu. Na zakazane przetwarzanie składają się pozyskiwanie, używanie, przetwarzanie oraz przekazywanie danych osobowych podmiotom trzecim, jak również sprzedaż, kupno, udostępnianie lub ujawnianie danych osobowych innych osób.

Urzeczywistnieniem zasady bezpieczeństwa ma być opracowanie i wdrożenie odpowiednich rozwiązań, których przykłady znalazły się w art. 51 PIPL. Dla ich opracowania PIPL wymaga uwzględnienia celu i metod przetwarzania, kategorii przetwarzanych danych, wpływu przetwarzania danych na prawa i wolności jednostek,

[536] O czym była już mowa, takie same działania należy podjąć, jeśli zaistnienie zdarzenia mogło mieć miejsce.

potencjalnych ryzyk dla bezpieczeństwa danych. Przykładowe rozwiązania w zakresie bezpieczeństwa danych to odpowiednia struktura organizacyjna ujęta w sformalizowanych procedurach, wdrożenie zarządzania danymi osobowymi opartego o kategoryzowanie danych, wdrożenie odpowiednich technicznych środków bezpieczeństwa, m.in. opartych o szyfrowanie danych, wprowadzanie limitów przetwarzania danych osobowych na poziomie operacyjnym (organizacyjnym) wraz z okresowym, regularnym szkoleniem pracowników w zakresie bezpieczeństwa danych osobowych, opracowanie i wdrożenie planów reagowania na incydenty naruszenie bezpieczeństwa danych osobowych. Ponadto, administratorzy są obowiązani do przeprowadzania okresowych przeglądów. Artykuł 54 PIPL wprowadza ogólny obowiązek regularnego audytowania przetwarzania danych w zakresie zgodności z przepisami prawa lub prawa administracyjnego.

Dla odpowiedniego wypełnienia obowiązków związanych z bezpieczeństwem danych istotne jest także przeprowadzenie oceny wpływu przetwarzania danych osobowych, o której mowa w art. 55-56 PIPL. Konieczność przeprowadzenia sformalizowanej oceny wpływu jest uzależniona od zaistnienia szczególnych przesłanek. Wśród okoliczności nakazujących przeprowadzenie oceny wpływu znalazły się przetwarzanie danych wrażliwych, wykorzystywanie danych osobowych do automatycznego podejmowania decyzji, powierzenie przetwarzania danych osobowych, udostępnianie danych osobowych innym administratorom, ujawnianie danych osobowych, transfer danych osobowych poza granice Chin. Nadto, przeprowadzenie oceny wpływu będzie konieczne w tych wszystkich sytuacjach, w których przetwarzanie danych wpływa znacząco na jednostkę. Procedura przeprowadzenie oceny wpływu przetwarzania nie została określona w PIPL, z wyjątkiem konieczności przeprowadzenia oceny wpływu z wyprzedzeniem. Treść oceny, zgodnie z art. 56 PIPL, powinna zawierać ocenę w zakresie zgodności z prawem, konieczności, celu przetwarzania, metod przetwarzania oraz pozostałych przesłanek zgodnego z prawem przetwarzania danych. Oprócz tego, należy umieścić ocenę wpływu przetwarzania na prawa i interesy jednostki, ocenę ryzyka dla bezpieczeństwa danych, a także ocenę przyjętych środków ochronnych. Środki ochronne należy ocenić w zakresie ich legalności, efektywności oraz odpowiedniości do stopnia ryzyka. Raport z przeprowadzonej oceny, wraz z dokumentacją statusu przetwarzania danych osobowych, należy przechowywać przez co najmniej 3 lata.

Dodatkowe obowiązki nałożono na administratorów, których działalność związana jest ze świadczeniem usług za pośrednictwem platform internetowych. Artykuł 58 PIPL zawiera trzy przesłanki, od zaistnienia których uzależniono zastosowanie dodatkowych obowiązków. Jeśli administrator świadczy ważne usługi platform internetowych, jego platforma posiada dużą liczbę użytkowników, a przyjęty model biznesowy jest skomplikowany, wówczas administrator powinien podjąć dodatkowe, cztery działania związane z zapewnieniem legalności przetwarzania danych. Administrator ma opracować i wdrożyć strukturę wraz z systemem zarządzania zgodnością ochrony danych osobowych, zgodnie z wymaganiami przepisów państwowych. W ramach swojej struktury organizacyjnej administrator ma stworzyć niezależną komórkę organizacyjną, do której zadań będzie należało sprawowanie nadzoru nad przestrzeganiem ochrony danych osobowych przez administratora. Dla zagwarantowania niezależności nadzoru, w skład komórki organizacyjnej mają wchodzić osoby spoza struktury administratora. Obok niezależnego wewnętrznego nadzoru, administrator jest zobowiązany do dopuszczania sprawowania nadzoru w zakresie ochrony danych osobowych sprawowanego przez społeczeństwo. Społeczny wymiar nadzoru wiąże się z obowiązkowym, okresowym publikowaniem przez administratora raportów na temat przetwarzania danych osobowych[537]. Ponadto, obowiązkiem administratora w ramach prowadzonej działalności jest przestrzeganie zasad otwartości, uczciwości i sprawiedliwości. Administrator ma także stworzyć regulamin platformy, który będzie określał zasady jej działania, oraz wdrożyć jasne zasady i obowiązki związane z przetwarzaniem danych osobowych przez dostawców produktów lub dostawców usług dostępnych na platformie[538].

Oprócz administratorów, obowiązek egzekwowalność zasad ochrony danych osobowych dotyczy także podmiotów, o których mowa w art. 59 PIPL. Chodzi o podmioty, którym administrator powierzył przetwarzanie danych osobowych. Ich obowiązkiem jest wspieranie administratorów w wypełnianiu obowiązków, które nakłada na niego PIPL. Nadto, art. 59 PIPL wymaga od podmiotów, którym administrator powierzył przetwarzanie danych osobowych zastosowania odpowiednich środków zapewniających bezpieczeństwo danych. Art. 59 PIPL wprost wskazuje na stosowanie środków, które wynikają z przepisów PIPL, przepisów prawa lub przepisów administracyjnych.

[537] Art. 58 PIPL zalicza raportowanie administratora w poczet obowiązków określanych mianem społecznej odpowiedzialność biznesu.

[538] Jeśli dostawca produktów lub dostawca usług dostępnych na platformie dopuści się poważnego naruszenia przepisów prawa lub przepisów administracyjnych, administrator, zgodnie z art. 58 PIPL, jest zobowiązany zaprzestać udostępniać produkty lub usługi takiego dostawcy na swojej platformie.

Egzekwowalność w PIPL to także odpowiednia reakcja na wyciek, nieuprawnioną modyfikację lub utratę danych osobowych, w tym także na potencjalne zaistnienie jednego z wymienionych zdarzeń. Zgodnie z art. 57 PIPL administrator powinien podjąć dwa rodzaje działań. Po pierwsze, powinien natychmiastowo wdrożyć odpowiednie środki naprawcze. Po drugie, powinien poinformować organ nadzoru i osobę, której dane dotyczą o zaistniałej sytuacji. Spełnienie obowiązku notyfikacyjnego jest wyłączone tylko w stosunku do osoby, której dane dotyczą, o ile wdrożone i zastosowane środki naprawcze skutecznie zapobiegają szkodzie, która może wyniknąć z wycieku, nieuprawnionej modyfikacji lub utraty danych osobowych. Co do zasady, wyłączenie obowiązku notyfikacyjnego jest warunkowe, ponieważ organ nadzorczy może odmiennie ocenić sytuację i uznać, że mimo zastosowania środków naprawczych szkoda mogła jednak zaistnieć. Na treść informacji przekazywanej osobie, której dane dotyczą oraz organowi nadzoru, zgodnie z art. 57 PIPL, składa się wskazanie okoliczności zdarzenia, w tym kategorii danych, przyczyn zdarzenia oraz szkód jakie mogły zostać wyrządzone wskutek zdarzenia, wskazanie podjętych przez administratora środków naprawczych, oraz środków naprawczych, które może podjąć osoba, której dane dotyczą, jak również wskazanie danych kontaktowych administratora.

Do administratorów danych, których siedziby znajdują się poza granicami Chin[539] adresowany jest dodatkowy obowiązek w zakresie ustanowienia odpowiedniego przedstawicielstwa. Art. 53 PIPL dopuszcza utworzenie w tym celu specjalnego podmiotu lub też powołania swojego przedstawiciela na terytorium Chin. Do zakresu obowiązków tak ustanowionego przedstawicielstwa będzie należało zajmowanie się sprawami związanymi z przetwarzaniem danych osobowych przez administratora, które dotyczą osób fizycznych znajdujących się w Chinach[540]. Ustanowienie przedstawicielstwa łączy się z wypełnieniem obowiązku notyfikacyjnego względem organu nadzoru, który polega na przekazaniu danych identyfikacyjnych wyznaczonego przedstawiciela[541] oraz informacji o dostępnych ścieżkach kontaktu.

Art. 39 PIPL odnosi się do egzekwowalności zasady transferów danych osobowych. Transfer danych osobowych poza terytorium Chin aktualizuje po stronie administratora danych wysyłającego dane, obowiązek notyfikacyjny. Jednocześnie, administrator jest zobligowany do pozyskania odrębnej zgody jednostki. Osoba, której dane dotyczą

[539] Dodatkowym warunkiem jest zastosowanie do przetwarzania danych prawa chińskiego, zgodnie z art. 3 zdanie drugie PIPL.
[540] Do takiego wniosku prowadzi lektura art. 3 zdanie drugie PIPL.
[541] Odpowiednio, specjalnego podmiotu lub przedstawiciela administratora

powinna zostać poinformowana o tożsamości odbiorcy danych, w tym sposobach w jakich może się z nim kontaktować, o celu przetwarzania, stosowanych metodach i kategoriach danych. W ramach notyfikacji, jednostka powinna także otrzymać informacje na temat dostępnych w państwie trzecim ścieżek realizacji jej praw przyznanych przez PIPL oraz o pozostałych zagadnieniach wpływających na możliwość realizacji jej praw.

Z zagadnieniem egzekwowalności zasad ochrony danych osobowych powiązany jest podmiot inspektora danych osobowych. Obowiązek powołania przez administratora inspektora danych osobowych został uzależniony od spełnienia przesłanki ilościowej. Zgodnie z art. 52 PIPL, dookreślenie przesłanki ilościowej jest zadaniem państwowego departamentu cyberbezpieczeństwa i informatyzacji. Zakres obowiązków inspektora danych został sformułowany ogólnie, art. 52 PIPL w otwartym katalogu, wskazuje na obowiązek nadzorowania czynności przetwarzania danych osobowych oraz nadzorowania przyjętych przez administratora rozwiązań w zakresie ochrony danych osobowych. Administrator jest obowiązany poinformować osoby, których dane dotyczą o dostępnych ścieżkach kontaktu z inspektorem danych osobowych, a także wskazać organowi nadzoru osobę inspektora wraz z dostępnymi ścieżkami kontaktu.

Przedstawiony powyżej opis obowiązków administratora danych osobowych wynikających z całokształtu przepisów chińskiego prawa ochrony danych osobowych wykazuje podobieństwo do rozwiązań wykorzystanych w RODO. Rozbudowane obowiązki w zakresie bezpieczeństwa danych osobowych ukazują jednolity kształt oczekiwanej ochrony danych osobowych, składającej się zarówno z zabezpieczeń organizacyjnych, jak i zabezpieczeń technicznych. Ogólne sformułowania wykorzystane do ich opisu wywierają skutki podobne do neutralności technologicznej w RODO w tym sensie, że nie ograniczają swobody administratora w wyborze konkretnych zabezpieczeń. Podobnie, oczekiwana reakcja administratora danych osobowych nie odbiega od konstrukcji wykorzystanej w RODO, z zastrzeżeniem realizacji obowiązku notyfikacyjnego na rzecz organu nadzoru. Przepisy nie określają bowiem terminu, w którym taka notyfikacja powinna nastąpić. Wątpliwości wywołują jednak przepisy związane z oceną skutków dla ochrony danych, które w PIPL zostały ograniczone do ściśle określonych sytuacji a nie tak jak ma to miejsce w RODO do poziomu ryzyka czynności przetwarzania danych. Nadto, jak słusznie zauważają niektórzy autorzy, przepisy związane z inspektorem danych osobowych wewnątrz struktury jednostki będącej administratorem danych osobowych są bardzo ogólne, co może podważać

skuteczność przestrzegania obowiązku ich wyznaczenia, w tym zwłaszcza mając na uwadze stosunkowo niski wymiar sankcji, jakie grożą za naruszenie tego obowiązku[542]. Nie bez znaczenia jest również brak wymogu niezależności inspektora danych osobowych[543].

4.3. Egzekwowalność zasad ochrony danych osobowych – obowiązki administratora w sektorze publicznym

Chińskie prawo ochrony danych osobowych, a zwłaszcza przepisy DSL, PIPL oraz c.k.c. wprowadzają zróżnicowane traktowanie podmiotów sektora prywatnego i publicznego. Zdaniem doktryny konsekwencją takiego zróżnicowania jest nierówne podejście do podmiotów sektora prywatnego i publicznego w zakresie nadzoru, gdzie to podmioty prywatne są poddawane większemu nadzorowi, w porównaniu z sektorem publicznym, skoro większość obowiązków jest adresowana właśnie do nich[544].

Organy państwa oraz podmioty upoważnione przez przepisy prawa do wykonywania spraw publicznych, zgodnie z art. 43 DSL stanowią odrębną grupę, do której adresowane są niektóre obowiązki. Artykuł 38 DSL dotyczy tych sytuacji, gdy organy państwa pozyskują lub przetwarzają dane w związku z wykonywaniem obowiązków nałożonych przez prawo. Wówczas, organy państwa powinny przetwarzać dane tylko w takim zakresie, w jakim jest to niezbędne dla realizacji wspomnianych obowiązków prawnych, z poszanowaniem procedur wynikających z tych przepisów prawa, w tym regulacji administracyjnych. Tym samym, faktycznie organy państwa powinny przestrzegać zasady celowości i minimalizacji. Jednocześnie, przetwarzając takie dane jak dane osobowe, dane prywatne, tajemnice handlowe lub poufne informacje handlowe, organy państwa mają zapewnić ich poufność. Z obowiązkiem zapewnienia poufności sprzężony jest zakaz nielegalnego rozpowszechniania lub udostępniania danych, które mają pozostać poufne. Jednocześnie, pominięto pozostałe atrybuty danych. Obowiązek wdrożenia systemu zarządzania bezpieczeństwem danych[545], o którym mowa w art. 39 zyskał ogólną postać, odwołując się generalnie do wymagań wynikających z przepisów prawa lub przepisów administracyjnych. Tym samym, organy państwa zyskały znaczną swobodę wyboru odpowiedniego modelu systemu bezpieczeństwa danych, co nie wyklucza implementacji rozwiązań adresowanych do podmiotów prywatnych. DSL odnosi się także do sytuacji upoważnienia podmiotów zewnętrznych

[542] C. Wang, J. Zhang, N. Lassi i in.: *Privacy Protection in*…, s. 10.
[543] C. You: *Half a Loaf*…, s. 17.
[544] H. Roberts: *Informational Privacy with*…, s. 4; T. Giladi Shtub, M.S. Gal: *The Competitive Effects*…, s. 15.
[545] W tym odpowiedniego podziału obowiązku oraz zapewnienia bezpieczeństwa tzw. danych rządowych.

do stworzenia lub zarządzania usługami *e-government* oraz sytuacji powierzenia podmiotom zewnętrznym przetwarzania danych rządowych. Zgodnie z art. 40 DSL zachodzi wówczas konieczność poddania takich podmiotów ścisłej weryfikacji, poprzedzającej powierzenie wskazanych czynności, a następnie sprawowania przez organy państwa nadzoru nad wykonywaniem obowiązków w zakresie bezpieczeństwa danych. Podmioty zewnętrzne wykonujące wskazane powyżej czynności są zobowiązane do przestrzegania stosownych przepisów prawa oraz umów łączących ich z organami państwa. Natomiast przetrzymywanie, wykorzystywanie, rozpowszechnianie danych lub ich udostępnianie innym podmiotom wymaga zgody organów państwa.

Z artykułu 1039 c.k.c. wynika nakaz zachowania poufności danych osobowych, adresowany do organów państwa i podmiotów wykonujących funkcje administracyjne, a także ich pracowników. Nadto zakazano ujawniania i nielegalnego udostępniania danych osobowych[546] przetwarzanych w ramach wykonywania obowiązków. Biorąc pod uwagę sposób, w jaki zredagowano przepis c.k.c. odnoszące się do ochrony danych osobowych, art. 1039 c.k.c. oznacza ograniczenie obowiązków adresowanych do państwa wyłącznie do zachowania poufności danych.

Obowiązkiem organów państwa w PIPL, zgodnie z art. 34 jest wykonywanie ustawowych obowiązków w zakresie uprawnień przyznanych przez przepisy prawa i przepisy administracyjne, w zgodzie z procedurami wynikającymi z tych przepisów. Jednocześnie, organy państwa, wykonując swoje obowiązki nie mogą wykraczać poza zakres danych osobowych, który jest konieczny dla realizacji tych obowiązków. W ten sposób ustawodawca rozciąga zastosowanie zasady minimalizacji na organy państwa. Z kolei art.. 35 PIPL nakazuje organom państwa przetwarzającym dane osobowe w ramach pełnionych obowiązków wypełnienie obowiązku informacyjnego. Wyjątkiem jest zaistnienie jednej z sytuacji, o których mowa w art. 18 zdanie pierwsze PIPL [547] lub zaistnienie takich okoliczności, w których realizacji obowiązków zakłócałaby wypełnienie obowiązków organów państwa.

Węższy zakres obowiązków podmiotów publicznych, w porównaniu z obowiązkami podmiotów prywatnych to kolejny przejaw różnic występujących między przepisami chińskiego prawa ochrony danych osobowych i RODO. Oczywistą konsekwencją takiego stanu rzeczy jest brak jednolitej ochrony jednostki.

[546] Art. 1039 c.k.c. jako dobro chronione, obok danych osobowych, wymienia prywatność.
[547] Administrator nie będzie musiał realizować obowiązku informacyjnego, jeśli przepisy prawa lub przepisy administracyjne nakazują zachowanie poufności lub uznają spełnienie obowiązku informacyjnego za zbędne.

4.4. Katalog praw przyznanych osobie, której dane dotyczą

Prawa jednostki, wespół ze środkami przyznanymi w razie naruszenia jej danych osobowych to gwarant rzeczywistej i skutecznej egzekwowalności zasad ochrony danych osobowych. Zasadniczo, o prawach jednostki wspominają CSL, c.k.c. i PIPL.

W przypadku CSL, ustawodawca w art. 43, jednoznacznie sformułował wyłącznie prawo do usunięcia danych lub ich sprostowania. Jednocześnie, dla obu praw osób, których dane dotyczą, operator sieci - administrator powinien wdrożyć odpowiednie ścieżki postępowania z żądaniami jednostki. Prawo do usunięcia danych, w porównaniu z jego kształtem wynikającym z przepisów RODO, jest ograniczone. Przepisy CSL możliwość żądania usunięcia danych uzależniają od spełnienia przesłanki niezgodnego z prawem postępowania z danymi przez administratora. Natomiast niezgodne z prawem przetwarzanie danych to tylko jedna z przesłanek zastosowania prawa do bycia zapomnianym na podstawie art. 17 ROOD. W CSL jednostka, która ustali, że jej dane są przetwarzane z pogwałceniem przepisów prawa, przepisów administracyjnych lub postanowień umowy łączącej jednostkę z operatorem sieci – administratorem ma prawo żądać, aby jej dane zostały usunięte. Oznacza to, że jednostka zanim zażąda usunięcia jej danych, za każdym razem powinna ustalić, czy została spełniona przesłanka naruszenia prawa lub łączącej strony umowy. W przypadku prawa do sprostowania danych, CSL uprawnia jednostkę do żądania poprawienia danych osobowych jej dotyczących, jeśli jednostka ustali, że dane osobowe pozyskane lub przechowywane przez operatora sieci – administratora zawierają błędy. Tym samym, prawo do sprostowania w CSL tylko częściowo odpowiada przepisom RODO, gdzie prawo do sprostowania nie ogranicza się wyłącznie do usuwania błędów w danych osobowych, ale uprawnia jednostkę także do uzupełnienia niekompletnych danych.

Analizując przepisy CSL, Q. Zhou wyjaśnia, że w CSL nie został zawarty katalog praw jednostki, przy czym z prawa do sprostowania danych lub ich usunięcia można wyinterpretować prawo do bycia zapomnianym[548]. Sądzę, że taka teza jest zbyt śmiała, biorąc pod uwagę ograniczenie żądania usunięcia danych w CSL wyłącznie do przypadku naruszenia przepisów prawa lub postanowień umowy. Zdaniem Z. Shi, ograniczony charakter prawa do usunięcia danych wynika z całościowego podejścia prawodawcy

[548] Q. Zhou: *Whose Data Is*…, s. 78.

chińskiego do jednostki w kontekście przetwarzania jej danych osobowych [549]. Zarazem, fakt, że prawo do usunięcia danych może być wykorzystane wyłącznie w sytuacji naruszenia prawa lub postanowień umowy nie wpływa negatywnie na swobodny przepływ danych osobowych na rynku[550].

Uwzględniwszy obowiązki operatora sieci – administratora w zakresie realizacji obowiązku informacyjnego, można rozważyć, czy CSL formułuje prawo do informacji na temat przetwarzania danych osobowych, stanowiące element prawa dostępu do danych. Całokształt regulacji sugeruje odpowiedź negatywną. Należy zauważyć, że przekazanie informacji na temat przetwarzania danych osobowych w CSL zostało ujęte w formie obowiązku operatora sieci – administratora, który polega na publikacji właściwych informacji, a więc na poinformowaniu jednostki. Przepisy CSL nie wskazują jednak żadnego uprawnienia, na podstawie którego osoba, której dane dotyczą mogłaby skierować odpowiednie żądanie do operatora sieci – administratora. Nadto, jak zauważają niektórzy autorzy, uznanie, że CSL zawiera w sobie prawo do informacji nie zmienia tego, że i tak będzie to prawo ograniczone, sprowadzające się do przekazania informacji na etapie pozyskiwania danych osobowych[551], a więc nie w każdym momencie.

Do przepisów określających prawa jednostki związane z przetwarzaniem danych osobowych zaliczają się przepisy c.k.c. Zgodnie z artykułem 1037 c.k.c., osoba fizyczna ma prawo dostępu do swoich danych osobowych przetwarzanych przez administratora oraz może żądać udostępnienia kopii jej danych. Z prawem dostępu skorelowano prawo do sprostowania ewentualnych błędów wykrytych w danych osobowych. Wówczas administrator jest obowiązany do wprowadzenia odpowiednich zmian w danych lub podjęcia innych kroków w rozsądnym terminie. Tak jak w CSL, prawo do sprostowania w c.k.c. nie odnosi się jednoznacznie do możliwości uzupełnienia brakujących danych. Osoba, której dane dotyczą może także żądać usunięcia jej danych osobowych. Prawo żądania usunięcia danych zostało ograniczone przez art. 1037 zdanie 2 c.k.c. do sytuacji, w których osoba, której dane dotyczą ustali, że administrator przetwarza jej dane z pogwałceniem przepisów prawa lub prawa administracyjnego albo z naruszeniem umowy łączącej administratora z osobą, której dane dotyczą. Jeśli przesłanka zostanie spełniona, administrator powinien usunąć dane w rozsądnym terminie. Bez wątpienia, w ten sposób ustawodawca zdecydował się na zachowanie jednolitego podejścia do

[549] Z. Shi: *The Right to Be Forgotten in China——A Third Way to Construct Public Sphere*. 3.04.2021. https://ssrn.com/abstract=3832803 [dostęp: 22.05.2023] s. 22.
[550] Ibid.
[551] X. Lin, H. Liu, Z. Li i in.: *Privacy Protection of*…, s. 3.

prawa do usunięcia danych, które pierwotnie wynika z CSL, a więc ograniczonej wersji prawa do usunięcia danych.

Najszerszy katalog praw osób, których dane dotyczą znalazł się w PIPL. Aby osoba, której dane dotyczą mogła korzystać ze swoich uprawnień, administrator, tak jak operator sieci w CSL, powinien stworzyć odpowiednie ku temu warunki. Obsługa żądań oraz pozostałych przejawów wykonywania przyznanych jej praw powinna zostać ujęta w formę wygodnej, przyjaznej dla jednostki procedury. Art. 50 PIPL wymaga także, aby każda odmowa realizacji uprawnienia jednostki została uzasadniona przez administratora.[552] Z odmową realizacji praw osoby, której dane dotyczą art. 50 PIPL wiąże uprawnienie do wystąpienia z powództwem do sądu (ludowego), zgodnie z właściwymi przepisami prawa.

Katalog praw osób, których dane dotyczą znajduje się w rozdziale IV, w art. 44 - 50 PIPL. Na uwagę zasługuje krąg podmiotów uprawnionych do korzystania z praw przyznanych jednostce, do którego oprócz jednostki należą także krewni zmarłej osoby, której dane dotyczą. Zgodnie z art. 49 PIPL krewni zmarłej jednostki mogą, dla potrzeby ich własnych praw i interesów, realizować prawa przyznane zmarłej jednostce. Jednakże, osoba, której dane dotyczą w stosownej dyspozycji złożonej przed śmiercią, może pozbawić krewnych tychże uprawnień. Wprowadzając taką konstrukcję, ustawodawca chiński rozstrzygnął *a priori* wątpliwości, z którymi zmaga się doktryna i orzecznictwo europejskie, rozważając w jaki sposób należy podchodzić do dziedziczenia praw osób, które dane dotyczą określonych w RODO.

Prawo dostępu do danych przetwarzanych przez administratora oraz uzyskania ich kopii znalazło się w art. 45 PIPL. Źródeł ograniczenia tego prawa należy się dopatrywać w tych sytuacjach, gdy przepisy prawa lub przepisy administracyjne nakazują zachowanie poufności lub uznają spełnienie obowiązku informacyjnego za zbędne [553]. Realizacja żądania w zakresie dostępu do danych lub uzyskania ich kopii powinna nastąpić niezwłocznie. Szczególną emanacją prawa dostępu jest prawo do żądania wyjaśnień. Zgodnie z art. 48 PIPL osoba, której dane dotyczą może żądać od administratora wyjaśniania zasad przetwarzania danych osobowych, które ten stosuje.

Jednostka ma także prawo do żądania ograniczenia przetwarzania danych. Artykuł 44 PIPL wprost wskazuje, że jednostka może żądać ograniczenia lub zaprzestania

[552] Odmowa realizacji uprawnienia jednostki przez administratora została skorelowana z prawem do skorzystania z drogi sądowej, na podstawie powództwa wytoczonego zgodnie z przepisami prawa. Szerzej ten temat w części rozdziału poświęconej środkom prawnym przyznanym jednostce.

[553] Art. 45 PIPL odsyła wprost do art. 18 zdanie pierwszej i art. 35 DSL.

przetwarzania jej danych osobowych, chyba że przepisy prawa lub przepisy administracyjne stanowią inaczej. Jest to więc konstrukcja mniej restrykcyjna, w porównaniu z art. 18 RODO, dopuszczającym żądanie ograniczenia przetwarzania w ściśle określonych przypadkach.

W artykule 45 PIPL zawarto także prawo do przenoszenia danych. Jednostka może wyznaczyć innego administratora, któremu dane mają być przekazane. Wówczas, dotychczasowy administrator jest zobowiązany zapewnić odpowiednią ścieżkę kontaktu dla przeniesienia danych, zgodną z warunkami określonym przez krajowy departament cyberbezpieczeństwa i informatyzacji. Jak zauważa I. Calzada, konieczność przestrzegania warunków przenoszenia danych określonych przez organy państwa stanowi niewątpliwe ograniczenie dla jednostki, którego brak w RODO[554]. Zdaniem C. You taka konstrukcja jest przejawem chęci ustawodawcy do zachowania równowagi pomiędzy ochroną danych osobowych a dalszym rozwojem rynku[555].

W razie wykrycia przez jednostkę, że dane przetwarzane przez administratora są błędne lub niekompletne, aktualizują się przesłanki zastosowania prawa do sprostowania danych zgodnie z art. 46 PIPL. Tym samym, tylko PIPL odpowiada kształtowi prawa do sprostowania danych określonemu w RODO. Kierowane przez jednostkę żądanie poprawienia danych lub ich uzupełnienia wymaga od administratora weryfikacji poprawności przetwarzanych danych, a w razie potwierdzenie uchybień, niezwłocznego podjęcia stosownych działań.

Art. 47 PIPL jest źródłem prawa do żądania usunięcia danych. Co do zasady, usunięcie danych w razie zaistnienia okoliczności, o których mowa w art. 47 PIPL jest obowiązkiem administratora, który powinien usunąć dane z własnej woli. Dopiero bierność administratora jest przesłanką uprawniającą jednostkę do żądania usunięcia swoich danych. Wśród okoliczności, które zobowiązują administratora do usunięcia danych znalazły się realizacja celu przetwarzania lub niemożliwość realizacji celu lub nieprzydatność danych do realizacji celu; zaprzestanie świadczenia usług lub dostarczania towarów, z którymi to aktywnościami łączyło się przetwarzanie danych; wycofanie zgody przez osobę, której dane dotyczą; przetwarzanie danych z pogwałceniem przepisów prawa, prawa administracyjnego lub umowy; upływ okresu retencji danych. Odnośnie do ostatniej przesłanki, obowiązek usunięcia danych nie powstaje, jeśli okres retencji wymagany przez przepisy prawa lub przepisy

[554] I. Calzada: *Citizens' Data Privacy*…, s. 1140.
[555] C. You: *Half a Loaf*…, s. 16.

administracyjne nie upłynął albo usunięcie danych trudne do wykonania z powodów technicznych. W takiej sytuacji, administrator powinien zaprzestać wszelkiego przetwarzania danych, które wykracza poza ich przechowywanie oraz stosowanie odpowiednich środków bezpieczeństwa. Porównując prawo do usunięcia danych wynikające z CSL i c.k.c., z przepisami PIPL, to właśnie te ostatnie zapewniają jednostce prawo najbardziej zbliżone do konstrukcji, o której mowa w art. 17 RODO. Według C. You prawo do usunięcia danych w PIPL można nawet traktować jako ekwiwalent przepisów RODO[556].

4.5. Katalog sankcji

Chińskie przepisy prawa ochrony danych osobowych zawierają rozbudowany katalog sankcji za, najogólniej mówiąc, naruszenie przepisów ochrony danych osobowych. Co oczywiste, przepisów sankcyjnych nie zawiera c.k.c.

W DSL nieprzestrzeganie zasad legalności i odpowiedniego zarządzania, o których mowa w art. 27 DSL, a także obowiązków w zakresie ryzyka wynikających z art. 29 i 30 DSL, zgodnie z art. 45 DSL uprawnia właściwy organ odpowiedzialny za nadzór do wydania ostrzeżenia, nakazania podjęcia działań naprawczych lub nałożenia kary grzywny na osobę bezpośrednio odpowiedzialną za bezpieczeństwo danych w kwocie od 10.000 do 100.000 yuan. Odmowa podjęcia działań naprawczych lub spowodowanie poważnych konsekwencji, w szczególności spowodowania wycieku danych na dużą skalę, uprawnia organ nadzoru do nałożenia grzywny w kwocie od 500.000 do 2.000.000 yuan, a także do zawieszenia niektórych istotnych operacji przetwarzania danych, zawieszenia operacji przetwarzania danych wymagających działań naprawczych lub cofnięcia przyznanych licencji lub pozwoleń. Osoba bezpośrednio odpowiedzialna za zarządzanie bezpieczeństwem danych może być ukarana grzywną w kwocie od 50.000 do 200.000 yuan. Odrębnie potraktowano naruszenie (bezpieczeństwa) narodowych systemów zarządzania danymi o kluczowym znaczeniu. W sytuacji naruszenia, które spowodowało zagrożenie dla suwerenności, bezpieczeństwa państwa lub jego interesów[557] art. 45 zdanie drugie DSL uprawnia właściwy organ odpowiedzialny za nadzór do nałożenia kary grzywny w kwocie od 2.000.000 do 10.000.000 yuan. Nadto, w zależności od całokształtu okoliczności, właściwy organ odpowiedzialny za nadzór może dodatkowo skorzystać z zawieszenia

[556] Ibid.
[557] Mowa tu o szczególnych interesach, tłumaczonych jako *development interests*, czyli interesy związane z rozwojem (interesy rozwojowe).

niektórych istotnych operacji przetwarzania danych, zawieszenia operacji przetwarzania danych wymagających działań naprawczych lub cofnięcia przyznanych licencji, lub pozwoleń. Jeśli naruszenie stanowi przestępstwo, jego ściganie ma nastąpić zgodnie z właściwymi przepisami. Transfer ważnych danych poza granice Chin, z naruszeniem art. 31 DSL, upoważnia właściwy organ odpowiedzialny za nadzór do wydania ostrzeżenia i nakazania podjęcia działań naprawczych, a także nałożenia grzywny w kwocie od 100.000 do 1.000.000 yuan, zawieszenia niektórych istotnych operacji przetwarzania danych, zawieszenia operacji przetwarzania danych, wymagających działań naprawczych lub cofnięcia przyznanych licencji lub pozwoleń, a także nałożenia kary na osobę bezpośrednio odpowiedzialną za zarządzanie bezpieczeństwem danych i pozostałych pracowników bezpośrednio odpowiedzialnych kwocie od 100.000 do 1.000.000 yuan.

Jeśli podmioty zaangażowane w usługi pośrednictwa w transakcjach danych nie wypełnią obowiązku, o którym mowa w art. 33 DSL, wówczas zgodnie z art. 47 DSL właściwy organ odpowiedzialny za nadzór może nakazać poprawę postępowania, konfiskatę niezgodnych z prawem zysków oraz karę grzywny w kwocie stanowiącej dziesięciokrotność niezgodnych z prawem zysków. W sytuacji, gdy nie powstały niezgodne z prawem zyski lub ich kwota jest niższa od 100.000 yuan, właściwy organ odpowiedzialny za nadzór może nałożyć karę grzywny w kwocie 100.000 do 1.000.000 yuan, a nadto może nałożyć karę zawieszenia niektórych istotnych operacji przetwarzania danych, zawieszenia operacji przetwarzania danych wymagających działań naprawczych lub cofnięcia przyznanych licencji lub pozwoleń. Osoba bezpośrednio odpowiedzialna za zarządzanie bezpieczeństwem danych i pozostali pracownicy bezpośrednio odpowiedzialni mogą być skazani na grzywnę kwocie 10.000 do 100.000 yuan. Karanym naruszeniem przepisów DSL jest także odmowa współpracy z organami ścigania w zakresie udostępnienia danych zgodnie z art. 35 DSL, o której szerzej będzie mowa w dalszej części rozdziału.

Przepisy sankcyjne odnoszą się także do sytuacji naruszenia przepisów przez organy państwa. Za sankcjonowane postępowanie uznano niewykonywanie obowiązków nałożonych przez przepisy DSL, odpowiedzialność ponosi wówczas osoba bezpośrednio zarządzająca lub pozostali pracownicy bezpośrednio odpowiedzialni. Sankcjonowanym postępowaniem jest także zachowanie pracowników państwowych zajmujących się zagadnieniami regulacyjnymi w zakresie bezpieczeństwa danych, polegające na zaniedbywaniu swoich obowiązków, nadużywaniu przyznanych uprawnień lub czerpania

zysku z zajmowanej pozycji. W obu przypadkach, odpowiednio art. 49 i 50 DSL nakazują karanie takiego postępowania zgodnie z właściwymi przepisami prawa.

Rozdział VI CSL zawiera rozbudowany katalog sankcji stosowanych w razie naruszenia poszczególnych przepisów CSL [558] . Pierwszym sankcjonowanym postępowaniem jest naruszenie przez operatora sieci art. 21 CSL, związanego z odpowiednim zabezpieczeniem sieci lub art. 25 CSL nakazującego niezwłoczną reakcję na ryzyka dla bezpieczeństwa sieci. Zgodnie z art. 59 CSL takie postępowanie operatora sieci uprawnia organ nadzorczy do nakazania poprawy postępowania oraz upomnienia operatora sieci. Jeśli działania poprawcze prowadzą do powstania szkody dla bezpieczeństwa sieci lub innych, podobnych konsekwencji albo operator sieci odmówi podjęcia działań naprawczych, wówczas organ nadzorczy nałoży na operatora sieci grzywnę między 10.000 a 100.000 yuan, jak również na osobę bezpośrednio odpowiedzialną w kwocie 5.000 a 50.000 yuan. Naruszenie przez operatora sieci związanego z infrastrukturą krytyczną obowiązków wynikających m.in z art. 34 i 38, a więc obowiązków w zakresie zabezpieczenie i przeglądu, wiąże się jedynie ze wzrostem grzywny nakładanej na operatora sieci do poziomu między 100.000 a 1.000.000 yuan, oraz na osobę bezpośrednio odpowiedzialną do poziomu między 10.000 a 100.000 yuan. Za odrębne naruszenie operatora sieci związanego z infrastrukturą krytyczną uznano przechowywanie danych sieciowych poza terytorium Chin lub ich udostępnianie podmiotom znajdującym się poza terytorium Chin. Zgodnie z art. 66 CSL właściwy organ nadzorczy powinien nakazać podjęcie działań naprawczych, upomnieć operatora sieci, skonfiskować uzyskane niezgodnie z prawem zyski oraz nałożyć karę grzywny w kwocie między 50.000 a 500.000 yuan. Dodatkowo właściwy organ nadzorczy może nakazać okresowego zawieszenia niektórych aktywności biznesowych, zaprzestania prowadzenia działalności do czasu poprawy, zamknięcie stron internetowych, anulowania licencji na wykonywanie niektórych aktywności biznesowych lub anulowania pozwolenia na prowadzenie działalności gospodarczej. Jednocześnie, osoba bezpośrednio zarządzająca i pozostałe osoby odpowiedzialne zostaną ukarane grzywną w kwocie między 10.000 a 100.000 yuan.

[558] Poza omówionymi przypadkami, rozdział VI CSL zawiera sankcje m.in. za naruszenia obowiązków, o których mowa w art. 46 i 48, związanych z odpowiedzialnością za strony internetowe i ich treść, dbałością o jakość informacji publikowanych i przesyłanych przez użytkowników sieci (w tym postępowanie z informacjami, których publikacja lub przesył są niezgodne z prawem), dbałością o jakość oprogramowania (w tym zakaz umieszczania w aplikacji lub oprogramowaniu informacji, których publikacja lub przesył są niezgodne z prawem).

Art. 64 CSL nakłada sankcje na operatorów sieci, a także dostawców produktów lub usług, którzy naruszają m.in. obowiązki wynikające z art. 41, 42 i 43 CSL, które dotyczą bezpośrednio ochrony danych osobowych. Naruszenie art. 41-43 CSL zostało uznane za naruszenie prawnej ochrony danych osobowych. Takie postępowanie pozwala właściwemu organowi nadzorczemu do nakazania poprawy postępowania oraz zastosowania zamiast lub obok nakazu poprawy upomnienia, konfiskaty uzyskanych niezgodnie z prawem zysków, kary grzywny odpowiadającej kwocie stanowiącej do dziesięciokrotności niezgodnie z prawem uzyskanych zysków[559], oraz kary grzywny na osobę bezpośrednio zarządzającą i pozostałe osoby odpowiedzialne w kwocie między 10.000 a 100.000 yuan. Jeśli okoliczności naruszenia prawnej ochrony danych osobowych są poważne, właściwy organ nadzorczy może nakazać okresowego zawieszenia niektórych aktywności biznesowych, zaprzestania prowadzenia działalności do czasu poprawy, zamknięcie stron internetowych, anulowania licencji na wykonywanie niektórych aktywności biznesowych lub anulowania pozwolenia na prowadzenie działalności gospodarczej. Odrębnie potraktowano naruszenie art. 44 CSL. Jeśli dojdzie do kradzieży, innego niezgodnego z prawem pozyskania, niezgodnej z prawem sprzedaży danych osobowych, które nie stanowią przestępstwa, organy bezpieczeństwa publicznego skonfiskują niezgodnie z prawem uzyskane zyski oraz nałożą grzywnę w kwocie stanowiącej do dziesięciokrotności niezgodnie z prawem uzyskanych zysków[560].

Katalog sankcji w CSL odnosi się także do niewypełniania obowiązków w zakresie bezpieczeństwa sieci wynikających z CSL przez organy państwa. Krąg podmiotów objętych art. 72 CSL obejmuje operatorów sieci związanych ze sprawami rządowymi organów państwa. Sankcją, które może nałożyć organ nadrzędny nad organem naruszającym lub inny właściwy organ jest nakazania poprawy postępowania. Osoba bezpośrednio zarządzająca oraz pozostały personel bezpośrednio odpowiedzialny będą także ukarani, przy czym art. 72 CSL nie określa na czym ma to polegać. Dodatkowym, sankcjonowanym postępowaniem organów państwa jest niezgodne z prawem wykorzystywanie informacji, w tym danych osobowych. Przepisy CSL nakazują organom nadzorczym odpowiednio postępować z informacjami pozyskiwanymi w toku wykonywanych czynności, w tym czynności nadzorczych. Artykuł 30 CSL zakazuje organom nadzorczym wykorzystywania pozyskanych

[559] Brak zysków nie pozbawia właściwego organu nadzorczego uprawnienia do nałożenia kary grzywny, ponieważ, w takiej sytuacji, określono maksymalną kwotę grzywny na poziomie 1.000.000 yuan.
[560] Brak zysków nie pozbawia właściwego organu nadzorczego uprawnienia do nałożeni kary grzywny, ponieważ, w takiej sytuacji, określono maksymalną kwotę grzywny na poziomie 1.000.000 yuan.

informacji w innym celu niż ochrona cyberbezpieczeństwa, w zakresie niezbędnym do jego realizacji. Rozwinięciem tego zakazu jest art. 45 CSL. Przywołany przepis, adresowany do organów nadzorczych i ich personelu, nakazuje stosowanie ścisłej ochrony poufności danych osobowych, informacji prywatnych oraz sekretów handlowych, które pozyskują w trakcie swoich zadań. Jednocześnie, art. 45 CSL zakazuje niezgodnego z prawem udostępniania, w tym sprzedaży i ujawniania takich informacji. Naruszenie obowiązku, o którym mowa w art. 30 CSL wiąże się z odpowiedzialnością osoby bezpośrednio zarządzającej oraz personelu bezpośrednio zaangażowanego i nałożenia sankcji zgodnie z art. 73 CSL. Podobnie potraktowano zaniedbywanie obowiązków przez organ nadzorczy, jak również przekraczanie uprawnień czy faworyzowanie, które, jeśli nie stanowią przestępstwa, stanowią podstawę do nałożenia sankcji, zgodnie z przepisami praw, jednakże art. 73 CSL nie wskazuje, kto i jakie kary może zastosować.

Wszelkie naruszenia obowiązków wynikających z CSL wiążą się ze swego rodzaju ostracyzmem. Art. 71 CSL nakazuje, aby informacja o naruszeniu była umieszczona w aktach kredytowych oraz została upubliczniona zgodnie z przepisami prawa i przepisami administracyjnymi.

Przetwarzanie danych z naruszeniem przepisów PIPL lub przetwarzanie danych bez wypełnienia obowiązków, które nakłada na administratora PIPL stanowi pierwszy rodzaj sankcjonowanego działania. W takiej sytuacji organ nadzorczy dysponuje karą nakazania poprawy postępowania, konfiskaty niezgodnych z prawem zysków oraz karą zawieszenia na poziomie prowincjonalnym lub wypowiedzenia usług świadczonych za pośrednictwem aplikacji przetwarzających dane niezgodnie z prawem. Odmowa wykonania nakazu poprawy postępowania uprawnia organ nadzorczy do zastosowania dodatkowej kary grzywny w kwocie do 1.000.000 yuan. Osoby bezpośrednio odpowiedzialne za zarządzanie bezpieczeństwem danych i pozostali pracownicy bezpośrednio odpowiedzialni mogą być ukarani grzywną w kwocie od 10.000 do 100.000 yuan. PIPL przewiduje także kwalifikowaną postać naruszenia swoich przepisów, która polega na poważnym naruszeniu przepisów lub niewypełnianiu obowiązków. Wówczas, organ nadzorczy na poziomie prowincjonalnym lub wyższym może orzec nakaz poprawy postępowania, konfiskaty niezgodnych z prawem zysków oraz nałożyć grzywnę w kwocie nie większej niż 50.000.000 yuan lub 5% rocznego obrotu, a nadto może dojść nałożenia kary zawieszenia niektórych aktywności biznesowych lub zaprzestania prowadzenia działalności do czasu poprawy. Organ nadzorczy na poziomie

prowincjonalnym lub wyższym może także złożyć raport właściwemu organowi i wnioskować cofnięcia przyznanych licencji administracyjnych lub cofnięcia pozwolenia na prowadzenie działalności gospodarczej. Kwalifikowana postać naruszenia oznacza surowsze kary dla osoby bezpośrednio odpowiedzialnej za zarządzanie bezpieczeństwem danych i pozostałych pracowników bezpośrednio odpowiedzialnych w postaci grzywny w kwocie od 100.000 do 1.000.000 yuan. Jednocześnie, organ nadzorczy może zakazać takim osobom zajmowania przez określony czas stanowiska dyrektorskiego, nadzorczego, managera wyższego stopnia lub inspektora danych osobowych.

Jeśli dojdzie do działań niezgodnych z PIPL, podobnie jak w CSL, takie działania zostaną podane do publicznej wiadomości oraz zostaną wprowadzone do teczek kredytowych, prowadzonych przez właściwe organy.

Odrębnie potraktowano naruszenie przepisów PIPL przez organy państwowe. Niewypełnienie obowiązków nałożonych przez PIPL będzie skutkowało nałożeniem kary nakazu poprawy postępowania Do nałożenia kary na organy państwowe jest uprawniony organ, który nadzoruje organ państwowy[561] lub organ nadzorczy Osoba bezpośrednio odpowiedzialna za zarządzanie bezpieczeństwem danych i pozostali pracownicy bezpośrednio odpowiedzialni zostaną ukarani zgodnie z przepisami szczególnymi. Natomiast, jeśli organ nadzorczy opuści się zaniedbania obowiązków, nadużycia władzy lub uprzywilejowanego traktowania, które nie stanowi jeszcze przestępstwa, będzie ukarany zgodnie z przepisami szczególnymi. Naruszenie przepisów PIPL, które jednocześnie powoduje naruszenie systemu bezpieczeństwa publicznego oznacza dopuszczalność nałożenia kary naruszenia systemu bezpieczeństwa publicznego, zgodnie z przepisami szczególnymi. W zakresie odpowiedzialności karnej za naruszenie przepisów PIPL, które jednocześnie wypełnia znamiona przestępstwa następuje odwołanie do przepisów szczególnych.

Sankcje, o których mowa CSL, DSL i PIPL są podobne do siebie. Ustawy przewidują kilkuelementowy katalog kar, stosowanych w zależności od rodzaju naruszenia. Przepisy nie określają jednoznacznie dyrektyw wymiaru kary, pozostawiając swobodę organom nadzoru. Penalizowane działania dotyczą naruszeń poszczególnych przepisów ustaw chińskiego prawa ochrony danych osobowych. W przypadku DSL i CSL dostrzegalne ograniczenie do naruszeń w zakresie bezpieczeństwa sieci lub danych, w tym danych osobowych. Katalog kar dzieli się na kary nakładane na administratora

[561] W ramach typowego nadzoru nad organami administracji.

danych oraz kary nakładane na osoby bezpośrednio zaangażowane w przetwarzanie danych. Oprócz kar pieniężnych, przepisy dopuszczają skorzystanie przez organ nadzorczych. Mimo rozbudowanego katalogu sankcji, sankcje finansowe, o których mowa w przepisach PIPL są uznawane za zbyt łagodne[562]. Podobnie traktowane są sankcje finansowe wynikające z CSL, choć w tym wypadku autorzy uznają, że możliwość skorzystania z innych sankcji innych niż finansowe rekompensuje niedoskonałości tych ostatnich[563].

5. Kryterium trzecie: kompetentny, niezależny organ nadzorczy

5.1. Uwagi wstępne

Istnienie niezależnego organu nadzorczego, którego szeroko pojęte zasoby pozwalają na rzeczywiste i skuteczne funkcjonowanie, jest istotnym elementem systemu prawnego państwa trzeciego, gwarantującym faktyczne przestrzeganie przyjętych zasad ochrony danych osobowych. Ażeby mówić o organie nadzorczym w rozumieniu RODO konieczne jest omówienie trzech cech organu nadzorczego, do których zaliczają się właściwość, przyznane uprawnienia oraz przymiot niezależności.

5.2. Właściwość organu nadzorczego

Właściwość chińskiego organu nadzorczego budzi wiele wątpliwości. Powodem takiego stanu rzeczy jest brak jednoznaczności ustawodawcy chińskiego w zakresie przyznania konkretnemu podmiotowi funkcji organu nadzorczego.

W ogólnym ujęciu, art. 7 DSL nakazuje państwu ochronę praw i interesów związanych z danymi, które dotyczą jednostek i organizacji. To państwo ma zachęcać do rozsądnego, efektywnego i zgodnego z prawem wykorzystywania danych oraz zapewniać zgodny z prawem, wolny przepływ danych. Zadaniem państwa jest także promowanie rozwoju gospodarki cyfrowej, dla której dane stanowią kluczowy czynnik działania i rozwoju. W ramach prowadzonych działań promocyjnych państwo, zgodnie z art. 9 DSL, powinno wspierać rozwój propagowania i edukacji w zakresie bezpieczeństwa danych. Nadto, DSL zawiera rozbudowany katalog zadań państwa, w szczególności dotyczących strategii, dalszego i bardziej szczegółowego rozwoju wykorzystywania danych, w tym rozwoju badań naukowych, rozwoju usług obejmujących oceny bezpieczeństwa i certyfikację, wprowadzenia systemu zarządzania transakcjami danymi[564]. W ramach części ustawy zawierającej ogólne przepisy, w art. 5-7 DSL omówiono syntetycznie

[562] C. Yan Wang: *Governing Data Markets*…, s. 42.
[563] E. Pernot-Leplay: *China's Approach on*…, s. 91.
[564] Por. art. 13 – 20 DSL.

podstawowe zadania poszczególnych organów nadzorczych, wraz z ich podziałem między poszczególne organy. DSL wyróżnia cztery typy organów nadzorczych: wiodący organ centralny; organy regionalne i departamenty; organy bezpieczeństwa publicznego i bezpieczeństwa narodowego oraz krajowy departament cyberbezpieczeństwa i informatyzacji. W żadnym z przepisów DSL ustawodawca nie wymienia nazwy konkretnego organu, ograniczając się jedynie do nazewnictwa organów przez nazwę ich podstawowego zadania. Dla ustalenia, który z funkcjonujących organów stanowi jednocześnie jeden z organów, o którym mowa w DSL należy sięgnąć do całokształtu przepisów prawa chińskiego. Jak wskazuje doktryna, w ten sposób możliwe jest ustalenie, że krajowy departament cyberbezpieczeństwa i informatyzacji to w istocie CAC[565]. Jeśli chodzi o departamenty, wymieniane obok organów regionalnych, można zakładać, że chodzi o departamenty sektorowe. Do takiego wniosku prowadzi art. 6 DSL, który wyjaśnia, że departamenty, które kierują m.in. takimi działami jak telekomunikacja, transport, finanse, środowisko, zdrowie, edukacja i technologia, w ramach nadzoru nad konkretnym działem, jednocześnie nadzorują zadania w zakresie bezpieczeństwa danych.

Opis organu nadzorczego wynikający z przepisów CSL, co do zasady, odpowiada opisowi zastosowanemu w DSL. W rozdziale I, który zawiera przepisy ogólne, najpierw, w art. 3 – 7 oraz 13 CSL określono zadania związane z bezpieczeństwem sieci nałożone na państwo, przy czym są to zadania o znacznym stopniu ogólności[566]. Następnie, w art. 8 CSL przedstawiono zasadniczy podział zadań nadzorczych pomiędzy poszczególne departamenty. Krajowy departament cyberbezpieczeństwa i informatyzacji uznano za podmiot odpowiedzialny za całościowe zarządzanie, w tym planowanie, i nadzór nad działaniami związanymi z bezpieczeństwem sieci. Departamenty Rady Państwa, w tym zwłaszcza departament telekomunikacji oraz departament bezpieczeństwa publicznego w ramach wykonywanych obowiązków mają zarządzać i nadzorować bezpieczeństwem sieci zgodnie z przepisami CSL oraz pozostałymi przepisami prawa i przepisami administracyjnymi[567]. W przypadku poszczególnych departamentów lokalnych władz na poziomie hrabstwa lub powyżej, właściwe przepisy państwowe określą zakres ich zadań w zarządzaniu i nadzorem nad

[565] Por. przypis nr 5 do tłumaczenia art. 5 DSL – DigiChina: *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*. 29.06.2021. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ [dostęp: 15.09.2022].
[566] Za takie zadania uznano m.in. promowanie konkretnego zachowania podczas korzystania z sieci (art. 6 DSL) czy obowiązek stworzenia i rozwijania strategii cyberbezpieczeństwa.
[567] Jednym z konkretnych obowiązków jest planowanie, zarządzanie oraz nadzór nad ochroną informacji związanych z infrastrukturą krytyczną.

cyberbezpieczeństwem. Do pewnego stopnia, przedstawiony opis odpowiada opisowi zawartemu w PIPL, z zastrzeżeniem, że w CSL nie zawarto jednoznacznego wyjaśnienia, że wymienione podmioty zbiorczo nazywa departamentami wypełniającymi obowiązki z zakresu bezpieczeństwa sieci[568]. Mimo tego, ustawodawca kilkukrotnie posługuje się podobnym terminem. Tym samym, dla podtrzymania jasności przekazu, tak jak miało to miejsce do tej pory, będę używał terminu organ nadzoru lub organ nadzorczy.

Sposób, w jaki PIPL odnosi się do organu nadzorczego przypomina strukturę znaną z przepisów RODO, ponieważ przepisy PIPL skupiają się na kompetencjach, w jakie został wyposażony organ nadzorczy. Niemniej jednak, PIPL tak, jak przywołane dotychczas ustawy, w art. 60 PIPL dokonuje podziału kompetencji nadzorczych między poszczególne podmioty. Wśród tych podmiotów znalazły się krajowy departament cyberbezpieczeństwa i informatyzacji, kompetentne departamenty Rady Państwa, jak również departamenty lokalnych władz na poziomie hrabstwa lub powyżej [569]. Należy podkreślić, że art. 60 PIPL w ostatnim zdaniu, na potrzeby PIPL wszystkie wymienione departamenty określa zbiorczo jako departamenty wypełniające obowiązki z zakresu ochrony danych osobowych. To właśnie ten termin jest używany w większości przepisów PIPL, choć zdarzają się wyjątki, kiedy ustawodawca wiąże konkretne uprawnienie z konkretnym departamentem, czego przejawem jest art. 62 PIPL, o którym mowa poniżej. Dla zachowania jasności przekazu, tak jak miało to miejsce do tej pory, będę używał terminu organ nadzoru[570].

Konsekwencją zastosowanej techniki prawodawczej jest trudność z ustaleniem, który z powyższych podmiotów jest (faktycznym) organem nadzorczym. Niektórzy autorzy za organ nadzorczy uznają CAC[571]. Zdaniem G. Greenleafa i S. Livingstona, na przykładzie przepisów CSL, nie sposób mówić o wyznaczeniu organu nadzorczego w rozumieniu RODO, przy czym, w ocenie autorów, funkcje nadzorcze pełni MIIT[572]. O MIIT jako podmiocie związanym z nadzorem wspomina także C. You, jednak jej zdaniem MIIT wraz z m.in. chińskim bankiem centralnym odpowiadają za wdrożenie przepisów ochrony danych osobowych (w tym wypadku PIPL), zaś zadaniem CAC jest

[568] Tak, jak w PIPL.
[569] Podział administracyjny Chin, co do zasady, składa się z czterech poziomów, czyli poziomu prowincjonalnego, poziomu regionalnego (niekiedy określanego jako poziom prefekturalny), poziomu hrabstwa oraz poziomu odpowiadającego gminom w rozumieniu europejskim.
[570] Wymiennie, z terminem organ nadzorczy.
[571] W. Chaskes: *The Three Laws*…, s. 1175; Wang, J. Zhang, N. Lassi i in.: *Privacy Protection in*…, s. 4; C. You: *Half a Loaf*…, s. 21.
[572] G. Greenleaf, S. Livingston: *China's New Cybersecurity*…, s. 8.

całościowe administrowanie ochroną danych osobowych[573]. Z kolei R. Creemers podkreśla, że mimo wyczerpującego opisu kompetencji organu nadzorczego, PIPL nie wskazało, który z podmiotów pełni funkcję zasadniczego organu nadzorczego[574]. Można więc mówić o wielopodmiotowym nadzorze, z CAC jako organem koordynującym.

5.3. Zadania i kompetencje organu nadzorczego

Tak jak opis właściwości, tak i opis zadań oraz kompetencji organu nadzorczego w Chinach wynika z przepisów DSL, CSL i PIPL.

W DSL, zadania wiodącego organu centralnego związane są z ogólnymi działaniami mającymi na celu realizację polityki w zakresie bezpieczeństwa danych na poziomie krajowym, m.in. poprzez wsparcie we wdrażaniu właściwych strategii czy polityk, a także całościowe koordynowanie najważniejszych zadań w zakresie bezpieczeństwa danych na poziomie krajowym. W przypadku organów regionalnych i departamentów, ich zadaniem jest dbałość, w tym w zakresie bezpieczeństwa, o dane wytworzone i zebrane dane na terytorium obejmującym ich obszar właściwości[575]. Do zadań organów bezpieczeństwa publicznego i bezpieczeństwa narodowego zaliczono nadzór nad bezpieczeństwem danych w zakresie obowiązków wykonywanych zgodnie z przepisami DSL i innych ustaw, w tym przepisów administracyjnych. Koordynowanie bezpieczeństwa danych oraz powiązanego z nim nadzoru, zgodnie z przepisami prawa i przepisami administracyjnymi, stanowi zadanie na krajowego departamentu cyberbezpieczeństwa i informatyzacji. Oprócz opisanych powyżej ogólnych zadań, DSL poświęca wiele miejsca opracowaniu i wdrożeniu systemu bezpieczeństwa danych oraz mechanizmu oceny ryzyka, w tym mechanizmu reagowania na zagrożenia, o czym mowa w art. 21-24 DSL. System bezpieczeństwa ma wprowadzać stopniową ochronę danych, w zależności od ich wagi dla gospodarczego i socjalnego rozwoju, wpływu na bezpieczeństwo narodowe, sprawy publiczne prawa i interesy jednostek lub organizacji, jeśli miałoby dojść do wycieku, zniszczenia, nieuprawnionej modyfikacji, nielegalnego dostępu lub nielegalnego użycia danych. Krajowy mechanizm koordynacji bezpieczeństwa danych ma koordynować kategoryzację danych przez poszczególne departamenty i zapewniać ściślejszą ochronę danych. Każdy region i departament powinien określić katalog ważnych danych dla danego regionu, departamentu czy branży.

[573] C. You: *Half a Loaf*…, s.21.
[574] R. Creemers: *China's Emerging Data*…, s. 14.
[575] Odpowiednio, w ramach nadzorowanego działu.

Danymi, które tworzą trzon krajowych danych są m.in. dane związane z bezpieczeństwem narodowym, żywotnością gospodarki krajowej, ważnymi aspektami życia ludzi czy ważnymi interesami publicznymi. Takie dane wymagają systemu zarządzania zapewniającego ściślejszą ochronę. Wspomniany mechanizm ryzyka ma być scentralizowanym, efektywnym narzędziem służącym ocenie ryzyka bezpieczeństwa danych oraz jego raportowania, monitorowania, współdzielenia informacji oraz wczesnego ostrzegania. Skoordynowane wsparcie zapewnianiające działanie tego mechanizmu stanowi zadanie poszczególnych departamentów. W naturalny sposób, z mechanizmem ryzyka wiąże się mechanizm reagowania na zagrożenia. Wdrożone plany mają zapewnić odpowiednio skoordynowane działania, które sprowadzają się do podjęcia odpowiednich kroków zaradczych zapobiegających zwiększeniu szkody, usunięciu luki, która spowodowała materializację zagrożenia oraz niezwłoczną publikację stosownego ostrzeżenia o zdarzeniu. Ostatnim elementem całościowego systemu zarządzania jest stworzenie systemu przeglądu bezpieczeństwa danych oraz przeprowadzanie przeglądów w zakresie bezpieczeństwa narodowego co do tych czynności przetwarzania, które mają lub mogą mieć wpływ na bezpieczeństwo narodowe. Decyzje dotyczące przeglądu bezpieczeństwa mają przymiot ostatecznych, jeśli zostały wydane zgodnie z prawem. DSL nakłada na państwo także ogólne zadania w zakresie kontroli transferów danych. Art. 25 DSL nakazuje wprowadzenie kontroli eksportu danych, które należą do kategorii kontrolowanych danych. Celem kontroli eksportu ma być zapewnienie bezpieczeństwa narodowego oraz wypełnianie międzynarodowych zobowiązań. Jednakże, podjęcie przez państwo trzecie lub jego część (region) wobec Chin działań o charakterze dyskryminacyjnym lub ograniczającym uprawnia Chiny do podjęcia identycznych działań w oparciu o zasadę wzajemności. Zgodnie z art. 26 DSL chodzi o dyskryminację lub inne ograniczenia związane z działaniami odnoszącymi się do danych, takie jak przykładowo inwestowanie w dane lub handel danymi, jak również m.in. inwestycje w technologie związane z danymi.

W przepisach CSL zabrakło jednak wydzielonego rozdziału, który omawiałby uprawnienia organów nadzorczych. Zamiast tego, uprawnienia nadzorcze zostały rozsiane po poszczególnych przepisach CSL[576]. Rozdział II CSL pośrednio odnosi się do

[576] O części z nich była już mowa, jak m.in. o obowiązku raportowania właściwemu organowi nadzorczemu przez operatorów sieci (por. art. 25 CSL) oraz jego kwalifikowanej postaci, raportowaniu przez operatorów sieci związanych z infrastrukturą krytyczną w związku z przeprowadzonym przeglądem (por. art. 38 CSL). Dodatkowo można wskazać na przeprowadzanie przeglądu w zakresie bezpieczeństwa produktów i usług nabywanych przez operatorów sieci związanych z infrastrukturą krytyczną (art. 35 CSL); konkretne zadania kierowane do poszczególnych departamentów związane z nadzorem nad infrastrukturą krytyczną

zagadnień związanych z nadzorem. W większości przepisy zostały zaadresowane do państwa, z wyjątkiem częściowo art. 15 oraz art. 16 i 19 CSL, w których niektóre obowiązki skierowano do konkretnych podmiotów[577]. Charakter obowiązków i zadań, o których mowa w rozdziale II CSL, można podsumować jako rozwój, promocję i edukację. Na szczególną uwagę zasługuje art. 50 CSL, umiejscowiony w rozdziale poświęconym ochronie danych osobowych. W przywołanym przepisie krajowy departament cyberbezpieczeństwa i informatyzacji wraz z pozostałymi, właściwymi departamentami został uprawniony do sprawowania nadzoru nad zgodnością z prawem bezpieczeństwa informacji w sieci[578]. Jeśli organ nadzoru ustali, że doszło do niezgodnych z prawem lub przepisami administracyjnymi publikacji lub przesyłu informacji, nakaże operatorowi sieci przerwanie przesyłu danych, podjęcie stosownych działań naprawczych[579]. Jako przykład takich działań wskazano usunięcie informacji. Odrębnie potraktowano sytuację, gdy przesyłane informacje pochodzą spoza terytorium Chin. Wówczas organ nadzoru nakaże operatorowi sieci podjęcie odpowiednich działań zmierzających do zablokowania transmisji danych.

Jak już wspominałem, opis kompetencji organu nadzorczego zajmuję szczególną pozycję w PIPL. Podstawowy podział kompetencji nadzorczych zawarty w art. 60 PIPL rozpoczyna wskazanie zadań krajowego departamentu cyberbezpieczeństwa i informatyzacji, do których należą planowanie i koordynowanie prac w zakresie ochrony danych osobowych, a także zarządzanie i nadzór. Kompetentne departamenty Rady Państwa w ramach wykonywanych obowiązków mają zarządzać i nadzorować ochroną danych osobowych zgodnie z przepisami PIPL oraz pozostałymi przepisami prawa i przepisami administracyjnymi. Jeśli chodzi o departamenty lokalnych władz na poziomie hrabstwa lub powyżej, będą one zarządzały i nadzorowały ochroną danych osobowych w zakresie zadań, który określają właściwe przepisy państwowe. W art. 61 PIPL rozwinięto ogólne zadania organów nadzorczych. Zawarte wyliczenie

(m.in. okresowa analiza ryzyka), których koordynacją ma się zająć krajowy departament cyberbezpieczeństwa i informatyzacji (art. 39 CSL); przepisy rozdziału V CSL, gdzie określono uprawnienia organów nadzorczych w związku z monitoringiem i reagowaniem na zagrożenia dla bezpieczeństwa sieci, zwłaszcza art. 56 CSL, który wyraźnie łączy uprawnienia dotyczące reakcji na wysokie ryzyko lub incydent bezpieczeństwa z pozycją właściwego departamentu w hierarchii (uprawnienie przyznano tylko departamentom zlokalizowanym co najmniej na poziomie prowincjonalnym).

[577] To jest m.in. do Rady Państwa (art. 15 CSL) czy do Rady Państwa, rządów na poziomie prowincji, regionów autonomicznych oraz rządów miast znajdujących się pod bezpośrednim zwierzchnictwem władz centralnych (art. 16 CSL).

[578] Mimo, że rozdział IV CSL odnosi się do ochrony danych osobowych, w art. 50 CSL skorzystano z szerszego pojęcia, bezpieczeństwa informacji. Tym samy, art. 50 CSL nie ogranicza się do ochrony danych osobowych.

[579] Dodatkowo, operator sieci powinien udokumentować zdarzenie, przechowując odpowiednie dowody.

zadań – obowiązków nie ma charakteru zamkniętego w tym sensie, że zawiera odesłanie do przepisów szczególnych, w których mogą być przewidziane dodatkowe zadania - obowiązki. Organy nadzorcze mają propagować ochronę danych osobowych, która może przybierać formę edukacji. Jednocześnie, organy nadzoru doradzają i nadzorują administratorów danych. Kolejnym zadaniem – obowiązkiem organów nadzoru jest rozpoznawanie skarg związanych z ochroną danych osobowych; jako osobne zadanie – obowiązek potraktowano prowadzenie postępowań i rozstrzyganie spraw w zakresie niezgodnego z prawem przetwarzania danych osobowych. Nadto, organy nadzorcze przeprowadzają oceny postępowania z danymi, w tym w zakresie przyjętych procedur i publikują ich wyniki. Odrębnie potraktowano krajowy departament cyberbezpieczeństwa i informatyzacji, dla którego w art. 62 PIPL określono szczególne zadania. Art. 62 PIPL plasuje krajowy departament cyberbezpieczeństwa i informatyzacji na wyższym poziomie w hierarchii pozostałych departamentów, ponieważ ma on koordynować promowanie przez pozostałe departamenty rezultatów prac, o których mowa w art. 62 PIPL. Katalog prac otwiera opracowywanie standardów przetwarzania danych osobowych o charakterze ogólnym, jak i szczególnym. Za szczególne przypadki uznano administratorów danych o małym rozmiarze, przetwarzanie danych związanych z nowymi technologiami, danymi wrażliwymi oraz przetwarzanie danych w ramach aplikacji stosujących takie rozwiązania jak m.in. rozpoznawanie twarzy czy sztuczna inteligencja. Zadaniem poszczególnych departamentów jest także propagowanie stworzenia uspołecznionego systemu usług ochrony danych osobowych, wspieranie poszczególnych instytucji w przeprowadzaniu ocen i certyfikacji w zakresie ochrony danych osobowych. Należy także dążyć do udoskonalania systemu raportowania i systemu skargowego. Za odrębne zadanie uznano wspieranie badań i rozwoju technologii umożliwiających weryfikację identyfikacji w bezpieczny i wygodny sposób wraz z promowanie prac nad publicznymi usługami, gdzie taka weryfikacja byłaby stosowana. Poza ogólnymi, podstawowymi zadaniami organów nadzorczych, w PIPL określono także ich konkretne uprawnienia. Zawarty w art. 63 PIPL katalog w pierwszej kolejności uprawnia organy nadzoru do prowadzenia postępowań wyjaśniających w zakresie weryfikowanego przetwarzania danych, w tym do przesłuchiwania zainteresowanych stron; pozyskiwania odpowiedniego materiału dowodowego, zwłaszcza dokumentów związanych z przetwarzaniem danych osobowych; przeprowadzania inspekcji w miejscu przetwarzania danych; prowadzenia śledztwa w sytuacji niezgodnego z prawem przetwarzania danych osobowych.

W ramach wykonywania przyznanych uprawnień, organy nadzoru mogą kontrolować sprzęt oraz przedmioty związane z przetwarzaniem danych osobowych. Jeśli istnieją dowody wskazujące na to, że sprzęt lub przedmioty mogły służyć do nielegalnego przetwarzania danych osobowych, wówczas kontrolujący, po pisemnym poinformowaniu kierownika organu nadzorczego, który reprezentuje, i za jego zgodą, może zabezpieczyć sprzęt lub przedmioty lub je skonfiskować. Z wykonywaniem opisanych uprawnień art. 63 PIPL wiąże po stronie podmiotów nadzorowanych i innych osób zaangażowanych, obowiązek współpracy i wspierana organów nadzoru, skorelowany z zakazem utrudniania wykonywania czynności przez organy nadzorcze. Co do zasady, obowiązek współpracy będzie się aktualizował tylko w tych przypadkach, gdy organy nadzorcze korzystają ze swoich uprawnień zgodnie z prawem. Szczególne uprawnienie organów nadzorczych wiąże się ze swego rodzaju funkcją prewencyjną. Jej pierwszy aspekt sprowadza się do mitygacji ryzyka. Jeśli w toku czynności organ nadzoru zidentyfikuje wysokie ryzyko związane z przetwarzaniem danych osobowych, w tym ich bezpieczeństwem, wówczas może, zgodnie z art. 64 PIPL przeprowadzić konsultacje z właściwym przedstawicielem administratora lub jego pełnomocnikiem. Ewentualnie organ nadzoru może polecić administratorowi przeprowadzenie audytu przetwarzania danych osobowych z wykorzystaniem wykwalifikowanego podmiotu zewnętrznego. Jednocześnie, administrator powinien podjąć odpowiednie środki zaradcze, wprowadzając właściwe poprawki i eliminując źródło ryzyka. Ten sam schemat postępowania znajdzie zastosowanie, jeśli w ramach wykonywania swoich zadań organ nadzoru odkryje, że doszło do naruszenia ochrony danych osobowych. Drugi aspekt funkcji prewencyjnej dotyczy przeciwdziałania naruszeniom prawa. Ujawnienie w toku wykonywanych czynności przetwarzania niezgodnego z prawem, które uzasadnia podejrzenie popełnienia przestępstwa, zgodnie z art. 64 zdanie drugie PIPL, nakazuje organowi nadzoru niezwłoczne przekazanie sprawy kompetentnym organom ścigania, które podejmą odpowiednie kroki.

5.3.1. Transfer danych osobowych jako okoliczność wpływająca na zadania organu nadzorczego

W odniesieniu do zagadnienia transferów danych osobowych, obok DSL, CSL i PIPL[580], dodatkowy podział kompetencji między poszczególne organy nadzoru przedstawiają wytyczne CAC dotyczące transferów danych.

[580] Artykuł 1 Wytycznych CAC dotyczących transferów danych jako swoją podstawę prawną wskazuje CSL, DSL i PIPL.

Podział zadań w wytycznych CAC dotyczących transferów danych skupia się na procedurze oceny bezpieczeństwa transferu. Art. 7 wytycznych CAC dotyczących transferów danych wyjaśnia, w jakim terminie i które zadania mają wykonać organy prowincjonalne i organy na szczeblu krajowym. Organy prowincjonalne są zobowiązane do weryfikacji kompletności otrzymanego wniosku o przeprowadzenie oceny, a w razie potrzeby, do zwrotu wniosku administratorowi celem uzupełnienia dostrzeżonych braków. Co do zasady, termin na wykonanie tych działań to 5 dni roboczych od dnia doręczenia wniosku organowi. Kompletny wniosek organ prowincjonalny przekazuje krajowemu departamentowi cyberbezpieczeństwa i informatyzacji. W terminie 7 dni roboczych od przekazania dokumentów, organ akceptuje bądź odmawia akceptacji wniosku o ocenę, o czym informuje administratora danych. Wykrycie braków na późniejszym etapie, zgodnie z art. 11 wytycznych CAC dotyczących transferów danych uprawnia krajowy departament cyberbezpieczeństwa i informatyzacji do wezwania administratora do uzupełnienia dokumentacji, pod rygorem zakończenia procedury oceny. Celowe dostarczenie organowi fałszywych dokumentów będzie równe negatywnemu zakończeniu oceny oraz będzie skutkowało wszczęciem właściwego postępowania, celem pociągnięcia administratora do odpowiedzialności. Krajowy departament cyberbezpieczeństwa i informatyzacji odgrywa także zasadniczą rolę na etapie właściwej oceny. Zgodnie z art. 12, w ciągu 45 dni roboczych od dnia wysłania potwierdzenia przyjęcia wniosku do administratora lub w dłuższym terminie, jeśli charakter sprawy jest skomplikowany lub zaszła potrzeba pozyskania dodatkowych materiałów lub poprawienia materiałów. O wydłużeniu terminu należy powiadomić administratora danych. Krajowy departament cyberbezpieczeństwa i informatyzacji będzie również rozpatrywał odwołanie od decyzji w sprawie oceny, złożone przez administratora. Termin na złożenie odwołania to 15 dni roboczych od dnia otrzymania pierwotnej decyzji. Decyzja podjęta w wyniku ponownego rozpatrzenia jest ostateczna. Krajowy departament cyberbezpieczeństwa i informatyzacji jest również uprawniony do nakazania zakończenia transferu danych. Taka sytuacja będzie miała miejsce, zgodnie z art. 17 wytycznych CAC dotyczących transferów danych, gdy organ ustali, że uprzednio zatwierdzony transfer danych nie odpowiada wymaganiom w zakresie bezpieczeństwa transferów. Administrator, po otrzymaniu powiadomienia krajowego departamentu cyberbezpieczeństwa i informatyzacji, może wprowadzić niezbędne zmiany odpowiadające wymaganiom w zakresie bezpieczeństwa danych i wystąpić o ponowną

ocenę. Skorzystanie z tej ścieżki jest możliwe, jeśli kontynuacja transferu jest dla administratora konieczna.

5.4. Niezależność organu nadzorczego

Żaden z przepisów chińskiego prawa ochrony danych osobowych nie odnosi się do zagadnienia niezależności organu nadzoru. W przeciwieństwie do przepisów RODO, zarówno DSL, CSL, jak i PIPL pomijają kwestię pozycji organu nadzoru, gwarancji jego niezależności, tak osobowych, jak i finansowych zasobów. Zdaniem doktryny w Chinach nie było i nie ma niezależnego organu nadzoru w rozumieniu europejskim[581]. Pozycja CAC oraz pozostałych organów nadzoru nie pozwalać więc mówić o niezależnym organie[582]. Zwłaszcza uwzględniając fakt, że odrębność CAC od Rady Państwa została potwierdzona dopiero w 2018 r.[583], przy czym wciąż nie sposób jednoznacznie stwierdzić, czy CAC to samodzielna agencja rządowa[584]. Nie dziwi więc spostrzeżenie o bliskich związkach CAC z organami politycznymi[585].

Mając na uwadze powyższe, wciąż aktualna pozostaje uwaga o utrzymaniu sektorowości nadzoru. Zasadniczym źródłem sektorowości są przepisy CSL[586], ale także DSL[587]. Natomiast to niejasności wynikające w CSL są uznawane za przyczynę utrzymujących się sporów w zakresie właściwości między CAC a MPS[588]. W całościowym ujęciu można się zgodzić ze stanowiskiem o braku dedykowanego, specjalnego organu nadzoru[589], o czym świadczy szeroki zakres właściwości CAC oraz przypisywanie nadzoru nad ochroną danych osobowym pozostałym organom, wyłącznie jako ich dodatkowego zadania. Niemniej jednak, zdaniem H. Dorwarta to CAC jako organ, dla którego regulacja sieci stanowi podstawowe zadanie, może górować nad innymi organami[590]. Prowadzi do sytuacji, gdzie *de facto* właściwość, jak i poszczególne uprawnienia nadzorcze zostaje przekazane różnym organom władzy[591]. Skoro różnym organom przypisywane są zbliżone, czy wręcz takie same uprawnienia, nie można

[581] B. Zhao: *Connected Cars in*…, s. 18; G. Greenleaf: *China Issues a*…, s. 10.
[582] L. Belli, D.Doneda: *Data Protection in*…, s. 11.
[583] Guowuyuan guanyu jigou shzhi de tongzhi (国务院关于机构设置的通知) [*Obwieszczenie Rady Państwa Chińskiej Republiki Ludowej w sprawie powołania instytucji*]. 24.03.2018. http://www.gov.cn/zhengce/content/2018-03/24/content_5277121.htm [dostęp: 3.06.2024].
[584] Por. Ibidem.
[585] G. Pyo: *An Alternate Vision*…, s. 236.
[586] E. Pernot-Leplay: *China's Approach on*…, s. 90; S. Wang Han, A.B. Munir: *Information Security Technology*…, s. 540.
[587] P. Cai, L. Chen: *Demystifying Data Law*…, s. 81.
[588] R. Creemers: *China's Emerging Data*…, s. 10.
[589] Y. Shao: *Personal Information Protection*…, s. 239–240.
[590] H. Dorwart: *Platform Regulation from*…, s. 384.
[591] Y. Yin: *Conflict and Balance*….; Y-L. Liu, L. Huang, W. Yan i in.: *Privacy in AI*…, s. 6–7.

wykluczyć, że ich działania będą na siebie nachodziły[592], w konsekwencji czego rzeczywista skuteczność nadzoru będzie niewielka. Nie można bowiem zapominać, że DSL, CSL i PIPL przypisują organom państwowym konkretne uprawnienia, które w oderwaniu od problematyki wielopodmiotowego nadzoru, można by uznać za bliskie uprawnieniom przyznanym organom nadzoru przez RODO.

Słaby nadzór zewnętrzny powoduje, że w praktyce o wiele ważniejszą rolę odgrywa samoregulacja, w tym nadzór realizowanych przez samych administratorów weryfikujących postępowanie pozostałych uczestników rynku[593]. O ile idea rozproszonego nadzoru współrealizowanego przez poszczególnych administratorów, którzy niejako mają nadzorować się nawzajem, jest ciekawym uzupełnieniem systemu ochrony danych osobowych, o tyle nie można uznać, że w ten sposób niwelowane są braki właściwego nadzoru, a więc niezależnego i kompetentnego organu[594].

6. Kryterium czwarte: środki prawne przyznane osobie, której dane dotyczą na wypadek naruszenia danych osobowych

Środki prawne przyznane jednostce to kolejna gwarancja egzekwowalności zasad ochrony danych osobowych, ale w szczególnych warunkach, jakimi są przypadki naruszenia danych osobowych.

Artykuł 12 DSL przyznaje każdej jednostce lub organizacji prawo do złożenia skargi lub złożenia doniesienia do właściwego organu nadzorczego. Przedmiotem skargi lub doniesienia mogą być działania niezgodne z przepisami DSL. Wniesienie skargi lub złożenie doniesienia nakazuje organowi nadzorczemu zapewnienie poufności danych osoby lub podmiotu skarżącego, jak również ochronę ich pozostałych praw i interesów. Otrzymana skarga lub doniesienia powinny zostać niezwłocznie rozpatrzone, z zastosowaniem właściwych przepisów prawa. Jednostka może również skorzystać z pozostałych ścieżek ochronnych przewidzianych przez przepisy. Artykuł 52 DSL wyjaśnia, że naruszenie przepisów DSL, które wywołało szkodę stanowi podstawę do pociągnięcia do odpowiedzialności cywilnej zgodnie z prawem. Jednocześnie, jeśli naruszenie przepisów DSL powoduje naruszenie zarządzania bezpieczeństwem publicznym, to takie naruszenie będzie karane sankcjami administracyjnymi za naruszenie bezpieczeństwa publicznego, zgodnie z właściwymi przepisami. W ten sam sposób należy postąpić, jeżeli naruszenie przepisów DSL wypełnia znamiona

[592] H. Dorwart: *Platform Regulation from*…, s. 383.
[593] B. Zhao and F. Yang: *Mapping the development*…, s. 3; X. Lin, H. Liu, Z. Li i in.: *Privacy Protection of*…, s. 18.
[594] D. Hanlin: *The System Position*…, s. 155.

przestępstwa, wszczynając właściwą procedurę. Natomiast naruszenie przepisów DSL powodujące naruszenie państwowego zarządzania bezpieczeństwem, wymaga zastosowania sankcji administracyjnych wynikających z właściwych przepisów dotyczących bezpieczeństwa publicznego. Jeśli naruszenie stanowi przestępstwo, jego ściganie nastąpi zgodnie z właściwymi przepisami. Zgodnie z art. 51 DSL, uzyskanie danych w drodze kradzieży lub z wykorzystaniem innych nielegalnych metod, jak również przetwarzanie danych w sposób ograniczający lub eliminujący konkurencję, przetwarzanie danych powodujące szkodę dla praw lub interesów jednostek lub organizacji powinno być karane zgodnie z właściwymi przepisami prawa lub przepisami administracyjnymi.

Zgodnie z art. 14 CSL, jednostki mogą zgłosić departamentowi cyberbezpieczeństwa i informatyzacji lub innemu właściwemu departamentowi, a więc organom nadzoru, postępowanie zagrażające bezpieczeństwu sieci. Po otrzymaniu zgłoszenia, organ nadzorczy powinien niezwłocznie zająć się sprawą, postępując zgodnie z przepisami prawa. Zdaniem Greenleafa i Livingstona, zakres pojęcia bezpieczeństwo sieci obejmuje także przetwarzanie danych osobowych, co powoduje, że art. 14 CSL jest źródłem prawa do skargi[595]. W tym względzie, art. 14 CSL podkreśla konieczność zachowania poufności informacji związanych z rozpoznawaną sprawą oraz ochrony prawi i interesów osoby zgłaszającej. Jeśli sprawa nie należy do zakresu właściwości organu nadzorczego, do którego została złożona, należy ją przekazać organowi właściwemu. O możliwości złożenia skargi wspomina także art. 49 CSL. Przepis jednoznacznie zobowiązuje operatora sieci do stworzenia systemu przyjmowania i obsługi skarg. O jego funkcjonowaniu, w tym zwłaszcza o możliwych sposobach złożenia skargi należy odpowiednio poinformować osoby, których dane dotyczą. Oprócz prawa do skargi, przepisy CSL wspominają o odpowiedzialności za szkodę wyrządzoną naruszeniem przepisów CSL. W takiej sytuacji, zgodnie z art. 74 CSL znajdą zastosowanie zasady odpowiedzialności cywilnej wynikające z właściwych przepisów praw. Natomiast, jeśli naruszenie przepisów CSL skutkuje naruszeniem państwowego zarządzania bezpieczeństwem, stosuje się sankcje administracyjne wynikające z właściwych przepisów dotyczących bezpieczeństwa publicznego, zaś jeśli naruszenie stanowi czyn zabroniony, będzie ścigane zgodnie z właściwymi przepisami. Przepisy CSL regulują także zręby postępowania w razie działalności zagrażającej krytycznej infrastrukturze, powodujące poważne konsekwencje, której źródłem są

[595] G. Greenleaf, S. Livingston: *China's New Cybersecurity*…, s. 8.

instytucje, organizacje lub jednostki spoza terytorium Chin. Jako przykłady takiej działalności wymieniono ataki, naruszenia lub działania wywołujące szkodę. Zgodnie z art. 75 CSL, takie podmioty zostaną pociągnięte do odpowiedzialności zgodnie z właściwymi przepisami prawa. Nadto, departamenty Rady Państwa związane z bezpieczeństwem publicznym wraz z pozostałymi departamentami mogą zastosować odpowiednie sankcje, w tym zamrożenie aktywów.

Mimo, że c.k.c. jednoznacznie wprowadza obowiązek prawnej ochrony danych osobowych, to z tą ochroną nie wiążą się odrębne, dedykowane środki prawne. Tak, jak w przypadku pozostałych przepisów chińskiego prawa ochrony danych osobowych, tak i w przypadku c.k.c., to ogólne zasady odpowiedzialności będą stanowiły źródło środków przyznanych jednostce. Należy zauważyć, że przepisy c.k.c. dotyczące ochrony danych osobowych opierają się o dualistyczne ujęcie. Jak już wspominałem, art. 1034 c.k.c. dotyka problematyki ochrony informacji prywatnych. Skutkiem wyodrębnienia dodatkowej kategorii informacji jest odrębny reżim ochronny, który polega na tym, że w pierwszej kolejności, do ochrony informacji prywatnych stosuje się przepisy o ochronie prawa do prywatności[596]. Dopiero w razie braku takich przepisów, należy stosować przepisy o ochronie danych osobowych. W oparciu o opisany model ochrony, informacje prywatne będą chronione m.in. przez art. 1032 c.k.c., który zakazuje osobom trzecim naruszania chronionej prawem prywatności w szczególności, poprzez szpiegowanie, ujawnianie (informacji) czy publikowanie. O ile w teorii takie rozwiązanie jawi się jako przejaw dodatkowej ochrony jednostki, o tyle jej praktyczne zastosowanie może budzić wątpliwości. Nie bez znaczenia pozostają uwagi zgłaszane przez doktrynę odnośnie do charakteru ochrony danych osobowych w c.k.c. [597] Sedno problemu sprowadza się do kwalifikacji prawnej ochrony danych osobowych, a więc uznania tej ochrony za prawo podmiotowe, na wzór prawa do prywatności[598] lub wyłącznie za prawnie chroniony interes jednostki[599]. Pojawia się także trzecia ścieżka interpretacyjna, uznającą ochronę prywatności i ochronę danych osobowych za dwa odrębne interesy jednostki[600]. Przyjęcie którejkolwiek z interpretacji, jako wiodącej, pociąga za sobą

[596] X. Li: *Information Privacy Protection*…, s. 318; S. Cui, P. Qi: *The Legal Construction…*, s. 13–14.
[597] B. Qu, C. Huo: *Privacy, National Security*…, s. 174–177; X. Duoye: *The Civil Code*…, s.197; Y. Shao: *Personal Information Protection*…, s. 231, 234.
[598] X. Li: *Information Privacy Protection*…, s. 318–319; B. Zhao, F. Yang: *Mapping the development*…, s. 11; por. G. Yang: T*heoretical Justification and Construction of the Prohibition on Right to Personal Information*. „Application of Law", 2023, nr 3.
[599] L. Zhang: *"Personal Information of*…, s. 3; X. Lin, H. Liu, Z. Li i in.: *Privacy Protection of*…, s. 3.
[600] X. Li *Information Privacy Protection*…, s. 318; L. Zhang: *"Personal Information of*…, s. 2–4; C. Wang, J. Zhang, N. Lassi i in.: *Privacy Protection in*…, s.11; X. Lin, H. Liu, Z. Li i in.: *Privacy Protection of*…, s. 19.

daleko idące skutki w zakresie ochrony przed naruszeniami. Niemniej jednak, część doktryny podkreśla, że ochrona danych osobowych i ochrona prywatności przenikają się, zaś tym co je odróżnia jest właśnie charakter ochrony, którą zapewniają [601]. Wynika to z zasadniczo różnych skutków, które wywoła naruszenie ochrony danych osobowych lub naruszenie prywatności, w konsekwencji czego dla obu sytuacji należy przewidzieć odmienne środki ochrony, gdzie dla ochrony danych osobowych bardziej odpowiednie są środki prewencyjne, w tym środki związane z kontrolą jednostki nad swoimi danymi[602]. Przedstawione rozumienie pozwala przyjąć, że to odmienne skutki naruszenia prywatności i ochrony danych osobowych kierowały ustawodawcą chińskim. Nie usuwa to jednak podstawowej wątpliwości związanych z brakiem definicji informacji prywatnych, o których była już mowa, a które bezpośrednio wpływają na stosowanie właściwego reżimu ochronne. Zapewne, rozstrzygającym dla zastosowania konkretnego reżimu kodeksowej odpowiedzialności będzie stan faktyczny sprawy, którego nie ułatwia podejście do ochrony prywatności, a także i danych osobowych zakorzenione w chińskim społeczeństwie. Dla obywateli chińskich wykorzystywanie niektórych danych osobowych jest niezbędne dla zwyczajowego życia w społeczeństwie, przy czym tym co wyróżnia pragmatyczne spojrzenie, jest fakt godzenia się na potencjalnie słabszą ochronę niektórych danych[603]. To z kolei otwiera drogę do argumentacji na rzecz wykazania, że konkretne informacje nie są blisko związane z ochroną prywatności[604], a przez to ich ochrona na podstawie przepisów o ochronie prywatności nie jest zasadna.

Jako bardziej pewna jawi się ochrona jednostki na podstawie przepisów c.k.c. statuujących reżim odpowiedzialności deliktowej. Szerokie ujęcie jej zakresu, o którym stanowi art. 1164 c.k.c. powoduje, że naruszenia prawnej ochrony danych osobowych nie są *ex definitione* wykluczone spod ochrony, tym bardziej, że ani c.k.c., ani pozostałe ustawy, nie określiły własnych zasad odpowiedzialności cywilnej [605]. Zresztą, taka konstrukcja funkcjonowała w chińskim systemie prawnym zanim doszło do wdrożenia przepisów chińskiego prawa ochrony danych osobowych[606]. Jednocześnie, art. 1164 c.k.c.

[601] R.Y. Gao: *Personal Information Protection*…, s. 175; 178; 180–181; X. Duoye: *The Civil Code*…, s. 193–194; Y. Shao: *Personal Information Protection*…, s. 232; 234–236.
[602] X. Li: *Information Privacy Protection*…, s. 332–333; S. Cui, P. Qi: *The Legal Construction*…, s.14.
[603] Y. Duan: B*alancing the Free*…, s. 6; X. Li: *Information Privacy Protection*…, s. 327–328; L. Zhang*"Personal Information of*…, s*. 1*2; X. Chen, Y. Zhang: *The Construct of*…, s. 45–52; F. Feng, X. Wang, T. Chen: *Analysis of the Attributes*…, s. 10; H. Roberts: *Informational Privacy with*…, s. 7.
[604] J. Liu, H. Zhao: *Privacy Lost: Appropriating Surveillance Technology in China's Fight against COVID-19*. „Business Horizons", 2021, nr 64, s.743; Y. Tang, L.Wang: *How Chinese Web*…, s.988.
[605] L. Yu, B. Ahl: *China's Evolving Data*…, s. 304.
[606] C. You: *Half a Loaf*…, s. 7.

uzupełnia ogólny, ochronny charakter art. 111 c.k.c.[607] Odpowiedzialność deliktowa w c.k.c., zgodnie z art. 1165, jest oparta na zasadzie winy. Ustalenie czy dana osoba ponosi winę za wyrządzenie szkody powinno się odbyć zgodnie z zasadami określonymi przez przepisy prawa. Na szczególną uwagę zasługuje art. 1170 c.k.c., który odnosi się do współodpowiedzialności dwóch lub więcej podmiotów. Co do zasady, w przypadku działania wielu podmiotów, c.k.c. dąży do ustalenia jednego, konkretnego sprawcy, który będzie ponosił odpowiedzialność także za działania pozostałych sprawców. Dopiero, gdy ustalenie jednego sprawcy nie jest możliwe, wówczas znajdzie zastosowanie odpowiedzialność solidarna wszystkich współsprawców. Skutkiem ustalenia odpowiedzialności za wyrządzenie szkody jest ponoszenie odpowiedzialności odszkodowawczej, której szczegółowe zasady zostały zawarte w art. 1179 i n. c.k.c. Potencjalnie, z przypadkami naruszenia ochrony danych osobowych mogą się wiązać także szczególne przepisy regulujące odpowiedzialność deliktową. Zgodnie z art. 1191 c.k.c. pracodawca ponosi odpowiedzialność za szkody wyrządzone przez pracownika. Zakres odpowiedzialności pracodawcy obejmuje działania pracownika podejmowane w ramach wykonywania swoich obowiązków. Pracodawca, który poniósł odpowiedzialność, może kierować roszczenia regresowe wobec pracownika, jeśli ten wyrządził szkodę umyślnie lub w wyniku rażącego niedbalstwa. W razie przydziału pracownika do wykonywania obowiązków u innego pracodawcy, inny pracodawca ponosi odpowiedzialność za szkodę wyrządzoną przez pracownika w ramach wykonywania swoich obowiązków. Nie bez znaczenia jest również art. 1194 c.k.c., odnoszący się do odpowiedzialności użytkowników sieci oraz dostawców sieci. Zarówno użytkownik, jak i dostawca, który narusza prawa lub interesy jednostki za pośrednictwem sieci ponosi odpowiedzialność deliktową, przy czym przepisy szczególne mogą wprowadzać odrębne zasady jej ponoszenia. Rozwinięciem art. 1194 c.k.c. jest art. 1195 c.k.c., który przyznaje poszkodowanemu uprawnienia związane z deliktem wyrządzonym za pośrednictwem sieci. Poszkodowany jest wówczas uprawniony do żądania od dostawcy sieci podjęcia takich działań, jak usunięcie, zablokowanie lub odłączenie od sieci. Zawiadomienie kierowane do dostawcy ma zawierać dane identyfikujące osobę sprawcy oraz dowód prima facie wyrządzonego deliktu. Po otrzymaniu zawiadomienia, dostawca sieci niezwłocznie informuje użytkownika sieci o zawiadomieniu oraz podejmuje niezbędne środki, opierając się na dostarczonych dowodach i charakterze

[607] O charakterze art. 111 c.k.c. wspomna Y. Lixin - Y. Lixin: *From the General Provisions of Civil Law to the General Rules of Civil Law: A Historic Leap*, „Social Sciences in China". 2020, nr 41, s. 19.

świadczonej za pośrednictwem sieci usługi. Brak niezwłocznego działania po stronie dostawcy sieci powoduje, że odpowiada on solidarnie ze sprawcą, za szkodę[608]. Jednocześnie, złożenie błędnego zawiadomienia, które spowodowało szkodę oznacza odpowiedzialność deliktową osoby zawiadamiającej, chyba że przepisy szczególne stanowią inaczej. Szczególną ochronę przyznano także pacjentowi. Art. 1222 c.k.c. jako okoliczność powodującą odpowiedzialność deliktową instytucji medycznej w stosunku do pacjenta, w pkt 3 wymienia utratę, ujawnienie lub niezgodne z prawem zniszczenie danych dotyczących historii leczenia pacjenta. Takie ujęcie odpowiedzialności instytucji medycznej wiąże się z art. 1225 c.k.c., który nakłada na instytucję medyczną wraz z jej pracownikami obowiązek właściwego prowadzenia oraz przechowywania dokumentacji pacjenta, składającej się na historię jego leczenia. Również art. 1226 c.k.c. nakazuje instytucji medycznej oraz jej pracownikom ochronę prywatności i danych osobowych pacjenta, w tym zachowanie poufności. Ujawnienie prywatności lub danych osobowych pacjenta poprzez ich publiczne udostępnienie, bez uprzedniej zgody pacjenta, stanowi podstawę odpowiedzialności deliktowej instytucji medycznej. Pacjent jest uprawniony do żądania wglądu w dokumentację oraz kopii jego danych stanowiących historię jego leczenia, na które to żądania instytucja medyczna powinna odpowiedzieć niezwłocznie.
W praktyce, ustalenie szkody związanej z naruszeniem ochrony danych osobowych przysparza wiele trudności. Jak wyjaśnia H. Dorwart, niektóre działania podmiotów naruszających ochronę danych osobowych, do których zalicza m.in. pozyskiwania danych bez zgody jednostki czy ich sprzedaż na rzecz innych podmiotów, w cywilistycznym ujęciu nie wywołają szkody majątkowej[609]. Zawodzi więc w tych sytuacjach, gdy nie doszło jeszcze do naruszenia kwalifikowanego jako delikt[610]. Natomiast szeroko pojęta problematyka odpowiedzialności za szkody niemajątkowe w praktyce sądów chińskich także nie może być postrzegana jako wolna od wad, w szczególności na tle odpowiedzialności za takie szkody, realizowanej względem organów państwowych, gdzie niewielka liczba spraw jest uznawana za potwierdzenie jej wątpliwej skuteczności w tym aspekcie[611]. Niemniej jednak to właśnie obowiązek ustalenia szkody i jej rozmiaru w przypadku naruszenia danych osobowych jest

[608] Art. 1195 c.k.c. wyraźnie ogranicza odpowiedzialność dostawcy sieci tylko do szkody przewyższającej pierwotną szkodę wyrządzoną przez użytkownika sieci.
[609] H. Dorwart: *Platform Regulation from*…, s. 373.
[610] R.Y. Gao: *Personal Information Protection*…, s. 171.
[611] H. Xing: *Government Data Sharing*…, s. 77.

postrzegany przez doktrynę jako zasadniczy problem ochrony jednostki na podstawie reżimu odpowiedzialności deliktowej[612].

Uprawnienia przyznane jednostce przez PIPL zasadniczo odpowiadają technice legislacyjnej wykorzystanej w omówionych aktach prawnych chińskiego prawa ochrony danych osobowych. Art. 65 PIPL przyznaje każdej jednostce lub organizacji prawo do złożenia skargi lub zgłoszenia niezgodnego z prawem przetwarzania danych do organu nadzorczego. Po otrzymaniu skargi lub zgłoszenia, organ nadzorczy powinien niezwłocznie rozpatrzyć je zgodnie z prawem oraz powiadomić osobę skarżącą lub zgłaszającą o wyniku postępowania. Dla ułatwienia wykonywania prawa do skargi, organ nadzorczy jest obowiązany do opublikowania metod kontaktu, umożliwiających składanie skarg lub zgłoszeń. Przepisy PIPL wprowadzają także autonomiczną podstawę dochodzenia roszczeń odszkodowawczych. Zgodnie z art. 69 PIPL przetwarzanie danych osobowych, naruszające prawa lub interesy związane z ochroną danych osobowych, może skutkować powstaniem szkody. Administrator może wyłączyć swoją odpowiedzialność, jeśli wykaże, że nie ponosi winy za działanie będące źródłem szkody. Zakres odpowiedzialności administratora wyznacza wielkość szkody. Wielkość szkody ustala się w oparciu rozmiar straty poniesionej przez poszkodowanego lub o rozmiar zysków, jakie wskutek wyrządzonej szkody osiągnął administrator. Gdyby określenie straty poniesionej przez poszkodowanego lub zysków, które osiągnął administrator było utrudnione, wówczas zakres odpowiedzialności wyznacza całokształt okoliczności sprawy. Zdaniem niektórych autorów, ustalenie właściwej wartości interesów jednostki, które ucierpiały wskutek naruszenia jej danych osobowych jest utrudnione, co potwierdza brak jednolitego stanowiska sądów chińskich[613]. Tym samym, zastrzeżenie odnośnie do ustalenia rozmiaru szkody w ramach reżimu odpowiedzialności deliktowej w c.k.c. pozostają aktualne także w PIPL.

Szczególnym środkiem ochrony praw i interesów jednostki jest art. 70 PIPL. Przywołany przepis przyznaje uprawnienie do wytoczenia pozwu zbiorowego. Przesłanką wytoczenia powództwa zbiorowego jest przetwarzanie danych osobowych w sposób niezgodny z przepisami PIPL, które powoduje naruszenie praw lub interesów wielu osób. W takiej sytuacji, Prokuratorzy Ludowi, organizacje ochrony praw konsumentów wskazane przez przepisy ustawowe oraz organizacje wskazane przez krajowy

[612] D. Xiaodong: *Personal Data Protection: Rethinking the Reason, Nature and Legal Framework*. W: *Paradigms of Internet Regulation in the European Union and China.* C. Krönke, M.W. Müller, W. Yu. Nomos, Baden-Baden 2018, s. 107; C. You: *Half a Loaf*…, s. 8.

[613] Por. L. Zhao, Y.Wei, Y. Liu: *Determination of the Amount of Damages in Civil Public Interest Litigation in the Field of Personal Information Protection*. „Chinese Procurators", 2023, nr 4.

departament cyberbezpieczeństwa i informatyzacji mogą wytoczyć powództwo przed sądem (ludowym), zgodnie z właściwymi przepisami prawa.

Dodatkową podstawą do złożenia skargi do organu nadzorczego są wytyczne CAC dotyczące transferów danych, których art. 16 uprawnia jednostkę lub organizację do złożenia skargi co najmniej do organu prowincjonalnego, na transfer danych przeprowadzany z pogwałceniem wytycznych CAC dotyczących transferów danych.

Przepisy chińskiego prawa ochrony danych osobowych, zasadniczo zawierają w sobie środki prawne odpowiadające środkom, o których mowa w RODO. Z wyjątkiem c.k.c., każda z ustaw przyznaje jednostce przyznane prawo do złożenia skargi do właściwego organu nadzoru, a także prawo do odszkodowania za szkodę wynikającą z naruszenia ochrony danych osobowych. Nadto, naruszenie ochrony danych osobowych, które wypełnia znamiona przestępstwa, ma być ścigane zgodnie z przepisami prawa karnego. O ile w teorii środki przyznane jednostce wydają się być porównywalne ze środkami wynikającymi z RODO, o tyle praktyka, w tym zwłaszcza praktyka sądów chińskich dostarcza wielu wątpliwości. Doktryna zauważa, że także w przypadku postępowań sądowych związanych z ochroną danych osobowych, należy się spodziewać rozstrzygnięcia odpowiadającego aktualnym oczekiwaniom politycznym [614] . Dodatkowo, nawet jeśli dojdzie do naruszenia ochrony danych osobowych przez duży podmiot, bardziej prawdopodobnym jest, że taka sprawa będzie rozpoznawana przez organy administracji publicznej, ponieważ postępowania sądowe dotyczą raczej mniejszym podmiotów[615]. Innymi słowy, w pierwszej kolejności zostaną wykorzystane środki zarezerwowane dla organów administracji publicznej, a dopiero gdy te zawiodą, sprawy dużych podmiotów, zwłaszcza dużych platform internetowych, będą rozpoznane przez właściwy sąd[616]. Przy tak zarysowanym krajobrazie chińskiego systemu ochrony danych osobowych, nie lada zaskoczeniem jest skuteczność ochrony realizowanej za pośrednictwem przepisów prawnokarnych. W szczególności, doktryna wyjaśnia, że penalizowane postępowanie wiąże się już z niewielką ilością danych osobowych dotkniętych naruszeniem, przy czym uznaje się, że dla podmiotów publicznych przetwarzających dane osobowe można mówić o bardziej surowych wymaganiach, odpowiadających połowie ilości danych dla podmiotów prywatnych[617]. Uzupełniona

[614] H. Dorwart: *Platform Regulation from*…, s. 378; A.S. Sweet, C. Bu: *Breaching the Taboo? Constitutional Dimensions of China's New Civil Code*. „Asian Journal of Comparative Law", 2023, nr 3, s. 11.
[615] H. Dorwart: *Platform Regulation from*…, s. 378; por. także: H. Dorwart: *Chinese Data Protection*….
[616] H. Dorwart: *Platform Regulation from*…, s. 383.
[617] Y. Feng: *The future of*…, s. 71.

środkami realizowanymi przed organami publicznymi, ochrona wynikająca z przepisów prawa karnego niewątpliwie stawia jednostkę w lepszej sytuacji, jednak wciąż gorszej w porównaniu z sytuacją podmiotów danych, o której mowa w RODO.

7. Kryterium piąte: dostęp organów państwowych do danych osobowych na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego

7.1. Uwagi ogólne

Wypracowane w orzecznictwie TSUE kryterium dostępu organów państwowych do danych osobowych wskazuje na problematykę pozycji jednostki w relacji z organami państwa. Nie jest to jednak zwyczajna sytuacja, ponieważ, w szerokim ujęciu, dotyczy działań związanych z zapewnieniem bezpieczeństwa publicznego. Co oczywiste, zagadnienie dostępu organów do danych dotyczy także przepisów chińskiego prawa ochrony danych osobowych.

Zasadnicze zainteresowanie dostępem do danych osobowych przez władze wiąże się z możliwością realizacji działań klasyfikowanych jako prewencja, która przybiera postać inwigilacji. Innymi słowy, chodzi o zapobieganie wystąpieniu zdarzeń niepożądanych. Problem wszechobecnej inwigilacji jest szczególnie dostrzegany w przypadku Chin. Jednak dla władz chińskich, dostęp do danych osobowych, powiązany z inwigilacją, mają charakter instrumentalny. Zdaniem doktryny, jednym z celów powszechnej inwigilacji w Chinach jest ułatwienie zarządzania państwem i jego obywatelami.[618] Wiąże się to z odpowiednim przekazem adresowanym do społeczeństwa. Y. Ka wyjaśnia, że dostęp do danych jest przedstawiany jako jedno z narzędzi zastępujących typowe narzędzia sił porządkowych[619]. W ten sposób, negatywnie postrzegane, zwiększanie uprawnień sił porządkowych, jest faktycznie wykonywane właśnie za pomocą dostępu do danych[620]. Jednocześnie, rosnące wskaźniki przestępczości są wykorzystywane jako argumentacja na rzecz konieczności ograniczenia wolności, przejawiającej się w dostępie organów do danych, w zamian za

[618] M. Hvistendahl: *A Revered Rocket Scientist Set in Motion China's Mass Surveillance of Its Citizens. Qian Xuesen's Systems Engineering Permeates Many Facets of Chinese Society*. 14.03.2018. https://www.science.org/content/article/revered-rocket-scientist-set-motion-china-s-mass-surveillance-its-citizens [dostęp: 28.03.2023]; por. Y-J. Chen, C-F. Lin, H-W. Liu: *"Rule of Trust,,,*; B. Aho, R. Duffield: *Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China*. „Economy and Society", 2020, nr 49, s. 187; Y. Feng: *The future of*…, s. 67; J. Liu: *China's data localization*…, s. 95; I. Qian, M. Xiao, P. Mozur i in.: *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State*. 21.06.2022. https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html [dostęp: 28.03.2023]; I. Calzada: *Citizens' Data Privacy*…, s. 1137; B. Zhao, F. Yang: *Mapping the development*…, s. 2.

[619] Y. Ka: *Inside China's Surveillance State, Built On High Tech And A Billion Spies*. 1.11.2022. https://worldcrunch.com/culture-society/china-surveillance-cameras [dostęp: 28.03.2023].

[620] Ibid.

wyższy poziom bezpieczeństwa[621]. Z. Yang podkreśla, że taka narracja prowadzi do najlepszych wyników, ponieważ Chińczycy są skłonni przystać na ograniczenie ich wolności i prywatności w imię bezpieczeństwa[622]. W ocenie B. Zhao i F. Yanga, wynika to z uznawania bezpieczeństwa publicznego jako jednej z podstawowych wartości[623]. Co istotne, powyższe nie oznacza aprobaty dla swobodnego dostępu do danych realizowanego przez podmioty prywatne. Zdaniem niektórych autorów, wraz z przedstawioną narracją, władze chińskie dokonują swego rodzaju przedefiniowania prywatności, wskutek którego państwo oraz jednostki stoją na straży działań podmiotów prywatnych chcących uzyskać dostęp do danych[624]. Konkretnym przejawem takich działań jest kształt poszczególnych ustaw związanych z ochroną prywatności, a więc CSL[625], DSL[626] i PIPL[627], gdzie to podmioty prywatne są poddawane daleko idącym ograniczeniom[628].

Dostęp organów państwa do danych osobowych, sprzężony z narzędziami inwigilacji stanowi powszechne zjawisko w Chinach. Komentatorzy podkreślają jednak, że pomimo omówionego powyżej poparcia obywateli dla ograniczania ich prywatności, władze chińskie bynajmniej nie dążą do transparentności w tym zakresie, co czasem utrudnia udowodnienie stosowania czy istnienia narzędzi inwigilujących[629]. W. Chaskes porównuje to zjawisko do czarnej skrzynki, której sposób działania jest znany wyłącznie wybranym podmiotom, czyli w przypadki Chin, organom władzy[630]. Nie oznacza to całkowitego braku dowodów. O faktycznym dostępie organów do danych osobowych można mówić m.in. na przykładzie:

---

[621] Ibid; Z. Yang: *The Chinese Surveillance State Proves That the Idea of Privacy Is More "Malleable" than You'd Expect*. 10.10.2022. https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/ [dostęp: 28.03.2023].
[622] Por. Ibidem.
[623] B. Zhao, F. Yang: *Mapping the development*…, s. 6; por. także D. Wawra, K. Kindsmüller, M. Tawfiq i in.: *Cultural influences on personal data disclosure decisions. Chinese Perspectives*. „University of Passau Institute for Law of the Digital Society Research Paper Series", 2022, nr 22–09.
[624] A. Gold: *China's New Privacy Law Leaves U.S. Behind*. 23.11.2021. https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [dostęp: 30.03.2023]; H. Roberts: *Informational Privacy with*…, s. 4; B. Allen-Ebrahimian: *China Makes Genetic Data a National Resource*. 29.05.2022. https://www.axios.com/2022/03/29/china-makes-genetics-data-national-resource [dostęp: 30.03.2023]; por. także: D. Wawra, K. Kindsmüller, M. Tawfiq i in.: *Cultural influences on*….
[625] G. Pyo: *An Alternate Vision*…, s. 272.
[626] Por. Z. Yang: *The Chinese Surveillance*….
[627] Por. C. Yan Wang: *Governing Data Markets*…; G. Greenleaf: *China Issues a*…, s. 12.
[628] Por. G. Greenleaf: *China Issues a*….
[629] Por. D. Gershgorn: *China's "Sharp*…; B. Zhao, F. Yang: *Mapping the development*…, s. 3–4; E. Feng: *"Surveillance State" Explores China's Tech and Social Media Control Systems*. 7.09.2022. https://www.npr.org/2022/09/07/1118105165/surveillance-state-explores-chinas-tech-and-social-media-control-systems [dostęp: 28.03.2023].
[630] W. Chaskes: *The Three Laws*…, s. 1182.

- żądania dostępu do danych zgromadzonych w ramach monitoringu wizyjnego hotelu należącego do sieci Marriott[631],
- żądania udostępniania przez gospodarzy lokali oferowanych za pośrednictwem platformy AirBnb danych dotyczących gości, z uwagi na rozciągnięcie zastosowania przepisów adresowanych do branży hotelarskiej na taką formę udostępniania miejsc noclegowych[632],
- cenzurowanie wiadomości wysyłanych przez użytkowników aplikacji Wechat, w tym także użytkowników zlokalizowanych poza granicami Chin[633],
- szeroko komentowaną problematykę dostępu władz chińskich do danych użytkowników platformy TikTok[634].

Nie bez znaczenia jest także bliska współpraca różnych podmiotów sektora prywatnego z organami państwa w zakresie dostarczania odpowiednich narzędzi, jak w przypadku Megvii[635], Hikvision[636], czy Dahua[637]. Mowa także o udostępnianiu danych osobowych, którego miały dokonać m.in. TikTok czy Wechat, ale także Apple[638]. Jak tłumaczą niektórzy autorzy, współpraca sektora prywatnego nie koniecznie oznacza dobrowolne zaangażowanie, a często stanowi wynik powszechnie znanej presji jaką wywierają władze chińskie na największe podmioty działające na ich terenie (w tym piastunów ich najwyższych organów)[639].

Potwierdzeniem zarówno roli, jaką odgrywa dostęp organów do danych w zarządzaniu państwem, a zarazem faktycznej aktywności władz chińskich w tym zakresie, były działania podjęte w ramach walki z pandemią Covid-19. Do takich działań należały m.in. konieczność założenia konta identyfikującego pasażera w celu korzystania z usług

---

631 Por. I. Qian, M. Xiao, P. Mozur i in.: *Four Takeaways From*….

632 BBC: *Airbnb to Give Chinese Authorities Guest Information*. 29.03.2018. https://www.bbc.com/news/business-43578948 [dostęp: 17.04.2023].

633 J. Whalen: *Chinese Censorship Invades the U.S. via WeChat*. 7.01.2021. https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban/ [dostęp: 30.06.2023]; J. Knockel, R. Xiong: *(Can't) Picture This 2. An Analysis of WeChat's Realtime Image Filtering in Chats*. *Research report*. [Dokument elektroniczny], University of Toronto, Toronto 2019, s. 122.

634 Por. J. Whalen: *Chinese Censorship Invades*…; Human Rights Watch: *Congressional-Executive Commission on China. Hearing on Techno-Authoritarianism: Platform for Repression in China and Abroad. Testimony of Yaqiu Wang Senior Researcher, China Human Rights Watch*. 17.11.2021. https://www.cecc.gov/sites/chinacommission.house.gov/files/documents/CECC%20Hearing%20Testimony%20-%20Yaqiu%20Wang.pdf [dostęp: 29.03.2023].

635 Por. I. Qian, M. Xiao, P. Mozur i in.: *Four Takeaways From*….

636 Por. Z. Yang: *The Chinese Surveillance*….

637 IPVM Team: *Dahua Provides "Uyghur Warnings" To China Police*. 9.02.2021. https://ipvm.com/reports/dahua-uyghur-warning [dostęp: 29.03.2023].

638 A. Kokas: *Cloud Control: China's 2017 Cybersecurity Law and Its Role in US Data Standardization*. 26.07.2019. https://ssrn.com/abstract=3427372 [dostęp: 8.05.2024], s. 11.

639 Por. D. Gershgorn: *China's "Sharp*…; por. Human Rights Watch: *Letter to House*….

metra[640], konieczność posługiwania się kodami QR, informującymi o bieżącym stanie zdrowotnym użytkownika, które faktycznie decydowały o jego swobodzie poruszania się[641] (którego dostawcą były podmioty sektora prywatnego), rozsyłanie wiadomości sms na temat poziomu rozprzestrzeniania się wirusa w miastach odwiedzonych przez konkretną osobą na przestrzeni ostatnich 15 lub 30 dni[642].

7.2. Podstawa prawna dostępu do danych

Jak już była o tym mowa, utylitarne podejście do dostępu organów do danych osobowych przejawia się w przepisach chińskiego prawa ochrony danych osobowych, których zastosowanie do omawianego zagadnienia budzi wątpliwości. Zdaniem doktryny, przepisy CSL chroniąc dane, jednocześnie są podstawą do ingerencji państwa[643]. Taka konstrukcja jest konsekwencją większego nacisku na bezpieczeństwo[644]. Stąd, jak twierdzą niektórzy autorzy, wpływ na stosowanie przepisów, w tym przepisów o ochronie danych osobowych wywiera bezpieczeństwo narodowe[645]. Niemniej jednak, to właśnie w ustawie związanej z danymi, w DSL, można się dopatrzyć ogólnego obowiązku udostępniania organom danych. Do takiego wniosku prowadzi analiza przepisów sankcyjnych, które za karane naruszenie przepisów DSL uznają odmowę współpracy z organami ścigania w zakresie udostępnienia danych, zgodnie z art. 35 DSL.

Punktem wyjścia dla omawianego zagadnienia są przepisy NSL. Szerokie pojęcie bezpieczeństwa narodowego, o którym mowa w art. 2 NSL, powoduje, że NSL może stanowić podstawę dostępu przez właściwe organy do danych osobowych. W pierwszej kolejności na uwagę zasługuje katalog obowiązków nałożonych na każdego obywatela i każdą organizację w celu zapewnienia bezpieczeństwa narodowego. Katalog jest rozwinięciem ogólnego obowiązku zapewnienia bezpieczeństwa narodowego, o którym mowa w art. 10 NSL. Art. 77 NSL oprócz nakazu przestrzegania przepisów prawa odnoszących się do bezpieczeństwa narodowego, czy wypełniania obowiązków nałożonych przez inne przepisy prawa lub przepisy administracyjne, nakłada na każdego obywatela lub organizację trzy zasadnicze obowiązki.

---

[640] J. Ko: *The Chinese Government Used Technology to Get a Grip on Coronavirus – and Take Control of Its People*. 14.04.2020. https://www.independent.co.uk/voices/coronavirus-china-technology-mass-surveillance-privacy-human-rights-a9463586.html [dostęp: 30.03.2023].
[641] Por. J. Ko: *The Chinese Government…*; por. F. Feng, X. Wang, T. Chen: *Analysis of the*….
[642] Por. J. Ko: *The Chinese Government…*.
[643] J.-A. Lee: *Hacking into China's*…, s. 100; L. Jacques: *Facial Recognition Technology and Privacy: Race and Gender - How to Ensure the Right to Privacy Is Protected*. „San Diego International Law Journal", 2021, nr 23, s. 134; A. Feder: *A Bull in a China Shop: How CFIUS Made TikTok a National Security Problem*. „Cardozo International & Comparative Law Review", 2022, nr 5, s. 660.
[644] A. Geller: *How Comprehensive Is*…., s. 1198; X. Fei: *National Security Considerations*…, s. 189, 193.
[645] P. Cai, L. Chen: *Demystifying Data Law*…, s. 88–90.

Pierwszy obowiązek to raportowanie zdarzeń, które mogą zagrażać bezpieczeństwu narodowemu. Drugi obowiązek to dostarczanie dowodów potwierdzających zaistnienie zdarzeń, które zagrażają bezpieczeństwu narodowemu. Trzeci obowiązek to szeroko pojętego niezbędnego wsparcia dla organów państwa, w tym organów wojskowych w związku z wykonywaniem zadań dla zapewnienia bezpieczeństwa narodowego. Z opisanym katalogiem obowiązków skorelowany jest zakaz podejmowania działań, które mogłyby zagrozić bezpieczeństwu narodowego oraz zakaz wspierania podmiotów, które zagrażają bezpieczeństwu narodowemu. Co do zasady, zgodnie z art. 78 – 79 NSL wspieranie państwa w zakresie bezpieczeństwa narodowego, w tym wdrożenia odpowiednich rozwiązań służących zapewnieniu bezpieczeństwa narodowego to także obowiązek przedsiębiorstw, organizacji społecznych oraz organizacji. Z zagadnieniem podstawy dostępu do danych jest związany art. 51 NSL. Przywołany przepis nakazuje państwu stworzenie systemu informacji wywiadowczych. System ma umożliwiać zbieranie, ocenę i wykorzystywanie informacji wywiadowczych. Pozyskiwanie informacji wywiadowczych, zgodnie z art. 52 NSL jest obowiązkiem organów państwa zajmujących się bezpieczeństwem publicznym, w tym organów narodowych oraz wojska. Dostęp organów do danych osobowych może wynikać także z art. 59 NSL, który nakazuje wdrożenie przez państwo systemu zarządzania nadzoru nad bezpieczeństwem narodowym. Przegląd bezpieczeństwa narodowego ma dotyczyć m.in. produktów i usług związanych z Internetem. Jako podstawą dostępu do danych osobowych można klasyfikować także art. 75 NSL, uprawniający organy państwa do podjęcia koniecznych środków i metod dla wykonania specjalnych zadań w zakresie bezpieczeństwa narodowego. Takie działania są uznane przez art. 75 NSL za zgodne z prawem.

Za podstawę dostępu organów państwa do danych osobowych wskazuje się także przepisy NIL [646] . Zakres wykorzystania informacji wywiadowczych jest szeroki. Artykuł 2 NIL oprócz wspierania działań w zakresie bezpieczeństwa narodowego, wskazuje także na podejmowanie kluczowych decyzji przez organy państwa czy kluczowe interesy narodowe. Art. 7 NIL nakazuje wszystkim obywatelom oraz organizacjom wspieranie państwa w wykonywaniu obowiązków związanych z informacjami wywiadowczymi, w tym poprzez współpracę z państwem. Spośród pozostałych przepisów, podstawą dostępu do danych mogą być art. 10 i 11 NIL.

[646] Por. Human Rights Watch: *Letter to House*…; T. Giladi Shtub, M.S. Gal: *The Competitive Effects*…, s. 11.

Należy także zauważyć, że zdaniem doktryny podstawą prawną dostępu organów do danych osobowych mogą być przepisy prawa karnego lub – ogólnie rzecz biorąc – ustaw antyszpiegowskich[647], czy prawa telekomunikacyjnego[648]. Tym samym, sytuacja jednostki jest dalece niepewna, skoro podstawą prawną uzyskania dostępu do jej danych są przepisy różnych ustaw, w efekcie czego, oprócz ustalenia czy działania organu były zgodne z przepisami ustawy, na podstawie której uzyskał dostęp do danych, niezbędna będzie także weryfikacja prawidłowości wyboru samej podstawy prawnej. Nadto, same przepisy wskazywane jako podstawa prawna dostępu organów do danych są na tyle ogólne, że ich interpretacja jest znacznie utrudniona, co wywołuje wątpliwości odnośnie do ich zgodności z zasadą proporcjonalności, przywoływaną przez TSUE.

7.3. Zakres dostępu organów do danych

Przepisy prawa będące podstawą dostępu organów do danych powinny wyznaczać zakres tego dostępu. W przypadku przepisów prawa chińskiego, wskazanie zakresu dostępu organów do danych zostało zredagowane w wysoce ogólny sposób.

Zgodnie z art. 7 NSL zapewnienie bezpieczeństwa narodowego ma się odbywać z poszanowaniem konstytucji, przepisów prawa, zasad socjalistycznych rządów prawa, praw człowieka oraz praw i interesów obywateli. Na zakres dostępu do danych może mieć także prewencyjne działanie, uznane przez art. 9 NSL za jedną z podstawowych zasad postępowania. Art. 83 NSL stanowi podstawę do ograniczenia praw i wolności obywateli w związku z zapewnianiem bezpieczeństwa narodowego. Treść przepisu przewiduje możliwość ograniczenia praw i wolności obywateli tylko, gdy zachodzi konieczność zastosowania specjalnych środków. Ustawodawca nie wyjaśnił czym są specjalne środki. Niemniej jednak, ich zastosowanie powinno odbywać się zgodnie z prawem i ograniczać się tylko do tego co konieczne ze względu na zapewnienie bezpieczeństwa narodowego. Specjalne środki można wiązać z art. 73 NSL, który stanowi przepis programowy, zachęcający do wdrażania osiągnięć technologicznych dla zapewnienia bezpieczeństwa publicznego. Art. 8 NIL wymaga, aby działania związane z informacjami wywiadowczymi były podejmowane zgodnie z prawem, a także z poszanowaniem praw człowieka oraz praw i interesów jednostek i organizacji.

Ponownie, rozwiązania zaproponowane przez ustawodawcę chińskiego nie licują ze standardem oczekiwanym przez przepisy prawa Unii Europejskiej.

[647] Y. Feng: *The future of*…, s. 74.
[648] C. You: *Half a Loaf*…, s. 20.

7.4. Nadzór nad dostępem organów do danych

Jako kolejny przejaw zróżnicowanego traktowania podmiotów publicznych i prywatnych, przepisy prawa chińskiego odnoszą się do nadzoru nad dostępem organów do danych osobowych w niewielkim zakresie.

NSL nie zawiera wielu odniesień do nadzoru nad wykonywaniem obowiązków przez organy państwa. Pośrednio, z zagadnieniem jest związany Art. 13 NSL, który w sposób ogólny odwołuje się do właściwych przepisów prawa w zakresie odpowiedzialności za naruszenie przez obywatela lub organizację przepisów NSL lub innych przepisów związanych z bezpieczeństwem narodowym. W podobny sposób jawi się NIL. Mimo dość rozbudowanego opisu organów zajmujących się działaniami związanymi z informacjami wywiadowczymi, w NIL brak wskazania organu, który ma sprawować nadzór.

Do zagadnienia nadzoru nad dostępem organów do danych będą stosowane również przepisy DSL. Będzie to jednak nadzór związany przede wszystkim z nakładaniem sankcji przewidzianych przez jego przepisy. Jak już była o tym mowa, karanym naruszeniem przepisów DSL jest także odmowa współpracy z organami ścigania w zakresie udostępnienia danych Za takie naruszenie przepisów DSL art. 48 DSL przewiduje karę nakazania podjęcia działań naprawczych, ostrzeżenia lub grzywny w kwocie od 50.000 do 500.000 yuan, a w przypadku osoby bezpośrednio odpowiedzialnej za zarządzanie bezpieczeństwem danych i pozostałych pracowników bezpośrednio odpowiedzialnych w kwocie 10.000 do 100.000 yuan.

To także DSL sankcjonuje niewłaściwe udostępnianie danych innym organom. Jeśli bez uprzedniej zgody właściwego chińskiego organu, na podstawie zagranicznego orzeczenia sądu lub żądania zagranicznego organów ścigania w zakresie pozyskiwania danych zostaną udostępnione dane, wówczas dojdzie do naruszenia przepisów DSL. W takiej sytuacji, właściwy organ odpowiedzialny za nadzór, zgodnie z art. 48 zdanie drugie DSL może nałożyć karę nakazania podjęcia działań naprawczych lub grzywny w kwocie 100.000 do 1.000.000 yuan oraz w kwocie 10.000 do 100.000 yuan osobę bezpośrednio odpowiedzialną za zarządzanie bezpieczeństwem danych i pozostałych pracowników bezpośrednio odpowiedzialnych. Jeśli takie udostępnienie spowoduje poważne konsekwencje, właściwy organ odpowiedzialny za nadzór nakłada karę grzywny w kwocie od 1.000.000 do 5.000.000 yuan wraz z karą zawieszenia niektórych istotnych operacji przetwarzania danych, zawieszenia operacji przetwarzania danych wymagających działań naprawczych lub cofnięcia przyznanych licencji lub pozwoleń,

wraz z karą grzywny w kwocie 50.000 do 500.000 yuan nakładaną na osobę bezpośrednio odpowiedzialną za zarządzanie bezpieczeństwem danych i pozostałych pracowników bezpośrednio odpowiedzialnych.

7.5. Środki przyznane osobie, której dane dotyczą w związku z dostępem do jej danych

Tak jak ogólne przepisy o ochronie danych osobowych, tak i przepisy związane z dostępem organów do danych osobowych powinny gwarantować jednostce odpowiednie środki ochronne.

Art. 82 NSL przyznaje każdemu obywatelowi oraz organizacji swego rodzaju głos doradczy w zakresie bezpieczeństwa narodowego. Narzędziem do realizacji przyznanego prawa jest formułowanie rekomendacji i krytycznych uwag na temat bezpieczeństwa narodowego i kierowanie ich do właściwych organów zajmujących się bezpieczeństwem narodowym. Jednocześnie, art. 82 NSL przyznaje każdemu obywatelowi oraz organizacji prawo do złożenia skargi na niezgodne z prawem działanie organów państwa i jego przedstawicieli. Nadto, art. 81 NSL w pewnym sensie stanowi podstawę do żądania odszkodowania za szkodę poniesioną w związku z wspieraniem lub asystowaniem organom państwa w pracach związanych z bezpieczeństwem narodowym. Szczegółowe zagadnienia związane z odszkodowaniem znajdują się we właściwych przepisach, do których odwołuje art. 81 NSL.

Przyznane środki zasadniczo nie różnią się od omówionych środków, o których wspominają przepisy chińskiego prawa ochrony danych osobowych, w efekcie czego poczynione uwagi i zastrzeżenia, wpasowują się w całej rozciągłości. Natomiast, dodatkowo warto zwrócić uwagę, że dostęp organów do danych może dotyczyć także obcokrajowców. Faktyczna pozycja obcokrajowca zwracającego się do chińskiego sądu o ochronę, i tak jest znacznie utrudniona; uwzględniając całokształt okoliczności, nie widać podstaw do uznania, że tylko na potrzeby ochrony jednostki przed nieuprawnionym dostępem do danych dojdzie do jakichkolwiek ułatwień w tym zakresie[649]. Zarazem, w Chinach ogromne znaczenie przypisuje się zasadzie wzajemności uznawania orzeczeń sądów zagranicznych, co bezpośrednio wpływa na uzasadnione wątpliwości co do skuteczności wykorzystania ochrony zapewnianej m.in. przez europejskie sądy[650].

[649] B. Zhao, G.P. Mifsud Bonnici: *Protecting EU Citizens*…, 132, 135–139; J. Huang: *Reciprocal Recognition and*…, s. 142; por. także J. Wang: *Dispute Settlement in*….
[650] J. Huang: *Reciprocal Recognition and*…, s. 134–135; J. Wang: *Dispute Settlement in*…, s. 13–14.

8. Poziom ochrony danych osobowych zapewnianych przez przepisy chińskiego prawa ochrony danych osobowych

Podsumowując powyższe rozważania należy rozpocząć od stwierdzenie, że chińskie prawo ochrony danych osobowych poddano znaczącym zmianom. Porównując treść CSL, c.k.c., PIPL, a także DSL z przepisami obowiązującymi przed październikiem 2017, a więc przed wejściem w życie CSL, dostrzegamy jak wiele nowych elementów typowych dla prawa ochrony danych osobowych wdrożono. Nasuwa się zasadnicze pytanie o jakość wprowadzonych zmian. Jakość rozumianą jako poziom gwarantowanej ochrony, rzecz jasna, z perspektywy standardu adekwatności. Nie sposób uznać, że samo dodanie jakichkolwiek przepisów związanych z ochroną danych osobowych do systemu prawnego automatycznie oznacza, że wzrasta poziom ochrony zapewniany przez ten system.

Na pierwszy rzut oka można odnieść wrażenie, że ochrona danych osobowych w Chinach wynikająca z CSL, c.k.c. i PIPL jest bliska, czy wręcz odpowiada standardowi adekwatności. Prawo chińskie zawiera podstawowe definicje pojęć ochrony danych osobowych, katalog zasad przetwarzania danych osobowych. Uregulowano także obowiązki administratora, jak i prawa przyznane osobie, której dane dotyczą. Wreszcie gwarantem ochrony mają być organy publiczne, nadzorujące przetwarzanie danych osobowych. Niestety, tak ogólne ujęcie nie odpowiada rzeczywistemu stanowi rzeczy.

Zestaw definicji, po latach implementowany do przepisów prawa powszechnie obowiązującego przejawia najwyższy poziom zgodności ze standardem adekwatności. Momentami może być interpretowany jako przykład nowego podejścia do niektórych definicji. W szczególności, dane wrażliwe zostały tak zdefiniowane, że przynajmniej teoretycznie zapewniają jednostce wyższy poziom ochrony, obejmując swoim zakresem szerszy katalog danych niż ma to miejsce w przepisach RODO. Co istotne, fakt, że definicje zostały zawarte w różnych ustawach nie jest aż tak poważnym problemem. Zdaniem C. You, definicje w CSL, c.k.c. i PIPL są do siebie zbliżone[651]. Wskazuje się jednak, że wykładania definicji przetwarzania danych osobowych powinna się odbywać z wykorzystaniem c.k.c. i PIPL[652].

Katalog zasad ochrony danych osobowych jest już bliższy tzw. chińskiej specyfice, przy czym dotyka ona przede wszystkim rzeczywistego stosunku

[651] C. You: *Half a Loaf*…, s. 12.
[652] H. Xing: *Government Data Sharing*…, s. 72.

administratorów danych do przestrzegania zasad. Tym samym, mniejsze znaczenie mają różnice w sformułowaniu poszczególnych zasad ochrony danych osobowych, jeśli ich faktyczne przestrzeganie jest mniej lub bardziej gwarantowane. Oczywiście, wciąż aktualne pozostają uwagi dotyczą m.in. podstaw przetwarzana danych osobowych i wyjątkowego statusu zgody, jako podstawy przetwarzania danych. Zdaniem doktryny to właśnie kombinacja zasad i ich egzekwowalności składa się na najpoważniejszą wadliwość PIPL[653]. W takim stanie rzeczy fakt, że zasady ujęte w c.k.c. i PIPL są zasadniczo zgodne ze sobą, a więc obie ustawy są podstawowym źródłem zasad ochrony danych osobowych w Chinach[654], traci na znaczeniu, skoro egzekwowalność oparta o obie ustawy jest poddawana krytyce jako nieskuteczna. Taki wniosek potwierdza praktyka. Przykładem wątpliwego przestrzegania zasad ochrony danych osobowych jest praktyka w zakresie udostępniania przez administratora danych osobowych na rzecz osób trzecich. Q. Zhou wyjaśnia, że odmowa osoby, której dane dotyczą na udostępnianie jej danych jest często niemile widziana, zaś konsekwencją odmowy udstostępnienia danych bywa utrata dostępu przez jednostkę do usługi[655].

W podobny sposób można podsumować problematykę praw osób, których dane dotyczą. Wang podkreśla, że wykładania praw jednostki, o których mowa w PIPL powinna uwzględniać następujące okoliczności, tj. fakt, że podejście do praw przyznanych osobie, której dane dotyczą wynika z decyzji samego ustawodawcy, natomiast prawa dotyczą przetwarzania danych, a nie danych osobowych jako takich i znajdują zastosowanie do określonych sytuacji, co przekreśla ich ogólny i absolutny charakter[656]. Tak zarysowana pozycja jednostki jest konsekwencją przyjęcia odmiennej optyki w odniesieniu do praw jednostki, która jest oderwana od potrzeby ochrony jej podstawowych praw i wolności, na korzyść zabezpieczenia interesów rynku[657]. Konsekwencją powyższego jest mniejsze znaczenie, momentami zaawansowanych obowiązków nakładanych na administratora. W tym stanie rzeczy nie dziwi więc spostrzeżenie, że w ramach procedury obsługi żądań jednostki, o której mowa w art. 50 PIPL wymóg przystępności czy też „wygody" obsługi żądania nie jest niezbędny[658].

[653] C. You: *Half a Loaf*…, s.12, 24; W. Xixin: *The Bundle of Personal Information Rights from the Perspective of State Protection*. „Social Sciences in China", 2022, nr 43, s. 48; por. G. Yang: T*heoretical Justification and*…; Q. Zhou: *Whose Data Is*…, s. 78.
[654] Por. H. Dorwart: *Chinese Data Protection*….
[655] Q. Zhou: *Whose Data Is*…, s. 85.
[656] W. Xixin: *The Bundle of*…, s. 37.
[657] B. Zhao, F. Yang: *Mapping the development*…, s. 11; R. Creemers: *China's Emerging Data*…, s. 14.
[658] X. Zhang: *On the Exercise of the Right to Request Protection of Personal Information*. „Political and Legal Forum", 2023, nr 2.

Co więcej, osoba, której dane dotyczą decydując się na skorzystanie z procedury sądowej dla realizacji swoich praw musi liczyć się z tym, że w praktyce to administrator będzie jednostronnie ustalał zasady rozwiązania takich sporów, w tym także będzie decydował o wyborze sądu właściwego[659]. Oczywiście, najczęściej będzie to sąd chiński, zaś prawem właściwym będzie prawo chińskie. Podmiotom zagranicznym pozostaje więc oczekiwać, że rację mają Jia i Ruan, wedle których, aplikacje i usługi chińskich przedsiębiorców, oferowane podmiotom zagranicznym są odrębnie traktowane i zapewniają wyższy poziom ochrony[660].

Jednostka nie może także liczyć na wsparcie ze strony organu nadzoru na takich samych zasadach jak ma to miejsce w UE. Dość wskazać, że przepisy PIPL nie zakreślają terminu, w którym należy dokonać notyfikacji zdarzenia na rzecz organu nadzoru[661], a także nie uprawniają organizacji pożytku publicznego ani podobnych podmiotów do wystąpienia do organu nadzoru w imieniu lub na rzecz jednostki[662]. Zasadniczym odstępstwem jest jednak brak organu nadzoru, który odpowiadałby standardowi adekwatności. Konsekwencją struktury nadzoru wynikającej z przepisów prawa chińskiego jest brak jednego, wyspecjalizowanego, a przede wszystkim niezależnego organu nadzoru. Zarówno dla CAC, jak i dla MPS czy MIIT ochrona danych osobowych to tylko dodatkowe zadanie, co powoduje, że różne uprawnienia związane z nadzorem nie są aż tak doniosłe jak mogłoby się wydawać. Jednocześnie, brak niezależności skutkuje tym, że ocena ewentualnych naruszeń, czy szerzej, nadzór nad ochroną danych osobowych będzie uwzględniał dodatkowe okoliczności, niekoniecznie istotne z perspektywy ochrony danych osobowych. Rację ma więc G. Greenleaf, który na tle przepisów dotyczących transferów danych osobowych zwraca uwagę na brak obiektywnych przesłanek decydujących o dopuszczalności transferu danych, co powoduje, że decyzja w tym względzie zależy *de facto* od uznania organu nadzoru, w tym przypadku CAC[663].

Bez wątpienia, spojrzenie ukierunkowane na praktyczne zastosowanie przepisów chińskiego prawa ochrony danych osobowych ukazuje najwięcej odstępstw od standardu adekwatności. Najpoważniejsze wątpliwości wywołuje mnogość ustaw, które, choćby potencjalnie, mogą znaleźć zastosowanie do czynności kwalifikowanych jako przetwarzanie danych osobowych. Z pozoru może się wydawać, że jest to typowa sytuacja z jaką przychodzi się zmierzyć uczestnikowi każdego systemu prawnego, gdy

[659] Q. Zhou: *Whose Data Is*…, s. 89.
[660] Por. L. Jia, L. Ruan: *Going Global: Comparing*…..
[661] C. You: *Half a Loaf*…, s. 17.
[662] G. Greenleaf: *China Issues a*…, s. 11; C. You: *Half a Loaf*…, s. 23.
[663] G. Greenleaf: *China Issues a*…, s. 12.

jedna czynność może być odrębnie kwalifikowana przez różne ustawy. Jednakże, w chińskim systemie prawnym mowa o zgoła innym problemie. O ile oczywistym było, że ustawy funkcjonujące w chińskim porządku prawnym sprzed 2017 roku zawierały szczegółowe przepisy adresowane do konkretnych branż, o tyle przepisy CSL, c.k.c., PIPL do pewnego stopnia powtarzają wiele ogólnych obowiązków adresowanych do administratora. Jak już wspominałem, zdaniem doktryny to dopiero kontekst faktyczny ma być rozstrzygnięciem, która ustawa lub które ustawy należy rzeczywiście stosować. Nie można jednak wykluczyć sytuacji, w której przedmiot działalności administratora pozwoli na taki zabieg, ale administrator nie będzie pewien czy przyjęta interpretacja jest prawidłowa, a wdrożone rozwiązania wystarczające. Podważa to więc skuteczność wdrożonych przepisów.

Nie inaczej jest w przypadku wątpliwej kwalifikacji organów państwa przetwarzających dane osobowe jako administratorów danych. Jak już była o tym mowa, zdaniem doktryny tylko teoretycznie można dopatrywać się rozciągnięcia przepisów chińskiego prawa ochrony danych osobowych na organy państwa. Całokształt okoliczności potwierdza, że takie teoretyczne ujęcie nie odpowiada rzeczywistości, w której organom państwa przypisywany jest wyjątkowy status. Dotyczy on tak zwykłego toku przetwarzania danych osobowych, jak i przetwarzania danych w ramach realizacji dostępu organów ścigania do danych. W obu przypadkach organom państwowym należałoby przypisać status administratora i oczekiwać przetwarzania danych zgodnego z prawem. Swoboda organów państwa zostałaby ograniczona. Nie taki był jednak zamysł ustawodawcy chińskiego, dla którego brak ograniczeń w szeroko rozumianym dostępie do danych osobowych jest istotny. Potwierdzeniem oczekiwanej swobody są uwagi zgłaszane przez przedstawicieli doktryny. Jedna z takich uwag dotyczy nieścisłości w przepisach CSL, DSL i PIPL, która prowadzi do braku odpowiedzialności organu państwa za przetwarzanie danych, ale przy jednoczesnym utrzymaniu odpowiedzialności indywidualnej osób zatrudnionych lub związanych z tym organem[664]. Nadto, doktryna podkreśla, że PIPL dotyka głównie podmiotów prywatnych, nie państwowych[665].

Oczekiwana swoboda organów państwa może posłużyć za wyjaśnienie wielu niejasności w przepisach chińskiego prawa ochrony danych osobowych, w tym zwłaszcza przepisach dotyczących dostępu organów ścigania do danych. Przedstawiona w pkt 7 niniejszego

[664] Por. Q. Peng: *Legal Liabilities of State Agencies Concerning Personal Information Protection—— Interpreting Article 68 of the Personal Information Protection Law of PRC*. „Studies in Comparative Law", 2023, nr 2.
[665] C. You: *Half a Loaf*…, s. 12; I. Calzada: *Citizens' Data Privacy*…, s. 1136.

rozdziału analiza przepisów regulujących dostęp organów ścigania do danych potwierdza, że przyjęte rozwiązana są dalekie od oczekiwanego przez standard adekwatności poziomu jednoznaczności oraz proporcjonalności. Sposób, w jaki sformułowano przepisy poszczególnych ustaw związanych z dostępem organów ścigania do danych nie pozwala zrekonstruować konkretnych przesłanek uzyskania dostępu czy jego ograniczeń. Jednakże, taka niejasność przepisów może być odczytywana jako zamierzone działanie ustawodawcy. Zyskuje on wówczas możliwość realizacji za pośrednictwem takich przepisów dodatkowych celów, w tym celów istotnych dla partii[666]. W szczególności, przepisy mogą być wykorzystane do walki z podmiotami niewygodnymi dla bieżącej polityki[667], czego konkretnym przykładem była m.in. sprawa Didi[668]. Ale także mogą posłużyć do lepszego zarządzania obywatelami, tak, ażeby przekaz polityczny lepiej trafiał do ich bieżących poglądów czy zainteresowań[669]. Takie podejście niekoniecznie odpowiada oczekiwaniom jednostek, dla których tworzenie przez państwo ogromnych baz danych na ich temat, a więc umożliwienie opracowania szczegółowych profili na temat jednostki, jest ryzykowne[670]. Niemniej jednak, oczekiwania jednostki w tym wypadku nie są najważniejsze.

9. Wnioski

Jak w wielu wypadkach rozwiązań prawnych Państwa Środka, tak i w przypadku prawa ochrony danych osobowych należy mówić o chińskiej specyfice[671]. Pogłębiona analiza przepisów chińskiego prawa ochrony danych osobowych pozwala dostrzec elementy znane choćby z prawa Unii Europejskiej czy prawa amerykańskiego[672]. Jednak dla Chin konieczna jest synergia między ochroną danych osobowych a gospodarką, która to ochrona nie powinna wpływać negatywnie na dalszy rozwój

[666] G. Greenleaf, S. Livingston: *PRC's New Data*…, s. 3; L. Jia, L. Ruan: *Going Global: Comparing…*; J. Liu, H. Zhao: *Privacy Lost: Appropriating*…, s. 8; G. Pyo: *An Alternate Vision*…, s. 268, 270; W. Chaskes *The Three Laws*…, s. 1176; A.S. Sweet, C. Bu: *Breaching the Taboo?*..., s. 1; G. Greenleaf: *China's Completed Personal*…, s. 6; por. H. Dorwart: *Chinese Data Protection*….

[667] G. Pyo: *An Alternate Vision*…, s. 249; B. Zhao, F. Yang: *Mapping the development*…, s. 12.

[668] A. Kharpal: *China Has Signaled Easing of Its Tech Crackdown — but Don't Expect a Policy U-Turn*. 17.05.2022. https://www.cnbc.com/2022/05/18/china-signals-easing-of-its-tech-crackdown-but-dont-expect-a-u-turn.html [dostęp: 29.03.2023].

[669] B. Aho, R. Duffield: *Beyond Surveillance Capitalism*…, s. 198–199; W. Liming: *The Basic Issues Concerning the Construction of the Rule of Law in China in the New Era*. „Social Sciences in China", 2020, nr 41, s. 22; por. Z. Yang: *The Chinese Surveillance*… ; W. Chaskes *The Three Laws*…, s. 1181.

[670] J. Liu, H. Zhao: *Privacy Lost: Appropriating*…, s. 744; H. Xing: *Government Data Sharing*…, s. 73–74; por. Z. Chen: *Rule of Law Response to Face Information Collection Activities of Administrative Agencies*. „Studies in Administrative Law", 2023 nr 3.

[671] D. Hanlin: *The System Position*…, s. 153–154; B. Qu, C. Huo: *Privacy, National Security*…, s. 364; E. Pernot-Leplay: *China's Approach on*…, s. 53–54; Y. Shao: *Personal Information Protection*…, s. 236–238.

[672] E. Pernot-Leplay: : *China's Approach on*…, s. 53–54, 81–82; R. Berti: *Data Protection Law*…, s. 37.

gospodarczy[673]. Jak zauważa doktryna wynika to z tego, że biznes w Chinach będzie legitymizowaną konstytucyjnie podstawą do regulacji ochrony danych osobowych[674]. W oparciu o przedstawioną analizę przepisów chińskiego prawa ochrony danych osobowych, na pytanie trzecie (P.3), należy odpowiedzieć, że system prawny Chin poddany analizie w oparciu o kryteria oceny systemu prawnego państwa trzeciego zapewnia poziom ochrony, który nie odpowiada standardom prawa Unii Europejskiej w przedmiocie ochrony danych osobowych w państwie trzecim.

Również w świetle przedstawionej analizy należy stwierdzić, że chińskie prawo nie zapewnia ochrony danych osobowych na poziomie odpowiadającym poziomowi wynikającemu ze standardu adekwatności. Do najważniejszych wad chińskiego prawa ochrony danych osobowych zaliczają się niejasny status organów państwa przetwarzających dane osobowe, brak niezależnego organu nadzoru oraz regulacja dostępu organów ścigania do danych, która nie odpowiada standardowi, określonemu przez Europejską Radę Ochrony Danych Osobowych. Powyższy wniosek jest szczególnie istotny dla dalszych rozważań na temat możliwej legalizacji przekazywania danych osobowych między UE a Chinami. W tym stanie rzeczy odpowiedź na pytanie czwarte (P.4) jest twierdząca, ponieważ poziom ochrony danych osobowych zapewniany przez przepisy chińskiego prawa ochrony danych osobowych wyklucza uzyskanie przez Chiny decyzji w sprawie adekwatności w rozumieniu art. 45 ust. 1 RODO.

[673] A. Boram Yang: *China in Global*…, s. 906; X. Duoye: *The Civil Code*…, s. 193; B. Qu, C. Huo: *Privacy, National Security*…, s. 361–362, 364; Y. Shao: *Personal Information Protection*…, s. 228, 233, 235; P. Cai, L. Chen: *Demystifying Data Law*…, s. 75, 88; L. Belli, D. Doneda: *Data Protection in*…, s. 3.
[674] Y. Feng: *The future of*… s. 64; B. Zhao: *Connected Cars in*…, s.21; J. Liu: *China's data localization*…, s. 91; L. Trakman, R. Walters, B. Zeller: *Digital consent and*…, s. 233; R. Creemers: *China's Emerging Data*…, s. 19; C. You: *Half a Loaf*…, s. 16; B. Zhao, F. Yang: *Mapping the development*…, s. 6, 12.

ROZDZIAŁ TRZECI
PRZEKAZYWANIE DANYCH OSOBOWYCH MIĘDZY UNIĄ EUROPEJSKĄ A CHINAMI ZGODNIE Z PRZEPISAMI RODO

1. Wprowadzenie

Każdego dnia niezmierzone ilości danych, w tym danych osobowych, są przekazywane między podmiotami zlokalizowanymi w Unii Europejskiej i Chinach. Wynika to ze stopnia intensywności współpracy gospodarczej między Unią Europejską a Chinami[675]. Tak, jak w przypadku innych kierunków transferów, transfery danych osobowe do Chin nie są zawieszone w legislacyjnej próżni. Zarówno przepisy RODO, jak i przepisy chińskiego prawa ochrony danych osobowych określają pożądany model przekazywania danych osobowych do państw trzecich. O czym była mowa w rozdziale drugim, przepisy chińskiego prawa ochrony danych osobowych zapewniają poziom ochrony danych osobowych nieodpowiadający standardowi adekwatności RODO. Różnice w poziomie ochrony danych osobowych w Unii Europejskiej i Chinach nie powodują jednak zaprzestania transferowania danych osobowych. Administratorzy i podmioty przetwarzające dane na zlecenie są zmuszeni do dostosowania swoich działań. Według stanu na styczeń 2024 r. Komisja Europejska wydała 15 decyzji w sprawie adekwatności. Ostatnia decyzja, dotycząca kolejnego już porozumienia w sprawie transferów danych osobowych do USA, została wydana w lipcu 2023 r.[676] i jak na razie nic nie wskazuje na to, że niebawem liczba krajów uznanych za adekwatne ulegnie zmianie. W szczególności, biorąc pod uwagę wnioski przedstawione rozdziale drugim, nie sposób oczekiwać, że do grona krajów objętych decyzjami w sprawie adekwatności dołączą Chiny. W takim stanie rzeczy administrator lub podmiot przetwarzający dane na zlecenie, który chce przekazać dane osobowe do Chin jest zmuszony sięgać po odpowiednie zabezpieczenia, o których mowa w art. 46 RODO lub odstępstwa, o których mowa w art. 49 RODO. Przypadek przekazywania danych osobowych z Unii Europejskiej do USA potwierdza jednak, że dla tak intensywnych transferów danych osobowych odpowiednie zabezpieczenia, a zwłaszcza odstępstwa, nie są rozwiązaniami, które we właściwy sposób chronią prawa jednostki.

[675] O czym była mowa we wstępie, Chiny to drugi partner handlowy Unii Europejskiej.
[676] Komisja Europejska: *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows*. 10.07.2023 https://ec.europa.eu/commission/presscorner/detail/eN/ip_23_3721 [dostęp: 28.05.2024].

Celem rozdziału trzeciego jest omówienie problematyki przekazywania danych osobowych między Unią Europejską a Chinami zgodnie z przepisami RODO. W związku z poszukiwaniem odpowiedzi na główne pytanie badawcze, w pierwszej części rozdziału omówione zostanie aktualne podejście administratorów i podmiotów przetwarzających dane na zlecenie do przekazywania danych osobowych między Unią Europejską a Chinami. Udzielona zostanie odpowiedź na pytanie piąte (P.5) „Czy odpowiednie zabezpieczenia w rozumieniu art. 46 RODO lub odstępstwa, o których mowa w art. 49 RODO, stosowane w sytuacji transferu danych osobowych między Unią Europejską a Chinami, gwarantują ochronę praw i wolności osób, których dane dotyczą?".

Druga część rozdziału przedstawia koncepcję wykorzystania porozumienia w sprawie legalizacji transferów danych osobowych między Unią Europejską a Chinami, na wzór porozumień zawieranych między Unią Europejską a USA, co wiąże się z odpowiedzią na szóste pytanie badawcze (P.6) „Czy pomimo istnienia różnic w poziomie ochrony danych osobowych w Chinach i Unii Europejskiej, dla zapewniania należytej ochrony praw i wolności osób, których dane dotyczą, możliwe jest zawarcie porozumienia międzynarodowego między Unią Europejską a Chinami, na wzór porozumień zawieranych między Unią Europejską a USA, w celu regulacji przekazywania danych osobowych?"

2. Przekazywanie danych osobowych między Unią Europejską a Chinami Aktualny stan

Poziom ochrony danych osobowych w Chinach nie odpowiada poziomowi, oczekiwanemu przez przepisy RODO. O czym była mowa w rozdziale II, przepisy chińskiego prawa ochrony danych osobowych cechują poważne różnice, w porównaniu z przepisami RODO i europejskim podejściem do ochrony danych osobowych. Tym samym, nie sposób oczekiwać, uznania chińskiego systemu prawnego za zapewniający adekwatny poziom ochrony danych osobowych i konsekwencji wydania decyzji w sprawie adekwatności. Również zaprzestanie przekazywania danych osobowych między podmiotami działającymi w Unii Europejskiej i Chinach jest oczekiwaniem nierealnym. W związku z tym, w obecnej sytuacji przekazywanie danych osobowych między Unią Europejską a Chinami wpisuje się w model przekazywania danych osobowych do państwa trzeciego nieobjętego decyzją w sprawie adekwatności.

2.1. Przekazywanie danych osobowych do państw trzecich zgodnie z przepisami RODO w sytuacji braku decyzji w sprawie adekwatności dotyczącej państwa trzeciego przeznaczenia danych

Fakt, że Chiny nie są objęte decyzją w sprawie adekwatności oznacza, że administratorzy lub podmioty przetwarzające dane na zlecenie muszą polegać na jednym z odpowiednich zabezpieczeń wskazanych w art. 46 RODO lub, wyjątkowo, na jednym z odstępstw wynikających z art. 49 RODO. O czym stanowi art. 44 RODO, celem przepisów RODO poświęconych transferom danych osobowych jest bowiem zapewnienie, aby nie doszło do naruszenia poziomu ochrony danych osobowych wynikającego z RODO.

2.1.1. Odpowiednie zabezpieczenia, o których mowa w art. 46 RODO

W myśl artykułu 46 ust. 1 RODO wykorzystanie odpowiednich zabezpieczeń stanowi obowiązek administratora danych lub podmiotu przetwarzającego. Celem takiego działania ma być uchronienie osoby, której dane dotyczą przed zagrożeniami związanymi z transferem danych osobowych do państw trzecich[677]. Odpowiednie zabezpieczenia pełnią więc funkcję rekompensaty braku ochrony danych osobowych w państwie trzecim[678]. Wyroki TSUE w sprawach Schrems I oraz Schrems II uzupełniły katalog zagrożeń, na jakie wystawiana jest jednostka wskutek transferu danych osobowych do państwa trzeciego. Szczególnym zagrożeniem stał się bowiem dostęp organów ścigania państwa trzeciego do przekazywanych danych osobowych.

Wybór administratora lub podmiotu przetwarzającego jest zasadniczo ograniczony do odpowiednich zabezpieczeń niewymagających uzyskania zezwolenia organu nadzorczego. Do tej grupy zaliczają się publiczno-prawny instrument, wiążące reguły korporacyjne (BCR), klauzule umowne (SCC), kodeks postępowania, certyfikacja. Dodatkowo, administrator lub podmiot przetwarzający mogą zdecydować się na wykorzystanie innego zabezpieczenia, przy czym w takiej sytuacji będą zmuszeni do uzyskania zezwolenia organu nadzorczego. Zdaniem części doktryny, taka konstrukcja oznacza, że katalog środków legalizacji transferów danych osobowych w RODO jest katalogiem otwartym, przy czym i tak każdy, niewymieniony wprost w RODO środek będzie podlegał zatwierdzeniu przez organ nadzoru[679]. Przykładowe zabezpieczenia,

[677] Por. motyw 108 RODO.
[678] M. Krzysztofek: *Komentarz do art. 46 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C. H. Beck, Warszawa 2016, s. 256; B. Fischer: *Komentarz do art. 46 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz.* Red. M. Sakowska-Baryła. C. H. Beck, Warszawa 2018. s. 472; P. Drobek: *Komentarz do art. 46*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2018.
[679] P. Fajgielski: *Komentarz do rozporządzenia nr 2016/679 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), art. 46.* W: *Ogólne rozporządzenie*

które należą do tej grupy to klauzule umowne oraz postanowienia uzgodnień administracyjnych między podmiotami lub organami publicznymi.

Nie jest jednak tak, że dla pierwszej grupy zabezpieczeń (art. 46 ust. 2 RODO) całkowicie zrezygnowano z konieczności ich zatwierdzenia. Różni się jednak moment i sposób uzyskiwania zatwierdzenia, udzielanego przez odpowiednio organ nadzorczy lub Komisję Europejską[680].

Podejmując decyzję o wyborze odpowiedniego zabezpieczenia, za każdym razem administrator lub procesor powinien uwzględnić całokształt okoliczności związanych z transferem danych i na tej podstawie dokonać wyboru zabezpieczenia. Jedynie w przypadku publiczno-prawnego instrumentu oraz postanowień uzgodnień administracyjnych ustawodawca wprowadził ograniczenie podmiotowe, rezerwując te zabezpieczenia dla podmiotów lub organów publicznych. W pozostałym zakresie, co do zasady, administrator i podmiot przetwarzający zachowują swobodę wyboru, z zastrzeżeniem nadrzędnego celu odpowiednich zabezpieczeń, jakim jest ochrona jednostki[681]. Można więc mówić o przejawie jednostronnego charakteru odpowiednich zabezpieczeń[682].

Sama implementacja odpowiednich zabezpieczeń nie będzie jednak wystarczająca, jeśli w systemie prawnym państwa trzeciego zabraknie egzekwowalnych praw oraz środków ochrony prawnej przyznanych jednostce. Uzupełnienie odpowiednich zabezpieczeń będzie także konieczne dla uchronienia jednostki przed skutkami dostępu do jej danych osobowych realizowanego przez organy ścigania państwa trzeciego[683]. Tym samym, wraz z podjęciem decyzji o wykorzystaniu jednego z odpowiednich zabezpieczeń wskazanych w art. 46 RODO, aktualizuje się obowiązek przeprowadzenia oceny państwa trzeciego w zakresie poziomu ochrony danych osobowych[684] .

---

o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.

[680] Zatwierdzenie zabezpieczenia może przyjąć postać stworzenia swego rodzaju wzoru (standardowe klauzule umowne), a niekiedy jest immanentnie związane z procedurą tworzenia i wdrażania danego zabezpieczenia (m.in. wiążące reguły korporacyjne czy certyfikacja, gdzie Komisja Europejska lub organ nadzorczy analizuje i zatwierdza konkretne zabezpieczenia, zaprojektowane na potrzeby konkretnego podmiotu).

[681] Zgodnie z motywem 108 RODO, odpowiednie zabezpieczenia mają służyć jednostce (chronić ją przed ryzykiem, jakie niesie za sobą transfer danych osobowych do państwa trzeciego) a nie administratorowi.

[682] OECD: *Fostering Cross-Border Data*…, s 19.

[683] P. Breitbarth: *A Risk-Based…,* s. 546; S. Winklbaue, R. Horner: *Austrian DPA Decides EU-U.S. Data Transfer Through the Use of Google Analytics to Be Unlawful*. „European Data Protection Law Review", 2022, nr 8, s. 78, 83; C. Kuner: *Komentarz do art. 46*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020, s. 799, 802.

[684] Lub w tym samym czasie, przy czym takie rozwiązanie może się okazać nieefektywne, w szczególności, jeśli przeprowadzona ocena poziomu ochrony danych osobowych w państwie trzecim wykaże istnienie

2.1.1.1. Obowiązek przeprowadzenia oceny systemu prawnego państwa trzeciego w związku ze stosowaniem odpowiednich zabezpieczeń

Administrator lub podmiot przetwarzający, wykorzystujący odpowiednie zabezpieczenia, o których mowa w art. 46 RODO, jest zobowiązany do przeprowadzenia oceny poziomu ochrony danych osobowych w państwie trzecim przeznaczenia danych[685]. Źródła obowiązku przeprowadzenia TIA należy się upatrywać w wyrokach TSUE zapadłych w sprawach Schrems I i Schrems II. O czym była mowa w rozdziale I, wyrok w sprawie Schrems I potwierdził, że państwo trzecie, na terytorium, którego mają trafić dane osobowe ma zapewniać odpowiedni, względem prawa Unii Europejskiej, poziom ochrony danych osobowych. Nie chodzi więc o poziom identyczny z poziomem wynikającym z przepisów RODO. Pewne odstępstwa od modelu ochrony danych osobowych Unii Europejskiej, a tym samym standardu adekwatności, są dopuszczalne. Granicą zmian jest jednak oczekiwany, równoważny (ekwiwalentny) poziom ochrony danych osobowych. W tym miejscu należy odwołać się do ustaleń poczynionych w rozdziale I niniejszej rozprawy i wskazanych tam kryteriów oceny systemu prawnego państwa trzeciego. O ekwiwalentnym poziomie ochrony danych osobowych w państwie trzecim będzie można mówić, jeśli jego system prawny zawiera zasady ochrony danych osobowych, które są egzekwowalne i odpowiadają rzeczywistości; jednostka została wyposażona w odpowiednie prawa związane z jej danymi osobowymi oraz środki zaradcze na wypadek naruszenia danych osobowych, zaś nad całością tak skonstruowanego systemu ochrony danych osobowych sprawuje nadzór niezależny, kompetentny organ nadzorczy. Nie bez znaczenia są też odpowiednie gwarancje i ograniczenia przeciwdziałające swobodnemu i nieograniczonemu dostępowi organów ścigania do danych osobowych.

Przedstawione, zwięzłe omówienie oczekiwań TSUE względem poziomu ochrony danych osobowych w państwie trzecim jest istotne z uwagi na konkluzje TSUE przedstawione w wyroku w sprawie Schrems II. TSUE stanął na stanowisku, zgodnie z którym weryfikacja poziomu ochrony danych osobowych w państwie trzecim, na terytorium którego trafiają dane osobowe jest obowiązkiem administratora lub podmiotu przetwarzającego dane stosującego odpowiednie zabezpieczenia. Samo wdrożenie odpowiednich zabezpieczeń nie jest wystarczające, ponieważ braki w ochronie danych

pewnych braków, które będzie trzeba uzupełnić przez wprowadzenie odpowiednich zmian w wykorzystywanym odpowiednim zabezpieczeniu.

[685] Powszechnie nazywanej Transfer Impact Assessment (TIA).

osobowych państwa przeznaczenia danych mogą być na tyle istotne, że będą wpływały na skuteczność odpowiednich zabezpieczeń. Tym samym, przeprowadzona ocena powinna być jednoznaczną wskazówką dla administratora lub podmiotu przetwarzającego w odniesieniu do wyboru odpowiednich zabezpieczeń i ich ewentualnego uzupełnienia o dodatkowe, techniczne lub organizacyjne zabezpieczenia.
Na tle przedstawionych uwag dotyczących obowiązku przeprowadzenia TIA, wątpliwości wywołuje przede wszystkim zakres przeprowadzanej oceny. Zasadniczo taka ocena powinna dotykać całokształtu okoliczności konkretnego transferu, w tym zwłaszcza przepisów obowiązujących w państwie przeznaczenia danych[686]. Biorąc pod uwagę konieczność oceny przepisów przyznających organom ścigania państwa trzeciego dostęp do danych osobowych, ocena powinna opierać się o faktyczne, historyczne informacje na temat dostępu tych organów do danych osobowych[687]. Zrównywanie oceny przeprowadzanej przez administratora lub podmiot przetwarzający w ramach TIA z oceną w sprawie adekwatności nie jest jednak oczywiste. Doktryna prezentuje w tym względzie odmienne stanowiska. Dla części autorów nie można stawiać znaku równości między obiema ocenami, ponieważ tym co wyróżnia TIA na tle oceny adekwatności są odstępstwa w systemie prawnym państwa trzeciego, które TIA akceptuje[688]. Inni autorzy opowiadają się za zrównaniem TIA z oceną adekwatności[689], wyjaśniając takie stanowisko m.in. identycznym poziomem naruszenia praw podstawowych jednostki w sytuacji transferu danych osobowych do państwa trzeciego bez względu na środek jego legalizacji[690]. To z kolei prowadzi do stanowiska, zgodnie z którym ocena w ramach TIA ma uwzględniać Kartę Praw Podstawowych jako kryterium oceny[691].

Uważam, że stanowisko traktujące ocenę państwa trzeciego w ramach TIA jako tożsamą z oceną w sprawie adekwatności za nieprawidłowe. Nie sposób bowiem uznać, że administrator lub podmiot przetwarzający, w ramach stosowania odpowiednich

[686] F. Blythe, V. Shankar: *Payments and EU Data Protection Law.* W: *Payment Services.* Red. J.Casanova, M. Savoie. Edward Elgar Publishing, Cheltenham 2022, s. 198.
[687] J. Liss, D. Peloquin, M. Barnes i in.: *Demystifying Schrems II for the cross-border transfer of clinical research data*. „Journal of Law and the Biosciences", 2021, nr 2, s. 5; U. Wuermeling, I. Oldani: *Regulation of International…,* s. 38; W.G. Voss: *Transatlantic Data Transfer Coimpliance*. „Boston University Journal of Science & Technology Law", 2022, nr 2, s. 193; L. Wittershagen: *Alternative Data Transfer Tools.* W: *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. Red. L. Wittershagen. De Gruyter, Berlin – Boston 2023, s. 221.
[688] C. Docksey, H. Hijmans: *The Court* of…, s. 300, 311; L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses*…, s. 25; C. Kuner *Komentarz do art. 46*…, s. 709, 802.
[689] Z. Gulczyńska: *A Certain Standard*…, s. 360; L. Drechsler, I. Kamara: *Essential equivalence as…,* s. 342.
[690] L. Drechsler, I. Kamara: *Essential equivalence as…,* s. 342.
[691] L. Wittershagen: *Alternative Data Transfer…,* s. 218.

zabezpieczeń, jest zobowiązany do przeprowadzenia tak obszernej analizy systemu prawnego państwa trzeciego, jaka ma miejsce podczas oceny w sprawie adekwatności. W podobny sposób ocenę państwa trzeciego w ramach TIA postrzega Europejska Rada Ochrony Danych Osobowych, sugerując ograniczenie oceny w ramach TIA do przepisów prawa państwa trzeciego istotnych dla przekazywanych danych osobowych [692]. Także w wytycznych Europejskiej Rady Ochrony Danych Osobowych dotyczących certyfikacji [693] podkreślono, że zakres oceny nie jest równy ocenie, o której mowa w art. 45 RODO. Wynika to z tego, że ocena w ramach TIA powinna bardziej ukierunkowana na zagadnienia istotne z perspektywy wykorzystywanego narzędzia, czyli m.in. na kwestię wpływu prawa państwa trzeciego na zobowiązania podmiotu, który uzyskał certyfikację[694]. Również francuski organ nadzorczy, w projekcie wytycznych w sprawie TIA, przyjął interpretację ograniczającą zakres oceny prawa państw trzeciego w ramach TIA[695].

2.1.2. Odstępstwa, o których mowa w art. 49 RODO

Przyjmuje się, że katalog środków legalizujących transfery danych ma postać hierarchiczną[696].W pierwszej kolejności należy więc skorzystać z decyzji w sprawie adekwatności (jeśli taka została wydana dla danego państwa trzeciego), a dopiero następnie, gdy brak takiej decyzji, otwiera się możliwość wykorzystania jednego z odpowiednich zabezpieczeń, o których mowa w art. 46 RODO, zaś jedynie wyjątkowych przypadkach można sięgnąć do katalogu odstępstw, o których mowa w art. 49 RODO[697].

---

[692] Europejska Rada Ochrony Danych Osobowych: *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data. Version 2.0*. 18.06.2021. https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [dostęp: 11.03.2024], pkt 32 "The scope of your assessment is thus limited to the legislation and practices relevant to the protection of the specific data you transfer, in contrast with the general and wide encompassing adequacy assessments the European Commission carries out in accordance with Article 45 GDPR".

[693] Europejska Rada Ochrony Danych Osobowych: *Guidelines 07/2022 on certification as a tool for transfers. Version 2.0.* 14.02.2023. https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf [dostęp: 16.10.2023], por. pkt 43, 45.

[694] Ibid, pkt 45.

[695] Commission Nationale de l'Informatique et des Libertés: *Draft Practical Guide. Transfer Impact Assessment*. 02.2024. https://www.cnil.fr/sites/cnil/files/2024-01/draft_practical_guide_transfer_impact_assessment.pdf [dostęp: 11.3.2024].

[696] P. Drobek: *Komentarz do art. 44*…; C. Kuner: *Komentarz do art. 44*…, s. 764-765.

[697] Artykuł 49 RODO jest nazywany katalogiem odstępstw, ponieważ zawiera listę przesłanek (przypadków) pozwalających na rezygnację z modelu przekazywania danych osobowych zgodnego z zasadą przekazywania danych do państw trzecich, o której mowa w art. 44 RODO – tak: M. Krzysztofek *Komentarz do art. 49 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C.H. Beck, Warszawa 2016, s. 256; pośrednio C. Kuner: *Komentarz do art. 49*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020, s. 843, 846–847.

Zawarty w art. 49 RODO katalog odstępstw dopuszcza jednorazowe lub wielokrotne przekazywanie danych osobowych do państw trzecich pomimo braku decyzji w sprawie adekwatności, czy odpowiednich zabezpieczeń. Jest jednak możliwe tylko, jeśli zostanie spełniona jedna z przesłanek określonych art. 49 ust. 1 RODO. Katalog, o którym mowa w art. 49 ust. 1 RODO składa się z dwóch części. Część pierwsza wskazuje na siedem przypadków, których zaistnienie uprawnia administratora lub podmiot przetwarzający do transferu danych osobowych. Do takich przypadków zaliczono:

1) pozyskanie od osoby, której dane dotyczą wyraźnej zgody na transfer danych osobowych, przy czym niezbędne jest jej poinformowanie o ewentualnych ryzykach, z którymi może się dla niej wiązać proponowany transfer danych (a wynikającymi z braku decyzji stwierdzającej odpowiedni stopień ochrony oraz braku odpowiednich zabezpieczeń);
2) przekazanie, które jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedkontraktowych podejmowanych na żądanie osoby, której dane dotyczą;
3) przekazanie, które jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną;
4) przekazanie, które jest niezbędne ze względu na ważne względy interesu publicznego;
5) przekazanie, które jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń;
6) przekazanie, które jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
7) przekazanie, które następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes, ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

Punktem wyjścia dla wyboru jednego z ww. przypadków jako podstawy transferu danych osobowych jest ustalenie, czy faktycznie konkretny transfer danych osobowych nie jest lub nie może być objęty jednym z mechanizmów wskazanych w rozdziale V RODO.

O ile ustalenie, że państwo przeznaczenia danych nie jest objęte decyzją w sprawie adekwatności nie przysparza wielu problemów, o tyle wątpliwości budzi pytanie o odpowiednie zabezpieczenia. Przyjmuje się, że o braku odpowiednich zabezpieczeń będzie mowa, gdy nie zostały one zastosowane w tym konkretnym przypadku, natomiast nie jest konieczne całkowite ich wykluczenie lub niekompatybilność dla danego przypadku[698]. Administrator lub podmiot przetwarzający nie powinien jednak zbyt łatwo decydować się na skorzystanie z odstępstw, o których mowa w art. 49 ust. 1 RODO. Dopiero niewspółmierne trudności związane z wykorzystaniem jednego z odpowiednich zabezpieczeń mogą uzasadnić posłużenie się jednym z omawianych odstępstw[699]. Jeśli administrator lub podmiot przetwarzający dysponuje środkami finansowymi i technicznymi umożliwiającymi wdrożenie odpowiednich zabezpieczeń, powinien z nich skorzystać[700].

Drugą część katalogu odstępstw znajduje się w akapicie drugim art. 49 ust.1 RODO. Przywołany przepis dopuszcza przekazanie danych osobowych do państwa trzeciego, gdy nie można wykorzystać decyzji w sprawie adekwatności, odpowiednich zabezpieczeń, jak również o jednego z odstępstw, o którym mowa w art. 49 ust. 1 akapit pierwszy RODO, przy jednoczesnej potrzebie przekazania danych do państwa trzeciego. Wówczas transfer danych osobowych może mieć miejsce, pod warunkiem, że:

- przekazanie danych nie będzie to powtarzalne[701],
- będzie dotyczyło ograniczonej liczby osób oraz
- będzie niezbędne dla ważnego, prawnie uzasadnionego interesu realizowanego przez administratora, którego nie przewyższają interesy jednostek[702].

Nadto, administrator lub podmiot przetwarzający musi dokonać oceny całokształtu okoliczności towarzyszących transferowi, której wyniki posłużą do wdrożenia

[698] U. Wuermeling, I. Oldani: *Regulation of International…,* s. 46.
[699] M. Krzysztofek *Komentarz do art. 49 RODO….,* s. 279; L. Wittershagen: *Transfer of Personal*…, s. 77.
[700] B. Fischer: *Komentarz do art. 49 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz.* Red. M. Sakowska-Baryła. C.H. Beck, Warszawa 2018 s. 484; P. Fajgielski *Komentarz do rozporządzenia nr 2016/679 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), art. 49.* W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.
[701] Zdaniem autorów powtarzalność transferu należy ustalać w odniesieniu do konkretnego podmiotu danych, którego dane mają być transferowane - por. U. Wuermeling, I. Oldani: *Regulation of International…,* s. 54.
[702] Ustawodawca oczekuje, że prawa i wolności jednostki nie będą miały w tym wypadku charakteru nadrzędnego. W przeciwnym razie, transfer będzie niemożliwy. Jednocześnie, prawnie uzasadniony interes administratora ulega ujawnieniu, w ramach informacji przekazywanej osobie, której dane dotyczą.

odpowiednich zabezpieczeń w zakresie ochrony danych osobowych[703]. Powyższy opis przedstawia więc szczególną przesłankę podstawy prawnej transferu danych osobowych, która dochodzi do głosu w ostateczności[704].

Art. 49 ust. 1 akapit 2 RODO jest oparty na przesłance ważenia interesów administratora oraz interesów osób, których dane dotyczą. W tym względzie wykazuje podobieństwo z testem uzasadnionego interesu, o którym mowa w art. 6 ust. 1 lit. f RODO, przy czym test na potrzeby transferu danych osobowych jest szerszy i obejmuje dodatkowe zagadnienia[705]. L. Wittershagen uważa, że zasadniczym problemem art. 49 ust. 1 akapit 2 RODO jest to, że zostały w nim wskazane typowe okoliczności, które kwalifikują się jako ważny prawnie uzasadniony interes administratora, przez co trudno sobie wyobrazić co jeszcze może stanowić taką okoliczność[706]. Zdaniem C. Kunera o posłużeniu się art. 49 ust. 1 akapit 2 RODO jako podstawie transferu danych osobowych można mówić w kontekście potrzeby przeprowadzenia badań naukowych[707]. Niemniej jednak, w praktyce jest to bardzo utrudnione[708]. Trudności w posługiwaniu się art. 49 ust. 1 akapit 2 RODO potęgują także pozostałe przesłanki jego zastosowania, w tym zwłaszcza warunek ograniczonej liczby. W odniesieniu do ograniczonej liczby osób, uznaje się, że transfer na podstawie art. 49 ust. 1 akapit 2 RODO ma dotyczyć skończonej ilości danych[709]. Natomiast warunek ograniczonej liczby wyklucza przyznanie jednorazowego, ale niczym nieograniczonego, z wyjątkiem ograniczenia czasowego, dostępu do danych[710].

2.2. Odpowiednie zabezpieczenia lub odstępstwa w rozumieniu RODO stosowane przez wybrane podmioty przekazujące dane osobowe z Unii Europejskiej do Chin

Przedstawiony w pkt 2.1 rozdziału przegląd odpowiednich zabezpieczeń i odstępstw, o których mowa w RODO wskazuje na możliwości, jakimi dysponuje administrator danych lub podmiot przetwarzający dane na zlecenie w sytuacji transferu

[703] Ocena i wykaz zabezpieczeń muszą znaleźć się w rejestrze czynności przetwarzania – por. art. 49 ust. 6 RODO.
[704] C. Kuner: *Komentarz do art. 49…,* s. 853; U. Wuermeling, I. Oldani: *Regulation of International…,* s. 53.
[705] U. Wuermeling, I. Oldani: *Regulation of International…*, s. 53.
[706] L. Wittershagen: *Alternative Data Transfer…,* s. 274; podobnie: P. Drobek *Komentarz do art. 49*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2018.
[707] C. Kuner: *Komentarz do art. 49…,* s. 854.
[708] H.B. Bentzen, O.H. Kvammen, G. Ursin: *Maximizing the GDPR…,* s. 3.
[709] Tak: P. Barta, P. Litwiński, M. Kawecki: *Komentarz do art. 49.* W: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. i swobodnym przepływem takich danych. Komentarz.* Red. P. Barta, P. Litwiński, M. Kawecki. C.H. Beck, Warszawa 2017, s. 660.
[710] Ibid.

danych osobowych do każdego państwa trzeciego nieobjętego decyzją w sprawie adekwatności. Z uwagi na przedmiot badań, szczególnie interesujący jest zestaw zabezpieczeń i odstępstw, o których mowa w RODO, które wykorzystują podmioty zaangażowane w przekazywanie danych osobowych z Unii Europejskiej do Chin. W związku z tym, poddałem analizie dokumenty informujące o przetwarzaniu danych osobowych, zwłaszcza polityki prywatności, wybranych przedsiębiorców chińskich obecnych na rynku europejskim. Przedmiot analizy stanowiły postanowienia polityk prywatności w zakresie przekazywania danych osobowych do państw trzecich, w tym w szczególności do Chin. Przedmiotem analizy[711] były polityki prywatności: Xiaomi[712], Huawei[713], ZTE[714], Hisense[715], Haier[716], Oppo[717], TikTok[718], Aliexpress[719], Tencent[720],

[711] O czym była mowa we wstępie, wybór 13 podmiotów był podyktowany popularnością oraz rozmiarem działalności wybranych marek na rynkach europejskich.

[712] Xiaomi: *Polityka Prywatności Xiaomi*. https://privacy.mi.com/all/pl_PL/ [dostęp: 10.08.2023], dalej: Polityka Xiaomi.

[713] Huawei: *Polityka Prywantości Huawei Polska*. https://consumer.huawei.com/pl/privacy/privacy-policy/ [dostęp: 10.08.2023], dalej: Polityka Huawei Polska; Huawei: *Privacy Policy Huawei Technologies LTD*. https://www.huawei.com/en/privacy-policy [dostęp: 10.08.2023], dalej: Polityka Huawei LTD.

[714] ZTE: *Privacy Policy ZTE Corpotation*. https://www.zte.com.cn/global/privacy_center/privacy_policy.html accessed [dostęp: 10.08.2023], dalej: Polityka ZTE; ZTE: *Privacy Policy ZTE Corporation - Devices*. https://ztedevices.com/en-us/legal/privacy-policy/ [dostęp: 10.08.2023], dalej: Polityka ZTE Devices.

[715] Hisense: *Polityka Prywatności Hisense Polska (Gorenje Polska)*. https://pl.hisense.com/polityka-prywatnosci-hisense [dostęp: 10.08.2023], dalej: Polityka Hisense Polska; Hisense: *Privacy Policy Hisense International Co., Ltd*. https://global.hisense.com/privacy-policy [dostęp: 10.08.2023], dalej: Polityka Hisense; Hisense: *Processing of Personal Data That You Enter in the Forms on the Website and E-News Subscription Hisense Europe*. https://www.hisense-europe.com/en/data_protection [dostęp: 10.08.2023], dalej: Polityka Hisense Europa; Hisense: *External Privacy Notice Hisense UK*. https://hisense.co.uk/external-privacy-notice/ [dostęp: 10.08.2023], dalej: Polityka Hisense UK.

[716] Haier: *Oświadczenie o Ochronie Prywatności Klientów Haier Europe (Candy Hoover Group S.r.l.).* https://www.haier-europe.com/pl_PL/polityka-prywatnosci/ [dostęp: 10.08.2023], dalej: Polityka Haier Europa; Haier: *Privacy Statement Haier Group (Haier Group Corporation)*. https://www.haier.com/global/privacy/ [dostęp: 10.8.2023], dalej: Polityka Haier.

[717] Oppo: *Privacy Notice Oppo Global*. https://www.oppo.com/en/privacy/# [dostęp: 10.8.2023], dalej: Polityka Oppo.

[718] TikTok: *Polityka prywatności.* https://www.tiktok.com/legal/page/eea/privacy-policy/pl-PL [dostęp: 10.08.2023], dalej: Polityka Tiktok – wersja dla Europy; TikTok: *Privacy Policy Tiktok (Wersja Dla Pozostałych Regionów).* https://www.tiktok.com/legal/page/row/privacy-policy/en. [dostęp: 10.08.2023], dalej: Polityka Tiktok - wersja dla pozostałych regionów.

[719] Aliexpress: *Privacy Policy Aliexpress*. https://terms.alicdn.com/legal-agreement/terms/suit_bu1_aliexpress/suit_bu1_aliexpress201909171350_82407.html [dostęp: 10.08.2023], dalej: Polityka Aliexpress.

[720] Tencent: *Privacy Policy Tencent*. https://www.tencent.com/en-us/privacy-policy.html [dostęp: 10.08.2023], dalej: Polityka Tencent; Tencent: *Privacy Policy Tencent Cloud*. https://www.tencentcloud.com/document/product/301/17345 [dostęp: 10.08.2023], dalej: Polityka Tencent Cloud.

QQ[721], Baidu[722], WeChat[723] oraz Weixin[724], będącej wersją Wechat działającą na terytorium Chin.

2.2.1. Zakres zastosowania polityk prywatności do przekazywania danych osobowych do państw trzecich

Część z podmiotów opublikowała polityki prywatności na jednej, ogólnoeuropejskiej stronie internetowej, natomiast niektóre podmioty stworzyły globalne i lokalne strony internetowe[725]. Niektóre polityki prywatności rozróżniają transfery, w zależności od miejsca przeznaczenia danych. Wówczas osobną kategorię stanowią transfery danych osobowych odbywające się między infrastrukturą lub jednostkami powiązanymi z administratorem, które są zlokalizowane w państwach trzecich[726] oraz transfery danych osobowych z terytorium EOG na terytorium państwa trzeciego. Na tle przywołanego podziału wyróżnia się przypadek TikTok, który dokładnie opisuje transfer danych osobowych z EOG do państw trzecich[727], oraz w osobnej części polityki przedstawia szczególne wymagania dotyczące transferów, które mogą wynikać z lokalnych jurysdykcji (np. w Argentynie, czy w Australii)[728]. Podobne rozwiązanie zastosował Aliexpress, przy czym opisy wymagań typowych dla poszczególnych jurysdykcji

[721] QQ: *QQ International Privacy Policy*. https://international.qq.com/privacy/privacy_En.html [dostęp: 10.08.2023], dalej: Polityka QQ.
[722] Baidu: *Baidu Privacy Statement*. https://ir.baidu.com/baidu-statement-privacy-protection/ [dostęp: 10.08.2023], dalej: Polityka Baidu; Baidu: *Privacy Policy Baidu USA.* https://usa.baidu.com/privacy [dostęp: 10.08.2023], dalej: Polityka Baidu USA.
[723] WeChat: *WeChat Privacy Policy*. https://www.wechat.com/en/privacy_policy.html. [dostęp: 10.08.2023], dalej: Polityka WeChat.
[724] Weixin: *Weixin Privacy Protection Guidelines*. https://weixin.qq.com/cgi-bin/readtemplate?lang=en_US&t=weixin_agreement&s=privacy&cc=CN [dostęp: 10.08.2023], dalej: Polityka Weixin.
[725] Polityka Huawei, Polityka Hisense, Polityka Haier.
[726] Polityka Xiaomi, Polityka Huawei, Polityka ZTE, Polityka Haier, Polityka Oppo, Polityka TikTok, Polityka AliExpress, Polityka QQ, Polityka Baidu, Polityka WeChat.
[727] Polityka TikTok – wersja dla Europy: "Gdy przekazujemy informacje o użytkowniku poza obszar EOG, Wielką Brytanię lub Szwajcarię, zapewniamy im odpowiedni poziom ochrony danych, polegając na:
Decyzjach stwierdzających odpowiedni stopień ochrony. Są to decyzje Komisji Europejskiej wydawane na podstawie art. 45 RODO (lub równoważne decyzje na mocy innych przepisów), w których uznaje ona, że dany kraj zapewnia odpowiedni stopień ochrony danych. Informacje o użytkowniku, jak opisano w sekcji „Jakie informacje zbieramy" przekazujemy do niektórych krajów na podstawie decyzji stwierdzających odpowiedni poziom ochrony dla tych krajów, które wymieniono tutaj; lub
Standardowych klauzulach umownych. Na mocy art. 46 RODO Komisja Europejska zatwierdziła klauzule umowne, które umożliwiają spółkom z EOG przekazywanie danych poza EOG. Te klauzule umowne (oraz ich zatwierdzone odpowiedniki dla Wielkiej Brytanii i Szwajcarii) to tzw. standardowe klauzule umowne. Polegamy na standardowych klauzulach umownych przy przekazywaniu informacji, jak opisano w sekcji „Jakie informacje zbieramy", określonym podmiotom w naszej Grupie korporacyjnej (jak opisano tutaj) oraz stronom trzecim w krajach, w których nie wydano decyzji stwierdzającej odpowiedni stopień ochrony. Aby uzyskać kopię decyzji stwierdzających odpowiedni poziom ochrony lub standardowych klauzul umownych, należy się skontaktować z nami, korzystając z danych podanych w poniższym punkcie „Kontakt z nami"."
[728] Polityka TikTok – wersja dla pozostałych regionów.

są mniej rozbudowane i ograniczają się do Chin, USA i Brazylii[729]. Na szczególną uwagę zasługuje przypadek Hisense oraz Tencent. Hisense przedstawiła zasady dotyczące transferów danych jedyne w lokalnej wersji polityki prywatności, adresowanej dla Zjednoczonego Królestwa[730]. Z kolei Tencent[731] nie zawarł informacji na temat transferów nie w ogólnej polityce prywatności, a wyłącznie w politykach prywatności związanych z poszczególnymi usługami[732].

Na aprobatę zasługuję wprowadzenie podziału na transfery danych między państwami trzecimi i transfery z EOG do państwa trzeciego. Dzięki temu jednostka jest w stanie zidentyfikować, które z postanowień polityki prywatności dotyczą jej przypadku. Wątpliwości wywołuje jednak praktyka Hisense oraz Tencent. W mojej ocenie taką praktykę można zakwalifikować jako wprowadzanie w błąd osoby, której dane dotyczą oraz naruszenie zasady przejrzystości przetwarzania danych. Zapoznając się z ogólnymi politykami prywatności tych podmiotów, osoba której dane dotyczą może odnieść wrażenie, że przetwarzanie jej danych osobowych nie wiąże się z transferem danych do państw trzecich, w tym do Chin. Temu wrażeniu przeczy wyłącznie lektura kolejnych polityk prywatność Hisense oraz Tencent. Tym samym, jednostka, po zapoznaniu się z dokumentacja dotyczącą przetwarzania danych Hisense oraz Tencent nie jest w stanie ustalić, czy transfer danych dotyczy tylko przypadku korzystania z konkretnej usługi

[729] Polityka AliExpress: "Depending on your location, the entity responsible for the handing of your personal information is:

- For users located in Mainland China: If you are a registered member of the Platform, and you are from mainland China, you are contracting with Hangzhou Alibaba Advertising Co., Ltd.
- For users located in the United States: If you are a registered member of the Platform, and you are from United States, you are contracting with AliExpress E-Commerce One Pte. Ltd.
- For users located in Brazil: Users in Brazil are contracting with Alibaba.com Singapore E-Commerce Private Limited (incorporated in Singapore with Company Reg. No. 200720572D).
- For users in other locations: If you are a registered member of the Platform, and either
    - (a) you are from a place other than mainland China, and United States; or
    - (b) you access and use the Platform from any of the Relevant Jurisdictions, you are contracting with Alibaba.com Singapore E-Commerce Private Limited (incorporated in Singapore with Company Reg. No. 200720572D).

Notwithstanding anything to the contrary in the foregoing provisions in this section, if you are a registered member of AliExpress, and you are resident in or access and use the Platform from any of the Relevant Jurisdictions, your contract is with AliExpress Russia Holding Private Limited (incorporated in Singapore with Company Reg. No. 201917627W).
"Relevant Jurisdictions" shall mean the Russian Federation, Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Turkmenistan, Tajikistan and Uzbekistan. In this regard, for users who access or use the Platform from a Relevant Jurisdiction, the Privacy Policy of "www.aliexpress.ru" and "www.tmall.ru" shall apply https://sell.aliexpress.com/ru/__pc/Zj6CxW2d6V.htm the extent that local data protection laws apply, the data controller of your personal information is the same as your contracting entity. For contact details, please see section O. HOW TO CONTACT US below."
[730] Polityka Hisense UK.
[731] Polityka Tencent.
[732] Polityka Tencent Cloud.

(Tencent), czy też korzystania z konkretnej usługi na terytorium wybranego państwa trzeciego (Hisense).

2.2.2. Odpowiednie zabezpieczenia w rozumieniu art. 46 RODO wykorzystywane przez podmioty chińskie

Poza przypadkiem Hisense, każda z polityk prywatności przedstawia pewne informacje na temat przyjętych zasad transferu danych osobowych do państw trzecich, w tym stosowanych odpowiednich zabezpieczeń w rozumieniu art. 46 RODO. Na potrzeby niniejszej pracy, ograniczam dalsze rozważania do zasad dotyczących transferów danych osobowych z EOG do państw trzecich. Najczęściej przywoływanym odpowiednim zabezpieczeniem w rozumieniu art. 46 RODO są klauzule umowne[733]. Niekiedy administratorzy wprost wskazują, że mowa o standardowych klauzulach umownych publikowanych przez Komisję Europejską[734]. Częściej jednak mowa po prostu o klauzulach umownych. Zdarza się także wzmianka o umownym zabezpieczeniu transferu[735].

Dla części z administratorów, dodatkowym środkiem legalizacji transferów danych są decyzje w sprawie adekwatności. W takiej sytuacji, opis zasad transferu danych osobowych do państw trzecich rozpoczyna wyjaśnienie, że dane mogą trafić na terytorium państwa objętego taką decyzją, a w razie jej braku zostaną zastosowane inne środki legalizacji[736]. Jak już była o tym mowa, dla polityk prywatności Huawei[737]

[733] Polityka Huawei Polska, Polityka Hisense UK, Polityka Xiaomi, Polityka Huawei LTD, Polityka Oppo, Polityka ZTE, Polityka Haier, Polityka Aliexpress, Polityka Tencent Cloud, Polityka WeChat.
[734] Polityka WeChat, Polityka Tencent Cloud.
[735] Np.: Polityka ZTE pkt 7: „Wherever ZTE may transfer your personal data, we will, pursuant to applicable laws, take every reasonable and necessary measure to ensure your data security, inform you of the destination, recipient, and other related information in a timely manner, and take appropriate measures to comply with this Policy and applicable local laws. For instance, to transfer your personal data, we will seek prior consent or sign a necessary data transfer contract with the receiver."
[736] Polityka Huawei Polska, Polityka Huawei LTD, Polityka Hisense UK, Polityka Oppo.
[737] Polityka Huawei LTD: "As a global company, your personal data collected by Huawei may be processed or accessed in the country/region where you use our products and services or in other countries/regions where Huawei or its affiliates, subsidiaries, service providers or business partners have a presence. These jurisdictions may have different data protection laws. In such circumstances, Huawei will take measures to ensure that data is processed as required by this Policy and applicable laws, which includes when transferring the data subject's personal data from the EU to a country or region which has not yet been acknowledged by the EU Commission as having an adequate level of data protection, we may use a variety of legal mechanisms, such as signing standard contractual clauses approved by the EU Commission, obtaining the consent to the cross-border transfer of a data subject in the EU, or implementing security measures like anonymizing personal data before cross-border data transfer. You can click here to obtain a copy of the EU's standard contractual clauses."
Polityka Huawei Polska pkt 3: "W jaki sposób udostępniamy dane użytkownika" pkt 6 " Dane osobowe użytkownika są przechowywane na terenie UE. Huawei przestrzega wszystkich obowiązujących wymogów prawnych, by chronić dane osobowe obywateli UE przekazywane poza EOG. Aby móc udostępniać dane w obrębie naszej grupy, stosujemy standardowe klauzule umowne UE lub udostępniamy dane do krajów wobec których została wydana decyzja stwierdzająca odpowiedni poziom ochrony danych w celu

Hisense[738] i TikTok są to jedyne, oprócz klauzul umownych, dostępne rozwiązania legalizacji transferu.

Cechą wspólną większości polityk prywatności jest brak enumeratywnej listy odpowiednich zabezpieczeń w rozumieniu art. 46 RODO, z których zamierza korzystać administrator. W otwartych katalogach, autorzy polityk prywatności powtarzaj frazę, której sensem jest zapewnienie jednostki o stosowaniu środków wymaganych przez przepisy RODO lub szerzej, przez prawo właściwe. Do tak ogólnego opisu ogranicza się polityka prywatności QQ[739] oraz polityka prywatności Xiaomi[740]. Pozostałe podmioty

---

zapewnienia jednakowego poziomu ochrony danych osobowych użytkownika nawet w miejscach, gdzie przepisy UE nie mają bezpośredniego zastosowania."

[738] Polityka Hisense UK pkt H "International transfer of Personal Data": "We transfer Personal Data to recipients in other countries. Where we transfer Personal Data from the EEA to a recipient outside the EEA that is not in an Adequate Jurisdiction, we do so on the basis of Standard Contractual Clauses."

[739] Polityka QQ: "How We Store and Share Your Personal Information" "In order to perform our contract with you, your personal information will be accessible from and will be processed on our servers. Our servers are located in the People's Republic of China. We are committed to maintaining the privacy and integrity of your personal information no matter where it is stored. Our group companies have information security and access policies that limit access to our systems and technology. We also protect data through the use of technological protection measures such as encryption. Your personal information will remain subject to our technical and organisational controls and our policies and procedures (including this Privacy Policy).

We share your personal information with selected third parties in and outside your country, including:

- third parties where you have requested that we share your data to allow you to use third party services; related group companies with whom we share all of your personal information to operate the Services. The transfers contemplated above are made pursuant to our contract with you;
- service providers who provide services on our behalf to support our Services. These services may include: fulfilling orders, payment processing, providing customer service, sending marketing communications, fulfilling subscription services, conducting research and analysis, and providing cloud computing infrastructure. These companies are authorized to retain, use, and disclose your personal information only as necessary to provide these services to us.
- law enforcement agencies, public authorities or other judicial bodies and organisations. We disclose information if we are legally required to do so, or if we have a good faith belief that such use is reasonably necessary to:
    - comply with a legal obligation, process or request;
    - enforce our terms of service and other agreements, policies, and standards, including investigation of any potential violation thereof;
    - detect, prevent or otherwise address security, fraud or technical issues; or
    - protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law (including exchanging information with other companies and organisations for the purposes of fraud protection); and
- a third party that acquires all or substantially all of us or our business. We will disclose information to a third party in the event that we sell or buy any business or undergo a merger, in which case we will disclose your data to the prospective buyer of such business. We will also disclose information to a third party if we sell, buy, merge or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets."

[740] Por. Polityka Xiaomi: "Za każdym razem, gdy Xiaomi udostępnia dane osobowe użytkowników z EOG zewnętrznym dostawcom usług, którzy mogą, ale nie muszą być jednostką Xiaomi poza EOG, udostępniamy je w zgodzie z klauzulami umownymi lub innymi środkami bezpieczeństwa zawartymi w RODO. Możesz dowiedzieć się o konkretnych zabezpieczeniach, które wprowadziliśmy lub poprosić o kopię, kontaktując się z nami pod adresem https://privacy.mi.com/support."

Polityka Aliexpres pkt M "INTERNATIONAL TRANSFERS OF PERSONAL DATA": "We take appropriate steps to ensure that recipients of your personal information are bound to duties of confidentiality and we implement appropriate measures to ensure your personal information will remain protected in

zasadniczo wskazują przykładowe lub preferowane środki legalizacji transferów poza EOG. Po raz kolejny, wyjątkiem jest polityka prywatności Hisense w wersji adresowanej dla Zjednoczonego Królestwa. Jako jedyna polityka prywatności nie zawiera ogólnego zdania o stosowaniu środków zgodnych z przepisami prawa. Zamiast tego jednoznacznie wskazano, że dane będą przekazywane na terytorium państw trzecich, które uzyskały decyzję w sprawie adekwatności, a w razie jej braku z wykorzystaniem standardowych klauzul umownych, których egzemplarz można pozyskać poprzez kontakt z infolinią[741]. Podobny model przyjęto także w polityce prywatności Oppo[742], która, tak jak Hisense, preferuje transfery danych osobowych do państw trzecich objętych decyzjami w sprawie adekwatności, a w braku takich decyzji, na podstawie standardowych klauzul umownych, dostępnych dla jednostki na życzenie. Najwyższy stopień precyzji cechuje politykę prywatności TikTok Europa, Tencent Cloud oraz WeChat. Tencent Cloud wyjaśnia, że transfery danych osobowych poza EOG lub UK będą się odbywały na podstawie standardowych klauzul umownych opublikowanych przez Komisję Europejską, odpowiednio w wersji dla stosunków administrator – administrator oraz administrator – podmiot przetwarzający[743]. Natomiast w przypadku WeChat ograniczono się do

---

accordance with this Privacy Policy, such as standard contractual clauses or other mechanism provided for in the applicable law."

[741] Polityka Hisense UK pkt H "International transfer of Personal Data": "We transfer Personal Data to recipients in other countries. Where we transfer Personal Data from the EEA to a recipient outside the EEA that is not in an Adequate Jurisdiction, we do so on the basis of Standard Contractual Clauses.
Because of the international nature of our business, we transfer Personal Data within the Hisense group, and to third parties as noted in Section (G) above, in connection with the purposes set out in this Notice. For this reason, we transfer Personal Data to other countries that may have different laws and data protection compliance requirements to those that apply in the country in which you are located.
Where we transfer your Personal Data from the EEA to recipients located outside the EEA who are not in Adequate Jurisdictions, we do so on the basis of Standard Contractual Clauses. You are entitled to request a copy of our Standard Contractual Clauses using the contact details provided in Section (Q) below.
Please note that when you transfer any Personal Data directly to a Hisense entity established outside the EEA, we are not responsible for that transfer of your Personal Data. We will nevertheless Process your Personal Data, from the point at which we receive those data, in accordance with the provisions of this Notice."

[742] Polityka Oppo Sekcja B. GDPR-specific provisions: "II Additional Information on How Your Personal Data Is Transferred Globally" "In case your personal data is transferred to jurisdictions located outside of Europe, we will ensure that appropriate safeguards exist and are applied, such as:
1. the recipient of the personal data is located within a country that benefits from an "adequacy" decision of the European Commission;
2. the recipient has signed a contract based on "model contractual clauses" approved by the European Commission, obliging them to protect your personal data;
3. or in the absence of the above appropriate safeguards, we will ask you for your explicit consent for the cross-border transfer of your personal data or take any other measures that are recognised as providing a sufficient level of protection for your personal data.
For more information about the safeguards relating to personal data transfers outside of Europe, please submit your request via our DSR platform (https://www.oppo.com/en/privacy-feedback/)."

[743] Polityka Tencent Cloud: "Our servers may be located outside of the country you are located, for example in Mainland China. See below at How We Disclose and Store Your Personal Information for more information."
"We may disclose your personal information with selected third parties in and outside your country,

stwierdzenia, że środkiem legalizacji transferów danych będą standardowe klauzule umowne opublikowane przez Komisję Europejską[744].

Dodatkowo, w niektórych politykach prywatności pojawiają się wzmianki o technicznych zabezpieczeniach transferu. Huawei [745] i QQ [746], które poprzez przykładowe wyliczenie wyjaśniają, że odpowiednim zabezpieczeniem transferowanych danych osobowych może być ich szyfrowanie lub anonimizacja. Natomiast w polityce prywatności Haier zawarto bardzo ogólną wzmiankę o wykorzystywaniu odpowiednich zabezpieczeń IT[747].

Uważam, że przedstawione powyżej opisy stosowanych odpowiednich zabezpieczeń cechuje wątpliwa jakość. Otwarte katalogi odpowiednich zabezpieczeń sformułowano w taki sposób, że nie wiadomo które z nich faktycznie znajdą zastosowanie i kiedy może to mieć miejsce, co unaocznia przypadek polityk prywatności QQ i Xiaomi. Taka konstrukcja stawia osobę, której dotyczą w sytuacji niepewności oraz

---

including:
Third Parties where we use a third party service to: (a) process payments ; (b) provide customer support (including provision of a support database and ticketing); (c) send SMS service notification; or (d) provide other services, support, features or functionality as part of the Services, including those listed on our Third Parties page. Related group companies, including the entities listed on our Third Parties page, with whom we share your personal information to operate our Services. To the extent data is transferred outside of the EEA or UK for processing (for example, to Mainland China), we rely on the European Commission's model contracts for the transfer of personal data to third countries (i.e., the standard contractual clauses), pursuant to Decision 2001/497/EC (in the case of transfers to a controller) and Decision 2004/915/EC (in the case of transfers to a processor)."

[744] Polityka WeChat: „6. WHERE DO WE PROCESS YOUR DATA? WeChat is a global platform. Our engineering, technical, and other support teams are based in our offices around the world (including Singapore and the Netherlands), and may have incidental access to certain of your information, for example, in order to fix technical issues that you report. The Personal Information that we collect from you will be transferred to, stored at, or processed in Singapore and Hong Kong SAR. We rely on the European Commission's model contracts for the transfer of personal data to third countries."

[745] Polityka Huawei LTD: „Huawei will take measures to ensure that data is processed as required by this Policy and applicable laws, which includes when transferring the data subject's personal data from the EU to a country or region which has not yet been acknowledged by the EU Commission as having an adequate level of data protection, we may use a variety of legal mechanisms, such as signing standard contractual clauses approved by the EU Commission, obtaining the consent to the cross-border transfer of a data subject in the EU, or implementing security measures like anonymizing personal data before cross-border data transfer. You can click here to obtain a copy of the EU's standard contractual clauses."
Polityka Huawei Polska: „W przypadku danych osobowych pochodzących z Unii Europejskiej i Szwajcarii postępujemy zgodnie ze stosownymi przepisami prawa zapewniającymi odpowiednie zabezpieczenia transferu danych osobowych do krajów spoza Europejskiego Obszaru Gospodarczego (EOG) i Szwajcarii. Stosujemy różne mechanizmy prawne, takie jak standardowe klauzule umowne dotyczące transgranicznego przesyłania danych osobowych, lub środki zabezpieczające, takie jak anonimizacja danych przed dokonaniem transgranicznego transferu danych."

[746] Polityka QQ: „Our servers are located in the People's Republic of China. We are committed to maintaining the privacy and integrity of your personal information no matter where it is stored. Our group companies have information security and access policies that limit access to our systems and technology. We also protect data through the use of technological protection measures such as encryption."

[747] Polityka Haier: "Where we transfer your data to a country or jurisdiction that cannot guarantee the required level of protection as required by applicable privacy laws, we have enhanced our IT security measures to increase the protection of your personal data."

faktycznie uniemożliwia skuteczne wykorzystanie przysługujących jej praw. Uważam, że biorąc pod uwagę treść analizowanych polityk prywatności posługiwanie się otwartymi katalogami odpowiednich zabezpieczeń jest pozbawione sensu. Wynika to z faktu korzystania przez administratorów z ograniczonego zasobu odpowiednich zabezpieczeń. Dominującą rolę odgrywają wyłącznie klauzule umowne, w tym standardowe klauzule umowne. Natomiast pozostałe odpowiednie zabezpieczenia wskazane w art. 46 RODO, w tym wiążące reguły korporacyjne czy zatwierdzona certyfikacja nie zostały nawet wzmiankowane w treści analizowanych polityk prywatności. Nadto, analizowane polityki prywatności często odwołują się do przekazywania danych osobowych na podstawie decyzji w sprawie adekwatności. Jednakże, Huawei, Hisense, Oppo nie wyjaśniają, które z państw przeznaczenia danych są objęte tymi decyzjami i które dane będą tam przekazane. Tym samym, zapoznając się z obowiązującymi postanowieniami analizowanych polityk prywatności osoba, której dane dotyczą nie jest w stanie odczytać, czy jej dane trafią do państwa, wobec którego wydano decyzję w sprawie adekwatności, czy nie. Jednostka wie tylko, że potencjalnie taka sytuacja może mieć miejsce. Takie działanie uznaję za wyraz braku należytej staranności administratora, który powinien dążyć do przekazania osobie, której dane dotyczą zrozumiałego komunikatu na temat przetwarzania jej danych osobowych. W tym względzie wyróżnia się polityka prywatności TikTok, która zawiera hiperłącze, odsyłające czytelnika do listę państw przeznaczenia danych, dla których wykorzystywane są decyzje w sprawie adekwatności[748].

W świetle powyższego, sądzę, że także w odniesieniu do opisu stosowanych odpowiednich zabezpieczeń można mówić o zarzucie naruszenia zasady przejrzystości przetwarzania danych. Pobocznie, warto zwrócić uwagę, że jedynie polityka prywatności QQ wskazuje konkretnie lokalizację swoich serwerów[749]. Pozostali administratorzy albo pomijają to zagadnienie, albo przedstawiają klika lokalizacji[750], wyjaśniając, że dane

[748] Polityka TikTok wersja dla Europy: (…) „Decyzjach stwierdzających odpowiedni stopień ochrony. Są to decyzje Komisji Europejskiej wydawane na podstawie art. 45 RODO (lub równoważne decyzje na mocy innych przepisów), w których uznaje ona, że dany kraj zapewnia odpowiedni stopień ochrony danych. Informacje o użytkowniku, jak opisano w sekcji „Jakie informacje zbieramy" przekazujemy do niektórych krajów na podstawie decyzji stwierdzających odpowiedni poziom ochrony dla tych krajów, które wymieniono tutaj."

[749] Które znajdują się na terytorium Chin - por. Polityka QQ: "In order to perform our contract with you, your personal information will be accessible from and will be processed on our servers. Our servers are located in the People's Republic of China."

[750] Por. Polityka WeChat: „The Personal Information that we collect from you will be transferred to, stored at, or processed in Singapore and Hong Kong SAR.";
Polityka Tencent Cloud: "Our servers may be located outside of the country you are located, for example in Mainland China."

mogą trafić do każdej z nich[751]. Co więcej, o braku transparentności analizowanych polityk prywatności świadczą także te fragmenty, które nakazują jednostce kontakt z centrum informacyjnym celem pozyskania informacji na temat konkretnie stosowanych rozwiązań[752].

2.2.3. Odstępstwa, o których mowa w art. 49 RODO stosowane przez podmioty chińskie

Niektóre polityki prywatności[753] uzupełniają katalog odpowiednich zabezpieczeń o odstępstwa, o których mowa w art. 49 ust. 1 RODO. Nie jest to jednak wyraźnie wyartykułowane. Autorzy analizowanych polityk prywatności w żadnym miejscu nie wskazali, że poszczególne przesłanki legalizacji transferu danych osobowych mają charakter wyjątkowy, tj., że znajdą zastosowanie w ostateczności, gdy pozostałe rozwiązania (przesłanki) okażą się niemożliwe do wykorzystania.

Najczęściej powoływanym odstępstwem jest zgoda, o której mowa w art. 49 ust. 1 lit. a RODO. Czytelnik polityk prywatności jest wówczas informowany, że jednym z możliwych do wykorzystania środków legalizacji, najczęściej obok klauzul umownych, jest zgoda osoby, której dane dotyczą na transfer danych osobowych do państwa trzeciego[754]. Tym samym, osoba, której dane dotyczą nie jest informowana, że ma do czynienia ze szczególną podstawą transferu danych osobowych do państwa trzeciego, jak również o warunkach w jakich zgoda ma być udzielona, w tym o informacjach, które zgodnie z art. 49 ust. 1 lit a RODO musi przekazać jej administrator.

---

[751] Na szczególną uwagę zasługuję przypadek Huawei, który w krajowej wersji polityki prywatności informuje o przetwarzaniu danych osobowych użytkownika w Unii Europejskiej. Natomiast w wersji ogólnej stwierdza, że dane mogą być przechowywane w różnych lokalizacjach – por. Polityka Huawei Polska: „Dane osobowego użytkownika są przechowywane na terenie UE.”; Polityka Huawei LTD: “As a global company, your personal data collected by Huawei may be processed or accessed in the country/region where you use our products and services or in other countries/regions where Huawei or its affiliates, subsidiaries, service providers or business partners have a presence.”

[752] Polityka Xiaomi: „Możesz dowiedzieć się o konkretnych zabezpieczeniach, które wprowadziliśmy lub poprosić o kopię, kontaktując się z nami pod adresem https://privacy.mi.com/support."

[753] Polityka ZTE, Polityka Huawei LTD, Polityka Oppo, Polityka WeChat, Polityka Baidu.

[754] Polityka ZTE pkt 7: „For instance, to transfer your personal data, we will seek prior consent or sign a necessary data transfer contract with the receiver.”;
Polityka Huawei LTD: „In such circumstances, Huawei will take measures to ensure that data is processed as required by this Policy and applicable laws, which includes when transferring the data subject’s personal data from the EU to a country or region which has not yet been acknowledged by the EU Commission as having an adequate level of data protection, we may use a variety of legal mechanisms, such as signing standard contractual clauses approved by the EU Commission, obtaining the consent to the cross-border transfer of a data subject in the EU, or implementing security measures like anonymizing personal data before cross-border data transfer.”;
Polityka Oppo, Sekcja B. GDPR-specific provisions: „3. or in the absence of the above appropriate safeguards, we will ask you for your explicit consent for the cross-border transfer of your personal data or take any other measures that are recognised as providing a sufficient level of protection for your personal data.”

O wykorzystaniu innych odstępstw wskazanych w art. 49 ust. 1 RODO świadczą polityki prywatności Baidu[755], WeChat[756] oraz QQ[757]. Także i w tym przypadku nie został wyeksponowany wyjątkowych charakter odstępstw, o których mowa w art. 49 RODO.

Układ polityki prywatności Baidu jest na tyle skomplikowany, że dopiero wnikliwe zapoznanie się z jej treścią prowadzi do wniosku, że te same okoliczności, które legalizują udostępnienie danych, są także przesłankami prawidłowego, w ujęciu Baidu, transferu

[755] Polityka Baidu: „In the following circumstances, Baidu will disclose your personal information as you wish or in accordance with the law. You will be responsible for any consequences arising thereof:

- Your prior authorization is obtained;
- The products and the services you request can only be provided after disclosure of your personal data;
- As per the requirements of the relevant laws and regulations;
- As per the requirements of the competent government authority;
- To safeguard the legitimate rights and interests of Baidu;
- You agree to share the data with third parties;
- We discover that you have violated or are violating Baidu's terms and conditions or rules of use of any other products or services; or
- We need to provide the companies providing products or service on our behalf with your personal data (unless we notify you, such companies shall have no right to use or process your personal data). Baidu will take all appropriate measures to prevent the illegal or unlawful disclosure, modification or destruction of user's information.)."

[756] Polityka WeChat: „We do not share your information with third parties, except where we need to in order to provide the service (e.g., SMS service providers) or if we are instructed to by a court, authority or compelled by law."

[757] Polityka QQ: „We share your personal information with selected third parties in and outside your country, including:

- third parties where you have requested that we share your data to allow you to use third party services;
- related group companies with whom we share all of your personal information to operate the Services. The transfers contemplated above are made pursuant to our contract with you;
- service providers who provide services on our behalf to support our Services. These services may include: fulfilling orders, payment processing, providing customer service, sending marketing communications, fulfilling subscription services, conducting research and analysis, and providing cloud computing infrastructure. These companies are authorized to retain, use, and disclose your personal information only as necessary to provide these services to us.
- law enforcement agencies, public authorities or other judicial bodies and organisations. We disclose information if we are legally required to do so, or if we have a good faith belief that such use is reasonably necessary to:
- comply with a legal obligation, process or request;
- enforce our terms of service and other agreements, policies, and standards, including investigation of any potential violation thereof;
- detect, prevent or otherwise address security, fraud or technical issues; or protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law (including exchanging information with other companies and organisations for the purposes of fraud protection); and
- a third party that acquires all or substantially all of us or our business. We will disclose information to a third party in the event that we sell or buy any business or undergo a merger, in which case we will disclose your data to the prospective buyer of such business. We will also disclose information to a third party if we sell, buy, merge or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets."

danych osobowych.[758] Identyczną konstrukcję można dostrzec w polityce prywatności QQ[759]. Lektura odnośnych fragmentów polityk prywatności Baidu[760], QQ[761] i WeChat[762] prowadzi do wniosku, że oprócz zgody, wśród możliwych do wykorzystania odstępstw

[758] Autorzy polityki prywatności Baidu najpierw, lakonicznie, wyjaśnili, że dane osobowe mogą być przekazywane do państw trzecich, przy czym cele takiego przekazania znajdują się w dalszej części tekstu – por. Polityka Baidu "Transfer of Personal Data": „Please be informed that your personal data may be transferred to locations outside of the territory where you are accessing Baidu's services or disclosed to our related corporations, licensees, business partners and/or service providers for the purposes described above." Następnie, w dalszej części znalazły się omawiane okoliczności, ale z zaznaczeniem, że mowa o udostępnieniu danych osobowych.

[759] Polityka QQ.

[760] Polityka Baidu: „In the following circumstances, Baidu will disclose your personal information as you wish or in accordance with the law. You will be responsible for any consequences arising thereof:

- Your prior authorization is obtained;
- The products and the services you request can only be provided after disclosure of your personal data;
- As per the requirements of the relevant laws and regulations;
- As per the requirements of the competent government authority;
- To safeguard the legitimate rights and interests of Baidu;
- You agree to share the data with third parties;
- We discover that you have violated or are violating Baidu's terms and conditions or rules of use of any other products or services; or
- We need to provide the companies providing products or service on our behalf with your personal data (unless we notify you, such companies shall have no right to use or process your personal data). Baidu will take all appropriate measures to prevent the illegal or unlawful disclosure, modification or destruction of user's information.)."

[761] Polityka QQ: „We share your personal information with selected third parties in and outside your country, including:

- third parties where you have requested that we share your data to allow you to use third party services;
- related group companies with whom we share all of your personal information to operate the Services. The transfers contemplated above are made pursuant to our contract with you;
- service providers who provide services on our behalf to support our Services. These services may include: fulfilling orders, payment processing, providing customer service, sending marketing communications, fulfilling subscription services, conducting research and analysis, and providing cloud computing infrastructure. These companies are authorized to retain, use, and disclose your personal information only as necessary to provide these services to us.
- law enforcement agencies, public authorities or other judicial bodies and organisations. We disclose information if we are legally required to do so, or if we have a good faith belief that such use is reasonably necessary to:
- comply with a legal obligation, process or request;
- enforce our terms of service and other agreements, policies, and standards, including investigation of any potential violation thereof;
- detect, prevent or otherwise address security, fraud or technical issues; or protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law (including exchanging information with other companies and organisations for the purposes of fraud protection); and
- a third party that acquires all or substantially all of us or our business. We will disclose information to a third party in the event that we sell or buy any business or undergo a merger, in which case we will disclose your data to the prospective buyer of such business. We will also disclose information to a third party if we sell, buy, merge or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets."

[762] Polityka WeChat: „We do not share your information with third parties, except where we need to in order to provide the service (e.g., SMS service providers) or if we are instructed to by a court, authority or compelled by law."

można odnaleźć tzw. przesłankę umowną (art. 49 ust. 1 lit. b RODO). Natomiast polityki prywatności Baidu i QQ wskazują również na przesłankę dochodzenia roszczeń (art. 49 ust. 1 lit. e RODO). Nadto, w politykach prywatności Baidu, QQ oraz WeChat za podstawę transferu danych uznano wykonanie orzeczenia sądowego lub nakazu organów administracji, w tym organów ścigania.

W mojej ocenie podejście administratorów do wykorzystywania odstępstw, o których mowa w art. 49 ust. 1 RODO jest kolejnym przejawem braku należytej transparentności polityk prywatności. Odstępstwa zostały potraktowane jako zwyczajne, dodatkowe podstawy przekazania danych osobowych do państwa trzeciego. Żadne z postanowień analizowanych polityk prywatności nie wyjaśnia czytelnikowi, że wykorzystywania odstępstw, o których mowa w art. 49 ust. 1 RODO wiąże się ze szczególnymi zasadami.

W szczególności, polityki prywatności nie tłumaczą czytelnikowi, że możliwość posłużenia się m.in. zgodą na przekazanie danych do państwa trzeciego jest ograniczona do tych przypadków, gdy odpowiednie zabezpieczenia, o których mowa w art. 46 RODO nie nadają się do wykorzystania. Jednocześnie, mimo odwoływanie się przez polityki prywatności do zgody, o której mowa w art. 49 ust. 1 lit. a RODO, jako przesłanki transferu danych, brak jest szczegółowych informacji na temat funkcjonujących sposobów wyrażenia wyraźnej zgody, oraz przekazywania informacji na temat ryzyk, z jakimi wiąże się transfer danych do państwa trzeciego.

O braku należytej transparentności analizowanych polityk prywatności świadczy także sposób w jaki opisano podstawę prawną transferu danych osobowych, o której mowa w art. 48 RODO. Wspomniane polityki prywatności [763] lakonicznie wymieniają wykonanie orzeczenia sądowego lub nakazu organów państwa jako potencjalną podstawę dla transferu danych, ponownie z pominięciem pozostałych elementów, koniecznych dla prawidłowego zastosowania art. 48 RODO.

2.2.4. Odwołania do przepisów chińskiego prawa ochrony danych osobowych

Pobocznym, aczkolwiek, istotnym wątkiem przekazywania danych osobowych między Unią Europejską a Chinami są obowiązujące przepisy chińskiego prawa ochrony danych osobowych. Jak już była o tym mowa, zarówno CSL, jaki PIPL prezentują restrykcyjne podejście do transferu danych osobowych poza terytorium Chin. Jednakże, żadna z analizowanych polityk prywatności nie wyjaśnia, czy przepisy

[763] Polityka Baidu, Polityka QQ i Polityka WeChat.

chińskiego prawa ochrony danych osobowych znajdują zastosowanie do działalności administratora. Nie sposób uznać za takie wyjaśnienie ogólnego odwołania do właściwych przepisów prawa[764]. Uważam, że osobna sekcja polityki prywatności powinna opisywać zasady stosowania chińskich przepisów prawa do danych osobowych, które trafią na terytorium Chin. Jest to szczególnie ważne w tych wszystkich sytuacjach, gdy sam administrator wskazuje, że dane osobowe mogą trafić na terytorium Chin, jak w przypadku QQ[765].

3. Ocena kompatybilności odpowiednich zabezpieczeń i odstępstw, o których mowa w RODO dla przekazywania danych osobowych między Unią Europejską a Chinami w świetle poglądów doktryny oraz wyników analizy polityk prywatności wybranych podmiotów chińskich

Przeprowadzona analiza treści wybranych polityk prywatności pozwala na przejście do dalszej części rozważań i omówienie, z uwzględnieniem poglądów doktryny, kompatybilności odpowiednich zabezpieczeń i odstępstw, o których mowa w RODO dla przekazywania danych osobowych między Unią Europejską a Chinami. Są to bowiem jedyne dostępne podstawy przekazywania danych osobowych do państwa trzeciego nieobjętego decyzją w sprawie adekwatności, a do tej kategorii zaliczają się Chiny. Uważam, że biorąc pod uwagę spostrzeżenia doktryny oraz treść analizowany polityk prywatności, można mówić o czterech okolicznościach dotyczących odpowiednich zabezpieczeń, które świadczą o ich ograniczonej przydatności dla wykorzystania na potrzeby transferów danych osobowych między Unią Europejską a Chinami.

3.1. Faktycznie ograniczony katalog odpowiednich zabezpieczeń

Artykuł 46 ust. 1 RODO za odpowiednie zabezpieczenia uznaje publiczno-prawny instrument, wiążące reguły korporacyjne (BCR), klauzule umowne (SCC), kodeks postępowania, certyfikacja. Dodatkowo, możliwe jest wykorzystanie innego zabezpieczenia, przy czym w takiej sytuacji konieczne jest uzyskania zezwolenia organu nadzorczego.

---

[764] Por. Polityka Baidu: „In the following circumstances, Baidu will disclose your personal information as you wish or in accordance with the law";
Polityka Huawei LTD: „In such circumstances, Huawei will take measures to ensure that data is processed as required by this Policy and applicable laws (…)";
Polityka Haier: "Where we transfer your data to a country or jurisdiction that cannot guarantee the required level of protection as required by applicable privacy laws, we have enhanced our IT security measures to increase the protection of your personal data."

[765] Które znajdują się na terytorium Chin - por. Polityka QQ: "In order to perform our contract with you, your personal information will be accessible from and will be processed on our servers. Our servers are located in the People's Republic of China."

Co potwierdza przeprowadzona analiza wybranych polityk prywatności podmiotów chińskich, spośród wszystkich odpowiednich zabezpieczeń, o których mowa w art. 46 RODO, to klauzule umowne są najczęściej stosowanym odpowiednim zabezpieczeniem. Rację ma więc M. Krzysztofek, uznający za zaletę standardowych klauzul umownych ich kompatybilność do legalizacji transferów, które są systemowe i o dużej skali [766]. Jednocześnie, w tym względzie przypadek transferów danych osobowych do Chin potwierdza, że w praktyce klauzule umowne stanowią najpopularniejszy środek legalizacji transferów danych osobowych[767].

Zgadzam się ze stanowiskiem, w myśl którego zaletą odpowiednich zabezpieczeń w ogólności jest możliwość ich zastosowania, w tym przystąpienia do nich, przez podmioty, które nie są objęte zakresem zastosowania RODO[768]. Popularność klauzul umownych, o której wspomina doktryna skutkuje jednak tym, że katalog odpowiednich zabezpieczeń jest faktycznie ograniczony.

Na szczególną uwagę zasługują w tym względzie wiążące reguły korporacyjne, za których zaletę poczytuje się szeroką definicję grupy [769]. Nadto, wiążące reguły korporacyjne cechuje większa stabilność w porównaniu ze standardowymi klauzulami umownymi, kodeksami postępowania czy odstępstwami (w szczególności z przesłanką zgody jako podstawy prawnej transferu danych osobowych)[770]. Jednakże, dla transferów danych osobowych do Chin wiążące reguły korporacyjne mają marginalne znaczenie.

[766] M. Krzysztofek: *Komentarz do art. 46 RODO…,* s. 259.
[767] Tak: L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses…,* s. 10; C. Kuner: *The Path to…,* s. 71; OECD: *Fostering Cross-Border*…, s. 19.
[768] C. Kuner: *Komentarz do art. 46…,* s. 807–808; C. Vander Maelen: *EDPB Releases Final Version of 'Guidelines 04/2021 on Codes of Conduct as Tools for Transfers' – An Important Step with Some Rough Edges*. „European Data Protection Law Review", 2022, nr 3, s. 392, 393; JD Supra: *Get Ready to Update Your Binding Corporate Rules Regulators Expand Requirements*. 7.07.2023, Newstex Blogs LexisNexis; L. Wittershagen: *Alternative Data Transfer…,* s. 227.
[769] M. Krzysztofek: *Komentarz do art. 47 RODO* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C.H. Beck, Warszawa 2016, s. 268; C. Kuner: *Komentarz do art. 47*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020, s. 820; U. Wuermeling, I. Oldani: *Data Transfers…,* s. 42; P. Fajgielski *Komentarz do rozporządzenia nr 2016/679 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), art. 47.* W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022; por. JD Supra: *Get Ready to*…; Odmiennie - L. Determann: *Determann's Field Guide to Data Privacy Law*. Edward Elgar Publishing, Cheltenham 2022, s. 43 - autor argumentuje swoje stanowisko koniecznością dodatkowego uregulowania transferów danych w ramach dalszego powierzenia przetwarzania, które jako nienależące do grupy, nie będą objęte wiążącymi regułami korporacyjnymi; L. Wittershagen: *Transfer of Personal…,* s. 72 - dla Wittershagena luźne relacje między członkami grupy wykluczają zastosowanie wiążących reguł korporacyjnych.
[770] A. Flor: *The Impact of Schrems II: Next Steps for U.S. Data Privacy Law*. „Notre Dame Law Review", 2021, nr 5, s. 2049; L. Determann: *Determann's Field Guide…,* s. 47.

Żadna z analizowanych polityk prywatności nie wzmiankuje o wdrożeniu przez administratora wiążących reguł korporacyjnych jako odpowiedniego zabezpieczenia dla transferu danych osobowych.

W przypadku kodeksów postępowania oraz certyfikacji poglądy doktryny skupiają się na ekspozycji problemów związanych z ich stosowaniem. Za wadę tak kodeksów postępowania, jak i certyfikacji uznaje się wątpliwe zdolności organów oceniających do oceny podmiotu ubiegającego się o przyłączenie do kodeksów postępowania lub przyznanie certyfikatu oraz oceny systemu prawnego państwa trzeciego[771]. Zwłaszcza ten ostatni element budzi wątpliwości, ponieważ, o czym wspominają L. Dreschler i I. Kamara[772], tak długo jak odpowiednie kryteria oceny systemu prawnego państwa trzeciego nie wynikają wprost z oceny przeprowadzanej w ramach przystąpienia, odpowiednio, do kodeksu postępowania lub certyfikacji, podmiot oceniający nie weźmie ich pod rozwagę. Trudno także oczekiwać, że taki podmiot będzie przeprowadzał pogłębioną analizę systemu prawnego importera danych, który ubiega się o przyłączenie do kodeksu postępowania lub certyfikacji[773]. Wadą kodeksów postępowania jest niejasna procedura ich zatwierdzania [774]. W mojej ocenie jest to najpoważniejsza wada kodeksów postępowania i certyfikacji. Zgadzam, się, że komplikacją, związaną ze stosowaniem certyfikacji lub kodeksu postępowania jest sformalizowanie wiążącego zobowiązania importera danych do przestrzegania zasad certyfikacji lub kodeksu postępowania, które zazwyczaj przybierze postać odpowiedniej umowy[775]. To z kolei uzasadnia stanowisko o niewielkiej popularności kodeksów postępowania jako środków legalizacji transferów danych osobowych[776]. Uważam, że dodatkową okolicznością, wpływającą na niewielką popularność stosowania kodeksów postępowania, jak i certyfikacji, jest ryzyko nadużyć. Parlament Europejski, oceniając funkcjonowanie Tarczy Prywatności, a więc swego

[771] L. Drechsler, I. Kamara: *Essential equivalence as…*; pośrednio C. Vander Maelen: *EDPB Releases Final…,* s. 396.
[772] L. Drechsler, I.Kamara: *Essential equivalence as…*, s. 245.
[773] Ibidem.
[774] C. Vander Maelen: *EDPB Releases Final…,* s. 394.
[775] R. Leenes: *Komentarz do art. 42.* W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020, s. 736; U. Wuermeling, I. Oldani: *Data Transfers…,* s. 43; L. Wittershagen: *Alternative Data Transfer*…, s. 257; Europejska Rada Ochrony Danych Osobowych: *Guidelines 07/2022 on*…, pkt 53.
[776] L. Wittershagen: *Alternative Data Transfer*…, s. 259 - autor zwraca uwagę, że w dacie sporządzania artykułu (artykuł został opublikowany w 2023 r.) nie było ani jednego zatwierdzonego kodeksu postępowania.

rodzaju certyfikacji, zwracał uwagę na zjawisko powoływania się przez przedsiębiorców na fakt posiadania certyfikatu, jeszcze przed jego formalnym przyznaniem[777].

Popularność klauzul umownych może wywołać złudne wrażenie o braku jakichkolwiek trudności dotyczących ich stosowania. L. Determann uważa, że ograniczenie swobody podmiotu korzystającego ze standardowych klauzul umownych, (ale także i wiążących reguł korporacyjnych czy certyfikacji) poprzez narzucenie sztywnych ram wskazanych zabezpieczeń, jest wadą[778]. Jest to szczególnie widoczne w przypadku standardowych klauzul umownych. Standardowe klauzule umowne dopuszczają jedynie niewielki stopień zmian ich treści, którego naruszenie skutkuje zmianą charakteru klauzul, tj. standardowe klauzule stają się klauzulami *ad hoc*, które wymagają zatwierdzenia przez właściwy organ nadzoru[779]. Sądzę, że zarzut niewielkiej swobody podmiotu korzystającego ze standardowych klauzul umownych nie jest w pełni uzasadniony. Implementacja odpowiedniego zabezpieczenia, którego pożądana treść jest odgórnie narzucona jest znacznym ułatwieniem dla administratorów lub podmiotów przetwarzających, którym można przypisać status mikro, małego lub średniego przedsiębiorstwa.

Sztywne ramy treściowe klauzul umownych, a w szczególności standardowych klauzul umownych stają się jednak poważną wadą na tle obowiązku ich ujednolicania i dostosowywania do przepisów także innych systemów prawnych lub organizacji, na terytorium których mają trafić dane osobowe[780]. W mojej ocenie jest to szczególnie problematyczne dla podmiotów, które przekazują dane osobowe do Chin, mając na względzie wątpliwy poziom ochrony danych osobowych zapewniany przez tamtejsze przepisy, a zarazem uprawnienia organów chińskich w zakresie dostępu do danych osobowych.

---

[777] *European Parliament Resolution on the Adequacy of the Protection Afforded by the EU- US Privacy Shield*. 26.06.2018, https://www.europarl.europa.eu/doceo/document/B-8-2018-0305_EN.pdf [dostęp: 19.10.2021], pkt 10.

[778] L. Determann: *Determann's Field Guide*…, s. 41.

[779] B. Fischer: *Komentarz do art. 46 RODO*…, s. 473–473; U. Wuermeling and I. Oldani: *Data Transfers in*…, s. 39; Fajgielski *Komentarz do rozporządzenia nr 2016/679 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), art. 46*…,; L. Determann: *Determann's Field Guide*…, s. 39; Odmiennie por. P. Jurcys, M. Corrales Compagnucci, M. Fenwick: *The future of international data transfers: Managing legal risk with a 'user-held' data model*. „Computer Law & Security Review", 2022, nr 46.

[780] L. Determann: *Determann's Field Guide*…, s. 40.

3.2. Nakłady i koszty związane ze stosowaniem odpowiednich zabezpieczeń

Stosowanie odpowiednich zabezpieczeń, w tym standardowych klauzul umownych, wiąże się wysokimi nakładami czasu i pracy. Koszty implementacji są przedstawiane jako czynnik odstraszający grupy przedsiębiorstw od stworzenia i implementacji wiążących reguł korporacyjnych [781]. Źródłem wysokich kosztów stworzenia i implementacji wiążących reguł korporacyjnych jest konieczność stworzenia kilku ich wersji. L. Determann tłumaczy to chęcią uniknięcia rozciągania surowych standardów RODO na wszelkie transfery danych osobowych, a więc także na te transfery, które nie mają źródła w Unii Europejskiej lub nie dotyczą danych osób znajdujących się w Unii Europejskiej [782]. Sądzę, że jest to dodatkowa okoliczność, wpływająca na niewielką popularność tego odpowiedniego zabezpieczania.

Wykorzystywanie standardowych klauzul umownych nie oznacza jednak braku jakichkolwiek nakładów. Według S. Pietrzak za zaletę wiążących reguł korporacyjnych uznaje się mniejsze nakłady pracy w porównaniu ze standardowymi klauzulami umownymi[783]. Autorka wyjaśnia, że jest to konsekwencją konieczności opracowania kilku rodzajów umów, stosownie do miejsca przeznaczenia danych, a następnie ich zawierania z różnymi podmiotami. Zgadzam się z tym stanowiskiem, w szczególności biorąc pod uwagę konieczność uzupełnienia treści odpowiednich zabezpieczeń, w tym klauzul umownych. Uważam, że niewielkie znaczenie ma w tym względzie fakt, że klauzule umowne, o których mowa w RODO mogą być uwzględnione w umowie powierzenia przetwarzania a nie muszą, każdorazowo, stanowić odrębną umowę[784].

Obowiązek uzupełnienia odpowiednich zabezpieczeń wiąże się z problematyką poziomu ochrony danych osobowych zapewnianego przez państwo trzecie. Jak zauważa L. Bradford, M. Aboy i K. Liddell RODO nie określa jednoznacznie skąd mają wynikać prawa jednostki, tj. czy ma to być prawo miejsca przeznaczenia danych czy miejsca ich eksportu[785]. Uzupełnienie odpowiednich zabezpieczeń może więc służyć zapewnieniu,

---

[781] S. Pietrzak: *Transborder Data Flows: Binding Corporate Rules as a global transfer mechanism and trusted data processing area* (praca magisterska - Master Thesis Law and Technology LLM - napisana pod kierunkiem dr I.E. Bayamlioglu; Mr.dr. C.M.K.C. Cuijpers) Tilburg University, Tilburg 2017, s. 20.

[782] L. Determann: *Determann's Field Guide*…, s. 43; pośrednio: Europejska Rada Ochrony Danych Osobowych: *Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)*. 20.06.2023. https://edpb.europa.eu/system/files/2023-06/edpb_recommendations_20221_bcr-c_v2_en.pdf [16.10.2023], pkt 11.

[783] S. Pietrzak: *Transborder Data Flows…,* s. 38 - autorka wyjaśnia, że wiąże się to z koniecznością opracowania kilku rodzajów umów, a następnie ich zawierania z różnymi podmiotami.

[784] Tak: U. Wuermeling and I. Oldani: *Data Transfers in…,* s. 34.

[785] L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses*…, s. 19.

że egzekwowalne prawa jednostki są obecne, bez względu na treść przepisów państwa przeznaczenia danych[786]. Na konieczność uzupełnienia odpowiednich zabezpieczeń może również wpływać problematyka dostępu organów ścigania państwa trzeciego do tychże danych[787]. Wówczas uzupełnienie odpowiednich zabezpieczeń będzie polegało na wyborze właściwych, uzupełniających zabezpieczeń ograniczających ten dostęp[788].

Zdaniem niektórych autorów, wadą standardowych klauzul umownych, co można odnieść także do pozostałych odpowiednich zabezpieczeń, jest faktyczne ograniczenie ich dostępności dla mniejszych podmiotów z uwagi na konieczność podjęcia dodatkowych działań, w tym przeprowadzenia oceny państwa trzeciego w ramach TIA[789]. Uważam, że jest to szczególnie istotne dla przypadku transferów danych osobowych do Chin, zwłaszcza mając na względzie skomplikowane relacje, jakie zachodzą między poszczególnymi przepisami chińskiego prawa ochrony danych osobowych. Zdaniem L. Dreschler i I. Kamary, ocena systemu prawnego państwa trzeciego w ramach TIA może odpowiadać ocenie przeprowadzanej na podstawie art. 45 RODO[790]. Stąd, dla X. Tracola obowiązek przeprowadzenia TIA powoduje, że przynajmniej w tym zakresie, różnice między standardowymi klauzulami umownymi a wiążącymi regułami korporacyjnymi zacierają się[791]. Zgadzam się z tą częścią doktryny, która uznaje obowiązek przeprowadzenia TIA za znaczne obciążenie administratora lub podmiotu przetwarzającego[792]. Sytuację administratora lub podmiotu przetwarzającego, działającego jako eksporter danych nieznacznie polepsza udział i wsparcie w przeprowadzeniu oceny w ramach TIA importera danych, a więc podmiotu

[786] P. Fajgielski: *Komentarz do rozporządzenia nr 2016/679 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), art. 46…,*; dotyczy to także klauzul *ad hoc* - tak: P. Barta, P. Litwiński, M. Kawecki: *Komentarz do art. 46.* W: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. i swobodnym przepływem takich danych. Komentarz.* Red. P. Barta, P. Litwiński, M. Kawecki. C.H. Beck, Warszawa 2017, s. 634–644.
[787] OECD: *Fostering Cross-Border…,* s. 27; A. Vats: *Data Free Flow with Trust: Is There a Solution in Sight?*. 28.01.2023. https://www.orfonline.org/expert-speak/data-free-flow-with-trust/ [dostęp:11.10.2023]; L. Wittershagen: *Alternative Data Transfer*…, s. 221, 260, 261; pośrednio - U. Wuermeling and I. Oldani: *Data Transfers in…* s. 36.
[788] L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses*…, s. 23–24, 32; por. Europejska Rada Ochrony Danych Osobowych: *Guidelines 07/2022 on…,* pkt. 22.
[789] L. Wittershagen: *Alternative Data Transfer*…, s. 238; A. Chander, P.M. Schwartz: *Privacy and/or Trade…,* s. 80.
[790] L. Drechsler, I. Kamara: *Essential equivalence as…,* s. 344–345.
[791] X. Tracol: *"Schrems II": The Return of the Privacy Shield*. „Computer Law & Security Review", 2020, nr 39, s. 9; pośrednio także: U. Wuermeling and I. Oldani: *Data Transfers in*…, s. 42.
[792] JD Supra: *10 Things You Should Know About the New Standard Contractual Clauses*. 7.06.2021. Newstex Blogs LexisNexis [dostęp: 13.10.2023]; U. Wuermeling and I. Oldani: *Data Transfers in*…, s. 35–36; L. Wittershagen: *Alternative Data Transfer*…, s. 221; por. JD Supra, *Get Ready to*….

zlokalizowanego w państwie przeznaczenia danych[793]. Wciąż jednak to administrator lub podmiot przetwarzający, czyli eksporter danych, ponosi odpowiedzialność za właściwe przeprowadzenie oceny w ramach TIA, która ma poprzedzać transfer danych[794]. Dlatego też wadą wiążących reguł korporacyjnych i standardowych klauzul umownych jest ciężar odpowiedzialności za ich naruszenie, który zasadniczo spoczywa na eksporterze danych osobowych, a więc na podmiocie zlokalizowanym na terytorium Unii Europejskiej[795].

Uważam, że rację ma L. Determann, dla którego utrudnieniem związanym ze stosowaniem standardowych klauzul umownych, czy klauzul umownych w ogólności, także w kontekście ich uzupełnienia, jest konieczność współpracy i negocjacji z podmiotami trzecimi, rozumianymi jako podmioty niepowiązane z podmiotem wysyłającym dane osobowe do państwa trzeciego (lub nienależącym do tej samej grupy co eksporter danych)[796]. L. Determann klasyfikuje takie sytuacje jako problematyczne, ponieważ wymagają dodatkowych nakładów czasu i pracy, ażeby przekonać i dostosować podmiot trzeci do przestrzegania określonych standardów ochrony danych osobowych, które stosują podmioty działające w Unii Europejskiej[797]. W mojej ocenie, jest to szczególna okoliczność utrudniająca posługiwanie się odpowiednimi zabezpieczeniami dla przekazywania danych osobowych do Chin. O czym była mowa w rozdziale II, chińskie prawo ochrony danych osobowych, a tym samym działające tam podmioty prezentują podejście do ochrony danych osobowych zgoła odmienne od podejścia Unii Europejskiej.

3.3. Wysoki poziom niepewności

Konsekwencją uzupełniania odpowiednich zabezpieczeń, poprzez wdrożenie dodatkowych, uzupełniających zabezpieczeń, jest wysoki poziom niepewności. Niepewność dotyczy samego wyboru uzupełniającego zabezpieczenia. Brak jest bowiem katalogu rozwiązań, które będą się nadawały do każdego przypadku. Nadto, odpowiednie

[793] O konieczności wsparcia eksporterów danych wspominają: L. Drechsler, I. Kamara: *Essential equivalence as…,* s. 343.
[794] U. Wuermeling and I. Oldani: *Data Transfers in*…, s. 36.
[795] L. Determann: *Determann's Field Guide*…, s. 46; podobnie: L. Drechsler, I. Kamara: *Essential equivalence as…,* s. 345 - autorki zwracają uwagę, że to właśnie podział odpowiedzialności będzie wpływał na rolę jaką odegra organ oceniający importerów danych w ramach kodeksów postępowania i certyfikacji. W obu wypadkach to i tak eksporter, a więc podmiot znajdujący się w Unii Europejskiej, odpowiada za prawidłowość zastosowanych zabezpieczeń, w tym także za przeporwadzoną ocenę w ramach TIA.
[796] L. Determann: *Determann's Field Guide*…, s. 43.
[797] Ibid.

zabezpieczenia są silnie podatne na zmiany w prawie państwa trzeciego[798], co również będzie wpływało na skuteczność wdrożonych, uzupełniających zabezpieczeń, w tym zabezpieczeń ograniczających dostęp organów ścigania do danych osobowych. W związku z tym, zdaniem L. Wittershagena, faworyzowanie szyfrowania jako dodatkowego zabezpieczenia jest niewłaściwe[799].

W mojej ocenie, poleganie na odpowiednich zabezpieczeniach wiąże się także z wysokim poziomem niepewności dla sytuacji osoby której dane dotyczą. Wynika to z tego, że organy państwa, w tym organy państwa przeznaczenia danych nie są związane odpowiednimi zabezpieczeniami wdrożonymi przez administratora lub podmiot przetwarzający [800], podobnie jak organy nadzoru działające na terytorium Unii Europejskiej[801]. Osoba, której dane dotyczą nie może być pewną, że jej dane osobowe na pewną będą odpowiednio chronione. Co więcej, z poziom niepewności potęguje fragmentaryzacja ochrony danych zapewnianej przez odpowiednie zabezpieczenia. Odpowiednie zabezpieczenia dotyczą wyłącznie relacji między ściśle określonymi podmiotami, tj. podmiotem wysyłającym dane a podmiotem odbierającym dane. Jednostka może więc nie spostrzec, że transfer jej danych osobowych do takiego samego państwa trzeciego, dokonywany w oparciu o te same odpowiednie zabezpieczenia, ale przez inne podmioty będzie gwarantował odmienny (niższy) poziom ochrony danych osobowych. Przejawem owej fragmentaryzacji (i niepewności) są analizowane polityki prywatności, które mimo stosowania identycznych odpowiednich zabezpieczeń, zapewniają zróżnicowany poziom ochrony danych osobowych które trafiają do Chin. Poddane analizie polityki prywatności, mimo polegania na odpowiednich zabezpieczenia, o których mowa w art. 46 RODO, w ogóle nie odnoszą się do wyników przeprowadzonej oceny chińskiego systemu prawnego, czy systemu prawnego innego państwa trzeciego, na terytorium którego trafią dane osobowe. Jednocześnie, nie pojawiają się jakiekolwiek odwołania do wdrożonych uzupełniających zabezpieczeń.

Powyższe okoliczności można uznać za uzasadnienie stanowiska L. Wittershagena, zdaniem, którego odpowiednie zabezpieczenia i odstępstwa z art. 49

[798] P. Jurcys, M. Corrales Compagnucci. M. Fenwick: *The future of*…, s. 6; L. Determann: *Determann's Field Guide*…, s. 47; pośrednio - L. Wittershagen: *Alternative Data Transfer*…, s. 224.
[799] L. Wittershagen: *Alternative Data Transfer*…, s. 235.
[800] L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses*…, s. 15; A. Flor: *The Impact of*…, s. 2035; L. Wittershagen: *Transfer of Personal…,* s. 70; L. Wittershagen: *Alternative Data Transfer*…, s. 252; H.B. Bentzen, O.H. Kvammen, G. Ursin: *Maximizing the GDPR*…, s. 3.
[801] U. Wuermeling, I. Oldani: *Data Transfers in*…, s. 39.

RODO cechuje konieczność wdrożenia bardziej intensywnego nadzoru i kontroli w porównaniu ze stosowaniem decyzji w sprawie adekwatności[802].

3.4. Utożsamianie odstępstw, o których mowa w art. 49 RODO z odpowiednimi zabezpieczeniami

Stosowaniem odpowiednich zabezpieczeń nie jest poleganie na jednym z odstępstw, o których mowa w art. 49 RODO. Artykuł 49 RODO jest odstępstwem od zasady transferu danych osobowych[803]. Przedstawiciele doktryny stoją na stanowisku, zgodnie z którym nie należy wypaczać sensu art. 49 RODO[804]. Za takie wypaczenie należy uznać ekstensywną i rozszerzającą interpretację art. 49 RODO. W związku z tym, w piśmiennictwie dominuje pogląd, zgodnie z którym art. 49 RODO i zawarte w nim odstępstwa należy wykładać ściśle, tak jak w przypadku każdego rodzaju wyjątków[805]. Odmienna interpretacja oznaczałyby, że administrator lub procesor projektując każdą czynność przetwarzania danych byłby zachęcany do skorzystania z wygodniejszych dla niego rozwiązań kosztem bezpieczeństwa osoby, której dane dotyczą[806].

Ścisłą wykładnię art. 49 RODO może jednak utrudniać sposób, w jaki sformułowano poszczególne przesłanki jego zastosowania. W szczególności, na uwagę zasługuje problem ustalenia niezbędności transferu. Jej wysoko ocenny charakter powoduje, że określenie jednoznacznych wskazówek interpretacyjnych jest niemożliwe i w praktyce administratorowi pozostaje ocena czy transfer jest „absolutnie konieczny" lub „ściśle związany"[807]. M. Krzysztofek podkreśla się jednak, że użyteczność transferu lub zwiększenie efektywności wykonywanych działań albo redukcja kosztów nie mogą być kwalifikowane jako uzasadnienie niezbędności transferu[808]. Nie bez znaczenia jest także

[802] L. Wittershagen: *Transfer of Personal…,* s. 81.
[803] Rozumianej jako wymóg utrzymania odpowiedniego poziomu ochrony danych osobowych w przypadku ich transferu poza terytorium Unii Europejskiej.
[804] P. Blume: *Transborder Data Flow*…, s. 65, 81; B. Fischer: *Komentarz do art. 49 RODO…,* s. 483; J. Hamilton: *Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems: Shattering the International Privacy Framework.* „Tulane Journal of International and Comparative Law", 2021, nr 29, s. 351; L. Drechsler, I. Kamara: *Essential Equivalence as*…., s. 349.
[805] M. Krzysztofek: *Komentarz do art. 46 RODO…,* s. 258; P. Barta, P. Litwiński, M. Kawecki: *Komentarz do art. 49 RODO*…, s. 656; B. Fischer: *Komentarz do art. 49 RODO…,* s. 483; P. Fajgielski *Komentarz do rozporządzenia nr 2016/679 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), art. 49…*; L. Wittershagen: *Alternative Data Transfer*…, s. 262–263; C. Kuner: *Komentarz do art. 49*…, s. 846.
[806] Takie skutki może wywołać zbyt częste opieranie transferów danych osobowych np. na zgodzie jednostki, o której wspomina art. 49 ust. 1 pkt a RODO.
[807] B. Fischer: *Komentarz do art. 49 RODO…,* s. 484–485.
[808] M. Krzysztofek: *Komentarz do art. 49 RODO…,* s. 282.

zakres danych osobowych, które mają być transferowane, który to zakres również wymaga wykładni przez pryzmat niezbędności[809].

Mimo przedstawionej, powszechnie akceptowanej wykładni art. 49 RODO, analizowane polityki prywatności nader często odwoływały się do odstępstw jako podstawy transferu danych osobowych do państwa trzeciego. Uważam, że jest to przejawem błędnego założenia, że stosowanie odstępstw, o których mowa w art. 49 RODO, w tym zwłaszcza przesłanki zgody czy realizacji obowiązków umownych, oznacza pozornie większą swobodę administratora[810]. Źródłem pozorność jest ścisła wykładnia, art. 49 RODO, o czym była mowa powyżej[811]. Potwierdzeniem błędnego podejścia do stosowania art. 49 RODO jest praktyka powoływania przez niektóre, spośród analizowanych polityk prywatności, zgody jako podstawy transferu danych osobowych do państwa trzeciego. W mojej ocenie przesłanka zgody jest wykluczona dla legalizacji regularnych, powtarzających się transferów[812], a zgoda powinna dotyczyć konkretnego transferu lub zestawu transferów[813]. Jednocześnie, pozyskanie zgody powinno uprzedzać transfer danych osobowych i nie może sprowadzać się do uznania, że zgodę wyraża bierna postawy jednostki[814]. Stąd, w praktyce właściwe pozyskanie zgody jest utrudnione, a niekiedy niemożliwe[815]. Z tego względu nadmierne poleganie na zgodzie jest ryzykownym posunięciem[816], podobnie jak posługiwanie odstępstwami, o których mowa w art. 49 RODO[817].

---

[809] Ibid, s. 283.
[810] L. Determann: *Determann's Field Guide*…, s. 41 i n.
[811] Czego przejawem jest m.in. ścisła wykładnia przesłanki ochrony żywotnych interesów, o której wspomina C. Kuner - C. Kuner: *Komentarz do art. 49*…, s. 852.
[812] J. Liss, D. Peloquin, M. Barnes i in.: *Demystifying Schrems II for…,* s. 13; w podobny sposób charakteryzowana jest przesłanka dochodzenia roszczeń - C. Kuner: *Komentarz do art. 49*…, s. 851 - C. Kuner wyjaśnia, że ta przesłanka nie nadaje się do legalizacji transferów danych osobowych na dużą skalę. Jednocześnie, autor podkreśla, że przesłanka dochodzenia rozczeń nie dotyczy transferów danych osobowych w celu realizacji żądań organów państw trzecich.
[813] M. Krzysztofek: *Komentarz do art. 49 RODO…,* s. 280; B. Fischer: *Komentarz do art. 49 RODO…,* s. 484; U. Wuermeling, I. Oldani: *Data Transfers in*…, s. 48.
[814] M. Krzysztofek: *Komentarz do art. 49 RODO…,* s. 280; B. Fischer: *Komentarz do art. 49 RODO…,* s. 484.
[815] B. Fischer: *Komentarz do art. 49 RODO…,* s. 484; L. Wittershagen: *Alternative Data Transfer*…, s. 266; M. Krzysztofek: *Komentarz do art. 49 RODO…,* s. 281 - autor zwraca uwagę m.in. na konieczność aktualizacji obowiązku informacyjnego, gdy zmieniają się okoliczności transferu; także:; C. Kuner: *Komentarz do art. 49 RODO…,* s. 847 - C. Kuner uważa, że zgoda nie może być zgodą blankietową; U. Wuermeling, I. Oldani: i: *Data Transfers in*…, s. 48 - autorzy sygnalizują, że nie zawsze będzie możliwe pozyskanie zgody od osoby, której dane dotyczą; L. Wittershagen: *Transfer of Personal…,* s. 78 - autor jest zdania, że zgoda, o której mowa w art. 49 RODO musi spełniać ogólne wymagania zgody, o których mowa w art. 7 RODO.
[816] Y.A. Vogel: *Stretching the Limit, The Functioning of the GDPR's Notion of Consent in the Context of Data Intermediary Services*. „European Data Protection Law Review", 2022, nr 2, s. 238; L. Wittershagen: *Alternative Data Transfer*…, s. 266.
[817] H.B. Bentzen, O.H. Kvammen, G. Ursin: *Maximizing the GDPR*…, s. 3.

3.5. Podsumowanie

W świetle przedstawionych powyżej uwag, przekazywanie danych osobowych do Chin na podstawie odpowiednich zabezpieczeń, o których mowa w art. 46 RODO lub odstępstw, wynikających z art. 49 RODO jawi się jako rozwiązanie o ograniczonej przydatności. Zasadniczym powodem dla takiej oceny odpowiednich zabezpieczeń jest rozmiar i intensywność przekazywania danych osobowych między Unią Europejską a Chinami. Fakt, że dane osobowe trafiają do różnych podmiotów zlokalizowanych w Chinach skutkuje fragmentarycznością ochrony osoby, której dane dotyczą. Każdy z administratorów lub podmiotów przekazujących dane osobowe do Chin korzysta wówczas z zabezpieczenia lub odstępstwa, które obejmuje ściśle określone podmioty i ściśle określone operacje przetwarzania danych. Osoba, której dane dotyczą nie może być więc pewną czy jej dane osobowe, przekazane do Chin, będą należycie chronione zarówno w tej części procesu, który został objęty odpowiednim zabezpieczeniem lub odstępstwem, jak i w sytuacji przekazania danych innym podmiotom zlokalizowanym w Chinach.

Powyższy problem wiąże się ze zjawiskiem dostępu organów państwa do danych osobowych. Uważam, że odpowiednie zabezpieczenia i odstępstwa, w tym szczególnie popularne klauzule umowne nie są w stanie skutecznie zabezpieczyć jednostkę przed uzyskaniem dostępu do jej danych osobowych przez organy ścigania państwa trzeciego. Jest to szczególny problem w chińskim systemie prawnym, gdzie uprawnienia organów ścigania w zakresie dostępu do danych osobowych zostały sformułowane w sposób na tyle ogólny, że nie można mówić o rzeczywistym ograniczeniu uprawnień organów państwa[818].

Dodatkową komplikację stanowi pomijanie w treści odpowiednich zabezpieczeń przepisów prawa państwa trzeciego. Jest to kolejna okoliczność, która zwiększa nakłady z jakimi związane jest wykorzystywanie odpowiednich zabezpieczeń. Niemniej jednak, aby wdrożenie odpowiednich zabezpieczeń, o których mowa w RODO, było skuteczne, należy mieć na uwadze wymagania, jakie stawiają wobec administratora lub podmiotu przetwarzającego przepisy prawa państwa trzeciego. Uważam, że w przypadku przekazywania danych osobowych między Unią Europejską a Chinami, wykorzystywanie odpowiednich zabezpieczeń, a zwłaszcza klauzul umownych dla

[818] O czym była mowa w rozdziale II.

przekazywania danych osobowych nie może mieć miejsca bez uwzględnienia lokalnych przepisów. Chińskie prawo ochrony danych osobowych wprowadza bowiem własne wymagania w odniesieniu do przekazywania danych osobowych poza terytorium Chin. Jeśli więc klauzule umowne mają być wykorzystywane dla transferu danych osobowych między Unią Europejską a Chinami, to takie klauzule powinny uwzględniać zarówno wymagania przepisów prawa Unii Europejskiej, jak i prawa chińskiego[819].

W mojej ocenie, najpoważniejszą przeszkodą dla wykorzystywania odpowiednich zabezpieczeń lub odstępstw dla przekazywania danych między Unią Europejską a Chinami jest poziom ochrony danych osobowych zapewniany przez przepisy prawa chińskiego. Przedstawione powyżej problemy traciłyby na znaczeniu, gdyby różnice w podejściu do ochrony danych osobowych w Unii Europejskiej i Chinach nie były aż tak znaczące. Jednakże przepisy chińskiego prawa ochrony danych osobowych, a także praktyka tamtejszy organów nadzorczych oraz administratorów lub podmiotów przetwarzających nie pozostawia złudzeń, że ochrona danych osobowych ma drugorzędne znaczenie. O czym była mowa w rozdziale II, dane, w tym dane osobowe, są dla władz chińskich, a tym samym, dla administratorów lub podmiotów przetwarzających działających na rynku chińskim, narzędziem. Mają przede wszystkim znaczenie gospodarcze. Konsekwencją takiego podejścia jest instrumentalne traktowanie przepisów prawa ochrony danych osobowych, które mogą dojść do głosu tylko, gdy nie uniemożliwiają lub nie utrudniają realizacji przedsięwzięć gospodarczych. Ochrona praw lub wolności jednostki nie większego znaczenia. W szczególności biorąc pod uwagę dostrzegalną w przepisach prawa chińskiego tendencją do osłabiania pozycji jednostki w konfrontacji z interesami zbiorowymi, a zwłaszcza takimi interesami jak dobro ogółu, bezpieczeństwo narodowe. Nie sposób więc uznać, że stosowanie odpowiednich zabezpieczeń i odstępstw będzie wolne od dążenia do ich dostosowania do przedstawionego podejście chińskiego. Potwierdza to treść analizowanych polityk prywatności, które cechuje wysoki poziom ogólności, bliższy przepisom chińskiego prawa ochrony danych osobowych niż przepisom RODO.

Mając na uwadze powyższe, stoję na stanowisku, że odpowiednie zabezpieczenia oraz odstępstwa wykorzystywane w taki sposób, jak czynią to chińskie podmioty przekazujące dane osobowe z terytorium Unii Europejskiej do Chin nie zapewniają

[819] G. Greenleaf: *China's Completed Personal Information Protection Law: Rights Plus Cyber-Security*. „Privacy Laws & Business International Report", nr 20, s. 4; W.G. Voss: *Transatlantic Data Transfer*…, s. 185; szerzej o wpływie przepisów państwa trzeciego na stosowanie klauzul umownych - U. Wuermeling, I. Oldani: *Data Transfers in*…, s. 37.

właściwej ochrony praw i wolności osoby, której dane dotyczą w sytuacji przekazywania danych osobowych między Unia Europejską a Chinami. Tym samym, na pytanie piąte (P.5), należy udzielić odpowiedzi przeczącej.

4. Przekazywanie danych osobowych między Unią Europejską a Chinami w oparciu o porozumienie w sprawie poziomu ochrony danych osobowych

Zakwestionowanie przydatności odpowiednich zabezpieczeń i odstępstw dla przekazywania danych osobowych między Unią Europejską a Chinami oznacza konieczność poszukiwania alternatywnego rozwiązania, które zapewni osobie, której dane dotyczą należytą ochronę, a zarazem nie będzie przeszkodą dla realizacji celów gospodarczych pozostałych uczestników procesu przetwarzania danych osobowych. Transfery danych osobowych między Unią Europejską a Chinami to element współczesnej codzienności. Ich częstotliwość nie jest równa transparentności opisu stosowanych środków legalizacji transferów danych osobowych. Opieranie transferów danych osobowych wyłącznie na klauzulach umownych lub jednym z odstępstw, o którym mowa w art. 49 ust. 1 RODO jest równoznaczne z dominacją interesów administratora danych osobowych. Mimo, że ochrona osoby, której dane dotyczą ma być priorytetem dla działań administratora, w praktyce traci na znaczeniu. Potwierdzają to poddane analizie fragmenty polityk prywatności administratorów danych osobowych (będących chińskimi przedsiębiorstwami). Nieczytelny obraz sytuacji jednostki, której dane opuszczają terytorium danych osobowych powoduje, że jednostka nie jest w stanie przewidzieć skutków, jakie wywoła transfer danych.

Zarówno doktryna, do której zalicza się autor niniejszej pracy, jak i praktyka zmierzają, świadomie lub nieświadomie, ku wyodrębnieniu nowego narzędzia legalizacji transferów danych osobowych[820].Istotą rzeczy staje się znalezienie rozwiązania, które będzie pewną postacią oceny systemu prawnego państwa trzeciego, ale oceną mniej restrykcyjną w porównaniu z oceną adekwatności, o której mowa w art. 45 RODO. Jednocześnie, ważne jest, aby został zachowany skutek, jaki wywiera pozytywna ocena adekwatności, a więc swoboda transferów danych osobowych do badanego państwa trzeciego.

[820] A.Chander: *Is Data Localization…*, s. 2–3; C. Kuner:*Komentarz do art.* 45…, s. 774; P. Breitbarth: *A Risk-Based Approach*…, s. 543; W.G. Voss: *Transatlantic Data Transfer*…, s. 177; OECD: *Fostering Cross-Border…,* s. 19; H.B. Bentzen, O.H. Kvammen, G. Ursin: *Maximizing the GDPR*…, s. 1; K. von Lewinski: *Collision of Data Protection Law Regimes*. W: *Data Disclosure. Global Developments and Perspectives*. Red. M. Hennemann, K. von Lewinski, D. Wawra i in. De Gruyter, Berlin – Boston 2023, s. 201.

Obecne podejście organów Unii Europejskiej do problematyki transferów danych osobowych do państw trzecich cechuje niewielkie zainteresowanie innymi miejscami przeznaczenia danych osobowych niż USA. Jednakże nie oznacza to, że dane osobowe nie trafiają na terytorium innych państw niż USA. Dzieje się tak, ponieważ w otaczającej rzeczywistości, aktywności gospodarcze nie mogą istnieć bez przepływu informacji, w tym danych osobowych[821], zaś jednostka coraz częściej nie jest w stanie zorientować się, że jej dane faktycznie są transferowane[822]. Stąd, faktyczne ograniczenia transferów danych osobowych do państw trzecich stają się niemożliwe[823]. Tym samym, organy Unii Europejskiej, celowo lub przypadkowo, nie zauważają, że dane osobowe Europejczyków są przekazywane do różnych miejsc na świecie[824]. Taktyka unikania tematu transferów danych osobowych do państw trzecich jest czymś niezrozumiałym, mając na uwadze kontekst prawa ochrony danych osobowych w Unii Europejskiej. Doktryna, mniej lub bardziej jednoznacznie uznaje, że optyka Unii Europejskiej w sprawie transferów danych osobowych do państw trzecich jest (a przynajmniej powinna być) oparta o ochronę praw podstawowych[825]. W tym stanie rzeczy, należałoby oczekiwać większej aktywności organów Unii Europejskiej, nie unikania tematu[826].

Skupienie uwagi organów Unii Europejskiej na problematyce przekazywania danych osobowych do USA spowodowało jednak, że doszło do faktycznego poszerzenia katalogu dostępnych środków legalizacji transferów danych osobowych do państw trzecich.

---

[821] Podobnie: C. Kuner: *The Path to*…, s. 70.
[822] Ibid.
[823] Ponownie, z pomoca przychodzi przykład USA. M. Zalnieriute: *Reforming the Australian Framework for International Data Sharing*. „International Data Privacy Law ", 2022, nr 12, s. 332, 332 - autorka wyjaśnia, że skutkiem pandemii Covid-19 jest uświadomienie społeczeństwa i prawodawców o braku możliwości ograniczenia czy zaprzestania transferów danych osobowych do USA, jeśli takie dane są przetwarzane przez amerykańskie firmy.
[824] Podobnie na tle przepisów Dyrektywy 2016/680 - L. Drechsler: *Wanted: LED Adequacy Decisions. How the Absence of Any LED Adequacy Decision Is Hurting the Protection of Fundamental Rights in a Law Enforcement Context.* „International Data Privacy Law ", 2021, nr 11, s. 182, 183.
[825] Grupa Robocza art. 29: *Opinion 01/2016 on*… s. 9; M. Burri: *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*. „U.C. Davis Law Review", 2017, nr 1, s. 13; L. Drechsler: *Wanted: LED Adequacy*…, s. 184; Z. Gulczyńska: *A certain standard*…, s. 3; C. Kuner: *The Path to*…, s. 77; A.B. Makulilo: *The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius*. „The International Journal of Human Rights", 2021, nr 25, s. 117, 123; A. Chander, M.E. Kaminski, W. McGeveran: *Catalyzing Privacy Law*. „Minnesota Law Review ", 2021, nr 105, s. 1733, 1747; U. Wuermeling, I. Oldani: *Data Transfers in*…, s. 22; L. Drechsler, I. Kamara: *Essential equivalence as*…, s. 326; A. Wright Fiero, E. Beier: *New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, And Russian Legislation*. „Stanford Journal of International Law", 2022, nr 58, s.151, 191; L. Wittershagen: *Transfer of Personal…,* s. 51; A. Chander, P.M. Schwartz: *Privacy and/or Trade*…, s. 89–90.
[826] Podobnie L. Drechsler, I. Kamara: *Essential equivalence as*…, s. 315.

4.1. Porozumienie jako nowy środek legalizacji transferów danych osobowych do państw trzecich

Z praktyki Komisji Europejskiej w ramach postępowania związanego z wydaniem decyzji w sprawie adekwatności wyłania się modyfikacja przedmiotu oceny. W niektórych przypadkach, Komisja Europejska, we współpracy z badanym państwem trzecim zdecydowała, że to nie system prawny państwa trzeciego będzie podlegał ocenie. Zamiast tego, przedmiotem oceny było porozumienie zawierane między Unią Europejską a państwem trzecim. Treść tego porozumienia obejmowała takie rozwiązania, które były istotne z perspektywy standardu adekwatności. Tym samym, to porozumienie, zespolone z wydawaną decyzją w sprawie adekwatności, zapewniało ochronę danych osobowych o odpowiednim poziomie. Taka konstrukcja była wykorzystywana w przypadku decyzji w sprawie adekwatności wydawanych w stosunku do USA, ale nie tylko[827].

Model, w którym decyzji w sprawie adekwatności towarzyszy porozumienie zapewniające oczekiwany poziom ochrony danych osobowych w państwie trzecim nawiązuje do koncepcji wykorzystania umowy międzynarodowej jako środka legalizacji transferów danych osobowych[828]. O tym, że umowy międzynarodowe odgrywają szczególną rolę świadczy preambuła RODO. W motywie 102 RODO ustawodawca potwierdza, że „Niniejsze rozporządzenie pozostaje bez uszczerbku dla umów międzynarodowych między Unią a państwami trzecimi regulujących przekazywanie danych osobowych, w tym zawierających odpowiednie zabezpieczania dla osób, których dane dotyczą. Państwa członkowskie mogą zawierać umowy międzynarodowe przewidujące m.in. przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych, o ile umowy takie nie wpływają na niniejsze rozporządzenie ani na inne przepisy prawa Unii i o ile przewidują odpowiedni stopień ochrony podstawowych praw osób, których dane dotyczą." Przywołana koncepcja opiera się na założeniu istnienia dwóch przeciwstawnych wartości, swobody transferów danych osobowych i potrzeby ochrony jednostki i jej praw podstawowych[829]. O ile zasadniczą motywacją dla usuwania istniejących różnic w podejściu do transferów danych osobowych jest

[827] Odpowiednie porozumienie jest podstawą decyzji w sprawie adekwatności wydanej dla Kanady (transfery danych osobowych w ramach PIPEDA), ale również i Japonii - tak na temat decyzji w sprawie adekwatności Japonii - W.G. Voss: *Cross-Border Data Flows*…, s. 485.

[828] J.A. Zimmerman: *Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism*. „Northwestern Journal of International Law & Business", 1982, nr 4, s. 601; także H.P. Lowry: *Transborder Data Flow*…, s. 159.

[829] J.A. Zimmerman: *Transborder Data* Flow…, s. 603; w odniesieniu do porozumień zawieranych z USA, w tym Safe Harbor i Tarczy Prywatności, które są przejawem próby pogodzenia tych sprzecznych wartości - A. Busch: *The Regulation of*…, s. 313, 318; *European Parliament Resolution of 26 May 2016*…, pkt 10; A. Mattoo, J.P. Meltzer: *International Data Flows*…, s. 769, 771.

współpraca gospodarcza, o tyle nie można oczekiwać, że wszelkie różnice znikną[830]. Potwierdza to przypadek USA[831].

4.1.1. Przekazywanie danych osobowych między Unią Europejską a USA jako źródło modelu wykorzystania porozumień towarzyszących decyzji w sprawie adekwatności

USA są postrzegane jako państwo trzecie, które usilnie promuje koncepcje swobodnych transferów danych osobowych[832]. Charakterystyczną cechą poglądów głoszonych przez zwolenników globalnego, jednolitego poziomu ochrony danych osobowych jest powoływanie się na konieczność opracowania równie globalnego porozumienia regulującego ten poziom. Zdaniem G. Greenleaf'a, pożądanym rozwiązaniem w tej sprawie jest wykorzystanie Rady Europy oraz jej Konwencji nr 108[833]. Nie bez znaczenia są także wytyczne w sprawie ochrony danych osobowych OECD, szczególnie w kontekście ich uznawania za forum dla urzeczywistnienia koncepcji Data Flow with Trust (DFFT)[834].

---

[830] L. Belli, D. Doneda: *Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence*. „International Data Privacy Law", 2022, nr 2; J. Paine: *G7 Leaders Must Overcome Differences to Ensure Continued Free Cross-Border Data Flow*. 29.04.2023. https://thediplomat.com/2023/04/g7-leaders-must-overcome-differences-to-ensure-continued-free-cross-border-data-flow/ [dostęp: 11.10.2023]; C. Ng: *Data Free Flows with Trust: From Concept to Reality*. 9.06.2023. https://www.uschamber.com/security/cybersecurity/data-free-flows-with-trust-from-concept-to-reality [dostęp: 11.10.2023]; *G7 Roadmap for Cooperation on Data Free Flow With Trust*. 2021. https://assets.publishing.service.gov.uk/media/609cf5e18fa8f56a3c162a43/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf [dostęp: 11.10.2023]; K. von Lewinski: *Collision of Data*…, s. 214; A. Chander, P.M. Schwartz: *Privacy and/or Trade*…, s. 103.
Istotną rolę ogdyrwają przy tym różnice kulturowe, które bezpośrednio wpływają na problematykę ochrony danych osobowych w konkretnym państwie - C. Kuner: *The Path to*…, s. 82; C. Pauletto: *Options towards a*…, s. 6- autor uważa, że to m.in. z tego powodu RODO nie stanie się globalbym standardem ochrony danych osobowych. Z kolei G. Greenleaf wyjaśnia, że problemem typowym dla państw azjatyckich jest funkcjonowanie organu nadzoru, który spełniałby kryterium niezależności - G. Greenleaf: *How Far Can Convention 108+ "Globalise"? Prospects for Asian Accessions*. „Computer Law & Security Review", 2021, nr 40, s. 6–7.

[831] Na tle projektu federalnej ustawy o ochronie danych osobowych w USA G. Greenleaf zauważa, że mimo trwającego od lat dialogu między USA i Unią Europejską, nadal w omawianym projekcie dostrzegalne są odstępstwa od modelu promowanego w Unii Europejskiej, jak m.in. faktyczne ograniczenie zasięgu ustawy tylko do sektora prywatnego - por. G. Greenleaf: *Proposed US Federal Data Privacy Law Offers Strong Protections but Only to US Residents*. „Privacy Laws & Business International Report", 2022, nr 179; podobnie także E.A. Ivers: *Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III*, „Boston College Law Review", 2021, nr 62, s. 2573.

[832] por. C. Si: *Research on Data Sovereignty Rules in Cross-Border Data Flow and Chinese Solution*. „US-China Law Review", 2021, nr 18, s. 261, 263.

[833] G. Greenleaf: *Renewing Data Protection Convention 108: The CoE's "GDPR Lite" Initiatives*. „University of New South Wales Law Research Series", 2016, nr 14, s. 8; G. Greenleaf: *How Far Can*…, s. 2; także P. Hustinx: *Data Protection and International Organizations: A Dialogue between EU Law and International Law*, „International Data Privacy Law", 2021, nr 11, s. 77, 79; C. Pauletto: *Options towards a*…, s. 8, 12; H. Miyashita: *Human-centric data protection laws and policies: A lesson from Japan*. „Computer Law & Security Review", 2021, nr 40, s. 1; *From Europe to the World. The EU and Council of Europe as Global Standard Setters in Data Protection*. 30.01.2021. Impact News Service LexisNexis [dostęp: 22.09.2023].

[834] World Economic Forum: *Data Free Flow…,* s. 17; OECD: *Fostering Cross-Border Data*…, s. 32; *Institutional Arrangement for Partnership (IAP)*. 2023. https://www.digital.go.jp/en/dfft-iap-en [dostęp:

Doktryna prezentuje zróżnicowane stanowisko w odniesieniu do postrzegania Konwencji nr 108 lub wytycznych w sprawie ochrony danych osobowych OECD w oparciu o standard adekwatności, o którym mowa w RODO. P. Hustinx uważa, że oba dokumenty są bliskie RODO[835]. Bardziej popularnym stanowiskiem jest jednak dostrzeganie bliskiej relacji Konwencji nr 108 i RODO[836]. Z kolei w przypadku relacji RODO i Wytycznych w sprawie ochrony danych osobowych OECD raczej mowa o pewnych elementach wspólnych[837]. W związku z tym, uznaje się, że Wytyczne w sprawie ochrony danych osobowych OECD nie zapewniają minimalnego, akceptowalnego z perspektywy RODO poziomu ochrony danych osobowych[838]. Natomiast Konwencja nr 108 jest postrzegana jako istotny element, który wpływa na poziom ochrony danych osobowych w państwie trzecim[839]. D. Erods uważa, że Konwencja nr 108 może nawet odpowiadać standardowi adekwatności[840]. Jest to jednak pogląd odosobniony, ponieważ większość doktryny uważa, że Konwencja nr 108 zapewnia poziom ochrony danych osobowych niższy od poziomu, który zapewniają przepisy RODO[841]. W przeciwieństwie do wytycznych w sprawie ochrony danych osobowych OECD, Konwencja nr 108 ma charakter wiążący, co postrzegane jest jako jej zaleta[842]. Podejście zarówno do Konwencji nr 108, jak i Wytycznych w sprawie ochrony danych osobowych OECD ukazuje, że z ich treścią

10.10.2023]; por. J. Paine: *G7 Leaders Must…*; por. A. Vats: *Data Free Flow…*; B. Echikson: *Japan's Data With Trust Offensive — A Solution to the World's Data Wars?*. 5.05.2023, https://cepa.org/article/japans-data-with-trust-offensive-a-solution-to-the-worlds-data-wars/ [dostęp: 11.10.2023].

[835] P. Hustinx: *Data Protection and…*, s. 79.

[836] G. Greenleaf, '*Renewing Data Protection…*, s. 1; G. Greenleaf: *"Modernised" Data Protection Convention 108 and the GDPR*. „Privacy Laws & Business International Report", 2018, nr 22, s. 2; H. Miyashita: *Human-centric data…*, s. 6–7; A.B. Makulilo: *The Long Arm…*, s. 126; R. Jansen, M. Reijneveld: *Convention 108+, the GDPR, and Data Processing in the National Security Domain*. „European Data Protection Law Review", 2022, nr 3, s. 429; D. Erdos: *The UK and…*, s. 10–11.

[837] W.G. Voss: *Cross-Border Data Flows…*, s. 509–510.

[838] Grupa Robocza art. 29.: *Opinion 2/99 on…*, s. 4; G. Greenleaf: *Accountability without Liability: "To Whom" and "with What Consequences"? (Questions for the 2019 OECD Privacy Guidelines Review).* „University of New South Wales Law Research Series ", 2019, nr 67, s. 7.

[839] G. Greenleaf: *Renewing Data Protection…*, s. 4; H. Miyashita: *Human-centric data protection…*, s. 8; por. E. Bertoni: *Convention 108 and the GDPR: Trends and Perspectives in Latin America*. „Computer Law & Security Review", 2021, nr 40; C. Kuner: *The Path to…,* s. 89–90; A.B. Makulilo: *The Long Arm…*, s. 124; D. Erdos: *The UK and…*, s. 2; pośrednio także - *Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield…*, s. 6.

[840] D. Erdos: *The UK and…*, s. 2.

[841] G. Greenleaf: *Renewing Data Protection…,* s. 5; S.L. Duque de Carvalho: *Key GDPR Elements…*, s. 61; Z. Gulczyńska: *A certain standard…*, s. 13; G. Greenleaf: *How Far Can…*, s. 2.

[842] G. Greenleaf: *Renewing Data Protection…,* s. 5; 7 - według autora skutkiem przystąpienia do Konwencji nr 108 jest formalny obowiązek jej przestrzegania; C. Kuner: *Komentarz do art.* 44…, s. 760; A.B. Makulilo: *The Long Arm…*, s.126; G. Greenleaf: *How Far Can…*, s. 2; C. Pauletto: *Options towards a…*, s. 16 - dla autora moc wiążąca Konwencji nr 108 jest zaletą, a zarazem wadą Wytycznych w sprawie ochrony danych OECD; podobnie: L. Wittershagen: *Transfer of Personal…,* s. 61 - autor uważa, że brak mocy wiążącej Wytycznych w sprawie ochrony danych OECD powoduje, że ich przydatność dla oceny poziomu ochrony danych osobowych w państwie trzecim jest niewielka.

utożsamiany jest minimalny, powszechnie akceptowalny poziom ochrony danych osobowych. Dla obu dokumentów wspólną wartością jest ochrona danych osobowych (prywatności) jednostki, ale przy jednoczesnym zachowaniem swobody transferów danych osobowych[843]. Ponadto, zdaniem C. Kunera, Rada Europy i OECD poprzez swoją aktywność w promocji ochrony danych osobowych, zacieśniają współpracę międzynarodową w tym zakresie[844].

Niemniej jednak, oczekiwanie ujednolicenia ogólnoświatowego poziomu ochrony danych osobowych, akceptowanego przez Unię Europejską, nie jest realne w perspektywie najbliższych lat. Stąd też zainteresowania USA skupiają się wokół alternatywnych rozwiązań, zwłaszcza, że w podejściu USA do przekazywania danych osobowych można dostrzec także elementy typowe dla koncepcji suwerenności danych, w szczególności w kontekście ochrony interesów ważnych z perspektywy USA[845].

Nie dziwi więc fakt, że uwzględniwszy różnice w poziomie ochrony danych osobowych, które zapewniają przepisy prawa amerykańskiego, zastosowanie wobec USA standardu adekwatności byłoby niemożliwe[846]. Stąd, od początku obowiązywania europejskich przepisów o ochronie danych osobowych, władze USA starały się objąć transfery między UE a USA decyzją w sprawie adekwatności, ale na odmiennych zasadach[847]. Tą odmiennością było właśnie wykorzystanie porozumień, które miały być źródłem ochrony danych osobowych Europejczyków przetwarzanych na terytorium USA. Niektórzy autorzy uważają, że w odniesieniu do porozumienia Safe Harbor[848], jak i Tarczy Prywatności[849], należy mówić o certyfikacji wspartej przez decyzję w sprawie adekwatności. Doktryna jednolicie uznaje, że porozumienia zawierane między Unią

[843] J.A. Zimmerman: *Transborder Data Flow*…, s. 620; M. Burri: *The Governance of*…, s. 11; C. Pauletto: *Options towards a*…, s. 5.
[844] C. Kuner: *The Path to*…, s. 90.
[845] C. Si: *Research on Data*…, s. 261 - zdaniem autorki jest to szczególnie dostrzegalne w relacjach USA - Chiny; szerzej o rosnącej popularności koncepcji suwerenności danych - por. OECD: *Fostering Cross-Border Data*….
[846] podobnie - B. Sandfuchs: *The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II*. „GRUR International", 2021, nr 3, s. 246.
[847] Podobnie, o potrzebie wykorzystania modelu porozumienia (umowy międzynardowej) po uchyleniu przez TSUE decyzji w sprawie adekwatności związanej z Privacy Shield - B. Sandfuchs: *The Future of Data*…, s. 248.
[848] D.J.B. Svantesson: *The regulation of cross-border data flows*. „International Data Privacy Law", nr 3, s. 190.
[849] U. Wuermeling, I. Oldani: *Data Transfers in*…, s. 33; JD Supra: *EU and U.S. Finalize Data Privacy Framework_ Heres How to Get Certified*. 11.07.2023. Newstex Blogs LexisNexis [dostęp: 22.09.2023]; JD Supra: *The EU-U.S. Data Privacy Framework A New Solution for the Free Flow of Personal Data*. 27.07.2023, Newstex Blogs LexisNexis [dostęp: 22.09.2023].

Europejską a USA, w ramach procedury wydawania decyzji w sprawie adekwatności, stanowiły umowę międzynarodową *sui generis*[850].

4.1.2. Cele wykorzystania porozumienia towarzyszącego decyzji w sprawie adekwatności

Przykład USA jest potwierdzeniem zainteresowania organów Unii Europejskiej wykorzystaniem umów międzynarodowych do legalizacji przekazywania danych osobowych do państw trzecich[851]. Takie umowy są szczególnie popularne dla legalizacji transferów danych osobowych objętych zakresem zastosowania Dyrektywy 2016/680[852]. Jednocześnie, umowy międzynarodowe są uznawane za preferowany sposób regulowana transgranicznego dostępu do danych osobowych przez organy ścigania[853]. W doktrynie pojawiają się głosy o wykorzystywaniu umów międzynarodowych także dla legalizacji transferów danych osobowych w ogólności[854]. Model porozumienia, towarzyszącego decyzji w sprawie adekwatności jest wyrazem szerszego dialogu Unii Europejskiej z państwami trzecimi w odniesieniu do ochrony danych osobowych, jak również handlu, bezpieczeństwa i związanych z tym interesów[855]. Przyjmuje się, że posłużenie się porozumieniem, na wzór porozumień dotyczących USA, jest rekomendowanym

---

[850] W odniesieniu do Safe Harbor - J.R. Reidenberg: *The Simplification of International Data Privacy Rules*. „Fordham International Law Journal", 2006, nr 29, s. 1128, 1132; *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*…, s. 2; J. Stoddart, B. Chan, Y. Joly: *The European Union's*…, s. 143, 145; W.G. Voss: *Cross-Border Data Flows*…, s. 511; A. Chander: *Is Data Localization…*, 2–3; pośrednio także S.R Salbu: *The European Union*…, s. 655, 681.
Na temat charakteru Privacy Shield wypowiadali się m.in. L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses*…, s. 12.
Podobnie charakteryzuje się także nowe Porozumienie - por. M. Broersma: *Council Of Europe*…; *Jumping On The EU-US Adequacy Decision Expert Says Wait And See*. 31.07.2023. Medtech Insight LexisNexis [dostęp: 22.09.2023].
Odmienne stanowisko prezentuje I. Małobęcka-Szwast, która porozumienia zawierane między Unią Europejską a USA traktuje jako przykład sektorowej decyzji w sprawie adekwatności – I. Małobęcka-Szwast: *Zastosowanie decyzji Komisji Europejskiej jako podstawy transferu danych osobowych* W: *Transfery danych osobowych na podstawie RODO*. Red. M. Sakowska-Baryła. Wolters Kluwer, Warszawa 2024, str. 133-163.
[851] Tak: Europejski Inspektor Ochrony Danych Osobowych.: *Opinion of the*…, pkt 40.
[852] L. Drechsler: *Wanted: LED Adequacy*…, s. 189.
[853] *European Parliament Resolution on the Adequacy of the Protection Afforded by the EU- US Privacy Shield*…, pkt 28.
[854] Jednoznacznie - L. Wittershagen: *Transfer of Personal…,* s. 58; pośrednio m.in. B. Fischer: *Komentarz do art. 45 RODO…,* s. 466; P. Drobek *Komentarz do art. 45 RODO…*; W.G. Voss: *Cross-Border Data Flows…,* s. 511; World Economic Forum: *Data Free Flow*…, s. 14 - autorzy raportu omawiają różne warianty wykorzystania umów międzynarodowych dla legalizacji transferów danych osobowych; C. Kuner: *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection*. „University of Cambridge Faculty of Law Research Paper", 2021, nr 20/2021, s. 25; OECD: *Fostering Cross-Border Data*…, s. 17.
[855] A. Busch: *The Regulation of*…, s. 313, 318; *European Parliament Resolution of 26 May 2016 on Transatlantic Data Flows…,* pkt 10; A. Mattoo, J.P. Meltzer: *International Data Flows*: s. 769, 771; A. Flor: *The Impact of*…, s. 2035, 2036.

rozwiązaniem dla systemów prawnych o skomplikowanej sytuacji[856]. Jak zauważa D.J.B. Svantesson[857], wspierany przez niektórych przedstawicieli doktryny[858], dzięki porozumieniu, Unia Europejska nie musi czekać, aż państwo trzecie wdroży w swoim systemie prawnym zmiany, które będą czyniły zadość oczekiwaniom Unii Europejskiej. G. Maldoff i O.Tene uważają, że to właśnie braki w systemie prawnym USA skłoniły Komisję Europejską do wykorzystania modelu porozumienia towarzyszącego decyzji w sprawie adekwatności.[859] Porozumienie tworzy bowiem własny prawny ekosystem, odrębny od systemu prawnego państwa trzeciego, ale wpływający na ten system[860]. Państwo trzecie zasadniczo jest traktowane jako nieadekwatne, bo adekwatność dotyczy wyłącznie ochrony danych zapewnianych w ramach wyodrębnionego systemu, który tworzy porozumienie[861]. Istotnym jest jednak to, że wyznacznikiem dla treści porozumienia staje się prawo Unii Europejskiej, zaś państwo trzecie w ramach porozumienia dostosowuje się do surowych wymagań Unii Europejskiej[862]. Dla Komisji Europejskiej porozumienie (umowa międzynarodowa) jest składową wydawanej decyzji w sprawie adekwatności, nawet jeśli Komisja Europejska prowadzi negocjacje dotyczące umowy w sprawie wolnego handlu[863]. Wiąże się z tym rezygnacja z pewnych praw lub obowiązków, które są postrzegane przez drugą stronę jako nadmierne obciążenie. Na co zwraca uwagę A. Zinser, to Komisja Europejska prowadzi negocjacje z państwem trzecich i może dostosowywać negocjacje do bieżącej sytuacji[864]. Z tego względu, model porozumienia towarzyszącego decyzji w sprawie adekwatności jest wyjątkowo atrakcyjny[865]. Dodatkowo, motywacją dla zawierania porozumień towarzyszących decyzji w sprawie adekwatności jest ułatwienie prowadzenia

[856] Grupa Robocza art. 29.: *Opinion 1/99 Concerning*…, pkt 2.
[857] D.J.B. Svantesson: *The regulation of*…, s. 191-192.
[858] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*…, s. 2; S. Sharma: *Data Privacy and*…, s. 169; Europejska Rada Ochrony Danych Osobowych.: *EU - U.S. Privacy Shield - Second Annual Joint Review*…, pkt 39.
[859] G. Maldoff, O. Tene: *Essential Equivalence and*…, s. 211, 223.
[860] A. Zinser: *European Data Protection*…, s. 171, 173.
[861] P. Barta, P. Litwiński, M. Kawecki: *Komentarz do art. 46*…, s. 636–637.
[862] *Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows*…, s. 8; Europejski Inspektor Ochrony Danych Osobowych.: *Opinion 4/2016 on…,* s. 6; C. Kuner: *Komentarz do art. 46*…, s. 802; por. M. Broersma: *Council Of Europe*….
[863] Pośrednio - Europejski Inspektor Ochrony Danych Osobowych.: *Opinion 4/2016 on…,* s. 6; *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*…, s. 6; B. Fischer *Komentarz do art. 45*…, s. 466; W.G. Voss: *Cross-Border Data Flows*…, s. 517; A. Chander, P.M. Schwartz: *Privacy and/or Trade*…, s. 52–53.
[864] A. Zinser: *European Data Protection*…, s. 171, 177.
[865] A. Hughes: *A Question of* …, s. 270, 271.

działalności przez przedsiębiorców[866]. To właśnie oczekiwania biznesu, a zwłaszcza małych i średnich przedsiębiorstw są uznawane za główny powód dla rychłego przyjęcia i wdrożenia Tarczy Prywatności[867].

Jednakże, dla części przedstawicieli doktryny, porozumienia dotyczące przekazywania danych osobowych między Unią Europejską a USA nie są aż tak korzystne dla przedsiębiorców. Wskazuje się, że model porozumień dotyczących USA przerzuca ciężar działań dostosowania systemu prawnego do oczekiwań Unii Europejskiej z państwa na przedsiębiorców[868]. Wynika to oparcia porozumień dotyczących USA na mechanizmie certyfikacji, który od początku był sugerowanym rozwiązaniem[869]. Jest przy tym działaniem o wątpliwej skuteczności, ponieważ, co wytknięto na etapie postępowania w sprawie Schrems II[870], zawarte porozumienie wiąże wyłącznie przedsiębiorców, którzy przystąpili do schematu certyfikacji, ale już nie organy państwa trzeciego[871].

4.1.3. Porozumienie towarzyszące decyzji w sprawie adekwatności jako możliwość usunięcia braków systemu prawnego państwa trzeciego

Zdaniem P. Blume'a, wykorzystanie porozumienia (umowy międzynarodowej) w sprawie legalizacji transferów danych pozwoli na ograniczenie ekstensywnej interpretacji odstępstw, o których była mowa w art. 26 Dyrektywy 95/46, a które obecnie wynikają z art. 49 RODO[872]. Swego rodzaju ułatwieniem zawierania porozumień legalizujących transfery danych mają być negocjacje, które stanowią integralną część procedury wydawania decyzji w sprawie adekwatności[873]. Dlatego też porozumienie (umowa międzynarodowa) daje nowe możliwości w zakresie usunięcia dostrzeżonych braków w systemie prawnym państwa trzeciego[874]. Przyjmuje się bowiem, że takie porozumienie (umowa) także musi dostarczać odpowiedniego poziomu ochrony danych osobowych, z czym wiąże się istnienie odpowiednich praw, obowiązków czy instytucji[875].

---

[866] S. Khan: *Invalidity of EU-US Safe Harbor: practical implications: Part 1*. „Compliance & Risk", 2016, nr 2, s. 3.
[867] Europejski Inspektor Ochrony Danych Osobowych.: *Opinion 4/2016 on…*, s. 6.
[868] S.R. Salbu: *The European Union*…, s. 655, 682; S. Varotto: *The Schrems Decision, the EU-US Privacy Shield and the Necessity to Rethink How to Approach Cross Border Personal Data Transfers at Global Level*. „Communications Law", 2016, nr 21, s. 78, 79; JD Supra: *New EU-U.S*…..
[869] Wyrok Schrems I, pkt 81.
[870] Ø. Saugmandsgaard: *Opinion of Advocate*…, pkt 193.
[871] Podobnie: Wyrok Schrems I, pkt 82; G. Maldoff, O. Tene: *Essential Equivalence and*…, s. 211, 221.
[872] P. Blume: *Transborder Data Flow*…, s. 81.
[873] B. Fischer: *Komentarz do art. 45 RODO*…, s. 466; pośrednio - A. Chander, P.M. Schwartz: *Privacy and/or Trade*…, s. 124.
[874] J.A. Zimmerman jest zdania, że zaletą stosowania umów międzynarodowych w sprawie transferu danych osobowych jest możliwość szybszego uchwycenia zmian, jakie zachodzą w środkowiskach technologicznym i prawnym - por. J.A. Zimmerman: *Transborder Data Flow*…, s. 619.
[875] C. Kuner tłumaczy, że możliwość wykorzystania umowy międzynarodowej dla legalizacji transferu opiera się na zapewnieniu, że tej umowie będzie towarzyszył odpowiedni poziom ochrony danych

Wskazuje się, że odpowiednie postanowienia porozumienia (umowy międzynarodowej) mogą prowadzić do usunięcia braku organu nadzoru, poprzez powołanie jednego, wspólnego organu dla stron porozumienia (umowy)[876]. Porozumienie może także określać kryteria okresowej oceny funkcjonującego organu nadzorczego; wówczas, przyjmując poglądy G. Greenleaf'a, można usunąć przeszkodę formalnej niezależności organu, którą zastąpi faktyczna niezależność, potwierdzana przez przeprowadzoną ocenę[877]. Dodatkowo, możliwa jest taka konstrukcja postanowień umownych, dzięki której będzie można zniwelować dostrzeżone braki (lub usunąć powstałe wątpliwości) w odniesieniu do poziomu ochrony praw człowieka w danym państwie trzecim[878]. W związku z powyższym, treść porozumienia (umowy międzynarodowej) legalizującego transfer danych osobowych do państwa trzeciego powinna być odpowiednio sformułowana. Szczególną rolę odegra tu etap negocjacji zainteresowanych stron. Dzięki temu, złagodzenie różnic, jakie występują w podejściu do ochrony danych osobowych, które prezentują organy Unii Europejskiej oraz konkretne państwo trzecie, staje się możliwe. Zgadzam się z tymi przedstawicielami doktryny, dla których to zasady ochrony danych osobowych stanowią element wspólny różnych systemów prawnych[879]. Na tej podstawie, umawiające się strony są w stanie osiągnąć kompromis, dostrzegając jak wiele elementów łączy ich systemy prawne, a tym samym, skupiając się na szczegółowych rozwiązaniach, dotyczących poszczególnych zasad[880]. Taki szczegółowym rozwiązaniem może być uwzględnienie różnic kulturowych jakie występują między system prawnym Unią Europejską a konkretnym państwem trzecim, a które pozostają w bezpośrednim związku z problematyką ochrony danych osobowych[881]. Dodatkowo, za pożądany elementem treści takiego porozumienia można

osobowych, a więc zasadniczo poziom odpowiadający standardowi adekwatności - C. Kuner: *Komentarz do art. 45 RODO*…, s. 777; podobnie: L. Drechsler: *Wanted: LED Adequacy*…., s. 190; L. Drechsler, I. Kamara: *Essential equivalence as*…, s. 327–328; pośrednio por. D. Khan: *Data Flow Challenges*….

[876] Na tle analizy współpracy UE i USA o podobnym rozwiązaniu w jednej ze swoich opinii wspomina Europejski Inspektor Ochrony Danych Osobowych - Europejski Inspektor Ochrony Danych Osobowych.: *Opinion 4/2016 on…,* s. 8–9.

[877] G. Greenleaf: *How Far Can*…, s. 12.

[878] M. Zalnieriute wspomina, że o zbliżonej konstrukcji mowa w przepisach amerykańskiej ustawy CLOUD Act - M. Zalnieriute: *Reforming the Australian*…, s. 338.

[879] Zdaniem J.A. Zimmerman to zasady ochrony danych osbowych przekładają się na minimalny poziom ochrony danych osobowych - por. J.A. Zimmerman: *Transborder Data Flow*…, s. 621 Por. także: J. Wagner: *The Transfer of*…, s. 329; G. Greenleaf: *California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?*, „Privacy Laws & Business International Report", 2020, nr 168, s. 540; G. Greenleaf,: *How Far Can*… s. 8; OECD: *Fostering Cross-Border Data*…, s. 20; S. Khan: *Invalidity of EU-US…*, s. 7.

[880] podobnie - OECD: *Fostering Cross-Border Data*…, s. 22.

[881] I tak w odniesieniu do państw azjatyckich różnice kultutowe będą dotyczyły znaczenia, jakie przypisuje się wizerunkowi i jego ochronie - por. w odniesieniu do Japonii H. Weiden, K.Takase: *Data Privacy* in…, s. 276; H. Miyashita: *Human-Centric Data*…, s. 7–8.

uznać uzgodnioną przez strony siatkę pojęciową[882]. Szczególnie ważne staje się także jednoznaczne określenie wpływu prawa państwa trzeciego na stosowanie postanowień umowy[883], w tym relacji jakie zachodzą między porozumieniem a prawem państwa trzeciego i prawem Unii Europejskiej [884] . Jednocześnie, porozumienie (umowa międzynarodowa) powinno dokładnie opisywać zasady wdrożenia jego postanowień, w tym zwłaszcza stosowania jego postanowień przez administratorów i procesorów danych [885]. Nie można także zapominać o jednostce, ponieważ to egzekwowalność przyznanych praw jest gwarantem ich skuteczności[886].

4.2. Porozumienie towarzyszące decyzji w sprawie adekwatności jako sposób przekazywania danych osobowych między Unią Europejską a Chinami

Transfery danych osobowych do Chin mają wiele wspólnego z transferami danych osobowych do USA. W obu wypadkach współpraca gospodarcza z Unią Europejską bezpośrednio wpływa na potrzebę przekazywania danych osobowych. Transfery odbywają się regularnie i są intensywne [887] , ponieważ znaczna część działalności gospodarczej podmiotów chińskich łączy się produktami lub usługami społeczeństwa informacyjnego. Oznacza to, że dane osobowe trafiają do różnych podmiotów zlokalizowanych w Chinach, co może powodować faktyczne zróżnicowanie poziomu ochrony danych osobowych. Źródłem owego zróżnicowania są obecnie stosowane środki legalizacji transferów danych osobowych do Chin. Przeprowadzona analiza środków legalizacji transferów danych osobowych stosowanych przez wybrane podmioty chińskie potwierdza, że spośród środków, o których mowa w rozdziale V RODO, praktyczne doniosłość mają jedynie klauzule umowne. Tym samym, stanowisko, zgodnie z którym klauzule umowne stanowią najpopularniejszy środek legalizacji transferów danych osobowych [888] znajduje odzwierciedlenie w praktyce. Zasadniczym skutkiem wykorzystywania przez podmioty

[882] Por. uwagi dotyczące niejasności wynikających z Tarczy Prywatności: Grupa Robocza art. 29: *Opinion 01/2016 on*…, s. 13.
[883] por. L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses*…, s. 8.
[884] Ponownie na tle relacji jakie zachodziły między prawem UE a Tarczą Prywatności - por. Grupa Robocza art. 29: *Opinion 01/2016 on*…, s. 20.
[885] P. Blume: *Transborder Data Flow*…, s. 78; Grupa Robocza art. 29: *EU – U.S. Privacy*…, s. 7–8; pośrednio P.H. Conac: *Public versus Private Enforcement in Corporate Governance*. W: *Research Handbook on Information Law and Governance*. red. S.K. Sandeen, C. Rademacher, A. Ohly, Edward Elgar Publishing, 2021 s. 412.
[886] G. Greenleaf: *NGO Involvement in*…, s. 2; C. Kuner: *Territorial Scope and*…, s. 26.
[887] L. Drechsler., I. Kamara: *Essential equivalence as*…, s. 315 - autorki uważają, że intensywność transferów danych wpływa na oczekiwany poziom ochrony danych osobowych, tj. im większa intensywność transferów, tym wyższy poziom ochrony jest oczekiwany.
[888] L. Bradford, M. Aboy, K. Liddell: *Standard contractual clauses*…, s. 10; C. Kuner: *The Path to*…, s. 71; OECD: *Fostering Cross-Border Data*…, s. 19.

chińskie wyłącznie odpowiednich zabezpieczeń, w tym klauzul umownych, jest tak faktyczna, jak i teoretyczna partykularyzacja poziomu ochrony danych. Dane osobowe, które są przekazywane do Chin na podstawie klauzuli umownych dotyczą konkretnego transferu. Innymi słowy, jednostka, której dane osobowe trafiają do Chin uzyskuje gwarancje ochrony tylko w przypadku transferu danych, który odbywa się między eksporterem A i importerem B. W praktyce będzie to oznaczało, że nawet jeśli umyślnie lub przypadkowo importer B przekaże dane osobowe innym podmiotom, to jednostka pozostanie *de facto* bez należytej ochrony. Będzie mogła jedynie zwracać się do importera B o podjęcie odpowiednich działań zaradczych lub pociągnąć do odpowiedzialności eksportera A, zlokalizowanego w UE. W obu wypadkach nie zostaną jednak usunięte zagrożenia dla jednostki z jakimi wiąże się przetwarzanie danych osobowych w państwie trzecim, w tym także w Chinach[889].

Źródłem zagrożeń dla osoby, której dane dotyczą w sytuacji przetwarzania danych w Chinach jest wątpliwy poziom chińskiego prawa ochrony danych osobowych. Przepisy chińskiego prawa ochrony danych osobowych nie zapewniają osobie, której dane dotyczą należytej ochrony. Powodem takiego stanu rzeczy są m.in. inne wartości, które legły u podstaw reformy prawa chińskiego, a które można streścić jako prymat potrzeby zapewnienia niezachwianego rozwoju technologicznego chińskich przedsiębiorców[890]. Ochrona osoby, której dane dotyczą, w przeciwieństwie do prawa Unii Europejskiej, nie jest zasadniczym zadaniem przepisów chińskiego prawa ochrony danych osobowych[891]. Nadto, w mojej ocenie dodatkowym zagrożeniem, dla osoby której dane dotyczą w sytuacji transferu jej danych do Chin są poważne naruszenia praw człowieka, których dopuszczają się władze chińskie. Uważam, że uchybienia w tym zakresie są niemniej istotne i apriorycznie wykluczają każde państwo trzecie z potencjalnych rozmów na temat legalizacji przekazywania danych osobowych, w tym zwłaszcza na podstawie decyzji w sprawie adekwatności[892].

Dlatego też, tak jak w przypadku USA, tak i w przypadku Chin, podstawowym środkiem legalizacji transferów danych osobowych powinna być decyzja w sprawie

[889] M. Krzysztofek: *Komentarz do art. 45 RODO*…, s. 237 - zgadzam się z M. Krzysztofkiem, że sama wiedza o przysługujących prawach znacznie polepsza sytuację jednostki, ale nie jest wystraczająca dla ich skutecznej realizacji.
[890] Y. Feng: *The future of China's*…, s. 64.; B. Zhao: *Connected Cars in…,* s. 21.; J. Liu: *China's data localization*…, s. 91.; L. Trakman, , R. Walters, B. Zeller: *Digital consent and…,* s. 233; R. Creemers: *China's Emerging Data*… s. 14; B. Zhao, F. Yang: *Mapping the development*… s. 6; 12.; C. You: *Half a loaf*…, s. 16.
[891] R. Creemers: *China's Emerging Data*… s. 14; B. Zhao, F. Yang: *Mapping the development*… s. 11.
[892] L. Drechsler, I. Kamara: *Essential equivalence as*…, s. 235.

adekwatności. Z oczywistych względów, Chiny nie są zdolne do uzyskania właściwej (zwykłej) decyzji w sprawie adekwatności. Stąd, uważam, że transfery danych osobowych do Chin powinny zostać zalegalizowane poprzez zawarcie porozumienia (umowy międzynarodowej), towarzyszącego decyzji w sprawie adekwatności, na kształt porozumień zawieranych z USA. Za sprawą takiego porozumienia będzie możliwe wypracowanie modelu ochrony danych osobowych, który rzeczywiście będzie respektowany przez władze chińskie. Nadto, odpowiednio sformułowane postanowienia porozumienia będą w stanie wyeliminować najpoważniejsze braki w chińskim systemie prawnym. Dodatkowo, porozumienie (umowa międzynarodowa), towarzysząca decyzji w sprawie adekwatności powinno ułatwić uzyskanie przez Unii Europejskiej tożsamego statusu w rozumieniu przepisów prawa chińskiego. O czym była mowa w rozdziale II, przepisy PIPL silnie akcentują zasadę wzajemności w zakresie uznawania poziomów ochrony danych osobowych przez państwa trzecie. Tym samym, podobnie jak miało to miejsce w przypadku decyzji w sprawie adekwatności dla Japonii, zawarcie porozumienia z Chinami otwiera ścieżkę dla wypracowania jednolitego mechanizmu dla transferów z Unii Europejskiej do Chin, jak i z Chin do Unii Europejskiej.

Mając na uwadze powyższe, uważam, że na pytanie szóste (P.6) należy odpowiedzieć twierdząco. Pomimo istnienia różnic w poziomie ochrony danych osobowych w Chinach i Unii Europejskiej, dla zapewniania należytej ochrony praw i wolności osób, których dane dotyczą, możliwe jest bowiem zawarcie porozumienia międzynarodowego między Unią Europejską a Chinami, na wzór porozumień zawieranych między Unią Europejską a USA, w celu regulacji przekazywania danych osobowych.

Sam fakt kompatybilności porozumienia (umowy międzynarodowej) towarzyszącej decyzji w sprawie adekwatności dla przypadku transferu danych osobowych między Unią Europejską a Chinami nie jest jednak wystarczający dla zawarcia porozumienia. Aby odnośne porozumienie rzeczywiście zostało zawarte, koniecznym elementem staje się wola współpracy obu zainteresowanych stron. O czym wielokrotnie wspominałem w tej pracy, szczególną rolę odgrywają bowiem czynniki pozaprawne, w tym zwłaszcza czynniki o charakterze politycznym. Motywowana politycznie potrzeba współpracy państwa trzeciego z Unią Europejską pozwala na wypracowanie wzajemnych ustępstw, bez których osiągnięcie porozumienia staje się niemożliwe. Potwierdza to przypadek USA, gdzie kombinacja okoliczności polityczno-gospodarczych, ważnych tak dla Unii Europejskiej, jak i USA trzykrotnie umożliwiła

stworzenie ram prawnych dla swobodnych transferów danych osobowych. Ram prawnych, które każdorazowo były wyrazem kompromisu ze strony amerykańskiej, godzącej się na przyjęcie rozwiązań opartych o przepisy prawa Unii Europejskiej, czyli rozwiązań bardziej restrykcyjnych w porównaniu z krajowymi standardami, ale także kompromisu po stronie Komisji Europejskiej, akceptującej często niedoskonałe i głośno krytykowane przez europejską doktrynę postanowienia poszczególnych porozumień, w imię utrzymania bliskiej współpracy gospodarczej z USA[893], jak również z uwagi na bliską współpracę Państw Członkowskich i USA w dziedzinie bezpieczeństwa [894] . Także w przypadku Izraela i Argentyny doniosłość relacji gospodarczych obu państw z Unią Europejską była motywacją dla wydania decyzji w sprawie adekwatności dotyczących każdego z nich[895].

4.3. Porozumienie towarzyszące decyzji w sprawie adekwatności jako sposób przekazywania danych osobowych między Unią Europejską a Chinami – pożądana treść

W świetle powyższego, wykorzystanie porozumienia towarzyszącego decyzji w sprawie adekwatności dla przekazywania danych osobowych między Unią Europejską a Chinami jest pożądanym rozwiązaniem. Potrzeba niezakłóconych transferów danych osobowych, motywowana przez realia trwającej współpracy gospodarczej powinna skłaniać do rychłego podjęcia rozmów przedstawicieli Unii Europejskiej i Chin celem osiągnięcia kompromisu. Biorąc pod uwagę rozważania zawarte w rozdziale II, pragnę przedstawić najważniejsze, w mojej ocenie, zagadnienia, które powinny zostać uwzględnione w przyszłym porozumieniu towarzyszącemu decyzji w sprawie adekwatności dla przekazywania danych osobowych między Unią Europejską a Chinami.

W pierwszej kolejności, należy mieć na uwadze, że w przeciwieństwie do USA oraz pozostałych państw trzecich, wobec których wydano decyzje w sprawie adekwatności, Chiny nie są państwem demokratycznym. Nadto, mając na uwadze instrumentalne podejście władz chińskich do ochrony danych osobowych, o którym była mowa w rozdziale II, nie sposób oczekiwać interpretacji potencjalnych wątpliwości na korzyść podmiotu danych, bez zobowiązań władz chińskich wynikających z treści

[893] Podobnie: *European Parliament Resolution of 26 May 2016 on Transatlantic Data Flows*…, pkt I; A. Flor: *The Impact of*…, s. 2036.
[894] *Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows*…, s. 2.
[895] P. Roth: *Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation*. „Journal of Law, Information and Science", 2017, nr 3, s. 49; N. Blackmore: *Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific*. 26.03.2019. https://kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific/ [dostęp: 17.10.2022].

porozumienia. To oznacza, że negocjacje porozumienia muszą zmierzać do maksymalnej ochrony praw i wolności osób, których dane dotyczą, pamiętając o tym, że to wyłącznie postanowienia owego porozumienia będą gwarancją ochrony jednostki.

Porozumienie zawierane między Unią Europejską a Chinami powinno wyczerpująco regulować całokształt zagadnień związanych z przekazywanych danych osobowych. Istotną rolę odegrają przy tym tak podstawowe elementy prawa ochrony danych osobowych jak siatka pojęciowa, czy zasady ochrony danych osobowych. Mimo, że przepisy chińskiego prawa ochrony danych osobowych zawierają wiele pojęć odpowiadających pojęciom zdefiniowanym w art. 4 RODO, jak również zasad, teoretycznie zbieżnych z zasadami, o których mowa w art. 5 RODO, to w świetle sygnalizowanych różnic interpretacyjnych, a zwłaszcza rozproszenia regulacyjnego, można oczekiwać, że to porozumienie będzie zawierało uzgodnioną i wiążącą siatkę pojęciową i katalog zasad ochrony danych osobowych.

Z problematyką zasad ochrony danych osobowych bezpośrednio wiąże się zagadnienie podstaw przetwarzania danych osobowych. Przepisy chińskiego prawa ochrony danych osobowych wciąż cechuje nadmierne poleganie na zgodzie jako podstawie przetwarzania danych osobowych. W tym stanie rzeczy, można oczekiwać, że z porozumienia będzie wynikał wyczerpujący i rozbudowany katalog podstaw przetwarzania danych osobowych.

O czym wspominałem w Rozdziale II, zasadniczym problemem chińskiego systemu prawnego jest również brak organu nadzorczego, który odpowiadałby standardom RODO. Sytuację dodatkowo komplikuje rozproszenie regulacyjne, właściwe dla chińskiego prawa ochrony danych osobowych, którego skutkiem jest przyznanie kompetencji nadzorczych różnym organom, ale bez wskazania jednego, wiodącego organu. Powierzenie tej funkcji jednemu z istniejących organów chińskich nie będzie, więc stanowiło należytej gwarancji ochrony praw jednostki. Stąd, porozumienie powinno ustanowić niezależny, kompetentny organ nadzorczy. Od woli stron negocjujących porozumienie zależy czy za organ nadzorczy zostanie uznany jeden z dotychczasowych organów chińskich, zwłaszcza CAC, czy tę rolę będzie sprawował podmiot odrębny od władz chińskich, ale powiązany z chińskim systemem prawnym, na wzór międzynarodowych organów arbitrażu. Sądzę, że z perspektywy pozycji ustrojowej organów chińskich, w tym CAC, dla zapewnienia skutecznej ochrony praw i wolności osoby, której dane dotyczą lepszym rozwiązaniem jest wybór organu odrębnego.

Postanowienia porozumienia mogą bowiem prowadzić powołania jednego, wspólnego organu nadzorczego dla obu stron porozumienia[896].

Porozumienie powinno także odnosić się do problematyki egzekwowalności zasad ochrony danych osobowych, w tym również naruszenia ochrony danych osobowych. Zdaniem doktryny to właśnie kombinacja wątpliwych zasad i ich egzekwowalności składa się na najpoważniejszą wadliwość PIPL, jednej z ustaw związanych z ochroną danych osobowych w Chinach[897]. W mojej ocenie w porozumieniu musi znaleźć się swego rodzaju zestaw postanowień, które jednoznacznie będą określały konkretne obowiązki administratorów, powiązane z przestrzeganiem zasad ochrony danych osobowych.

W porozumieniu należy także określić przewidywaną ścieżkę dochodzenia naruszeń odnośnych postanowień porozumienia tak przez podmioty prywatne, jak i podmioty publiczne. Zwłaszcza ta ostatnia grupa wymaga szczególnej uwagi, ponieważ w obecnym kształcie przepisy prawa chińskiego są ukierunkowane na podmioty prywatne, zaś status organów publicznych nie jest jednoznacznie przesądzony[898]. To prowadzi do sytuacji, w której takie samo działanie podjęte przez przedsiębiorcę i organ państwa wywoła skrajnie odmienne skutki.

Ostatnim zagadnieniem, którego nie można pominąć w porozumieniu jest problematyka ustanowienia zasad dostępu organów państwa do danych osobowych, które trafią na terytorium Chin. Prawo chińskie przyznaje organom państwa szerokie uprawnienia, które można określić mianem nieograniczonego dostępu. W związku z tym, porozumienie powinno jednoznacznie określać przesłanki dostępu organów państwa do danych oraz zapewniać jednostce egzekwowalne prawa, które zapewnią skuteczną ochronę przed nieuzasadnionym dostępem do ich danych osobowych. W tym względzie inspiracją dla stron negocjujących porozumienie mogą być przepisy wypracowane przez rząd amerykański na etapie zawierania Tarczy Prywatności, a następnie Ram Ochrony Prywatności.

5. Wnioski

Nieustanny przepływ danych osobowych między Unią Europejską a Chinami, w świetle braku decyzji w sprawie adekwatności powoduje konieczność sięgania przez

[896] Europejski Inspektor Ochrony Danych Osobowych.: *Opinion 4/2016*…, s. 8–9.
[897] C. You: *Half a Loaf*…, s. 12, 24; W. Xixin: *The Bundle of*…, s. 48; por. G. Yang: T*heoretical Justification and*…; Q. Zhou: *Whose Data Is*…, s. 78.
[898] Por. B. Allen-Ebrahimian: *China Makes Genetic*….

administratorów lub podmioty przetwarzające dane na zlecenie do odpowiednich zabezpieczeń wskazanych w art. 46 RODO lub odstępstw wynikających z art. 49 RODO.

Praktyka podmiotów chińskich, wynikająca z analizy wybranych polityk prywatności, potwierdza spostrzeżenia doktryny co do braku należytej ochrony praw i wolności osób, których dane dotyczą, gdy wykorzystywane są odpowiednie zabezpieczenia, o których mowa w art. 46 RODO lub odstępstwa wynikające z art. 49 RODO. Tym samym, na piąte pytanie badawcze (P.5) należy udzielić odpowiedzi przeczącej.

Potrzeba niezakłóconych przepływów danych osobowych między Unią Europejską a Chinami prowadzi do konieczności poszukiwania alternatywnych rozwiązań. Ich celem ma być zapewnienie swobody transferu danych osobowych, a zarazem ochrona praw i wolności osób, których dane dotyczą na należytym poziomie. Obie cechy spełnia porozumienie (umowa międzynarodowa) towarzyszące decyzji w sprawie adekwatności. Model ten nawiązuje do koncepcji wykorzystania umowy międzynarodowej jako środka legalizacji transferów danych osobowych [899], a jednocześnie wynika z praktyki Komisji Europejskiej w odniesieniu do legalizacji przekazywania danych osobowych między Unią Europejską a USA.

Zawarcie stosownego porozumienia jest rozwiązaniem gwarantującym negocjującym stronom, tj. Komisji Europejskiej oraz państwu trzeciemu, szerszy zakres swobody. Porozumienie pozwala bowiem na urzeczywistnienie skutecznej ochrony praw i wolności osób, których dane dotyczą, przy jednoczesnym poszanowaniu interesów konkretnego państwa trzeciego. W tym stanie rzeczy, szczególną rolę dla wypracowania należy przypisać czynnikom pozaprawnym, czyli czynnikom natury polityczno-gospodarczej. To od ich wystąpienia uzależniona jest możliwość wypracowania porozumienia, co potwierdza praktyka Komisji Europejskiej, zwłaszcza w odniesieniu do USA.

W świetle powyższego, odpowiedzią na szóste pytanie pomocnicze (P.6) jest odpowiedź twierdząca. Sposobem dla należytego zapewnienia prawa i wolności osób, których dane dotyczą, o których mowa w RODO, w sytuacji transferu ich danych osobowych z terytorium znajdującego się w Unii Europejskiej na terytorium Chin jest zawarcie stosownego porozumienia. Za sprawą takiego porozumienia będzie możliwe wypracowanie takiego modelu ochrony danych osobowych, który rzeczywiście będzie

[899] J.A. Zimmerman: *Transborder Data* Flow…, s. 601; H.P. Lowry: *Transborder Data Flow*…, s. 159.

respektowany przez władze chińskie. Nadto, odpowiednio sformułowane postanowienia będą w stanie wyeliminować najpoważniejsze braki w chińskim systemie prawnym.

ZAKOŃCZENIE

1. Prawne kryteria oceny systemu prawnego państwa trzeciego

Pierwsze pytanie pomocnicze (P.1) dotyczyło wpływu przepisów RODO na katalog kryteriów oceny systemu prawnego państwa trzeciego.

Przedstawione w rozdziale I rozważania prowadzą do wniosku, że ocena systemu prawnego państwa trzeciego jest przeprowadzana z wykorzystaniem przepisów RODO[900], przy czym owe przepisy wyłącznie pośredni charakter. Przepisy RODO stanowią podstawę oceny systemu prawnego państwa trzeciego, jednakże na ich interpretację i stosowanie mają wpływ poglądy doktryny oraz orzecznictwo TSUE.

Sugerowane przez doktrynę katalogi kryteriów są zasadniczo zbieżne i dotykają tych samych zagadnień. Odnosząc się do proponowanych przez doktrynę katalogów kryteriów, zgadzam się z C. Kunerem, według którego nie należy przyjmować sztywnego podejścia do oceny systemu prawnego państwa trzeciego. Za dobrą praktykę poczytuje posługiwanie się dodatkowymi kryteriami oceny w celu pogłębionej analizy systemu prawnego państwa trzeciego, w szczególności dla dogłębniejszego poznania sytuacji jednostki. Uważam, że kryterium zasad ochrony danych osobowych oraz kryterium nadzoru, realizowanego przez organ nadzorczy, można uznać za minimalny, niezbędny katalog kryteriów. Do takiego stanowiska prowadzi w pierwszej kolejności treść art. 45 ust. 2 RODO, jak również analiza praktyki Komisji Europejskiej, dla której szczególne znaczenie mają dokumenty WP12 i WP254. Tym samym, nie popieram stanowiska prezentowanego przez S.L. Duque Carvahlo, która twierdzi, że brak w systemie prawnym państwa trzeciego niektórych spośród zasad ochrony danych osobowych zawartych w RODO jest akceptowalny. Takie stanowisko pozwalałoby na kwestionowania istnienia wszystkich zasad wymienionych w RODO.

Sądzę, że drugorzędne znaczenie mają te kryteria, które dążą do ustalenia źródła uregulowania zasad ochrony danych osobowych w państwie trzecim. Całościowa ocena systemu prawnego może prowadzić do wniosku, że to właśnie samoregulacja jest doskonałym rozwiązaniem, gwarantującym skuteczną ochronę dla podmiotów danych. Oczywistym jest jednak to, że umocowanie nadzoru, jak i jego podstawowe uprawnienia powinny mieć umocowanie w regulacji ustawowej. Samoregulacja może być podstawą dla doposażenia organu nadzorczego w pewne dodatkowe uprawnienia. Za podstawowe

[900] A także Dyrektywy 95/46 w odnośnym okresie.

uprawnienia organu nadzoru uznaję te uprawnienia, które pozwalają organowi nadzorczemu na skuteczne działanie i wykonywanie swoich zadań.

Uważam, że badanie problematyki dostępu organów państwa trzeciego do danych jest obowiązkowym elementem oceny. Stanowi to bezpośrednią konsekwencję wyroków TSUE w sprawach Schrems I i Schrems II. Wraz z C. Kunerem, za źródło tego kryterium uznaję Kartę Praw Podstawowych. Nadto, w pełni podzielam pogląd C. Kunera, zgodnie z którym usprawiedliwieniem braków w systemie prawnym państwa trzeciego nie może być argument występowania tożsamych braków w porządkach prawnych państw członkowskich Unii Europejskiej.

W związku z powyższym, na pytanie pierwsze udzieliłem odpowiedzi twierdzącej, jako że prawne kryteria oceny systemu prawnego państwa trzeciego wynikają z przepisów RODO. Za zrekonstruowane prawne kryteria oceny państwa trzeciego uznaję:

1) Kryterium podstawowych zasad ochrony danych osobowych,
2) Kryterium egzekwowalności podstawowych zasad ochrony danych osobowych,
3) Kryterium kompetentnego, niezależnego organu nadzorczego,
4) Kryterium środków prawnych przyznanych osobie, której dane dotyczą na wypadek naruszenia ochrony danych osobowych, obejmujący środki administracyjne i sądowe,
5) Kryterium dostępu organów państwa na potrzeby ścigania przestępstw i zapewnienia bezpieczeństwa narodowego do danych osobowych przekazanych na terytorium państwa trzeciego.

2. Pozaprawne kryteria oceny systemu prawnego państwa trzeciego

Drugie pytanie pomocnicze (P.2) również wiązało się z problematyką kryteriów oceny systemu prawnego państwa trzeciego, przy czym skupia się na potwierdzeniu lub zaprzeczeniu wpływu czynników pozaprawnych na interpretację i stosowanie tychże kryteriów.

O czym była mowa w rozdziale I, ocena systemu prawnego państwa trzeciego opiera się na kryteriach oceny wynikających z przepisów RODO, ale nie ogranicza się wyłącznie do ich stosowania. Istotną rolę odgrywają czynniki o charakterze pozaprawnym, które wpływają na interpretację, a następnie stosowanie kryteriów prawnych. Te czynniki wyznaczają rzeczywiste podejście Komisji Europejskiej do badanego państwa trzeciego, a w szczególności decydują o akceptacji lub jej braku dla dostrzeżonych wad systemu prawnego państwa trzeciego.

Stoję na stanowisku, zgodnie z którym obecna praktyka Komisji Europejskiej w zakresie stosowania kryterium ochrony praw człowieka i rządów prawa, jak również kryterium międzynarodowych zobowiązań państwa trzeciego można uznać za przejaw wpływu czynników pozaprawnych na przeprowadzaną ocenę, a zarazem naruszenie art. 45 ust. 2 RODO. Katalog kryteriów, o którym mowa w art. 45 ust. 2 RODO określa minimalną treść oceny systemu prawnego państwa trzeciego. Należy więc oczekiwać od Komisji Europejskiej, że treść decyzji w sprawie adekwatności będzie wspominała o tych wszystkich kryteriach oceny, na które wprost wskazuje art. 45 ust. 2 RODO. Natomiast przywołane kryterium ochrony praw człowieka i rządów prawa, jak również kryterium międzynarodowych zobowiązań państwa trzeciego były stosowane dowolnie.

Konsekwencją wpływu czynników pozaprawnych na ocenę systemu prawnego państwa trzeciego jest brak jednoznaczności standardu adekwatności, a jednocześnie wzrost znaczenia zarzutu nieuzasadnionego zróżnicowanego traktowania poszczególnych państw trzecich. Obecnie trudno wskazać czym jest wymagana przez przepisy RODO adekwatność. Zarzucana niejednoznaczność standardu adekwatności wynika z rozbieżności między faktycznym zakresem oceny systemu prawnego państwa trzeciego, a zakresem wynikającym z art. 45 ust. 2 RODO. Analiza treści decyzji w sprawie adekwatności wydanych na podstawie RODO prowadzi do wniosku, że dla uzyskania przez państwo trzecie pozytywnego wyniku oceny nie jest niezbędne spełnienie wszystkich kryteriów wskazanych w art. 45 ust. 2 RODO. Wspomniane decyzje w sprawie adekwatności kładły nacisk na niektóre elementy badanego systemu prawnego państwa trzeciego, tj. istnienie egzekwowalnych zasad ochrony danych osobowych, praw przyznanych jednostce (wraz z odpowiednimi środkami pozwalającymi na reakcję na naruszenie jej danych osobowych), niezależnego i kompetentnego organu nadzoru, a także istnienie ograniczeń w dostępie organów ścigania do danych osobowych. Przywołane, faktyczne kryteria oceny pokrywały się z katalogiem kryteriów zawartym w art. 45 ust. 2 RODO, ale tylko częściowo. Rację ma więc Parlament Europejski, dla którego dokument WP254 określa niezbędny, minimalny zakres oceny. Tym samym, ocenie poddane zostaną tylko takie elementy systemu prawnego państwa trzeciego, co do których uznanie równoważnego poziomi ochrony danych osobowych, w porównaniu z poziomem w Unii Europejskiej, będzie możliwe. To z kolei oznacza, że standard adekwatności przyjmuje dwie postaci. Pierwszą postać wyznacza Dokument WP254 i można go określić jako minimalny standard adekwatności. Druga postać to standard adekwatności, którego źródłem jest art. 45 ust. 2 RODO.

Uważam, że dwojakie rozumienie standardu adekwatności to bezpośrednia konsekwencja wpływu czynników pozaprawnych na ocenę systemu prawnego państwa trzeciego, zatem i na stosowane kryteria oceny i ich wykładnię.

Tym samy, również na pytanie drugie udzieliłem odpowiedzi twierdzącej, ponieważ czynniki pozaprawne wpływają na interpretację i stosowanie kryteriów oceny systemu prawnego państwa trzeciego. Pozaprawnymi czynnikami wpływające na ocenę systemu prawnego są:

1) relacje handlowe z państwem trzecim,
2) nasilenie przepływów danych osobowych, w tym z uwagi na więzy kulturowe,
3) wiodąca rola państwa trzeciego w ochronie danych osobowych,
4) szeroko pojęte relacje polityczne i współpraca.

3. Poziom ochrony danych osobowych w Chinach w świetle standardu adekwatności, o którym mowa w art. 45 RODO

Trzecie pytanie pomocnicze (P.3) było ukierunkowane na ustalenie poziomu ochrony danych osobowych w Chinach oparciu o kryteria oceny systemu prawnego państwa trzeciego. Ustalenia w tym zakresie były kluczowe z perspektywy czwartego pytania pomocniczego (P.4), które konfrontowało poziom ochrony danych osobowych w Chinach ze standardem adekwatności wynikającym z art. 45 RODO.

W pierwszej kolejności ustaliłem, że lektura przepisów CSL, c.k.c., DSL i PIPL nie pozwala na jednoznaczne przypisanie tylko jednej z ustaw funkcji ustawy o podstawnym znaczeniu, która będzie bezwzględnie stosowana do każdego przypadku powiązanego z ochroną danych osobowych. Spośród wymienionych ustaw tylko DSL jawi się jako ustawa o luźniejszych związkach z ochroną danych osobowych, przy czym można ją postrzegać jako wsparcie administratora w realizacji obowiązków zabezpieczenia danych. Także w przypadku CSL związek z ochroną danych osobowych jest osłabiony, co skłania ku uznaniu CSL za sektorową regulację ochrony danych (w ramach środowiska sieciowego). Niemniej jednak, z uwagi na aprobatę dla scenariusza jednoczesnego stosowania kilku ustaw, to CSL, c.k.c., DSL oraz PIPL zbiorczo określam jako chińskie prawo ochrony danych osobowych. Taki scenariusz skutkuje wieloma wątpliwościami natury praktycznej, w tym zwłaszcza czynników, które mają zdecydować o prawidłowym wdrożeniu przepisów przez administratora.

Niezależnie od powyższego, przeprowadzona analiza prowadzi do wniosku, że zestaw definicji wynikających z przepisów prawa chińskiego, cechuje wysoki poziom zgodności ze standardem adekwatności. Na uwagę zasługuje definicja danych

wrażliwych, która przynajmniej teoretycznie, zapewnia jednostce wyższy poziom ochrony, obejmując swoim zakresem szerszy katalog danych niż ma to miejsce w przepisach RODO.

Nie można jednak tracić z oczu niejasnego statusu organów państwa. Tylko w teorii, chińskie przepisy prawa ochrony danych osobowych będą dotyczyły także organów państwa, którym zostanie przypisany status administratora. Zamysłem ustawodawcy nie było jednak ograniczenia organów władzy. Brak ograniczeń państwa w szeroko rozumianym dostępie do danych osobowych jest istotny. Potwierdzeniem oczekiwanej swobody są m.in. uwagi na temat nieścisłości w przepisach CSL, DSL i PIPL, których skutkiem jest brak odpowiedzialności organu państwa za przetwarzanie danych (przy jednoczesnym utrzymaniu odpowiedzialności indywidualnej osób zatrudnionych lub związanych z tym organem), czy twierdzenie, jakoby PIPL było regulacją adresowaną do podmiotów prywatnych nie państwowych.

Także w przypadku pozostałych elementów systemu ochrony danych osobowych w Chinach trudno mówić o zgodności ze standardem adekwatności. W szczególności katalog zasad ochrony danych osobowych jest przejawem tzw. chińskiej specyfiki, co przejawia się w rzeczywistym stosunku administratorów danych do przestrzegania zasad. Tracą na znaczeniu różnice w sposobie sformułowania poszczególnych zasad ochrony danych osobowych, ponieważ ich faktyczne przestrzeganie nie jest jednakowo gwarantowane. Doktryna wyjaśnia, że kombinacja zasad i ich (niedoskonałej) egzekwowalności stanowi najpoważniejszą wadę PIPL, a tym c.k.c., jako że oba katalogi zasad są identyczne.

Na podobną ocenę zasługują prawa osób, których dane dotyczą. Pozycja jednostki w Chinach ma niewiele wspólnego z potrzebą ochrony jej podstawowych praw i wolności, z uwagi na konieczność zabezpieczenia interesów rynku. Do takiego wniosku prowadzi stanowisko Wanga. Autor wyjaśnia, że na potrzeby wykładani praw jednostki, o których mowa w PIPL należy m.in. wziąć pod uwagę fakt, że prawa dotyczą przetwarzania danych, nie danych osobowych jako takich, co wyłącza ich ogólny i absolutny, ponieważ owe prawa są stosowane w określonych sytuacjach. W świetle powyższego, nawet zaawansowane obowiązki nakładane na administratora na niewiele się zdadzą.

Ponadto, osoba, której dane dotyczą decydująca się na skorzystanie z procedury sądowej dla realizacji swoich praw możne znaleźć się w sytuacji, gdy to administrator będzie jednostronnie ustalał zasady rozwiązania sporów, wybierając także sąd właściwy. To z kolei oznacza, że najczęstszym wyborem administratora będzie sąd chiński,

a prawem właściwym będzie prawo chińskie. Jednostka może więc tylko liczyć, że prawdziwe jest stanowisko L. Jia i L. Ruan, wedle których, w odniesieniu do zagranicznych użytkowników aplikacji i usług chińskich przedsiębiorców, mowa o odrębnym traktowaniu i wyższym poziomie ochrony.

Pozycja jednostki w chińskim systemie prawnym jest osłabiona także z uwagi na brak wsparcia organu nadzoru na takich zasadach jak ma to miejsce w Unii Europejskiej. Brak jest bowiem który odpowiadałby standardowi adekwatności. W chińskim systemie prawnym nie ma jednego, wyspecjalizowanego, niezależnego organu nadzoru. Ochrona danych osobowych realizowana przez CAC, jak i dla MPS czy MIIT jest wyłącznie dodatkowym ich zdaniem. Przepisy PIPL nie wskazują terminu dla notyfikacji zdarzenia na rzecz organu nadzoru, jak również nie przyznają organizacji pożytku publicznego (czy podobnym podmiotom) uprawnienia do wystąpienia do żądaniem kierowanym do organu nadzoru w mieniu lub na rzecz jednostki. Wskutek braku niezależności wspomnianych organów nie można wykluczyć wpływu czynników natury pozaprawnej na ocenę potencjalnych naruszeń, czy też podjęcie decyzji w przedmiocie udzielenia zgody na transfer danych osobowych poza Chiny.

Oceniając chiński sytemu ochrony danych osobowych nie można pominąć zagadnienia dostępu organów ścigania do danych. Funkcjonujące rozwiązana są dalekie od oczekiwanego przez standard adekwatności poziomu jednoznaczności oraz proporcjonalności. Przepisy nie określają konkretnych przesłanek tak uzyskania dostępu, jak i jego ograniczeń. Organy państwa dysponują więc dyskrecjonalną władzą, co pozwala realizować w ten sposób cele istotne z punktu widzenia partii, do których zalicza się m.in. walkę z podmiotami uznanymi za niewygodne dla bieżącej polityki chińskiej, jak również sprawne zarządzanie obywatelami, w tym poprzez tworzenie szczegółowych profili na ich temat.

Uważam, że pozornie ochrona danych osobowych w Chinach wynikająca z CSL, c.k.c. i PIPL jest bliska, czy wręcz odpowiada standardowi adekwatności. Jest to jednak wyłącznie złudne wrażenie, któremu przeczą przedstawione powyżej wnioski. Dlatego też odpowiedzią na pytanie trzecie (P.3) jest stwierdzenie, że poziom ochrony danych osobowych w Chinach nie odpowiada standardowi ochrony danych osobowych wymaganemu przez przepisy prawa Unii Europejskiej. W związku z tym, na pytanie czwarte (P.4) udzieliłem odpowiedzi twierdzącej, ponieważ aktualny poziom ochrony danych osobowych w Chinach wyklucza uznanie Chin za państwo, wobec którego może zostać wydana decyzja w sprawie adekwatności w rozumieniu art. 45 ust. 1 RODO.

4. Wykorzystanie odpowiednich zabezpieczeń, o których mowa w art. 46 RODO oraz odstępstw zawartych w art. 49 RODO dla przekazywania danych osobowych do Chin

Piąte pytanie pomocnicze (P.5) dotykało problematyki należytej ochrony jednostki, której dane osobowe mogą być przekazywane do Chin na podstawie odpowiednich zabezpieczeń, o których mowa w art. 46 RODO lub odstępstw wynikających z art. 49 RODO.

Nadrzędnym celem prawa ochrony danych osobowych w Unii Europejskiej jest ochrona praw i wolności osoby, której dane są przetwarzane. Nie chodzi przy tym o całkowity zakaz przetwarzania danych osobowych. Przeciwnie. Należy poszukiwać takiego rozwiązania (operacji przetwarzania), które pozwoli realizację założeń administratora lub podmiotu przetwarzającego, przy jednoczesnym poszanowaniu praw i wolności osoby, której dane dotyczą tylko o takie opracowanie każdej z operacji na danych osobowych. Z perspektywy jednostki, o skutecznej ochronie danych osobowych można mówić, jeśli przyjęte rozwiązania cechuje transparentność oraz pewność. Transparentność oznacza, że jednostka wie, co dzieje się z jej danymi osobowymi, ale także jest świadoma z jakich praw może korzystać. Natomiast pewność to nie tyle niezmienność sytuacji, ale gwarancja dla jednostki, że w każdych warunkach jej dane osobowe będą odpowiednio chronione. Obie cechy powinny dotyczyć także transferów danych osobowych. Jednak tym, co wyróżnia transfery danych osobowych jest zmiana otoczenia prawnego, w którym znajdą się dane osobowe, a któremu to zdarzeniu najczęściej towarzyszy wzrost ryzyka naruszenia praw i wolności osoby, której dane dotyczą. Stosowanie dla transferów danych osobowych do Chin tak odpowiednich zabezpieczeń o których mowa w art. 46 RODO, jak i odstępstw, których katalog znajduje się w art. 49 RODO przeczy obu wskazanym powyżej cechom.

Przeprowadzona w rozdziale III analiza wybranych polityk prywatności podmiotów chińskich, potwierdza, że zakres zastosowania odpowiednich zabezpieczeń, jak i odstępstw, o których mowa w rozdziale V RODO jest ograniczony. To z kolei przekłada się na poziom ochrony danych osobowych, który gwarantują odpowiednie zabezpieczenia i odstępstwa. Przyczyną takiej oceny jest przede wszystkim wysoki poziomem niepewności, dla osoby której dane dotyczą, ponieważ ani organy Unii Europejskiej, ani organy chińskie nie są związane odpowiednimi zabezpieczeniami. Co więcej, osoba, której dane dotyczą musi mieć świadomość, że poziom ochrony danych osobowych gwarantowany przez wybrane odpowiednie zabezpieczenie jest ograniczony

podmiotowo, tj. wiążę on ściśle określone podmioty. Stąd, dalsze przekazanie danych osobowych innemu administratorowi lub podmiotowi przetwarzającemu nie będzie automatycznie oznaczało zagwarantowania jednostce jakiejkolwiek ochrony. Niepewność cechuje także pozycję administratora lub podmiotu przetwarzającego, który decyduje się na wykorzystanie jednego z odpowiednich zabezpieczeń m.in. z uwagi brak jednoznacznych przesłanek wyboru uzupełniających zabezpieczeń czy wpływ przepisów prawa państwa trzeciego na stosowane odpowiednie zabezpieczenia oraz odstępstwa. Dodatkowo, okolicznością istotną dla administratorów lub podmiotów przetwarzających danej są wysokie nakłady czasu i pracy, z którymi wiążę zaprojektowanie i implementacja odpowiedniego zabezpieczenia lub odstępstwa.

Co szczególnie istotne dla należytej ochrony osoby, której dane dotyczą, a co wynika z treści analizowanych polityk prywatności, nieprawidłową praktyką jest utożsamianie odstępstw zawartych w art. 49 RODO z odpowiednimi zabezpieczeniami, których katalog zawiera art. 46 RODO. Wiąże się to z nieuprawnionym traktowaniem odstępstw, o których mowa w art. 49 RODO jako kolejnej, zwykłej podstawy transferu danych osobowych. Tym samym, traci na znaczeniu wyjątkowy charakter art. 49 RODO. Potwierdza to zwłaszcza praktyka wybranych podmiotów chińskich w odniesieniu do przesłanki zgody, o której mowa w art. 49 ust. 1 lit. a RODO. W mojej ocenie przesłanka zgody nie może być wykorzystana dla legalizacji regularnych i powtarzalnych transferów, a powinna dotyczyć konkretnego transferu lub zestawu transferów. Tymczasem, żadna z analizowanych polityk prywatności, w której treści znalazło się odwołanie do zgody jako podstawy transferu danych osobowych, nie zawierała elementów wskazanych w art. 49 ust. 1 lit. a RODO.

Ponadto, na ochronę praw i wolności osób, których dane dotyczą, gdy podstawą transferu jest jedno z odpowiednich zabezpieczeń lub jedno z odstępstw, o których mowa w rozdziale V RODO, wpływa poziom ochrony danych osobowych w państwie trzecim. Wątpliwy poziom ochrony danych osobowych w Chinach, wynikający m.in. z instrumentalnej roli przepisów prawa chińskiego, jak również nieograniczonego dostępu organów chińskich do danych osobowych jest zatem okolicznością, która dodatkowo nakazuje kwestionować przydatność odpowiednich zabezpieczeń o których mowa w art. 46 RODO, jak i odstępstw, których katalog znajduje się w art. 49 RODO dla przekazywania danych osobowych do Chin.

W tym stanie rzeczy, na piąte pytanie badawcze (P.5) udzieliłem odpowiedzi przeczącej. Ani odpowiednie zabezpieczenia o których mowa w art. 46 RODO, ani

odstępstwa wskazane w art. 49 RODO nie gwarantują należytej ochrony praw i wolności osób, których dane dotyczą.

5. Przekazywanie danych osobowych na podstawie porozumienia wzorowanego na porozumieniach w sprawie transferów danych zawieranych między Unią Europejską a USA

Szóste pytanie pomocnicze (P.6) miało na celu ustalenie, czy dopuszczalnym jest wykorzystanie dla transferów danych osobowych między Unią Europejską a Chinami porozumienia, dla którego wzorem będą porozumienia w sprawie transferów danych osobowych zawierane między Unią Europejską a USA.

Z przeprowadzonych badań wynika, że Komisja Europejska, w ramach postępowań związanych z wydaniem decyzji w sprawie adekwatności, wypracowała praktykę modyfikacji przedmiotu oceny. Niekiedy, Komisja Europejska, współpracująca z badanym państwem trzecim, decydowała, że w miejsce systemu prawnego państwa trzeciego, ocenie zostanie poddane porozumienie zawierane między Unią Europejską a owym państwem trzecim. W tym modelu, decyzji w sprawie adekwatności towarzyszy porozumienie, które zapewnia oczekiwany poziom ochrony danych osobowych w państwie trzecim (jest to jednocześnie nawiązanie do koncepcji wykorzystania umowy międzynarodowej w sprawie transferów danych osobowych).

Taki model odegrał szczególną rolę w relacjach Unii Europejskie i USA. Początek obowiązywania europejskich przepisów o ochronie danych osobowych to także początek zainteresowania władz USA objęciem transferów między Unią Europejską a USA decyzją w sprawie adekwatności, ale na innych warunkach. Różnice w poziomie ochrony danych osobowych, który wynika z prawodawstwa USA, odgórnie wyłączały możliwość spełnienia przez USA standardu adekwatności. Natomiast porozumienie tworzy bowiem własny prawny ekosystem. Jest on odrębny od systemu prawnego państwa trzeciego, ale i tak wpływa na ten system. Fakt, że negocjacje z państwem trzecim prowadzi Komisja Europejska pozostawia niezbędny zakres swobody i otwiera drogę dla wzajemnych ustępstw. Niemniej jednak, porozumienie musi dostarczać odpowiedniego poziomu ochrony danych osobowych. W związku z tym w jego treści m.in. mogą być przewidziane prawa osób, których dane dotyczą, obowiązki administratora; za sprawą porozumienia może dojść do wypracowania pożądanej konstrukcji organu nadzoru (nawet poprzez powołanie jednego, wspólnego organu dla obu stron porozumienia), czy wręcz usunięcia, w drodze odpowiednich postanowień porozumienia, najpoważniejszych wątpliwości związanych z zagadnieniem ochrony praw człowieka w danym państwie trzecim.

Wykluczenie zastosowania odpowiednich zabezpieczeń i odstępstw, o których mowa w rozdziale V RODO dla przekazywania danych osobowych do Chin skłania ku poszukiwaniu rozwiązania alternatywnego. Takie spojrzenie jest podyktowane brakiem szans na ujednolicenie ogólnoświatowego poziomu ochrony danych osobowych, akceptowanego przez Unię Europejską, w perspektywie najbliższych lat. Nie bez znaczenia jest też potrzeba zapewnienia właściwej ochrony praw i wolności jednostki, której dane osobowe i tak trafią na terytorium Chin. Stąd realnym alternatywnym rozwiązaniem jest porozumienie w sprawie transferów danych osobowych.

Przyjmuje się, że posłużenie się porozumieniem w sprawie transferów danych osobowych jest rozwiązaniem sugerowanym dla systemów prawnych o skomplikowanej sytuacji. Co potwierdza przeprowadzona ocena systemu prawnego Chin, do tej kategorii zaliczają się Chiny. Dodatkowo, sytuacja Chin ma wiele wspólnego z sytuacją USA w kontekście transferów danych osobowych z Unii Europejskiej W obu przypadkach, współpraca gospodarcza z Unią Europejską ma znaczący wpływ na potrzebę przekazywania danych osobowych, a transfery są regularnie i intensywne (znaczna część działalności gospodarczej również i podmiotów chińskich łączy się produktami lub usługami społeczeństwa informacyjnego). Dane osobowe trafiają zatem do różnych podmiotów zlokalizowanych w Chinach, przez co dochodzi do faktycznego różnicowa poziomu ochrony danych osobowych. Sytuacja Chin jest o tyle wyjątkowa, o ile poziom ochrony danych osobowych zapewniany prze tamtejsze prawodawstwo można uznać za źródło zagrożeń dla osoby. Przepisy chińskiego prawa ochrony danych osobowych cechuje prymat potrzeby zapewnienia niezachwianego rozwoju technologicznego chińskich przedsiębiorców.

Taki stan rzeczy powoduje, że podstawowym środkiem legalizacji transferów danych osobowych do Chin powinna być decyzja w sprawie adekwatności. Chiny, z oczywistych względów, nie spełniają kryteriów niezbędnych dla uzyskania typowej decyzji w sprawie adekwatności. Dlatego też, w mojej ocenie, najlepszym rozwiązaniem dla legalizacji transferów danych osobowych do Chin jest zawarcie porozumienia towarzyszącego decyzji w sprawie adekwatności, na kształt porozumień zawieranych z USA.

Aby doszło do zawarcia takiego porozumienie, koniecznym elementem staje się wola współpracy obu zainteresowanych stron, a więc wystąpienie czynników o charakterze pozaprawnym w postaci woli współpracy obu stron, motywowanej interesami politycznymi. Dzięki temu strony będą mogły rozpocząć negocjacje,

a następnie wypracować taki model ochrony danych osobowych, który rzeczywiście będzie respektowany przez władze chińskie oraz będzie gwarantował poziom ochrony danych osobowych zgodny z RODO. Warunkiem zawarcia porozumienia między Unią Europejską a Chinami jest bowiem wyeliminowanie za pomocą jego postanowień najpoważniejszych braków w chińskim systemie prawnym, do których zaliczają się m.in. zasady ochrony danych osobowych wraz z mechanizmami gwarantującymi ich przestrzeganie, podstawy przetwarzania danych osobowych, skuteczne ograniczenia dostępu organów chińskich do transferowanych danych osobowych.

Nie bez znaczenia jest fakt, że zawarcie porozumienia będzie otworzy Unii Europejskiej drogę do uzyskania tożsamego statusu w rozumieniu przepisów prawa chińskiego, z powodu znaczenia jakie prawo chińskie przypisuje zasadzie wzajemności.

Mając na uwadze powyższe, na szóste pytanie pomocnicze (P.6.) udzieliłem odpowiedzi twierdzącej. Z uwagi na istnienie różnic w poziomie ochrony danych osobowych w Chinach i Unii Europejskiej, dla zapewniania należytej ochrony praw i wolności osób, których dane dotyczą, pożądanym jest zawarcie porozumienia międzynarodowego w celu regulacji przekazywania danych osobowych między Unią Europejską a Chinami, na wzór porozumień zawieranych między Unią Europejską a USA.

6. Należyte zabezpieczenia praw i wolności osób, których dane dotyczą w sytuacji transferu ich danych osobowych z terytorium znajdującego się w Unii Europejskiej na terytorium Chin

Ocena poziomu ochrony danych osobowych w państwie trzecim jest przeprowadzana w oparciu o kryteria wynikające z przepisów RODO. Ich interpretacja i stosowanie uwzględnia także czynniki natury pozaprawnej, w tym zwłaszcza czynniki o charakterze polityczno-gospodarczym.

Przepisy chińskiego prawa ochrony danych osobowych, poddane analizie w oparciu o kryteria oceny systemu prawnego państwa trzeciego wynikające z RODO, zapewniają poziom ochrony danych osobowych, który nie odpowiada standardom prawa Unii Europejskiej. Z tego względu, wobec Chin nie może zostać wydana decyzja w sprawie adekwatności, o której mowa w art. 45 ust. 1 RODO.

Brak decyzji w sprawie adekwatności czyni koniecznym wykorzystywanie dla transferów danych osobowych do Chin odpowiednich zabezpieczeń, o których mowa w art. 46 RODO lub odstępstw, wynikających z art. 49 RODO. Jednakże ani odpowiednie zabezpieczenia ani odstępstwa nie zapewniają nie gwarantują należytej ochrony praw i wolności osób, których dane dotyczą.

Intensywność współpracy gospodarczej Chin z Unią Europejską oraz wątpliwy poziom ochrony danych osobowych w Chinach, sugerują poszukiwanie rozwiązania alternatywnego dla decyzji w sprawie adekwatności. Za takie rozwiązanie uznaje się porozumienie w sprawie transferów danych osobowych, zawierane między Unią Europejską a państwem trzecim.

W świetle powyższego, na główne pytanie badawcze należy udzielić następującej odpowiedzi: aby należycie zabezpieczyć prawa i wolności osób, których dane dotyczą, o których mowa w RODO, w sytuacji transferu ich danych osobowych z terytorium znajdującego się w Unii Europejskiej na terytorium Chin najkorzystniejszym rozwiązaniem staje się zawarcie porozumienia w sprawie transferów danych, wzorowanego na porozumieniach zawieranych między Unią Europejską a USA, które to porozumienie będzie towarzyszyło decyzji w sprawie adekwatności.

BIBLIOGRAFIA

Literatura

1. Aho B., Duffield R.: *Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China*. „Economy and Society", 2020, nr 49.
2. Austin G.: *Cybersecurity in China. The Next Wave*. Springer, Cham 2018.
3. Barta P., Litwiński P., Kawecki M.: *Komentarz do art. 44.* W: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. i swobodnym przepływem takich danych. Komentarz.* Red. P. Barta, P. Litwiński, M. Kawecki. C.H. Beck, Warszawa 2017.
4. Barta P., Litwiński P., Kawecki M.: *Komentarz do art. 46.* W: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. i swobodnym przepływem takich danych. Komentarz.* Red. P. Barta, P. Litwiński, M. Kawecki. C.H. Beck, Warszawa 2017.
5. Barta P., Litwiński P., Kawecki M.: *Komentarz do art. 49.* W: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. i swobodnym przepływem takich danych. Komentarz.* Red. P. Barta, P. Litwiński, M. Kawecki. C.H. Beck, Warszawa 2017.
6. Belli L., Doneda D.: *Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence*. „International Data Privacy Law", 2022, nr 2.
7. Bentzen H.B., Kvammen O.H., Ursin G.: *Maximizing the GDPR potential for data transfers: first in Europe.* „The Lancet Regional Health - Europe", 2023, nr 27.
8. Berti R.: *Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union*. „European Journal of Privacy Law & Technologies", 2020, nr 34.
9. Bertoni E.: *Convention 108 and the GDPR: Trends and Perspectives in Latin America*. „Computer Law & Security Review", 2021, nr 40.
10. Blume P.: *Transborder Data Flow: Is There a Solution in Sight*. „International Journal of Law and Information Technology", 2000, nr 1.
11. Blume P.: *EU Adequacy Decisions: The Proposed New Possibilities*. „International Data Privacy Law", 2015, nr 1.

12. Blythe F., Shankar V.: *Payments and EU Data Protection Law.* W: *Payment Services.* Red. J.Casanova, M. Savoie. Edward Elgar Publishing, Cheltenham 2022.
13. Boram Yang A.: *China in Global Trade: Proposed Data Protection Law and Encryption Standard Dispute*, „A journal of Law and Policy for the Information Society", 2008, nr 3.
14. Bot Y.: *Opinion Of Advocate General Bot Case C-362/14 Maximillian Schrems v Data Protection Commissioner (Request for a Preliminary Ruling from the High Court (Ireland))*. 23.9.2015. ECLI:EU:C:2015:627.
15. Bourgeois J., Kerry C.F., Long W.R.M. i in.: *Essentially Equivalent. A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States*. Sidley, Austin 2019.
16. Bradford L., Aboy M., Liddell K.: *Standard contractual clauses for cross-border transfers of health data after Schrems II*. „Journal of Law and the Biosciences", 2021, nr 1.
17. Breitbarth P.: *A Risk-Based Approach to International Data Transfers*. „European Data Protection Law Review", 2021, nr 4.
18. Burri M.: *Introduction.* W: *Big Data and Global Trade Law*. Red. M. Burri. Cambridge University Press, Cambridge 2021.
19. Burri M.: *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*. „U.C. Davis Law Review", 2017, nr 1.
20. Busch A.*: The Regulation of Transborder Data Traffic: Disputes across the Atlantic*. „Security and Human Rights", 2012, nr 4.
21. Cai P., Chen L.: *Demystifying Data Law in China: A Unified Regime of Tomorrow*. „International Data Privacy Law", 2022, nr 5.
22. Calzada I.: *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*. „Smart Cities", 2022, nr 5.
23. Chander A.: *Is Data Localization a Solution for Schrems II?*. „Journal of International Economic Law ", 2020, nr 3.
24. Chander A., Kaminski M.E., McGeveran W.: *Catalyzing Privacy Law*. „Minnesota Law Review ", 2021, nr 105.
25. Chander A., Schwartz P.M.: *Privacy and/or Trade*. „University of Chicago Law Review", 2023, nr 1.

26. Chaskes W.: *The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet*. „Washington and Lee Law Review", 2022, nr 79.
27. Chen J., Sun J.: *Understanding the Chinese Data Security Law*. „International Cybersecurity Law Review", 2021, nr 2.
28. Chen L.: *Continuity and Change: Some Reflections on the Chinese Civil Code*. „Asia Pacific Law Review", 2021, nr 2.
29. Chen X., Zhang Y.: *The Construct of Information Privacy Concerns in the Chinese Cultural Setting*. „Nankai Business Review International", 2021, nr 12.
30. Chen Y-J., Lin C-F., Liu H-W.: *"Rule of Trust": The Power and Perils of China's Social Credit Megaproject*. „Columbia Journal of Asian Law", 2018, nr 1.
31. Chen Z.: *Rule of Law Response to Face Information Collection Activities of Administrative Agencies*. „Studies in Administrative Law", 2023 nr 3.
32. Clausius M.: *The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes*. „Washington University Global Studies Law Review", 2022, nr 21.
33. Creemers R.: *China's Emerging Data Protection Framework*. „Journal of Cybersecurity", 2022, nr 1.
34. Cui S., Qi P.: *The Legal Construction of Personal Information Protection and Privacy under the Chinese Civil Code*. „Computer Law & Security Review", 2021, nr 41.
35. Czarnocki J., Giglio F., Kun E., Petik M., Royer S.: *Government access to data in third countries. Final report*. Milieu Consulting SRL, European Data Protection Board, Bruksela 2021.
36. de Hert P., Papakonstantinou V.: *The data protection regime in China. In-depth analysis*, Parlament Europesjki, Bruksela 2015.
37. Deighton A.: *The EU-US Privacy Shield - Is It Strong Enough?*. „Privacy & Data Protection ", 2016, nr. 4.
38. Determann L.: *Determann's Field Guide to Data Privacy Law*. Edward Elgar Publishing, Cheltenham 2022.
39. Docksey C., Hijmans H.: *The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law*. „European Data Protection Law Review", 2019, nr 5.

40. Dorwart H.: *Chinese Data Protection in Transition: A Look at Enforceability of Rights and the Role of Courts*. W: *Data Protection and Privacy. In Transitional Times.* T.15. Red. H. Matsumi, D. Hallinan, D. Dimitrova i in., Bloomsbury Publishing, Londyn 2023.
41. Dorwart H.: *Platform Regulation from the Bottom up: Judicial Redress in the United States and China*. „Policy & Internet", 2021, nr 14.
42. Drechsler L.: *Wanted: LED Adequacy Decisions. How the Absence of Any LED Adequacy Decision Is Hurting the Protection of Fundamental Rights in a Law Enforcement Context.* „International Data Privacy Law ", 2021, nr 11.
43. Drechsler L., Kamara I.: *Essential equivalence as a benchmark for international data transfers after Schrems II*. W: *Research Handbook on EU Data Protection Law*. Red. E. Kosta, R. Leenes, I. Kamara, Edward Elgar Publishing, Cheltenham 2022.
44. Drobek P.: *Komentarz do art. 44*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2018.
45. Drobek P.: *Komentarz do art. 45*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2018.
46. Drobek P.: *Komentarz do art. 46*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2018
47. Drobek P.: *Komentarz do art. 49*. W: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. E. Bielak-Jomaa, D. Lubasz. [Dokument elektroniczny], Wolters Kluwer, Warszawa 2018
48. Du L., Wang M.: *Genetic Privacy and Data Protection: A Review of Chinese Direct-to-Consumer Genetic Test Services*. „Frontiers of Law in China ", 2020, nr 11.
49. Duoye X.: *The Civil Code and the Private Law Protection of Personal Information*. „Tsinghua China Law Review", 2020, nr 13.
50. Duque de Carvalho S.L.: *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108*. „European Data Protection Law Review (EDPL)", 2019, nr 1.

51. Erdos D.: *The UK and the EU Personal Data Framework after Brexit: A New Trade and Cooperation Partnership Grounded in Council of Europe Convention 108+?*. „Computer Law & Security Review", 2022, nr 44.
52. Fajgielski P.: *Komentarz do rozporządzenia nr 2016/679 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), art. 44*. W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.
53. Fajgielski P.: *Komentarz do rozporządzenia nr 2016/679 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), art. 45*. W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.
54. Fajgielski P.: *Komentarz do rozporządzenia nr 2016/679 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), art. 46*. W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.
55. Fajgielski P.: *Komentarz do rozporządzenia nr 2016/679 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), art. 47*. W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.
56. Fajgielski P.: *Komentarz do rozporządzenia nr 2016/679 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), art. 49*. W: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* [Dokument elektroniczny], Wolters Kluwer, Warszawa 2022.

57. Feder A.: *A Bull in a China Shop: How CFIUS Made TikTok a National Security Problem*. „Cardozo International & Comparative Law Review", 2022, nr 5.
58. Fei X.: *National Security Considerations in China's Trade Legislations: Offensive or Defensive?*. „US-China Law Review", 2022, nr 19.
59. Feng F., Wang X., Chen T.: *Analysis of the Attributes of Rights to Inferred Information and China's Choice of Legal Regulation*. „Computer Law & Security Review", 2021, nr 41.
60. Feng Y.: *The future of China's personal data protection law: challenges and prospects*. „Asia Pacific Law Review", 2019, nr 1.
61. Wright Fiero A., Beier E.: *New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, And Russian Legislation*. „Stanford Journal of International Law", 2022, nr 58.
62. Fischer B.: *Komentarz do art. 44 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz.* Red. M. Sakowska-Baryła. C.H. Beck, Warszawa 2018.
63. Fischer B.: *Komentarz do art. 45 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz.* Red. M. Sakowska-Baryła. C.H. Beck, Warszawa 2018.
64. Fischer B.: *Komentarz do art. 46 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz.* Red. M. Sakowska-Baryła. C.H. Beck, Warszawa 2018.
65. Fischer B.: *Komentarz do art. 49 RODO*. W: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz.* Red. M. Sakowska-Baryła. C.H. Beck, Warszawa 2018.
66. Flor A.: *The Impact of Schrems II: Next Steps for U.S. Data Privacy Law*. „Notre Dame Law Review", 2021, nr 5.
67. Gao R.Y.: *Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era*. „Tsinghua China Law Review", 2020, nr 13.
68. Geller A.: *How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective*. „GRUR International", 2020, nr 69.

69. Greenleaf G.: *Accountability without Liability: "To Whom" and "with What Consequences"? (Questions for the 2019 OECD Privacy Guidelines Review.* „University of New South Wales Law Research Series ", 2019, nr 67.
70. Greenleaf G.: *California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?*. „Privacy Laws & Business International Report", 2020, nr 168.
71. Greenleaf G.: *China's Completed Personal Information Protection Law: Rights Plus Cyber-Security*. „Privacy Laws & Business International Report", nr 20.
72. Greenleaf G.: *China Issues a Comprehensive Draft Data Privacy Law*. „Privacy Laws & Business International Report", 2020, nr 168.
73. Greenleaf G.: *Global Data Privacy Laws 2021: Uncertain Paths for International Standards*. „Privacy Laws & Business International Report", 2021, nr 169.
74. Greenleaf G.: *How Far Can Convention 108+ "Globalise"? Prospects for Asian Accessions*. „Computer Law & Security Review", 2021, nr 40.
75. Greenleaf G.: *"Modernised" Data Protection Convention 108 and the GDPR*. „Privacy Laws & Business International Report", 2018 nr 22.
76. Greenleaf G.: *NGO Involvement in the Evaluation and Follow-Up Mechanisms for Data Protection Convention 108+ (Submission to the Consultative Committee of Data Protection Convention 108 by the Australian Privacy Foundation (APF).* „University of New South Wales Law Research Series ", 2019, nr 19.
77. Greenleaf G.: *Proposed US Federal Data Privacy Law Offers Strong Protections but Only to US Residents*. „Privacy Laws & Business International Report", 2022, nr 179.
78. Greenleaf G.: *Renewing Data Protection Convention 108: The CoE's "GDPR Lite" Initiatives*. „University of New South Wales Law Research Series", 2016, nr 14.
79. Greenleaf G., Livingston S.: *China's New Cybersecurity Law – Also a Data Privacy Law?*. „Privacy Laws & Business International Report", 2016, nr 19.
80. Greenleaf G., Livingston S.: *PRC's New Data Export Rules: "Adequacy with Chinese Characteristics"?*. „Privacy Laws & Business International Report", 2017, nr 147.
81. Guangping W.: *Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction*. „China Legal Science", 2021, nr 9.
82. Gulczyńska Z.: *A certain standard of protection for international transfers of personal data under the GDPR.* „International Data Privacy Law", 2021, nr 4.

83. Gur B.A.: *The Normative Power of the EU: A Case Study of Data Protection Laws of Turkey*. „International Data Privacy Law", 2020, nr 4.
84. Hamilton J.: *Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems: Shattering the International Privacy Framework*. „Tulane Journal of International and Comparative Law", 2021, nr 29.
85. Wang Han S., Munir A.B.: *Information Security Technology – Personal Information Security Specification: China's Version of the GDPR?*. „European Data Protection Law Review", 2018, nr 4.
86. Hanhua Z.: *Consumer Data Protection in China*. W: *Consumer Data Protection in Brazil, China and Germany. A Comparative Study.* Red. R. Metz, J. Binding, P. Haifeng i in. Göttingen University Press, Göttingen 2016.
87. Hanlin D.: *The System Position and Protection of Personal Information Right in General Provisions of the Civil Law*. „US-China Law Review", 2018, nr 3.
88. Hu B., Liu Y-L., Yan W.: *Should I Scan My Face? The Influence of Perceived Value and Trust on Chinese Users' Intention to Use Facial Recognition Payment*. „Telematics and Informatics", 2023, nr 78.
89. Huang J.: *Reciprocal Recognition and Enforcement of Foreign Judgments in China: The Proposal of a Registration System*. W: *Commercial Issues in Private International Law: A Common Law Perspective*. Red. M. Douglas, M. Keyes, A. Dickinson. Hart Publishing, Oxford 2019.
90. Hughes A.: *A Question of Adequacy - The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (CTH)*. „University of New South Wales Law Journal", 2001, nr 1.
91. Hustinx P.: *Data Protection and International Organizations: A Dialogue between EU Law and International Law*. „International Data Privacy Law", 2021, nr 11.
92. Ivers E.A.: *Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III*. „Boston College Law Review", 2021, nr 62.
93. Jacques L.: *Facial Recognition Technology and Privacy: Race and Gender - How to Ensure the Right to Privacy Is Protected*. „San Diego International Law Journal", 2021, nr 23.
94. Jansen R., Reijneveld M.: *Convention 108+, the GDPR, and Data Processing in the National Security Domain*. „European Data Protection Law Review", 2022, nr 3.

95. Jia L., Ruan L.: *Going Global: Comparing Chinese Mobile Applications' Data and User Privacy Governance at Home and Abroad*. „Internet Policy Review", 2020, nr 9.
96. Jurcys P., Corrales Compagnucci M., Fenwick M.: *The future of international data transfers: Managing legal risk with a 'user-held' data model*. „Computer Law & Security Review", 2022, nr 46.
97. Knockel J., Xiong R.: *(Can't) Picture This 2. An Analysis of WeChat's Realtime Image Filtering in Chats*. *Citizen Lab Research Report No. 122*. [Dokument elektroniczny], University of Toronto, Toronto 2019.
98. Khan D.: D*ata Flow Challenges to International Trade Law and the Global Economy*. „Indian Journal of Law and Legal Research", 2023, nr 5.
99. Khan S.: *Invalidity of EU-US Safe Harbor: practical implications: Part 1*. „Compliance & Risk", 2016, nr 2.
100. Kossof P.: *Chinese legal research*. Carolina Academic Press, Durham, Karolina Północna 2014.
101. Krzysztofek M.: *Komentarz do art. 44 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C.H. Beck, Warszawa 2016.
102. Krzysztofek M.: *Komentarz do art. 45 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C.H. Beck, Warszawa 2016.
103. Krzysztofek M.: *Komentarz do art. 46 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C.H. Beck, Warszawa 2016.
104. Krzysztofek M.: *Komentarz do art. 47 RODO* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C.H. Beck, Warszawa 2016.
105. Krzysztofek M.: *Komentarz do art. 49 RODO.* W: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego.* C.H. Beck, Warszawa 2016.
106. Kuner C.: *Developing an Adequate Legal Framework for International Data Transfers*. W: *Reinventing Data Protection?* Red. S. Gutwirth, Y. Poullet, P. de Hert i in. Springer Science+Business Media B.V., [b.m.w.] 2009.

107. Kuner C.: *Reality and Illusion in EU Data Transfer Regulation Post Schrems*. „German Law Journal". 2017, nr 4.
108. Kuner C.: *Komentarz do art. 44*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020.
109. Kuner C.: *Komentarz do art. 45*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020.
110. Kuner C.: *Komentarz do art. 46*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020.
111. Kuner C.: *Komentarz do art. 47*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020.
112. Kuner C.: *Komentarz do art. 49*. W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020.
113. Kuner C.: *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection*, „University of Cambridge Faculty of Law Research Paper", 2021, nr 20/2021.
114. Kuner C.: *The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards*, „National Law Review of India", 2021, nr 1.
115. Lee J.-A.: *Hacking into China's Cybersecurity Law*. „Wake Forest Law Review", 2018, nr 53.
116. Leenes R.: *Komentarz do art. 42.* W: *The EU General Data Protection Regulation (GDPR). A commentary.* Red. C. Kuner, L.A. Bygrave, L. Drechsler. Oxford University Press, Oxford 2020.
117. Lehdonvirta V.: *European Union Data Protection Directive: Adequacy of Data Protection in Singapore*. „Singapore Journal of Legal Studies ", 2004, nr 2.
118. Pernot-Leplay E.: *China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU?*. „Penn State Journal of Law and International Affairs", 2020, nr 8.

119. Li X.: *Information Privacy Protection in the New Chinese Civil Code: Priority or Replacement?*. „Frontiers of Law in China ", 2020, nr 15.
120. Lin X., Liu H., Li Z. i in.: *Privacy Protection of China's Top Websites: A Multi-Layer Privacy Measurement via Network Behaviours and Privacy Policies*. „Computers & Security", 2022, nr 114.
121. Liss J., Peloquin D., Barnes M. i in.: *Demystifying Schrems II for the cross-border transfer of clinical research data*. „Journal of Law and the Biosciences", 2021, nr 2.
122. Liu J.: *China's data localization*. „Chinese Journal of Communication", 2020, nr 1.
123. Liu J., Zhao H.: *Privacy Lost: Appropriating Surveillance Technology in China's Fight against COVID-19*. „Business Horizons", 2021, nr 64.
124. Liu Y.-L., Huang L., Yan W. i in.: *Privacy in AI and the IoT: The Privacy Concerns of Smart Speaker Users and the Personal Information Protection Law in China*. „Telecommunications Policy", 2022, nr 46.
125. Lixin Y.: *From the General Provisions of Civil Law to the General Rules of Civil Law: A Historic Leap*. „Social Sciences in China", 2020, nr 41.
126. Lowry H.P.: *Transborder Data Flow: Public and Private International Law Aspects*. „Houston Journal of International Law", 1984, nr 2.
127. Lynskey O.: *Delivering Data Protection: The next Chapter*. „German Law Journal", 2020, nr 1.
128. Vander Maelen C.: *EDPB Releases Final Version of 'Guidelines 04/2021 on Codes of Conduct as Tools for Transfers' – An Important Step with Some Rough Edges*. „European Data Protection Law Review", 2022, nr 3.
129. Makulilo A.B.: *Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?*. „International Data Privacy Law ", 2013, nr 1.
130. Makulilo A.B.: *The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius*. „The International Journal of Human Rights", 2021, nr 25.
131. Maldoff G. and Tene O.: *Essential Equivalence and European Adequacy after Schrems: The Canadian Example*. „Wisconsin International Law Journal", 2016, nr 2.
132. Marcinkowski B.: *Privacy Paradox(Es): In Search of a Transatlantic Data Protection Standard*'. „Ohio State Law Journal ", 2013, nr 6.

133. Mattoo A., Meltzer J.P.: *International Data Flows and Privacy: The Conflict and Its Resolution*. „Journal of International Economic Law", 2018, nr 4.

134. McKeaver E.D.: *Is It Best Not to Regulate Transborder Data Flow*. „International Business Lawyer", 1984, nr 4.

135. Mishra N., Mitchell A.D., Sheargold E.: *Restrictions on cross-border data transfers*. W: *Principles of International Trade and Investment Law*. Red. A.D. Mitchell, E. Sheargold. Edward Elgar Publishing, Cheltenham 2021.

136. Miyashita H.: *Human-centric data protection laws and policies: A lesson from Japan*. „Computer Law & Security Review", 2021, nr 40.

137. Murray A.D.: *Data Transfers between the EU and UK Post Brexit?*. „International Data Privacy Law", 2017, nr 3.

138. [brak danych autora]: *National Security Law — Surveillance — Court of Justice of the European Union invalidates the EU-U.S. Privacy Shield. — Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020)*. „Harvard Law Review", 2021, nr 134.

139. Ntouvas I.: *Exporting Personal Data to EU-Based International Organizations under the GDPR*. „International Data Privacy Law", 2019, nr 4.

140. Pauletto C.: *Options towards a Global Standard for the Protection of Individuals with Regard to the Processing of Personal Data*. „Computer Law & Security Review ", 2021, nr 40.

141. Peng Q.: *Legal Liabilities of State Agencies Concerning Personal Information Protection——Interpreting Article 68 of the Personal Information Protection Law of PRC*. „Studies in Comparative Law", 2023, nr 2.

142. Pietrzak S.: *Transborder Data Flows: Binding Corporate Rules as a global transfer mechanism and trusted data processing area* (praca magisterska - Master Thesis Law and Technology LLM - napisana pod kierunkiem dr I.E. Bayamlioglu; Mr.dr. C.M.K.C. Cuijpers) Tilburg University, Tilburg 2017.

143. Pyo G.: *An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts*. „Columbia Journal of Transnational Law", 2021, nr 1.

144. Qi A., Shao G., Zheng W.: *Assessing China's Cybersecurity Law*. „Computer Law & Security Review: The International Journal of Technology Law and Practice", 2018, nr 6.

145. Qian J., Chu I., Kirby P. i in.: *Leading Chinese cross-border brands The Top 50*. [Dokument elektroniczny], KPMG, 2018.

146. Qu B., Huo C.: *Privacy, National Security, and Internet Economy: An Explanation of China's Personal Information Protection Legislation*. „Frontiers of Law in China", 2020, nr 3.

147. Quinn J.: *A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law*. „Science and Technology Law Review", 2018, nr 20.

148. Roberts H.: *Informational Privacy with Chinese Characteristics*. W: *Digital Ethics Lab Yearbook 2021.* J. Mökander, M. Ziosi, Springer, Cham 2022.

149. Roth P.: *Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation*. „Journal of Law, Information and Science", 2017, nr 3.

150. Reidenberg J.R.: *The Simplification of International Data Privacy Rules*. „Fordham International Law Journal", 2006, nr 29.

151. Ryngaert C.M.J., van Eijk N.A.N.M.: *International Cooperation by (European) Security and Intelligence Services: Reviewing the Creation of a Joint Database in Light of Data Protection Guarantees*. „International Data Privacy Law", 2019, no. 1.

152. Salbu S. R.: *The European Union Data Privacy Directive and International Relations*. „Vanderbilt Journal of Transnational Law", 2002, nr 2.

153. Sandfuchs B.: *The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II*. „GRUR International", 2021, nr 3.

154. Saugmandsgaard Ø.: *Opinion of Advocate General Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, Interveners:The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance, Inc., Digitaleurope*.19.12.2019. ECLI:EU:C:2019:1145.

155. Schwartz P. M.: *European Data Protection Law and Restrictions on International Data Flows*. „Iowa Law Review ", 1995, nr 3.

156. Schwartz P.M.: *The EU-U.S. privacy collision: a turn to institutions and procedures*. „Harvard Law Review", 2013, nr 126.

157. Vecellio Segate R.: *Litigating Trade Secrets in China: An Imminent Pivot to Cybersecurity?*. „Journal of Intellectual Property Law & Practice", 2020, nr 15.

158. Shao Y.: *Personal Information Protection: China's Path Choice*, „US-China Law Review". 2021, nr 18.

159. Sharma. S.: *Data Privacy and GDPR Handbook*, Wiley, Hoboken, New Jersey 2019.

160. Si C.: *Research on Data Sovereignty Rules in Cross-Border Data Flow and Chinese Solution*. „US-China Law Review", 2021, nr 18.

161. Giladi Shtub T., Gal M.S.: *The Competitive Effects of China's Legal Data Regime*. „Journal of Competition Law and Economics", 2022, nr 4.

162. Slokenberga S., Rachel J., Niringiye R. i in.: *EU Data Transfer Rules and African Legal Realities: Is Data Exchange for Biobank Research Realistic?*. „International Data Privacy Law", 2019, nr 1.

163. Stoddart J., Chan B., Joly Y.: *The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research*. „Journal of Law, Medicine and Ethics", 2016, nr 1.

164. Svantesson D.J.B.: *The regulation of cross-border data flows*. „International Data Privacy Law", nr 3.

165. Sweet A.S., Bu C.: *Breaching the Taboo? Constitutional Dimensions of China's New Civil Code*. „Asian Journal of Comparative Law", 2023, nr 3.

166. Małobęcka-Szwast I.: *Zastosowanie decyzji Komisji Europejskiej jako podstawy transferu danych osobowych*. W: *Transfery danych osobowych na podstawie RODO.* Red. M. Sakowska-Baryła. Wolters Kluwer, Warszawa 2024.

167. Tang Y., Wang L.: *How Chinese Web Users Value Their Personal Information: An Empirical Study on WeChat Users*. „Psychology Research and Behavior Management", 2021, nr 14.

168. Tiwari A.: *The Comparison between Indian Personnel and PRC New Civil Code, Cyber Laws, and Privacy*. „Jus Corpus Law Journal", 2022, nr 2.

169. Trakman L., Walters R., Zeller B.: *Digital consent and data protection law – Europe and Asia-Pacific experience*. „Information & Communications Technology Law", 2020, nr 2.

170. Tracol X.: *"Schrems II": The Return of the Privacy Shield*. „Computer Law & Security Review", 2020, nr 39.

171. Tzanou M.: *European Union Regulation of Transatlantic Data Transfers and Online Surveillance*. „Human Rights Law Review ", 2017, nr 3.

172. Vogel Y.A.: *Stretching the Limit, The Functioning of the GDPR's Notion of Consent in the Context of Data Intermediary Services*. „European Data Protection Law Review", 2022, nr 2.

173. von Lewinski K.: *Collision of Data Protection Law Regimes*. W: *Data Disclosure. Global Developments and Perspectives*. red. M. Hennemann, K. von Lewinski, D. Wawra i in. De Gruyter, Berlin – Boston 2023.

174. Wang C., Zhang J., Lassi N. i in.: *Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective*. „Healthcare", 2022, nr 10.

175. Wang J.: *Dispute Settlement in the Belt and Road Initiative: Progress, Issues, and Future Research Agenda*. „The Chinese Journal of Comparative Law", 2020, nr 1.

176. Yan Wang C.: *Governing Data Markets in China: From Competition Litigation and Government Regulation to Legislative Ordering*. „George Mason International Law Journal", 2022, nr 1.

177. Wagner J.: *The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?*. „International Data Privacy Law", 2018, nr 8.

178. Wawra D., Kindsmüller K., Tawfiq i in M.: *Cultural influences on personal data disclosure decisions. Chinese Perspectives*. „University of Passau Institute for Law of the Digital Society Research Paper Series", 2022, nr 22–09.

179. Weber R.H.: *Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives*. „International Data Privacy Law", 2013, nr 2.

180. Weiden H., Takase K.: *Data Privacy in Europe and Its Reception under Japanese Law*. W: *Research Handbook on Information Law and Governance*. Red. S.K. Sandeen, C. Rademacher, A. Ohly. Edward Elgar Publishing, Cheltenham 2021.

181. White A.: *Control of Transborder Data Flow: Reactions to the European Data Protection Directive*. „International Journal of Law and Information Technology", 1997, nr 2.

182. Winklbaue S., Horner R.: *Austrian DPA Decides EU-U.S. Data Transfer Through the Use of Google Analytics to Be Unlawful*. „European Data Protection Law Review", 2022, nr 8.

183. Wittershagen L.: *Alternative Data Transfer Tools.* W: *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. Red. L. Wittershagen. De Gruyter, Berlin – Boston 2023.

184. Wittershagen L.: *Transfer of Personal Data to Third Countries under the European Data Protection Laws*. W: *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. Red. L. Wittershagen. De Gruyter, Berlin – Boston 2023.

185. Wolf J.: *Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*. „Washington University Journal of Law & Policy", 2013, nr 43.

186. Wuermeling U., Oldani I.: *Data Transfers in Clouds: The Impact of the GDPR*. W: *Cloud Computing Law*. Red. C. Millard. Oxford University Press, wyd. 2, Oxford 2021.

187. Varotto S.: *The Schrems Decision, the EU-US Privacy Shield and the Necessity to Rethink How to Approach Cross Border Personal Data Transfers at Global Level*. „Communications Law", 2016, nr 21.

188. Voss W.G.: *Cross-Border Data Flows, the GDPR, and Data Governance*. „Washington International Law Journal", 2020, nr 29.

189. Voss W.G.: *Transatlantic Data Transfer Coimpliance*. „Boston University Journal of Science & Technology Law", 2022, nr 2.

190. Xiaodong D.: *Personal Data Protection: Rethinking the Reason, Nature and Legal Framework*. W: *Paradigms of Internet Regulation in the European Union and China.* Red. C. Krönke, M.W. Müller, W. Yu. Nomos, Baden-Baden 2018.

191. Xinbao Z.: *China's Strategy for International Cooperation on Cyberspace*. „Chinese Journal of International Law", 2017, nr 16.

192. Xing H., *Government Data Sharing and Personal Information Protection*. „Administrative Law Research", 2023, nr 2.

193. Xixin W.: *The Bundle of Personal Information Rights from the Perspective of State Protection*. „Social Sciences in China", 2022, nr 43.

194. Yang G.: T*heoretical Justification and Construction of the Prohibition on Right to Personal Information*. „Application of Law", 2023, nr 3.

195. Yin Y.: *Conflict and Balance Between Private Information Protection and Public Interests Against the Background of Normalization of Epidemic Prevention and Control*. „Hebei Law Science ", 2023, nr 41.

196. You C.: *Half a Loaf Is Better than None: The New Data Protection Regime for China's Platform Economy*. „Computer Law & Security Review", 2022, nr 45.

197. Yu L., Ahl B.: *China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform*. „Hong Kong Law Journal", 2021, nr 51.

198. Yuexin Z.: *Cyber Protection of Personal Information in a Multi-Layered System*. „Tsinghua China Law Review", 2019, nr 12.

199. Zalnieriute M.: *Reforming the Australian Framework for International Data Sharing*. „International Data Privacy Law ", 2022, nr 12.

200. Zeno-Zencovich V.: *Free-Flow of Data. Is International Trade Law the Appropriate Answer?* W: *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*. Red. F. Fabbrini, E. Celeste, J. Quinn. Hart Publishing, Oxford 2021.

201. Zhang L.: *"Personal Information of Privacy Nature" under Chinese Civil Code*. „Computer Law & Security Review", 2021, nr 43.

202. Zhang X.: *On the Exercise of the Right to Request Protection of Personal Information*. „Political and Legal Forum", 2023, nr 2.

203. Zhao B.: *Connected Cars in China: Technology, Data Protection and Regulatory Responses*. W: *Grundrechtsschutz im Smart Car. DuD-Fachbeiträge*. Red. A. Roßnagel, G. Hornung. Springer Vieweg, Wiesbaden 2019.

204. Zhao B., Mifsud Bonnici G.P.: *Protecting EU Citizens' Personal Data in China: A Reality or a Fantasy?*. „International Journal of Law and Information Technology", 2016, nr 126.

205. Zhao B., Yang F.: *Mapping the development of China's data protection law: Major actors, core values, and shifting power relations*. „Computer Law & Security Review", 2021, nr 40.

206. Zhao L., Wei Y., Liu Y.: *Determination of the Amount of Damages in Civil Public Interest Litigation in the Field of Personal Information Protection*. „Chinese Procurators", 2023, nr 4.

207. Zheng G.: *Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China*. „Computer Law & Security Review", 2021, nr 43.
208. Zhou Q.: *Whose Data Is It Anyway? An Empirical Analysis of Online Contracting for Personal Information in China.* „Asia Pacific Law Review", 2023, nr 31.
209. Zimmerman J.A.: *Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism*. „Northwestern Journal of International Law & Business", 1982, nr 4.
210. Zinser A.: *International Data Transfer out of The European Union: The Adequate Level of Data Protection According to Article 25 of The European Data Protection Directive*. „The John Marshall Journal of Information Technology & Privacy Law", 2003, nr 4.
211. Zinser A.: *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*. „Tulane Journal of Technology and Intellectual Property", 2004, nr 6.

Akty prawne

Prawo Unii Europejskiej

1. Traktat o Unii Europejskiej (Dz. U. z 2004 r. Nr 90, poz. 864/30 ze zm.).
2. Karta praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 ze. zm.).
3. 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze. zm.).
4. 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. UE. L. z 1995 r. Nr 281, str. 31 ze zm.).
5. Decyzja Komisji z dnia 26 lipca 2000 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Szwajcarii (Dz. U. UE. L. z 2000 r. Nr 215, str. 1 ze zm.).

6. Decyzja 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. UE. L. z 2000 r. Nr 215, str. 7, ze zm.).
7. Decyzja Komisji z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych (Dz. U. UE. L. z 2002 r. Nr 2, str. 13 ze zm.).
8. Decyzja Komisji z dnia 30 czerwca 2003 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Argentynie (Dz. U. UE. L. z 2003 r. Nr 168, str. 19 ze zm.).
9. Decyzja Komisji z dnia 21 listopada 2003 r. w sprawie właściwej ochrony danych osobowych w Guernsey (Dz. U. UE. L. z 2003 r. Nr 308, str. 27 ze zm.).
10. Decyzja Komisji z dnia 28 kwietnia 2004 r. w sprawie odpowiedniej ochrony danych osobowych na wyspie Man (Dz. U. UE. L. z 2004 r. Nr 151, str. 51 ze zm.).
11. Decyzja Komisji z dnia 8 maja 2008 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony danych osobowych na Jersey (Dz. U. UE. L. z 2008 r. Nr 138, str. 21 ze zm.).
12. Decyzja Komisji z dnia 6 września 2005 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Imiennym Rejestrze Pasażerów linii lotniczych, przekazanym do Agencji Służb Granicznych Kanady (Dz. U. UE. L. z 2006 r. Nr 91, str. 49).
13. Decyzja Komisji z dnia 5 marca 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie właściwej ochrony na podstawie ustawy Wysp Owczych w sprawie ochrony danych osobowych (Dz. U. UE. L. z 2010 r. Nr 58, str. 17 ze zm.).
14. Decyzja Komisji z dnia 19 października 2010 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Andorze (Dz. U. UE. L. z 2010 r. Nr 277, str. 27 ze zm.).

15. Decyzja Komisji z dnia 31 stycznia 2011 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Państwie Izrael w odniesieniu do zautomatyzowanego przetwarzania danych osobowych (Dz. U. UE. L. z 2011 r. Nr 27, str. 39 ze zm.).
16. Decyzja wykonawcza Komisji z dnia 21 sierpnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych przez Wschodnią Republikę Urugwaju w odniesieniu do zautomatyzowanego przetwarzania danych osobowych (Dz. U. UE. L. z 2012 r. Nr 227, str. 11 ze zm.).
17. Decyzja wykonawcza Komisji z dnia 19 grudnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie odpowiedniej ochrony danych osobowych w Nowej Zelandii (Dz. U. UE. L. z 2013 r. Nr 28, str. 12 ze zm.).
18. Decyzja wykonawcza Komisji (UE) 2019/419 z dnia 23 stycznia 2019 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Japonię na mocy ustawy o ochronie informacji osobowych (Dz. U. UE. L. z 2019 r. Nr 76, str. 1).
19. Decyzja wykonawcza Komisji (UE) 2021/1772 z dnia 28 czerwca 2021 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo (Dz. U. UE. L. z 2021 r. Nr 360, str. 1 ze zm.).
20. Decyzja wykonawcza Komisji (UE) 2022/254 z dnia 17 grudnia 2021 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 stwierdzająca odpowiedni stopień ochrony danych osobowych przez Republikę Korei na mocy ustawy o ochronie danych osobowych (Dz. U. UE. L. z 2022 r. Nr 44, str. 1).

Prawo chińskie

1. Zhonghua Renmin Gongheguo Xianfa (中华人民共和国宪法) [Konstytucja Chińskiej Republiki Ludowej] (tekst ogłoszony przez Ogólnochińskie Zgromadzenie Przedstawicieli Ludowych 3.11.2018, data wejścia w życie: 3.11.2018, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).
2. Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [Ustawa o bezpieczeństwie narodowym Chińskiej Republiki Ludowej] (tekst

ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 1.07.2015, data wejścia w życie: 1.07.2015, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

3. Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Ustawa o cyberbezpieczeństwie Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 07.11.2016, data wejścia w życie: 1.06.2017, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).
4. Zhonghua Renmin Gongheguo Guojia Qingbao Fa (中华人民共和国国家情报法) [Ustaw o wywiadzie Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 27.04.2018, data wejścia w życie: 27.04.2018, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).
5. Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Kodeks cywilny Chińskiej Republiki Ludowej] (tekst ogłoszony przez Ogólnochińskie Zgromadzenie Przedstawicieli Ludowych 28.05.2020, data wejścia w życie: 1.01.2021, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).
6. Zhonghua Renmin Gongheguo shuju Anquan Fa (中华人民共和国数据安全法) [Ustawa o bezpieczeństwie danych Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 10.06.2021, data wejścia w życie: 1.09.2021, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).
7. Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Ustawa o ochronie danych osobowych Chińskiej Republiki Ludowej] (tekst ogłoszony przez Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych 20.08.2021, data wejścia w życie: 1.11.2021, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).
8. Shuju Chujing Anquan Pinggu Banfa (数据出境安全评估办法) [Wytyczne oceny bezpieczeństwa transferu danych] (tekst ogłoszony przez Chińską Administrację Cyberprzestrzeni 7.07.2022, data wejścia w życie: 1.09.2022, tekst wersji angielsko-chińskiej pozyskano z bazy danych PKU Law).

Umowy i inne dokumenty międzynarodowe

1. Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze. zm.)
2. Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 ze zm.).
3. Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r., zmieniona 11 lipca 2013 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami.

Orzecznictwo

1. Wyrok TSUE z 6.10.2015 r., C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650.
2. Wyrok TSUE z 16.07.2020 r., C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559.

Dokumenty Europejskiej Rady Ochrony Danych Osobowych (Grupy Roboczej art. 29) oraz Europejskiego Inspektora Ochrony Danych Osobowych:

1. Europejska Rada Ochrony Danych Osobowych: *Adequacy Referential WP 254*. 28.11.2017. https://webcache.googleusercontent.com/search?q=cache:qz03vIIbQwsJ:https://ec.europa.eu/newsroom/article29/redirection/document/57550+&cd=2&hl=pl&ct=clnk&gl=pl&client=safari [dostęp: 26.10.2021].
2. Europejska Rada Ochrony Danych Osobowych.: *Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan*. 5.12.2018. https://edpb.europa.eu/sites/default/files/files/file1/2018-12-05-opinion_2018-28_art.70_japan_adequacy_en.pdf [dostęp: 26.05.2021].
3. Europejska Rada Ochrony Danych Osobowych.: *EU - U.S. Privacy Shield - Second Annual Joint Review*. 22.01.2019. https://edpb.europa.eu/sites/default/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf [dostęp: 19.10.2021].
4. Europejska Rada Ochrony Danych Osobowych: *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU*

Level of Protection of Personal Data. Version 2.0. 18.06.2021. https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf. [dostęp: 11.03.2024].

5. Europejska Rada Ochrony Danych Osobowych, *Recommendations 01/2021 on the Adequacy Referential under the Law Enforcement Directive*. 2.02.2021. https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf [dostęp: 26.05.2021].
6. Europejska Rada Ochrony Danych Osobowych: *Opinion 14/2021 Regarding the European Commission Draft Implementing Decision Pursuant to Regulation (EU) 2016/679 on the Adequate Protection of Personal Data in the United Kingdom*. 13.04.2021. https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf [dostęp: 26.05.2021].
7. Europejska Rada Ochrony Danych Osobowych: *Opinion 32/2021 Regarding the European Commission Draft Implementing Decision Pursuant to Regulation (EU) 2016/679 on the Adequate Protection of Personal Data in the Republic of Korea Version 1.0*. 24.09.2021. https://edpb.europa.eu/system/files/2021-09/edpb_opinion322021_republicofkoreaadequacy_en.pdf [dostęp: 21.10.2021].
8. Europejska Rada Ochrony Danych Osobowych: *Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)*. 20.06.2023. https://edpb.europa.eu/system/files/2023-06/edpb_recommendations_20221_bcr-c_v2_en.pdf [dostęp: 16.10.2023].
9. Europejska Rada Ochrony Danych Osobowych: *Guidelines 07/2022 on certification as a tool for transfers. Version 2.0.* 14.02.2023. https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf [dostęp: 16.10.2023].
10. Europejska Rada Ochrony Danych Osobowych*: Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework*. 28.02.2023. https://www.edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [dostęp: 16.02.2024].

11. Europejski Inspektor Ochrony Danych Osobowych.: *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU"*. 20.02.2014. https://edps.europa.eu/sites/default/files/publication/14-02-20_eu_us_rebuliding_trust_en.pdf [dostęp: 7.10.2021].
12. Europejski Inspektor Ochrony Danych Osobowych.: *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*. 30.05.2016. https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf [dostęp: 12.10.2021].
13. Grupa Robocza art. 29.: *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*. 26.06.1997. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf [dostęp: 7.09.2021].
14. Grupa Robocza art. 29.: *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*. 24.7.1998. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf [dostęp: 7.09.2021].
15. Grupa Robocza art. 29.: *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions between the European Commission and the United States Government*. 26.01.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf [dostęp: 7.10.2021].
16. Grupa Robocza art. 29.: *Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" Issued by the US Department of Commerce on 19th April 1999*. 3.03.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp19_en.pdf [dostęp: 7.10.2021].
17. Grupa Robocza art. 29.: *Opinion 5/99 on The Level of Protection of Personal Data in Switzerland*. 7.06.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp22_en.pdf [dostęp: 27.04.2021].

18. Grupa Robocza art. 29.: *Opinion 6/99 Concerning The Level of Personal Data Protection in Hungary*. 7.09.1999. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp24_en.pdf [dostęp: 12.05.2021].
19. Grupa Robocza art. 29: *Opinion 4/2000 on the Level of Protection Provided by the "Safe Harbor Principles"*. 16.05.2000. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf [dostęp: 12.05.2021].
20. Grupa Robocza art. 29.: *Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act*. 26.01.2001. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf [dostęp: 27.04.2021].
21. Grupa Robocza art. 29.: *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*. 26.01.2001. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp40_en.pdf [dostęp: 27.04.2021].
22. Grupa Robocza art. 29.: *Opinion 4/2002 on the Level of Protection of Personal Data in Argentin*a. 3.10.2002. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp63_en.pdf [dostęp: 27.04.2021].
23. Grupa Robocza art. 29.: *Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data*. 13.06.2003. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp78_en.pdf [dostęp: 12.05.2021].
24. Grupa Robocza art. 29.: *Opinion 5/2003 on the Level of Protection of Personal Data in Guernsey*. 13.06.2003. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp79_en.pdf [dostęp: 27.04.2021].
25. Grupa Robocza art. 29.: *Opinion 6/2003 on the Level of Protection of Personal Data in the Isle of Man*. 21.11.2003. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp82_en.pdf [dostęp: 27.04.2021].
26. Grupa Robocza art. 29.: *Opinion 1/2004 on the Level of Protection Ensured in Australia for the Transmission of Passenger Name Record Data from Airlines*.

16.01.2004. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp85_en.pdf [dostęp: 12.05.2021].

27. Grupa Robocza art. 29.: *Opinion 3/2004 on the Level of Protection Ensured in Canada for the Transmission of Passenger Name Records and Advanced Passenger Information from Airlines*. 11.02.2004. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp88_en.pdf [dostęp: 17.05.2021].
28. Grupa Robocza art. 29: *Opinion 1/2005 on the Level of Protection Ensured in Canada for the Transmission of Passenger Name Record and Advance Passenger Information from Airlines*. 19.01.2005. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp103_en.pdf [dostęp: 17.05.2021].
29. Grupa Robocza art. 29.: *Opinion 8/2007 on the Level of Protection of Personal Data in Jersey*. 9.10.2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp141_en.pdf [dostęp: 4.05.2021].
30. Grupa Robocza art. 29.: *Opinion 9/2007 on the Level of Protection of Personal Data in the Faroe Islands*. 9.10.2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp142_en.pdf [dostęp: 4.05.2021].
31. Grupa Robocza art. 29.: *Opinion 6/2009 on the Level of Protection of Personal Data in Israel*. 1.12.2009. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf [dostęp: 4.05.2021].
32. Grupa Robocza art. 29.: *Opinion 7/2009 on the Level of Protection of Personal Data in the Principality of Andorra*. 1.12.2009. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp166_en.pdf [dostęp: 4.05.2021].
33. Grupa Robocza art. 29.: *Opinion 6/2010 on the Level of Protection of Personal Data in the Eastern Republic of Uruguay*. 12.10.2010. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf [dostęp: 4.05.2021].
34. Grupa Robocza art. 29.: *Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand*. 4.04.2011. https://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2011/wp182_en.pdf [dostęp: 4.05.2021].

35. Grupa Robocza art. 29.: *Opinion 07/2012 on the Level of Protection of Personal Data in the Principality of Monaco*. 19.07.2012. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp198_en.pdf [dostęp: 26.05.2021].
36. Grupa Robocza art. 29: *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes*. 10.04.2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf [dostęp: 7.10.2021].
37. Grupa Robocza art. 29.: *Opinion 7/2014 on the Protection of Personal Data in Quebec*. 4.06.2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf[dostęp: 26.05.2021].
38. Grupa Robocza art. 29: *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes*. 5.12.2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf [dostęp: 7.10.2021].
39. Grupa Robocza art. 29: *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision*. 12.04.2016. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [dostęp: 12.10.2021].
40. Grupa Robocza art. 29: *Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection through Surveillance Measures When Transferring Personal Data (European Essential Guarantees)*. 13.04.2016. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf [dostęp: 26.10.2021].
41. Grupa Robocza art. 29: *EU – U.S. Privacy Shield – First Annual Joint Review*. 28.10.2017. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782 [dostęp: 12.10.2021].

Źródła internetowe:

1. *Adequacy Decisions*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. [dostęp: 14.09.2021].
2. Allen & Overy: *Global policy makers take further steps to support data free flow with trust*. 19.05.2023. https://www.jdsupra.com/legalnews/global-policy-makers-take-further-steps-2406526/ [dostęp; 11.10.2023].
3. Aliexpress: *Privacy Policy Aliexpress*. https://terms.alicdn.com/legal-agreement/terms/suit_bu1_aliexpress/suit_bu1_aliexpress201909171350_82407.html [dostęp: 10.08.2023].
4. Alsop T.: *Most valuable technology brands worldwide 2023*. 7.03.2024. https://www.statista.com/statistics/267966/brand-values-of-the-most-valuable-technology-brands-in-the-world/ [dostęp: 17.05.2024].
5. Baidu: *Baidu Privacy Statement*. https://ir.baidu.com/baidu-statement-privacy-protection/ [dostęp: 10.08.2023].
6. Baidu: *Privacy Policy Baidu USA.* https://usa.baidu.com/privacy [dostęp: 10.08.2023].
7. BBC: *Airbnb to Give Chinese Authorities Guest Information*. 29.03.2018. https://www.bbc.com/news/business-43578948 [dostęp: 17.04.2023].
8. Bertuzzi L.: *Is data localization coming to Europe?* 23.08.2022. https://iapp.org/news/a/is-data-localization-coming-to-europe [dostęp: 24.05.2024].
9. Blackmore N.: *Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific*. 26.03.2019. https://kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific/ [dostęp: 17.10.2022].
10. Boulanger M.-H., Burkert H., Havelange B. i in.: *Preparation of a Methodology for Evaluating the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data. Annex to the Annual Report 1998 (XV D/5047/98) of the Working Party Established by Article 29 of Directive 95/46/*EC.1998. https://ec.europa.eu/justice/article-29/documentation/annual-report/files/1998/wp14_en.pdf. [dostęp: 06.09.2021].
11. Broersma M.: *Council Of Europe Warns Over Data Protection Rights*. 30.1.2023, *silicon.co.uk* LexisNexis, [dostęp: 22.09.2023].

12. Bu S.: *Chinese Smart Hardware Brands Flooding Into Europe: How to Divide the Spoils?* 7.07.2023. https://equalocean.com/analysis/2023070719866 [dostęp: 17.05.2024].
13. *Chinese companies see revenue growth in Europe: report*. 15.11.2023 https://english.news.cn/europe/20231115/3aad1c1399ef4054bf7865f505775852/c.html [dostęp; 17.05.2024].
14. Commission Nationale de l'Informatique et des Libertés: *Draft Practical Guide. Transfer Impact Assessment*. 02.2024. https://www.cnil.fr/sites/cnil/files/2024-01/draft_practical_guide_transfer_impact_assessment.pdf [dostęp: 11.03.2024].
15. *Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU-U.S. Privacy Shield.* 18.10.2017. http://webcache.googleusercontent.com/search?q=cache:8suwjp581o0J:ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D47799+&cd=2&hl=pl&ct=clnk&gl=pl&client=safari [dostęp: 19.10.2021].
16. *Commission Staff Working Document Accompanying the Document Report From the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 19.12.2018. https://ec.europa.eu/info/sites/default/files/staff_working_document_-_second_annual_review.pdf [dostęp: 19.10.2021].
17. *Commission Staff Working Document Accompanying the Document Report From the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 23.10.2019. https://ec.europa.eu/info/sites/default/files/staff_working_document_-_third_annual_review.pdf [dostęp: 19.10.2021].
18. *Communication from the Commission to the European Parliament and the Council* on *the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*. 27.11.2013. https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.05/DOC_1&format=PDF [dostęp: 7.10.2021].
19. *Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows*. 27.11.2013. https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF [dostęp: 7.10.2021].

20. *Communication from the Commission to the European Parliament and the Council A New EU Framework to Strengthen the Rule of Law*. 11.03.2014. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0158 [dostęp: 13.10.2023].
21. *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*. 10.01.2017. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN [dostęp: 02.11.2021].
22. Dawson C.: *Alibaba's Tmall Global takes European Brands into China*. 14.11.2023. https://channelx.world/2023/11/alibabas-tmall-global-takes-european-brands-into-china/ [dostęp: 17.05.2024].
23. DigiChina: *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*. 29.06.2021. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ [dostęp: 15.09.2022].
24. Duan Y.: B*alancing the Free Flow of Information and Personal Data Protection*. 3.4.2019. https://ssrn.com/abstract=3484713 [dostęp: 26.04.2023].
25. Allen-Ebrahimian B.: *China Makes Genetic Data a National Resource*. 29.05.2022. https://www.axios.com/2022/03/29/china-makes-genetics-data-national-resource [dostęp: 30.03.2023].
26. Echikson B.: *Japan's Data With Trust Offensive — A Solution to the World's Data Wars?*. 5.05.2023. https://cepa.org/article/japans-data-with-trust-offensive-a-solution-to-the-worlds-data-wars/ [dostęp: 11.10.2023].
27. *European Parliament Resolution of 26 May 2016 on Transatlantic Data Flows*. 26.05.2016. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0233_EN.pdf [dostęp: 19.10.2021].
28. *European Parliament Resolution of 13 December 2018 on the Adequacy of the Protection of Personal Data Afforded by Japan*. 13.12.2018. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0529_EN.pdf [dostęp: 31.05.2021].
29. *European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 — Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP))*.

20.05.2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0256 [dostęp: 16.02.2024].

30. *European Parliament Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework*. 11.05.2023. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html [dostęp: 8.04.2024].
31. *European Parliament Resolution on the Adequacy of the Protection Afforded by the EU- US Privacy Shield*. 5.07.2018. https://www.europarl.europa.eu/doceo/document/B-8-2018-0305_EN.pdf [dostęp: 19.10.2021].
32. EY Switzerland: *Chinese company takeovers in Europe fall to 12-year low – more investments in Switzerland.* 27.02.2024. https://www.ey.com/en_ch/news/2024/02/chinese-company-takeovers-in-europe-fall-to-12-year-low-more-investments-in-switzerland [dostęp: 17.05.2024].
33. Feng E.: *"Surveillance State" Explores China's Tech and Social Media Control Systems*. 7.09.2022. https://www.npr.org/2022/09/07/1118105165/surveillance-state-explores-chinas-tech-and-social-media-control-systems [dostęp: 28.03.2023].
34. *From Europe to the World. The EU and Council of Europe as Global Standard Setters in Data Protection.* 30.01.2021. Impact News Service LexisNexis [dostęp: 22.09.2023].
35. *G7 Roadmap for Cooperation on Data Free Flow With Trust*. 2021. https://assets.publishing.service.gov.uk/media/609cf5e18fa8f56a3c162a43/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf [dostęp: 11.10.2023].
36. Gburek A.: *Świat według chińczyków (raport)*. 5.02.2024. https://geekweek.interia.pl/raport-swiat-wedlug-chinczykow/news-tania-chinszczyzna-te-produkty-podbijaja-swiat-i-sa-dobrej-j,nId,7307968 [dostęp: 17.05.2024].
37. Gershgorn D.: *China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space The program turns neighbors into agents of the surveillance state*. 2.03.2021. https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015 [dostęp: 28.03.2023].

38. Gold A.: *China's New Privacy Law Leaves U.S. Behind*. 23.11.2021. https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [dostęp: 30.03.2023].
39. Guowuyuan guanyu jigou shzhi de tongzhi (国务院关于机构设置的通知) [*Obwieszczenie Rady Państwa Chińskiej Republiki Ludowej w sprawie powołania instytucji*]. 24.03.2018. http://www.gov.cn/zhengce/content/2018-03/24/content_5277121.htm [dostęp: 3.06.2024].
40. Haier: *Oświadczenie o Ochronie Prywatności Klientów Haier Europe (Candy Hoover Group S.r.l.)*. https://www.haier-europe.com/pl_PL/polityka-prywatnosci/ [dostęp: 10.08.2023].
41. Haier: *Privacy Statement Haier Group (Haier Group Corporation)*. https://www.haier.com/global/privacy/ [dostęp: 10.08.2023].
42. Hisense: *External Privacy Notice Hisense UK*. https://hisense.co.uk/external-privacy-notice/ [dostęp: 10.08.2023]
43. Hisense: *Polityka Prywatności Hisense Polska (Gorenje Polska)*. https://pl.hisense.com/polityka-prywatnosci-hisense [dostęp: 10.08.2023].
44. Hisense: *Privacy Policy Hisense International Co., Ltd*. https://global.hisense.com/privacy-policy [dostęp: 10.08.2023].
45. Hisense: *Processing of Personal Data That You Enter in the Forms on the Website and E-News Subscription Hisense Europe*. https://www.hisense-europe.com/en/data_protection [dostęp: 10.08.2023].
46. Huawei: *Polityka Prywantości Huawei Polska*. https://consumer.huawei.com/pl/privacy/privacy-policy/ [dostęp: 10.08.2023].
47. Huawei: *Privacy Policy Huawei Technologies LTD*. https://www.huawei.com/en/privacy-policy [dostęp: 10.08.2023].
48. Human Rights Watch: *Congressional-Executive Commission on China. Hearing on Techno-Authoritarianism: Platform for Repression in China and Abroad. Testimony of Yaqiu Wang Senior Researcher, China Human Rights Watch*. 17.11.2021. https://www.cecc.gov/sites/chinacommission.house.gov/files/documents/CECC%20Hearing%20Testimony%20-%20Yaqiu%20Wang.pdf [dostęp: 29.03.2023].
49. Human Rights Watch: *Letter to House Committee on Energy and Commerce*. 16.03.2023.

https://www.hrw.org/sites/default/files/media_2023/03/Letter%20to%20House%20Committee%20on%20TikTok%20-%20web.pdf [29.03.2023].

50. Hvistendahl M.: *A Revered Rocket Scientist Set in Motion China's Mass Surveillance of Its Citizens. Qian Xuesen's Systems Engineering Permeates Many Facets of Chinese Society*. 14.03.2018. Science https://www.science.org/content/article/revered-rocket-scientist-set-motion-china-s-mass-surveillance-its-citizens [dostęp: 28.03.2023].
51. *Institutional Arrangement for Partnership (IAP)*. 2023. https://www.digital.go.jp/en/dfft-iap-en [dostęp: 10.10.2023].
52. *International Trade in Goods by Partner*. 06.2023. https://ec.europa.eu/eurostat/statisticsexplained/index.php?title=International_trade_in_goods_by_partner [dostęp 24.11.2023].
53. IPVM Team: *Dahua Provides "Uyghur Warnings" To China Police*. 9.02.2021. https://ipvm.com/reports/dahua-uyghur-warning [dostęp: 29.03.2023].
54. JD Supra: *10 Things You Should Know About the New Standard Contractual Clauses*, 7.06.2021. Newstex Blogs LexisNexis [dostęp: 13.10.2023].
55. JD Supra: *EU and U.S. Finalize Data Privacy Framework_ Heres How to Get Certified*'. 11.07.2023. *Newstex Blogs* LexisNexis [dostęp: 22.09.2023].
56. JD Supra: *Get Ready to Update Your Binding Corporate Rules Regulators Expand Requirements*. 7.07.2023. Newstex Blogs LexisNexis [dostęp: 23.9.2023].
57. JD Supra: *New EU-U.S. Data Privacy Framework Legalizes Personal Data Transfers from the EU to US*. 1.08.2023. Newstex Blogs LexisNexis [dostęp: 23.09.2023].
58. JD Supra: *The EU-U.S. Data Privacy Framework A New Solution for the Free Flow of Personal Data*. 27.07.2023. Newstex Blogs LexisNexis [dostęp: 22.09.2023].
59. *Jumping On The EU-US Adequacy Decision Expert Says Wait And See*. 31.07.2023. *Medtech Insight* LexisNexis [dostęp: 22.09.2023].
60. Ka Y.: *Inside China's Surveillance State, Built On High Tech And A Billion Spies*. 1.11.2022. https://worldcrunch.com/culture-society/china-surveillance-cameras [dostęp: 28.03.2023].
61. Zweifel-Keegan C.: *A new era of US privacy policy? National security restrictions on personal data transactions*. 4.03.2024. https://iapp.org/news/a/a-

new-era-of-u-s-privacy-policy-national-security-restrictions-on-personal-data-transactions/ [dostęp: 20.05.2024].

62. Zweifel-Keegan C.: *A view from DC: US House ready to pass data broker bill*. 15.03.2024. https://iapp.org/news/a/a-view-from-dc-us-house-is-ready-to-pass-a-data-broker-bill/ [dostęp: 20.05.2024].
63. Kharpal A.: *China Has Signaled Easing of Its Tech Crackdown — but Don't Expect a Policy U-Turn*. 17.05.2022. https://www.cnbc.com/2022/05/18/china-signals-easing-of-its-tech-crackdown-but-dont-expect-a-u-turn.html [dostęp: 29.03.2023].
64. Ko J.: *The Chinese Government Used Technology to Get a Grip on Coronavirus – and Take Control of Its People*. 14.04.2020. https://www.independent.co.uk/voices/coronavirus-china-technology-mass-surveillance-privacy-human-rights-a9463586.html [dostęp: 30.03.2023].
65. Kokas A.: *Cloud Control: China's 2017 Cybersecurity Law and Its Role in US Data Standardization*. 26.07.2019. https://ssrn.com/abstract=3427372 [dostęp: 8.05.2024].
66. Komisja Europejska: *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows*. 10.07.2023. https://ec.europa.eu/commission/presscorner/detail/eN/ip_23_3721 [dostęp: 28.05.2024].
67. Krstinovska A.: *For Chinese Companies, Better Access to the EU Single Market Leads through the Western Balkans*. 11.01.2024. https://chinaobservers.eu/for-chinese-companies-better-access-to-the-eu-single-market-leads-through-the-western-balkans/ [dostęp: 17.05.2024].
68. Kucharczyk K.: *Chiny podbijają rynek IT*. 3.10.2018 https://cyfrowa.rp.pl/it/art18011891-chiny-podbijaja-rynek-it [dostęp: 17.05.2024].
69. Liu C.: *Chinese brands make a mark in Europe*. 6.03.2016. https://www.chinadaily.com.cn/kindle/2016-03/06/content_23758762.htm [dostęp: 17.05.2024].
70. Nan L.: *TikTok, Huawei, Lenovo lead Kantar's China top 50 global brands ranking*. 6.07.2023. https://jingdaily.com/posts/tiktok-huawei-lenovo-lead-kantars-china-top-50-global-brands-ranking [dostęp: 17.05.2024].

71. Ng C.: *Data Free Flows with Trust: From Concept to Reality*. 9.06.2023. https://www.uschamber.com/security/cybersecurity/data-free-flows-with-trust-from-concept-to-reality [dostęp:11.10.2023].
72. OECD: *Fostering Cross-Border Data Flows with Trust.* 2022. https://www.oecd.org/publications/fostering-cross-border-data-flows-with-trust-139b32ad-en.htm [dostęp: 10.10.2023].
73. Oppo: *Privacy Notice Oppo Global*. https://www.oppo.com/en/privacy/# [dostęp: 10.08.2023].
74. Paine J.: *G7 Leaders Must Overcome Differences to Ensure Continued Free Cross-Border Data Flow*. 29.04.2023. https://thediplomat.com/2023/04/g7-leaders-must-overcome-differences-to-ensure-continued-free-cross-border-data-flow/ [dostęp: 11.10.2023].
75. QQ: *QQ International Privacy Policy*. https://international.qq.com/privacy/privacy_En.html [dostęp: 10.08.2023].
76. Qian I., Xiao M., Mozur P. i in.: *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State*. 21.06.2022. https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html [dostęp: 28.03.2023].
77. Raab C.D., Bennet C.J., Gellman R.M. i in.*: Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Tran*. 1998. https://op.europa.eu/en/publication-detail/-/publication/fd67e466-699b-4491-af96-2f3169a92c4d [dostęp: 6.09.2021].
78. *Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU–U.S. Privacy Shield*. 18.10.2017. https://ec.europa.eu/info/sites/default/files/report_on_the_first_annual_review_of_the_eu-us_privacy_shield_2017.pdf [dostęp: 19.10.2021].
79. *Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 19.12.2018. https://ec.europa.eu/info/sites/default/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf [dostęp: 19.10.2021].

80. *Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield*. 23.10.2019. https://ec.europa.eu/info/sites/default/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf [dostęp: 19.10.2021].
81. *Report from the Commission to the European Parliament and the Council on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) of Directive 95/46/EC*. 15.01.2024. https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf [dostęp: 17.01.2024].
82. Shi Z.: *The Right to Be Forgotten in China——A Third Way to Construct Public Sphere*. 3.04.2021 https://ssrn.com/abstract=3832803 [dostęp: 22.05.2023].
83. Soong C.: *Expert opinions about EU-China relations in 2024*. 25.01.2024 https://merics.org/en/comment/expert-opinions-about-eu-china-relations-2024 [dostęp: 20.05.2024].
84. Southey F.: *Alibaba on the 'continued desire' for European brands in China: 'Consumers are willing to pay for quality and provenance'*. 7.11.2023. https://www.foodnavigator.com/Article/2023/11/07/alibaba-on-the-continued-desire-for-european-brands-in-china-consumers-are-willing-to-pay-for-quality-and-provenance [dostęp: 17.05.2024].
85. Tencent: *Privacy Policy Tencent*. https://www.tencent.com/en-us/privacy-policy.html. [dostęp: 10.08.2023].
86. Tencent: *Privacy Policy Tencent Cloud*. https://www.tencentcloud.com/document/product/301/17345 [dostęp: 10.08.2023].
87. The Committee on Energy and Commerce: *Experts Agree: ByteDance is Beholden to the CCP and Cannot Be Allowed to Exploit Americans' Data*. 7.03.2024. https://energycommerce.house.gov/posts/experts-agree-byte-dance-is-beholden-to-the-ccp-and-cannot-be-allowed-to-exploit-americans-data [dostęp: 20.05.2024].
88. The Diplomatic Service of the European Union: *EU-China Relations factsheet*. 7.12.2023. https://www.eeas.europa.eu/eeas/eu-china-relations-factsheet_en [dostęp: 20.05.2024].

89. *The Fight against the EU_s New Data Deal_ Will Google_ Facebook and Amazon Be Allowed to Send Personal Information of Users to the US? The EU's Agreeement Is Wobbing*. 17.07.2023. Die Welt (English) LexisNexis [dostęp: 22.09.2023].
90. Thomala L.L.: *Most valuable Chinese brands by Brand Finance 2023*. 19.01.2024. https://www.statista.com/statistics/259063/most-valuable-chinese-brands/ [dostęp: 17.05.2024].
91. TikTok: *Polityka prywatności* https://www.tiktok.com/legal/page/eea/privacy-policy/pl-PL [dostęp: 10.08.2023].
92. TikTok: *Privacy Policy Tiktok (Wersja Dla Pozostałych Regionów)*. https://www.tiktok.com/legal/page/row/privacy-policy/en. [dostęp: 10.08.2023].
93. Vats A.: *Data Free Flow with Trust: Is There a Solution in Sight?*. 28.01.2023. https://www.orfonline.org/expert-speak/data-free-flow-with-trust/ [dostęp: 11.10.2023].
94. WeChat: *WeChat Privacy Policy*. https://www.wechat.com/en/privacy_policy.html. [dostęp: 10.08.2023].
95. Weixin: *Weixin Privacy Protection Guidelines*. https://weixin.qq.com/cgi-bin/readtemplate?lang=en_US&t=weixin_agreement&s=privacy&cc=CN [dostęp: 10.08.2023].
96. Whalen J.: *Chinese Censorship Invades the U.S. via WeChat*. 7.01.2021. https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban/ [dostęp: 30.06.2023].
97. World Economic Forum: *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. 5.2020. https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf [dostęp: 11.10.2023].
98. Xiaomi: *Polityka Prywatności Xiaomi*. https://privacy.mi.com/all/pl_PL/ [dostęp: 10.08.2023].
99. Xijia Q., Qingrui C.: *China signs 18 deals with France to expand economic cooperation, opening up wider for France, Europe*. 7.05.2024. https://www.globaltimes.cn/page/202405/1311825.shtml [dostęp: 20.05.2024].
100. Yang Z.: *The Chinese Surveillance State Proves That the Idea of Privacy Is More "Malleable" than You'd Expect*. 10.10.2022.

https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/ [dostęp: 28.03.2023].

101. Zhonghua renmin gongheguo guowuyuan ling (中华人民共和国国务院令) [*Rozporządzenie Rady Państwa Chińskiej Republiki Ludowej*]. 30.07.2021. http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?mc_cid=da5881cf31&mc_eid=a268621911 [dostęp: 3.06.2024].

102. ZTE: *Privacy Policy ZTE Corpotation*. https://www.zte.com.cn/global/privacy_center/privacy_policy.html accessed [dostęp: 10.08.2023].

103. ZTE: *Privacy Policy ZTE Corporation - Devices*. https://ztedevices.com/en-us/legal/privacy-policy/ [dostęp: 10.08.2023].