Wojciech Rafał Wiewiórowski

Rozdział 1.
Wpływ RODO na rozwój prawa ochrony danych osobowych poza Unią Europejską

1. Uwagi wprowadzające

Gdy w 2012 r. Komisja Europejska przedstawiła projekt ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych)[1], stało się jasne, że jego ewentualne uchwalenie rozpocznie szerszą światową dyskusję na temat przyszłego kształtu prawa ochrony prywatności i ochrony danych osobowych. W trakcie prac Parlamentu Europejskiego i Rady, które toczyły się w latach 2012–2016, dyskusja ta miała przede wszystkim wymiar europejski. Próbowano oceniać różnice w podejściu do kwestii prywatności pomiędzy poszczególnymi krajami członkowskimi UE, poszczególnymi kulturami prawnymi istniejącymi w Europie oraz wychwytywać różnice w implementacji wcześniejszej dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2]. Nikt nie miał wątpliwości, że kraje europejskie – tak często traktowane jako jedna całość – nie opierają się na homogenicznych podstawach kulturowych i prawnych. W tej sytuacji praca nad projektem nowego rozporządzenia była bardzo skomplikowana i poruszała tematy, które różne kultury istniejące w Europie inaczej adresują.

Uchwalony tekst RODO stał się wyznacznikiem tematów do dyskusji podejmowanych przy wszystkich pracach legislacyjnych, niezależnie od tego,

[1] Dz.Urz. UE L Nr 119, s. 1 ze zm.
[2] Dz.Urz. UE L Nr 281, s. 31 (nie obowiązuje).

w jakim systemie i na jakim poziomie – regionalnym, krajowym czy lokalnym – się one toczyły. Oczywiście nie wszędzie oznacza to, że dyskutuje się tylko te problemy, które znalazły się w tekście RODO, bądź tylko te, które były rozważane podczas jego tworzenia. Prawdą jest jednak, że we wszystkich pracach legislacyjnych możemy znaleźć bezpośrednio odniesienia do rozwiązań prawnych, które przyjęła UE[3].

Celem niniejszego rozdziału jest przedstawienie perspektyw globalnego, regionalnego i krajowego prawodawstwa w zakresie ochrony prywatności i ochrony danych osobowych na całym świecie oraz ocena, na ile RODO może wpływać na przyjęte w poszczególnych krajach bądź regionach rozwiązania, i czy może stać się zalążkiem do rozwiązania ogólnoświatowego.

2. Kontynuacja?

Przy wszystkich wątpliwościach, które mogło wywoływać RODO, nikt z komentatorów nie kwestionuje, że jest to kolejny etap rozwoju europejskiego podejścia do ochrony danych osobowych, mającego swe korzenie jeszcze w latach 70. i 80. XX w. Rozporządzenie RODO bazuje na wszystkich doświadczeniach zebranych przez państwa członkowskie UE w trakcie prawie 40 lat obowiązywania Konwencji Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonej w Strasburgu 28.1.1981 r.[4] oraz kilkunastu lat praktycznego wykorzystywania rozwiązań dyrektywy 95/46/WE oraz rozporządzenia (WE) 45/2001(WE) Parlamentu Europejskiego i Rady z 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[5].

Warto zwrócić uwagę, że RODO zawiera co najmniej kilka elementów, które są swoistym importem do prawa europejskiego rozwiązań powstałych na innych kontynentach. W tym znaczeniu jest ono aktem prawnym odwołującym się do globalnych doświadczeń z zakresu ochrony prywatności. Dwa najbardziej charakterystyczne przykłady takiego importu to:

1) zasada *privacy by design* (motyw 78 i art. 25 RODO), mająca swoje źródła w rozważaniach filozoficznych i prawnych, rozpoczętych ponad 10 lat

[3] *C. Kuner, K. Kittichaisare*, La creciente importancia del Derecho de la Protection de datos personales en el Derecho Internacional, Rev. RLPDP 2016, Nr 2–1, s. 17–26.

[4] Dz.U. z 2003 r. Nr 3, poz. 25.

[5] Dz.Urz. UE L Nr 8, s. 1 (nie obowiązuje). Rozporządzenie to zostało uchylone 10.12.2018 r. przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) Nr 45/2001 i decyzji Nr 1247/2002/WE z 21.11.2018 r., Dz.Urz. UE L Nr 295, s. 39.

temu przez rzecznika ochrony prywatności kanadyjskiej prowincji Ontario *A. Cavoukian*[6] oraz

2) nakaz przeprowadzania oceny wpływu różnego rodzaju przedsięwzięć na ochronę danych osobowych (motywy 76–77, 83–84, 89–95 oraz art. 35 RODO), która pod nazwą oceny wpływu na prywatność (ang. *Privacy Impact Assessment* – PIA), istniała w wielu krajach anglosaskich. Przeprowadzana była w amerykańskiej[7], australijskiej[8], kanadyjskiej[9] czy nowozelandzkiej[10] administracji publicznej i w zasadzie stamtąd, poprzez prawo angielskie i irlandzkie, pojawiła się na kontynencie europejskim[11].

3. Traktatowe i konstytucyjne podstawy prawa do ochrony danych osobowych

Prawo ochrony danych osobowych swe traktatowe podstawy znajduje w art. 16 TFUE oraz w Karcie Praw Podstawowych z 30.3.2010 r.[12]. Artykuł 16 TFUE, po zmianach wprowadzonych przez Traktat z Lizbony z 13.12.2007 r.[13], statuuje prawo do ochrony danych osobowych jako jedno

[6] Pojęcie *privacy by design* zostało wprowadzone do dyskursu o ochronie prywatności przez *A. Cavoukian* jako wynik wieloletnich prac nad wprzęgnięciem zasad ochrony prywatności do nowych projektów infrastrukturalnych realizowanych w Kanadzie. Nie zaproponowano jak dotąd powszechnie akceptowanego tłumaczenia tego pojęcia na język polski, stąd też w niniejszym tekście używane jest ono zamiennie z terminem „ochrona prywatności w fazie projektowania", gdyż takie tłumaczenie przyjęto w niektórych oficjalnych tłumaczeniach przygotowanych na potrzeby procesu legislacyjnego w UE. *Privacy by design* w ujęciu *A. Cavoukian* ma stanowić kompleksową odpowiedź na narastające, systemowe efekty zastosowania ICT i rozbudowanej infrastruktury teleinformatycznej. Określenie to zakłada zarówno filozoficzne, jak i praktyczne podejście do prywatności jako pewnej wartości, której ochrona powinna być częścią rozważań i praktycznych działań podejmowanych przy prowadzeniu wszelkich projektów w sferze publicznej i prywatnej. Zob. *W. Wiewiórowski*, Privacy by Design jako paradygmat ochrony prywatności, w: *G. Szpor, W. Wiewiórowski* (red.), Internet. Prawno-informatyczne problemy sieci, portali i e-usług, Warszawa 2012, s. 13–30.

[7] *K. Bamberger*, *D. Mulligan*, PIA requirements and privacy decision-making in US government agencies, w: *D. Wright*, *P. de Hert* (red.), Privacy Impact Assessment, Dordrecht 2012, s. 225–250; Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service, US CIO Council, Chief Aquisition Officers Council, Federal Cloud Computing Committee, Washington 2012.

[8] *R. Clarke*, PIAs in Australia. A work-in-progress report, w: *D. Wright, P. de Hert* (red.), Privacy Impact Assessment, Dordrecht 2012, s. 119–148.

[9] *R. Bayley*, *C. Bennett*, Privacy impact assessments in Canada, w: *D. Wright, P. de Hert* (red.), Privacy Impact Assessment, Dordrecht 2012, s. 161–185.

[10] *J. Edwards*, PIA in New Zealand, w: *D. Wright*, *P. de Hert* (red.), Privacy Impact Assessment, Dordrecht 2012, s. 187–204. Np. Ministry of Business, Innovation and Employment, Privacy Impact Assessment. Collection and Handling of Biometrics at the Ministry of Business, Innovation and Employment, Wellington 2012.

[11] *M. Oetzel*, *S. Spiekermann*, Privacy-by-Design Through Systematic Privacy Impact Assessment – A Design Science Approach, ECIS – Conference Proceedings, Barcelona 2012.

[12] Dz.Urz. UE C Nr 83, s. 389.

[13] Dz.U. z 2009 r. Nr 203, poz. 1569. Zob. *H. Hijmans*, The European Union as a Constitutional Guardian of Internet Privacy and Data Protection. The Story of Article 16 TFEU, Amsterdam 2016, s. 216–221. O formie Traktatu z Lizbony zob. *J. Barcz*, Traktat z Lizbony. Wybrane aspekty działań implementacyjnych, Warszawa 2012, s. 145–147.

z podstawowych praw[14] przysługujących każdej osobie fizycznej, nie wprowadzając przy tym żadnych ograniczeń podmiotowych[15]. Dużo większe praktyczne znaczenie ma jednak art. 16 ust. 2 TFUE, w którym – w bardzo rozbudowany sposób – przyznano Parlamentowi Europejskiemu i Radzie prawo do określenia, co wchodzi w zakres prawa podstawowego opisanego w ust. 1, a co legislator unijny chciałby pozostawić poza jego zakresem. Zgodnie z tym przepisem legislatorzy unijni, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych tak przez organy i instytucje unijne, jak i przez państwa członkowskie[16]. Przepis ten jest więc traktatową podstawą do tworzenia prawa wtórnego UE, rozwijającego przepisy art. 16 TFUE. Opierają się więc na nim tak RODO, jak i dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 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[17] oraz specjalne rozporządzenie dotyczące przetwarzania danych osobowych przez instytucje, agencje i inne ciała działające w strukturze samej UE, czyli rozporządzenie 2018/1725. Zarówno TFUE, tak jak Konwencja Nr 108 wymagają również, aby przestrzeganie zasad ochrony danych osobowych, a także zasad dotyczących swobodnego przepływu takich danych, podlegało kontroli niezależnych organów nadzorczych.

Jednocześnie w wielu krajach UE prawo ochrony prywatności i prawo ochrony danych osobowych znajdują swoje źródło również w przepisach konstytucji krajowych. Z taką sytuacją mamy również do czynienia w Polsce[18], gdzie art. 47 Konstytucji RP statuuje prawo do ochrony prywatności („każdy ma prawo do ochrony życia prywatnego rodzinnego czci i dobrego imienia oraz decydowania o swoim życiu osobistym"), a art. 51 Konstytucji RP określa podstawowe komponenty prawa do ochrony danych osobowych. Co prawda samo sformułowanie „dane osobowe" nie pojawia się w tych przepisach, jednak

[14] *M. Tzanou,* The Fundamental Right to Data Protection. Normative value in the context of counter terrorism surveillance, Oksford–Portland 2017, s. 38–44; *M. Sakowska-Baryła,* Prawo do ochrony danych osobowych, Wrocław 2015, s. 59–60.

[15] *M. Kawecki,* Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych, Warszawa 2017, s. 86–95.

[16] *H. Hijmans*, The European Union, s. 145–156 oraz 545–549.

[17] Dz.Urz. UE L Nr 119, s. 89.

[18] *M. Sakowska-Baryła*, Prawo do ochrony danych osobowych, s. 85–94; *M. Pisz,* Konstytucyjne i ustawowe uwarunkowania ochrony danych osobowych w polskim porządku prawnym, w: *A. Zwara, A. Mednis, M. Pisz* (red.), RODO. Przewodnik dla adwokatów i aplikantów adwokackich, Warszawa 2018, s. 2–10; *J. Rzucidło*, Prawo do prywatności i ochrona danych osobowych, w: *M. Jabłoński* (red.), Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym, Wrocław 2014, s. 153–177; *I. Lipowicz*, W obronie cyfrowej prywatności, w: *M. Kałużyńska-Jasak* (red.), 1998–2013. 15 lat ustawy o ochronie danych osobowych w Polsce, Warszawa 2013, s. 34–38.

nigdy nie było wątpliwości, że sformułowanie „informacje dotyczące osoby" jest konstytucyjnym odpowiednikiem sformułowania „dane osobowe", wynikającego z Konwencji Nr 108, dyrektywy 95/46/WE (oczywiście nieobowiązującej jeszcze w Polsce w momencie wejścia w życie Konstytucji RP), a później wprowadzonych do ustawy z 29.8.1997 r. o ochronie danych osobowych[19]. Artykuł 51 Konstytucji RP możemy traktować – biorąc pod uwagę uwarunkowania historyczne – za przejaw globalnego wpływu dyrektywy 95/46/WE, na tej samej zasadzie, jak dziś oceniamy konstytucyjne i ustawowe efekty RODO w odniesieniu do krajów, które chcą przystąpić do UE i wprost wdrażają rozwiązania prawne wynikające z prawa wtórnego UE (np. Albania, Czarnogóra, Mołdowa, Północna Macedonia czy Serbia).

4. Rozporządzenie RODO a prawo Rady Europy i Organizacji Współpracy Gospodarczej i Rozwoju

W polskiej literaturze przyjęło się traktować całość rozważań dotyczących Konwencji Nr 108 oraz OECD wytycznych OECD – rekomendacji Rady OECD z 23.9.1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami[20] jako historyczną podstawę dla później rozwiniętego prawa wtórnego UE. Nie jest to do końca prawidłowe podejście. Tworząc RODO europejski legislator musiał wprost odnieść się tak do dokumentów Rady Europy[21], jak i dokumentów OECD[22]. W przypadku Konwencji Nr 108 wynikało to z faktu, że akt ten – jako traktat międzynarodowy – stanowił pełnoprawną część prawa wewnętrznego wszystkich państw członkowskich UE. Jednocześnie w tym samym czasie, gdy powstawało RODO, akt ten podlegał daleko idącej rewizji. Po części wynikała ona z konieczności modernizacji w samej Konwencji Nr 108 ze względu na postęp w rozwoju gospodarki, technologii i rozwiązań prawnych, z którymi

[19] T.j. Dz.U. z 2016 r. poz. 922 ze zm. (nie obowiązuje).

[20] Zob. http://www.oecd.org/sti/ieconomy/15590241.pdf [dostęp z 6.4.2019 r.]. Zob. też *H. Hijmans*, The European Union, s. 68–73; *M. Sakowska-Baryła*, Prawo do ochrony danych osobowych, s. 52–58.

[21] Poza Konwencją Nr 108 mowa tu przede wszystkim zaleceniach Komitetu Ministrów:
1) Rec(2019)2 w sprawie ochrony danych dotyczących zdrowia z 27.3.2019 r.;
2) Rec(2010)13 w sprawie ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania z 23.11.2010 r.;
3) Rec(85)20 w sprawie ochrony danych osobowych wykorzystywanych do celów marketingu bezpośredniego z 25.10.1985 r.;
4) Rec(87)15 regulujące wykorzystywanie danych osobowych przez policję z 17.9.1987 r.;
5) Rec(95)4 dla państw członkowskich w sprawie ochrony danych osobowych w dziedzinie usług telekomunikacyjnych, ze szczególnym uwzględnieniem usług telefonicznych z 7.2.1995 r.;
6) Rec(89)2 w sprawie ochrony danych osobowych wykorzystywanych w związku z zatrudnieniem z 18.1.1989 r.;
7) Rec(97)5 w sprawie ochrony danych medycznych z 13.2.1997 r.

[22] Rolę wytycznych OECD – tak w wersji pierwotnej, jak po nowelizacji z 2001 r., omówiono w: Thirty Years After the OECD Privacy Guidelines, Paryż 2011, s. 6–89.

spotykają się państwa członkowskie Rady Europy, po części zaś z reakcji na samą reformę prawa unijnego. Ostatecznie ponad połowa państw Rady Europy jest jednocześnie państwami członkowskimi UE. Można więc powiedzieć, że w pewnym momencie trwał swoisty dialog pomiędzy reformami zachodzącymi w obu organizacjach międzynarodowych. Trudno jednak stwierdzić, by był to dialog równorzędnych partnerów. Mimo wszystkich prób zachowania pozorów państwa członkowskie UE były raczej zainteresowane dostosowaniem Konwencji Nr 108 do wymagań nowego prawa unijnego niż uwzględnieniem jakichkolwiek szczególnych koncepcji Rady Europy w RODO. Doprowadziło to w pewnym momencie prac w Komitecie Konsultacyjnym do spraw Konwencji o ochronie osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (tzw. Komitecie T-PD)[23] do poważnego konfliktu. Komisja Europejska próbowała bowiem narzucić państwom członkowskim swoje stanowisko negocjacyjne, eufemistycznie nazywając takie rozwiązanie „koordynacją działań państw członkowskich UE". Spotkało się to z niechętną reakcją samych państw członkowskich UE. Co najważniejsze jednak, zostało bardzo źle odebrane przez pozostałe państwa członkowskie Rady Europy, które uznały, że są *de facto* poddane dyktatowi Komisji Europejskiej.

Ostatecznie, przełamując różne inne opory polityczne, 128. sesja ministerialna Komitetu Ministrów Rady Europy, która odbyła się w Elsinore w Danii 18.5.2018 r., przyjęła protokół zmieniający Konwencję Nr 108 wraz z wyjaśniającym go raportem. Dnia 25.6.2018 r. w Strasburgu podczas 3. sesji Zgromadzenia Parlamentarnego ministrowie, przyjmując Protokół Nr 223[24], zawierający zmiany do Konwencji Nr 108, podkreślili wagę, jaką przywiązują do jak najszybszej ratyfikacji zmian przez jak największą liczbę państw-stron w celu wzmocnienia reżimu prawnego Konwencji Nr 108 oraz rozpoczęcia procesu dostosowania prawa krajowego do jej wymagań. W przypadku państw członkowskich Rady Europy, które nie należą do UE, można takie sformułowanie przyjmować za dobrą monetę. W przypadku krajów UE zaś, dokument został wyłożony do podpisu po rozpoczęciu pełnego stosowania RODO, w momencie gdy większość krajów członkowskich przyjęła już przepisy uzupełniające RODO o krajowe rozwiązania prawne. Nie mógł więc mieć on zbyt dużego wpływu na to, jak naprawdę wygląda prawo wewnętrzne tych państw. Stąd też w przypadku Konwencji Nr 108 należy wskazać na dostosowanie reżimu konwencyjnego do zmian w prawie unijnym, a tym samym do RODO[25]. Właściwie jedynie w przypadku Rosji, Szwajcarii, Gruzji i w mniejszym stopniu państw bałkańskich nienależących do UE, mieliśmy do czynienia z podkreśle-

[23] Członkiem Komitetu T-PD z ramienia Polski jest Prezes UODO.

[24] Sam protokół Nr 223 został wyłożony do podpisu państw członkowskich 10.10.2018 r. Tego samego dnia podpisały go 23 państwa-strony dotychczasowej Konwencji Nr 108.

[25] O roli Konwencji Nr 108 jako swego rodzaju uniwersalnego słownika prawa ochrony danych dla całego świata zob. *G. Greenleaf*, Data protection Convention 108 accession eligibility. 80 Parties now possible, Privacy Laws & Business International Report 2017, Nr 148, s. 12–16.

niem znaczenia Konwencji Nr 108 – niekiedy w opozycji do zmian w prawie unijnym (przede wszystkim w przypadku Rosji).

5. Perspektywy globalnego porozumienia w sprawie ochrony prywatności

G. Greenleaf słusznie zwraca uwagę, że po raz pierwszy w historii doszliśmy do punktu, w którym większość państw posiadających horyzontalne akty prawne dotyczące ochrony danych osobowych leży poza Europą. Tym samym bardziej widoczne jest, że rozwój prawa ochrony danych osobowych następuje nie tylko w Brukseli i Strasburgu, a globalny obraz podejścia do ochrony prywatności jest dziś z pewnością bardziej wielowątkowy niż kilka czy kilkanaście lat temu[26]. Jednocześnie nie ulega wątpliwości, że wszystkie nowo tworzone na świecie przepisy prawne dotyczące ochrony prywatności, ochrony danych osobowych, a nawet szerzej rozumianego bezpieczeństwa informacyjnego, muszą odnosić się wprost lub nie wprost do reformy dokonanej w ostatnich latach w UE. Każdy nowy akt prawny, który pojawia się na świecie, oraz duża część orzecznictwa sądów krajów nienależących do UE podawane są od razu konfrontacji z RODO. W kilka dni po stworzeniu projektu jakiegokolwiek aktu prawnego, uchwaleniu go czy wydaniu znaczącego orzeczenia przez sądy pojawiają się mniej lub bardziej oficjalne opracowania, porównujące zaproponowane lub przyjęte rozwiązania z RODO[27]. Z pewnością zaś jest dziś co porównywać.

W kwietniu 2019 r. w 134 państwach świata istniały akty prawne obejmujące całościowo zagadnienie ochrony danych osobowych. Prawdą jest, że nie wszędzie dotyczyło to jednocześnie sektora publicznego i prywatnego. Jednak owe 134 państwa należy uznać za środowisko, które odnosi się poprzez swe

[26] *G. Greenleaf*, 'European' data privacy standards implemented in laws outside Europe, Privacy Laws & Business International Report 2018, Nr 149, s. 21–23. Zob. również *C. Bennett, S. Oduro-Marfo*, Global Privacy Protection. Adequate Laws, Accountable Organizations and/or Data Localization? Conference: the 2018 ACM International Joint Conference and 2018 International Symposium, Singapur 8–12.10.2018 r., s. 881–890 oraz *L. Bygrave*, Legal Scholarship on Data Protection. Future Challenges and Directions, w: *C. de Terwangne, E. Degrave, S. Dusollier* (red.), Law, Norms and Freedoms in Cyberspace. Liber Amicorum Yves Poullet, Bruksela 2018, s. 499.

[27] Jako przykład zob.: *L. de la Torre*, GDPR matchup. The California Consumer Privacy Act 2018, IAPP z 31.7.2018 r., https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act [dostęp z 6.4.2019 r.]; *G. Somers*, *L. Boghaert*, The California Consumer Privacy Act and the GDPR. Two of a kind?, Financier Worldwide z 11.2018 r., https://www.financierworldwide.com/the-california-consumer-privacy-act-and-the-gdpr-two-of-a-kind/#.XF7IBrhCe00 [dostęp z 6.4.2019 r.]; *G. Zanfir-Fortuna, M. Bae*, CCPA, face to face with the GDPR. An in depth comparative analysis, Future of Privacy Forum z 28.11.2018 r., https://fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/ [dostęp z 6.4.2019 r.]; *S. Hospelhorn*, California Consumer Privacy Act (CCPA) vs. GDPR, Varonis z 5.11.2018 r., https://www.varonis.com/blog/ccpa-vs-gdpr [dostęp z 6.4.2019 r.]. *H. Miyashita*, Right to be Forgotten, from the Trans-Atlantic to Japan, w: *D. Svanteson, D. Kloza* (red.), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, Cambridge–Antwerpia–Portland 2017, s. 321–330.

działania prawne do RODO. Kolejne 30 państw świata ma rozwiązania dotyczące ochrony danych osobowych, które zawarte są w aktach niższego rzędu niż ustawy lub w aktach prawnych, które nie mają do końca wiążącego charakteru. Szczególnie burzliwy rozwój przeżywa prawo ochrony danych osobowych w Afryce i w Azji. O ile bowiem w przypadku Ameryki Południowej w wielu krajach mamy do czynienia z uchwaleniem aktów przygotowywanych już od lat bądź ze zmianą obowiązującego już wcześniej porządku prawnego, o tyle w Azji i w Afryce dochodzi do tworzenia rozwiązań nowych oraz wyboru ścieżek rozwoju prawa ochrony danych przez państwa dotychczas prawa takiego niemające. Ocena – nawet ilościowa – takich zmian ma więc duże znaczenie dla określenia, na ile RODO staje się standardem globalnym, bądź na ile ma wpływ na rozwiązania o charakterze regionalnym. Najpoważniejsze w ostatnich latach zmiany w zakresie ochrony prywatności i ochrony danych osobowych miały miejsce w Japonii, Brazylii, Indiach oraz w niektórych stanach Stanów Zjednoczonych. Przewiduje się również, że do grona państw posiadających przynajmniej formalne prawo ochrony danych osobowych dołączy wkrótce Chińska Republika Ludowa.

Formalna ocena krajowych systemów ochrony danych osobowych jest oczywiście znacznie łatwiejsza niż ocena rzeczywistej mocy wprowadzonych w poszczególnych państwach przepisów. Tradycyjnie bowiem na mapach krajów mających ustawy o ochronie danych osobowych[28] białymi plamami pozostają Stany Zjednoczone czy Chiny, a nawet Izrael, podczas gdy kraje takie jak Rosja trafiają do grupy krajów od lat mających prawo o ochronie danych osobowych. Kiedy próbujemy jednak ocenić „siłę" rozwiązań prawnych w poszczególnych państwach, ocena wygląda zupełnie inaczej[29]. Stany Zjednoczone, nie mając wspólnego i całościowego systemu ochrony danych osobowych, mają jednocześnie bardzo rygorystyczne przepisy w zakresie ochrony np. danych medycznych oraz danych finansowych. Mają również organy ochrony konsumentów, które wielokrotnie działają znacznie sprawniej niż organy nadzorcze w krajach UE[30]. Jednocześnie określenie Rosji jako kraju o silnym systemie ochrony prywatności byłoby zupełnym nieporozumieniem. Tak więc rygorystyczne systemy ochrony bezpieczeństwa, istniejące w Rosji czy w Chinach[31], nie mogą być same w sobie traktowane jako dowód na silną ochronę

[28] *D. Banisar*, National Comprehensive Data Protection/Privacy Laws and Bills 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 [dostęp z 25.1.2018 r.].

[29] Takiej oceny próbuje dokonywać kancelaria prawnicza DLA Piper, która w swym serwisie internetowym prezentuje interaktywną mapę regulacji na świecie – zob. https://www.dlapiperdataprotection.com/index.html?_lrsc=fffb07eb-8d06-4cef-8c90-584160de530b [dostęp z 13.1.2019 r.]. Zob. również *D. Spieler*, Data Protection Laws Interactive Map, http://dataprivacysite.com/2017/01/30/data-protection-laws-interactive-map/ [dostęp z 6.4.2019 r.].

[30] *H. Hijmans*, The European Union, s. 362–363.

[31] *Z. Weng*, Systematic Government Access to Private-Sector Data in China, w: *F. Cate, J. Dempsey* (red.), Bulk Collection. Systematic Government Access to Private-Sector Data, Oksford 2017, s. 241–258.

danych osobowych w tych państwach. Jednocześnie w innych państwach sam brak jednego aktu o ochronie danych osobowych nie może być uważany za dowód braku takiej ochrony.

Od 1970 r. corocznie co najmniej 2–3 kraje przyjmowały nowe rozwiązania prawne, umożliwiające dołączenie do listy krajów prawnie chroniących dane osobowe. W ostatniej dekadzie liczba krajów wprowadzających takie rozwiązania wzrosła do 5 w każdym roku. Wiele krajów wprowadziło bardzo silne metody ochrony danych osobowych, odwołując się do drugiej generacji zasad ochrony danych wynikającej z prawa unijnego i tworząc dobrze wyposażone prawnie i praktycznie organy nadzorcze. Do krajów takich w ostatnich latach należy zaliczyć Japonię[32], Koreę, Taiwan (mimo braku wyspecjalizowanego organu ochrony danych) oraz Hongkong, Nową Zelandię i Australię, gdzie klasyczna ochrona danych ma nieco dłuższą historię[33]. Wiele krajów podjęło również działania w celu dostosowania swojego reżimu prawnego do wymagań RODO. Do krajów takich należy zaliczyć Argentynę, Indie, Indonezję, Nową Zelandię, Tajlandię czy Tunezję. Można też wskazać na kraje, w których prawo ochrony konsumentów zaczyna pełnić rolę prawa ochrony prywatności (np. Chiny i Stany Zjednoczone – na poziomie stanowym Kalifornii, Północna Karolina czy Waszyngton).

Wspomniane wcześniej wytyczne OECD (rekomendacja Rady OECD w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami) oraz Konwencja Nr 108 stworzyły 9 głównych elementów definiujących prawo ochrony prywatności, dziś uważanych za zasady pierwszej generacji[34]. W 1995 r. prawo wspólnotowe uzupełniło o 10 kolejnych zasad (tzw. druga generacja zasad ochrony danych osobowych). Większość z tych zasad znajduje swoje odbicie we wszystkich 134 systemach prawnych wskazywanych przez doktrynę w 2018 r., w których istnieje ogólny standard ochrony danych osobowych wynikający z krajowej legislacji. W co najmniej połowie z tych państw standard ten jest zbliżony do tego, który wynika z prawa unijnego. Nie o taką jednak formalną zgodność chodzi, gdy próbujemy określić wpływ RODO na inne jurysdykcje na świecie. Zgodność zasad może być bowiem spowodowana nie tyle opieraniem się na rozwiązaniach europejskich przez twórców nowych aktów prawnych, lecz albo na wspólnym rozumieniu prywatności, albo wspólnej tradycji prawnej. Należy znacznie uważniej przyjrzeć się tym jurysdykcjom, w których zmiany po 2016 r. wprost dotyczyły rozwiązań nowych bądź znacząco unowocześnionych

[32] Problemy nadzoru nad przestrzeganiem ochrony danych osobowych w Japonii przed reformą z 2016 r. omawia *H. Miyashita*, A Tale of Two Privacies. Enforcing Privacy with Hard Power and Soft Power in Japan, w: *D. Wright, P. de Hert* (red.), Enforcing Privacy. Regulatory, Legal and Technological Approaches, Springer 2016, s. 105–122.

[33] *G. Greenleaf,* Asian Data Privacy Laws. Trade and Human Rights Perspectives, Oksford 2017, s. 9–13.

[34] *G. Greenleaf*, 'European' data privacy standards, s. 21–23.

w RODO. Do takich elementów, w których wpływ RODO jest w oczywisty sposób widoczny w nowych przepisach prawnych uchwalonych na świecie, zaliczyć możemy m.in.:

1) uprawnienie organów nadzorczych do wydawania wiążących decyzji i nakładania sankcji administracyjnych, włączając w to kary finansowe;
2) prawo do sprzeciwu wobec przetwarzania danych przez administratora[35];
3) prawo do sprzeciwu w sytuacji, gdy uzasadniony interes administratora wykorzystywany jest jako podstawa przetwarzania, czy
4) wprowadzenie systemu zawiadamiania organu nadzorczego – lub same osoby – o incydentach, naruszających ochronę danych osobowych[36].

System europejski wynikający z RODO, i podobne systemy w rozporządzeniu Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (EIDAS)[37] i dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS)[38], mają jednak cechy charakterystyczne, które dadzą rozpoznać się w poszczególnych nowych aktach prawnych o ochronie danych osobowych. Zwiększone wymagania wobec zgody, włączenie danych biometrycznych i danych genetycznych lub danych o genomie do listy danych wrażliwych (niezależnie od tego, czy pojęcie „dane wrażliwe" lub „dane szczególnie chronione" jest w danym akcie używane), obowiązek powoływania inspektora ochrony danych przez podmiot, który wykonuje pewne rodzaje operacji przetwarzania danych.

6. Współpraca międzynarodowa w dziedzinie ochrony prywatności

Chociaż tematyka związana z ochroną prywatności była wielokrotnie przywoływana podczas dyskusji ONZ[39], a organizacja ta powołała specjalnego sprawozdawcę do spraw ochrony prywatności, którym został mianowany *J. Cannataci*, nie możemy dzisiaj wskazać na jakikolwiek podmiot, w którym rządy państw całego świata prowadzą globalną dyskusję nad ochroną prywatności bądź ochroną danych osobowych. Co pewien czas liderzy polityczni

[35] *M. Krzysztofek,* Prawo sprzeciwu wobec przetwarzania danych osobowych w RODO, w: *B. Fischer*, *M. Sakowska-Baryła* (red.), Realizacja praw osób, których dane dotyczą, na podstawie RODO, Wrocław 2017, s. 289–306.

[36] W tym przypadku oceniać należy jednak szczegóły rozwiązań przyjmowanych w poszczególnych krajach. Trzeba bowiem pamiętać że Stany Zjednoczone mają w tym zakresie znacznie dłuższe i znacznie bogatsze doświadczenia niż Europa, mając osobne systemy *data breech notification* w 51 stanach i terytoriach.

[37] Dz.Urz. UE L Nr 257, s. 73.

[38] Dz.Urz. UE L Nr 195, s. 1.

[39] How to Talk About the Right to Privacy at the UN. A Brief Guide, Privacy International 2017, s. 4–13.

wzywają do podjęcia takiej dyskusji[40], nie widać jednak perspektyw do jej faktycznego prowadzenia[41]. Na przełomie 2018 i 2019 r. coraz częściej do stworzenia takiego standardu zaczynają też nawoływać przedstawiciele wielkich graczy biznesowych[42], choć w przypadku ich działań często trudno ocenić, na ile kieruje nimi przekonanie o potrzebie ogólnoświatowej ochrony prywatności, a na ile ograniczenie „inwencji twórczej" poszczególnych państw na rzecz kompromisowych rozwiązań implementowanych w ten sam sposób na wszystkich rynkach, na których ci gracze są obecni.

Główna rola w przepływie informacji o zmianach prawnych w poszczególnych jurysdykcjach spada na organy nadzorcze oraz – paradoksalnie – na samych administratorów danych. Organy nadzorcze współpracują w ramach co najmniej kilku globalnych, i całej serii regionalnych, forów współpracy, które niekiedy mają charakter bardziej zorganizowany, a nawet przyznają sobie prawo do wydawania rekomendacji wobec państw członkowskich. Niekiedy zaś są jedynie areną wymiany praktycznych informacji o problemach związanych z poszczególnymi technologiami przetwarzania danych bądź modelami biznesowymi wykorzystywanymi przez administratorów bądź prawnymi narzędziami używanymi przez te organy[43].

Najważniejszym forum wymiany doświadczeń pomiędzy organami nadzorczymi na poziomie ogólnoświatowym jest doroczna Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności (ang. *International Conference of Data Protection and Privacy Commissioners* – ICDPPC) dwukrotnie zorganizowana w Polsce w 2013 r. w Warszawie, a w 2004 r. – we

[40] *H. Hijmans*, The European Union, s. 489–492 oraz 522–524; *P. de Hert, V. Papakonstantinou,* Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialised United Nations Agency. Addressing the Deficit in Global Cooperation for the Protection of Data Privacy, w: *D. Svanteson, D. Kloza* (red.), Trans-Atlantic Data Privacy Relations, s. 521–532.

[41] Odmienne zdanie wyraża wciąż *G. Greenleaf,* wzywając do uznania za taki standard Konwencji Nr 108 – zob. *G. Greenleaf,* The UN Should Adopt Data Protection Convention 108 as a Global Treaty. Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council and to the Special Rapporteur on the Right to Privacy, UNSW Law Research Paper z 8.4.2018 r. Zob. również *C. Bennet*, The European General Data Protection Regulation. An instrument for the globalization of privacy standards?, Information Polity 2018, Nr 23, https://content.iospress.com/articles/information-polity/ip180002, s. 239–246 [dostęp z 6.4.2019 r.].

[42] Za przykłady niech służą wypowiedzi *T. Cooka* podczas 40. Międzynarodowej Konferencji Rzeczników Prywatności i Ochrony Danych w Brukseli w październiku 2018 r. – zob: *S. Salinas, S. Meredith*, Tim Cook: Personal data collection is being ‚weaponized against us with military efficiency' (relacja prasowa z załączonym pełnym tekstem wystąpienia *T. Cooka*), CNBC 25.10.2018, https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html [dostęp z 6.4.2019 r.] – oraz artykuł *M. Zuckerberga* opublikowany w Washington Post – *M. Zuckerberg,* The Internet needs new rules. Let's start in these four areas, Washington Post, 30.3.2019 r., https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.aaa809dcbd8a [dostęp z 6.4.2019 r.].

[43] *D. Barnard-Wills, D. Wright*, Co-ordination and co-operation between Data Protection Authorities. PHAEDRA Improving Practical and Helpful co-operation between Data Protection Authorities Workstream 1 report, Bruksela 2014, s. 77–130.

Wrocławiu. Mimo nazwy „międzynarodowa konferencja" i corocznego charakteru, mamy do czynienia z forum, które z wolna przekształca się w organizację międzynarodową i posiada permanentnie działający komitet wykonawczy. Drugim bardzo istotnym forum wymiany informacji jest Światowa Sieć Egzekwowania Przepisów o Ochronie Prywatności (ang. *Global Privacy Enforcement Network* – GPEN), zrzeszająca te organy nadzorcze, które mają prawo wydawania wiążących decyzji wobec administratorów i chcą współpracować praktycznie przy podejmowaniu decyzji w sprawach o charakterze ponadkrajowym. Najważniejszym forum współpracy technicznej organów nadzorczych z zakresu prywatności jest Międzynarodowa Grupa Robocza ds. Ochrony Danych w Telekomuniacji (ang. *International Working Group on Data Protection in Telecommunications*) zwana potocznie Grupą Berlińską. Swoje znaczenie ma również Komisja ds. Informacji Komputerowej i Prywatności Organizacji Współpracy Gospodarczej i Rozwoju (ang. *Organisation for Economic Co-operation and Development* – OECD. Z organizacji regionalnych istotną praktyczną rolę odgrywa tzw. grupa frankofońska (franc. *Association francophone des autorités de protection des données personnelles* – AFAPDP), ibero-latynoamerykańska (hiszp. *Red Iberoamericana de Protection de Datos* – RIPD), azjatycko-pacyficzna (ang. *Asia Pacific Privacy Authorities* – APPA Forum), grupa działająca w ramach Wspólnoty Gospodarczej Azji i Pacyfiku (ang. *Asia-Pacific Economic Co-operation* – APEC) oraz w mniejszym stopniu grupa organów nadzorczych z Europy Środkowej i Wschodniej (ang. *Central and Eastern European Data Protection Authorities* – CEEDPA) oraz grupa nordycka[44]. W Europie harmonizowaniem rozwiązań prawnych pomiędzy poszczególnymi systemami oraz uwspólnianiem wykładni prawa zajmują się Konferencja Wiosenna Rzeczników Ochrony Danych oraz Komitet T-PD. Tak Międzynarodowa Konferencja, jak Komitet T-PD odgrywają pośrednio bardzo istotną rolę w dyskusji na tematy wynikające wprost z RODO oraz w omawianiu wpływu RODO na działalność podejmowaną w innych jurysdykcjach.

Główną koordynatorką działań rzeczników ochrony danych w UE jest jednak oczywiście EROD, będąca bezpośrednią następczynią Grupy Roboczej Art. 29 do spraw Ochrony Danych. Podmiot ten jest ciałem unijnym, składającym się z przedstawicieli 28 państw członkowskich oraz z EIOD, sprawującego nadzór nad przetwarzaniem danych w instytucjach i agencjach unijnych[45]. Stanowi wewnętrzne ciało doradcze wobec innych instytucji i organów UE. Jednocześnie Radzie przyznano jednak prawo do uzupełniającej interpretacji RODO. Bardzo istotną rolę odgrywa EROD przy wydawaniu decyzji o ade-

[44] Szczegółowy opis działań wszystkich wymienionych forów zob. *ibidem*, s. 105–132.

[45] *M. Kawecki,* Reforma, s. 165–171; *J. Goerick,* Współpraca międzynarodowa organów ochrony danych osobowych państw członkowskich Unii Europejskiej przed i po wejściu w życie ogólnego rozporządzenia o ochronie danych, Disputatio 2017, t. XXIV, s. 19–28.

kwatności rozwiązań prawnych w państwach trzecich[46] wobec prawa unijnego. W tej sytuacji praktyczny wpływ RODO na prawodawstwo państw trzecich jest w dużym stopniu determinowany przez działania Rady.

7. Bliskie sąsiedztwo

7.1. Europejski Obszar Gospodarczy

W czasie gdy państwa należące do UE przygotowały akty prawne uzupełniające RODO oraz akty wdrażające dyrektywę 2016/680 pozostałe państwa Europy przyglądały się z zainteresowaniem tym pracę legislacyjnym, czekając jednocześnie na zakończenie prac nad nowelizacją Konwencji Nr 108. Kraje należące do EFTA musiały po wejściu w życie RODO formalnie odnieść się do jego obowiązywania na swoim terytorium. Przypomnijmy, że trzy z krajów EFTA – Norwegia, Islandia i Lichtenstein – tworzą jednocześnie EOG i na ich terenie po podjęciu odpowiedniej decyzji w ramach EFTA prawo unijne obowiązuje wprost[47]. Czwarty z krajów należących do EFTA – Szwajcaria, która nie ratyfikowała Traktatu z Porto z 2.5.1992 r.[48] – pozostaje poza EOG i prawo europejskie obowiązuje tam tylko na tyle, na ile zostanie to osobno implementowane do szwajcarskiego systemu przez tamtejszego prawodawcę.

W tej sytuacji Islandia, Norwegia i Liechtenstein traktowane są praktycznie równorzędnie z państwami członkowskimi UE. Szwajcaria zaś trafia do grupy tzw. państw trzecich. Po wejściu w życie decyzji EFTA, uznającej RODO za część porządku prawnego EOG (decyzja została podjęta i weszła w życie po upływie terminu na ewentualne referendum w Liechtensteinie), możemy wprost powiedzieć, że RODO obowiązuje w całości na obszarze trzech państw EOG. Organy nadzorcze z tych trzech państw biorą udział w pracach EROD praktycznie z tymi samymi uprawnieniami, co inne organy nadzorcze z państw unijnych, nie mając jednak prawa do głosu. Mogą natomiast – z czego zawsze korzystają – podać do protokołu, jakie jest ich zdanie w głosowanej kwestii (zob. motyw 7 oraz art. 4 ust. 1 i art. 21 Regulaminu EROD z 23.11.2018 r.[49]).

Należy pamiętać, że transgraniczny przepływ danych do państw członkowskich EOG w celach wychodzących poza zakres rynku wewnętrznego, np. w celu prowadzenia dochodzeń karnych, nie podlega przepisom ogólnym o ochronie danych wynikającym z dyrektywy 2016/680 lub z RODO. Nie

[46] O pojęciu państwa trzeciego zob. *D. Karwala*, Komercyjne transfery danych osobowych do państw trzecich, Warszawa 2018, s. 54–57.
[47] *Ibidem*, s. 109–111.
[48] Porozumienie o Europejskim Obszarze Gospodarczym (Dz.Urz. WE z 1994 r. L 1, s. 3–522, polskie wydanie specjalne: Roz. 11, t. 52, s. 3–366).
[49] Regulamin dostępny jest na stronie EROD https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop2_adopted_23112018_en.pdf.pdf [dostęp z 6.4.2019 r.].

jest zatem objęty zasadą swobodnego przepływu danych. Wszystkie natomiast państwa członkowskie EOG są jednocześnie sygnatariuszami Konwencji Nr 108 i część rozwiązań dotyczących przepływu danych może być oparta na przepisach tej konwencji.

7.2. Bałkany Zachodnie

Grupa krajów Bałkanów Zachodnich kandydujących do członkostwa w UE podjęła działania dążące do stosowania własnego prawa krajowego do rozwiązań RODO. Kraje te – Albania, Czarnogóra, Macedonia Północna i Serbia – uczestniczą w pracach EROD jako obserwatorzy. Chociaż wciąż wobec żadnego z tych krajów nie wydano decyzji dotyczącej adekwatności jego systemu prawnego do wymagań RODO, możemy w uproszczeniu traktować kraje te jako stosujące system ochrony danych zbliżony do systemu wynikającego z RODO. Wszelkie odmienności, które zostałyby poddane ocenie, gdyby kraje wystąpiły z wnioskiem o wydanie decyzji o adekwatności, należy traktować jako wyjątki, niekiedy wynikające ze szczególnej sytuacji geopolitycznej. Kraje te możemy ogólnie określić jako wprost podlegające merytorycznemu wpływowi RODO, gdyż wykładnia RODO przyjmowana przez TSUE lub przez EROD niejako automatycznie staje się częścią porządku prawnego państw, które mają zamiar stosować w przyszłości całe *acquis communautaire*[50].

W praktyce bardzo podobnie wygląda pozycja prawna RODO i znaczenie jego wykładni w Bośni i Hercegowinie oraz w Kosowie. Państwa te mają inny status, jeśli chodzi o stosunki ogólne z UE niż wcześniej wymienione kraje Bałkanów Zachodnich. Mają również szczególną sytuację narodowościową, a w przypadku Bośni i Hercegowiny – federalny charakter. Wdrożenie w praktyce zasad RODO jest tam znacznie trudniejsze. Dodatkowo Kosowo nie może liczyć na wsparcie we współpracy z EROD ze strony co najmniej jednego ważnego członka Rady, tj. Hiszpanii, która niepodległości Kosowa nigdy nie uznała. Choć oba państwa nie mają w najbliższych latach szans na dogonienie swych sąsiadów w rozwoju instytucjonalnej współpracy w zakresie ochrony danych osobowych, to należy spodziewać się, że rozwój prawodawstwa w tej dziedzinie i jego upodabnianie się do RODO będzie postępował w sposób zbliżony – być może z niewielkimi opóźnieniami – do krajów zachodniobałkańskich.

[50] Tempo adaptacji do rozwiązań proponowanych w RODO może być jednak bardzo różne. Serbski parlament już we wrześniu 2018 r. przyjął nową ustawę o ochronie danych osobowych, która – zdaniem jej twórców – adoptowała już większość nowości, które niesie RODO, będąc w wielu miejscach kopią jego przepisów. W Albanii w kwietniu 2018 r. parlament w rezolucji wezwał do dokonania szybkich zmian w prawie krajowym dostosowującym albańskie przepisy do standardu RODO. Mimo tej deklaracji, postęp prac przez kolejny rok należy uznać za mizerny. Natomiast w Północnej Macedonii, mimo że prace nad nowym prawem rozpoczęto już w 2017 r., a w styczniu 2018 r. po raz pierwszy z jej wynikami zapoznano przedstawicieli UE, to w momencie pisania tego opracowania prace wciąż trwają i istnieje jedynie nadzieja, że zakończą się pozytywnym efektem w 2019 r.