Uniwersytet Wrocławski

Magdalena Abu Gholeh

Dominika Kuźnicka-Błaszkowska

Ochrona danych osobowych w wybranych państwach Azji

Wrocław 2019

Ochrona danych osobowych w wybranych państwach Azji

Prace Naukowe
Wydziału Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego

Seria: **e-Monografie** Nr 155

Dostęp online: https://www.bibliotekacyfrowa.pl/publication/112255
DOI: 10.34616/23.19.155

Ochrona danych osobowych w wybranych państwach Azji

Magdalena Abu Gholeh
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
Katedra Prawa Konstytucyjnego
ORCID 0000-0003-0354-7581

Dominika Kuźnicka-Błaszkowska
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
Katedra Prawa Konstytucyjnego
ORCID: 0000-0001-8804-569X

Wrocław 2019

Recenzent: *dr hab. Paweł Kuczma, prof. Uniwersytetu Zielonogórskiego*

Korekta: *Anna Noga-Grochola*
Projekt i wykonanie okładki: *Karolina Drozd*
Skład i opracowanie techniczne: *Aleksandra Kumaszka, eBooki.com.pl*

Druk: *Drukarnia Beta-druk, www.betadruk.pl*

Wydawca
E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa.
Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

ISBN 978-83-66066-87-8 (druk)
ISBN 978-83-66066-88-5 (online)

Spis treści

Słowem wstępu

Ogólne rozporządzenie o ochronie danych osobowych[1] stanowi kolejny krok na gruncie ewolucji systemu ochrony prywatności i danych osobowych w Unii Europejskiej. Wywołało ono słuszny zamęt we wszystkich państwach członkowskich oraz w tych, które chcą oferować swoje usługi podmiotom fizycznym i prawnym z nich pochodzącym. Sposób, w jaki przedsiębiorcy na całym świecie zareagowali na wprowadzenie nowej regulacji, próbując dostosować swoją działalność do jej wymogów, pokazuje, jak ważnym rynkiem zbytu i partnerem gospodarczym jest Unia Europejska.

W niniejszym opracowaniu zdecydowałyśmy się na zbadanie, w jaki sposób ochrona danych osobowych jest regulowana w państwach, które zarówno geograficznie, jak i kulturowo położone są zdecydowanie poza obszarem wpływów europejskich. Celem publikacji było spojrzenie na regulacje związane z ochroną danych w krajach azjatyckich właśnie z perspektywy europejskiego prawnika. Wynika to nie tylko z ilości usług oferowanych przez przedsiębiorców pochodzących z Azji na rynku europejskim, ale także z tego – jak się nam wydaje – że porządek przyjęty obecnie w Unii Europejskiej w sposób najszerszy gwarantuje ochronę interesów jednostki.

[1] 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). Dalej jako: RODO.

Zarówno system prawny, w jakim funkcjonujemy, jak i edukacja prawna przez nas odebrana (oparta wszak na polskim i europejskim porządku prawnym) sprawiają, że pewną impertynencją byłaby próba spojrzenia na porządek prawny obowiązujący w państwach Azji z perspektywy prawnika innego niż europejski. Dodatkowo, niniejsza monografia ma na celu nie tylko przybliżenie polskiej nauce prawa tej tematyki, ale również ma stanowić wskazówkę dla przedsiębiorców, którzy prowadzą relacje gospodarcze z państwami azjatyckimi. Ze wskazanych powyżej powodów zdecydowałyśmy się przyjąć rozwiązania unijne za wyznacznik oceny regulacji przyjętych w omawianych państwach Azji.

Ramy niniejszej monografii nie pozwoliły na przeanalizowanie i opisanie wszystkich państw regionu i konieczne było ograniczenie rozważań do tych, które bądź intensywnie współpracują gospodarczo z Unią Europejską, bądź których system prawny jest na tyle odmienny od unijnego, że nieuwzględnienie go w takim opracowaniu byłoby niewybaczalnym błędem. Ostatecznie zdecydowałyśmy się przedstawić polskiemu czytelnikowi stan regulacji w następujących krajach (w kolejności alfabetycznej): Bahrajn (z uwagi na szczególną nową i zaskakująco surową regulację), Chiny (trudno bowiem pominąć najbardziej zaludnione państwo świata, które dodatkowo charakteryzuje się tak odmiennym od europejskiego systemem ochrony danych osobowych), Indie (jako przykład najbardziej liczebnej demokracji oraz ze względu na zakres i ilość usług outsourcingowych oferowanych państwom członkowskim UE oraz poczynione próby stworzenia własnego modelu ochrony danych osobowych), Japonia (jako przykład pierwszego państwa azjatyckiego, co do którego wydano decyzję o adekwatności ochrony), Malezja (ze względu na wprowadzenie rozwiązań prawnych nieco odmiennych od tych znanych z porządku europejskiego), Międzynarodowe Centrum Finansowe Dubaju (jako przykład obszaru, dla którego ochrona danych osobowych tak mocno wiąże się z gospodarką, iż przyjęto nietypowe rozwiązania w kontekście krajowego systemu prawnego), Rosja (z uwagi na bliskie położenie geograficzne,

a jednocześnie tak inne rozumienie pojęć prawa do prywatności i ochrony danych osobowych) i Singapur (gdyż trudno pominąć jego rolę we współpracy gospodarczej z podmiotami unijnymi).

Przedstawiane w opracowaniu porządki prawne często nie mogą poszczycić się długą tradycją ochrony prywatności (Bahrajn, Chiny) bądź ich historycznie wykształcone podejście w znaczny sposób odbiega od tego, który powstał na starym kontynencie (Japonia). Badania uatrakcyjnia również fakt, że chociaż w krajach Azji dominuje model ochrony danych osobowych gwarantujących przede wszystkim ochronę praw jednostki (Japonia, Malezja, Bahrajn), to w niektórych przypadkach głównym beneficjentem przepisów w tym zakresie jest państwo i administracja publiczna (Chiny, Rosja), a niektóre kraje starają się wypracować własny, odmienny system ochrony (Indie, Międzynarodowe Centrum Finansowe Dubaju).

Warto zauważyć, że niemal wszystkie kraje, które w ostatnich latach znowelizowały przepisy dotyczące ochrony danych osobowych (lub wciąż pracują nad ich kształtem), zrobiły to albo z chęci ułatwienia współpracy gospodarczej między podmiotami krajowymi i pochodzącymi z Unii Europejskiej, albo z powodu zwiększającego się obecnie zagrożenia cyberprzestępczością. Odnotować należy, że państwa z pierwszej grupy wprowadziły regulacje podobne lub w praktyce tożsame z prawem unijnym (Singapur, Międzynarodowe Centrum Finansowe Dubaju, Japonia), a te, które znowelizowały przepisy w celu ochrony przed cyberprzestępczością, często stworzyły przepisy sprzeczne z porządkiem przyjętym w Unii Europejskiej (Rosja, Chiny). Znamienne jest, że żadne z państw nie zdecydowało się znowelizować przepisów wyłącznie z powodu chęci zwiększenia ochrony prywatności jednostki.

Chociaż zbadanie, w jaki sposób kształtuje się ochrona danych osobowych w poszczególnych krajach regionu, było zdecydowanie zadaniem trudnym, aczkolwiek niezwykle ciekawym, zdajemy sobie sprawę, że tym, czego poszukuje polski czytelnik w tego typu opracowaniach, są

zagadnienia praktyczne. Z tego powodu każdy rozdział zawiera część poświęconą efektywności stanowionego prawa oraz aktualnemu stanowi stopnia ochrony. Pokusiłyśmy się również o ocenę, czy przyjęte regulacje i dotychczasowa praktyka uzasadniają uznanie tych państw za zapewniające odpowiedni stopień ochrony, a co za tym idzie – gwarantują ochronę prywatności i danych osobowych jednostki oraz umożliwiają swobodny przepływ danych między Unią Europejską a badanym państwem.

Oceniając, czy stopień ochrony w państwie trzecim jest odpowiedni i czy możliwe jest uznanie takiego państwa za zapewniające odpowiedni stopień ochrony w rozumieniu RODO, Komisja Europejska zobowiązana jest uwzględnić następujące elementy: praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe, 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 oraz 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. W naszych rozważaniach dowodzimy, że pomimo przyjęcia w ostatnich dwóch latach kompleksowych regulacji w zakresie ochrony danych osobowych, wiele z badanych przez nas państw ma trudności z uzyskaniem decyzji o adekwatności ochrony. Związane jest to przede wszystkim z brakiem odpowiednich gwarancji w zakresie poszanowania praw człowieka i podstawowych wolności lub niewłaściwego egzekwowania obowiązujących przepisów.

Wyrażamy nieśmiałą nadzieję, że niniejsze opracowanie stanowić będzie istotny element debaty na temat ochrony danych osobowych, jaka podejmowana jest przez praktyków i teoretyków prawa, i pozwoli w szerszy sposób spojrzeć na regulacje Unii Europejskiej w tym zakresie.

Dodatkowo, liczymy na to, że poczynione przez nas badania w zakresie regulacji obowiązujących w państwach azjatyckich przyczynią się do prowadzenia dalszych rozważań w zakresie funkcjonujących systemów prawnych w Azji, wciąż stosunkowo mało obecnych w polskiej teorii prawa.

Na koniec tego wstępu chciałybyśmy podziękować Promotorowi naszych rozpraw doktorskich, prof. dr. hab. Mariuszowi Jabłońskiemu, który nie tylko umożliwił opublikowanie niniejszej monografii, ale również służył radą i pomocą w czasie jej powstawania, zachęcając nas do przekraczania kolejnych barier i pokonywania trudności związanych z pracą badawczą.

Życzymy inspirującej lektury.
Magdalena Abu Gholeh
Dominika Kuźnicka-Błaszkowska

1. Regulacje Unii Europejskiej jako przyjęty model ochrony

1.1. Ogólne założenia ochrony danych osobowych w RODO

Model ochrony danych osobowych obowiązujący w państwach Unii Europejskiej od lat stanowi punkt odniesienia dla pozostałych porządków prawnych. Gwarancje stworzone przez prawodawcę unijnego uznawane były za swoisty złoty standard jeszcze na długo przed wejściem w życie ogólnego rozporządzenia o ochronie danych osobowych. Nie ulega wszakże wątpliwości, iż to dyrektywa 95/46/EC[2] stanowiła podwalinę obecnego systemu ochrony. Dynamiczny rozwój technologii zmusił jednak prawodawcę do nowelizacji przepisów, co jednocześnie stało się okazją do zrewidowania poziomu regulacji. RODO, w przeciwieństwie do uprzedniej dyrektywy, obowiązuje bezpośrednio we wszystkich państwach członkowskich. Rozporządzenie ujednoliciło prawo ochrony danych osobowych, pozostawiając jednak krajowym ustawodawcom swobodę uregulowania niektórych kwestii. Wydaje się jednak, iż ramy stworzone przez art. 23 RODO nie pozwalają państwom członkowskim na nadmierną ingerencję w unijny model ochrony. Tym samym należy stwierdzić,

[2] 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.Urz. WE L 281 z 23.11.1995, s. 31–50. Dalej jako: Dyrektywa 95/46/WE.

iż ogólne rozporządzenie o ochronie danych osobowych stanowi główne źródło unijnego systemu ochrony danych osobowych.

Zakres zastosowania rozporządzenia został określony w sposób szeroki. Stosuje się je zarówno do zautomatyzowanych, jak i niezautomatyzowanych operacji przetwarzania danych osobowych. Prawodawca zastrzega jednak, iż ochrona obejmuje wyłącznie dane stanowiące część zbioru danych lub mające stanowić ją w przyszłości. Wykładnia językowa art. 2 nakazuje jednak przyjąć, iż dane osobowe podlegać będą ochronie niezależnie od tego, czy ostatecznie trafią do wspomnianego zbioru[3].

RODO przewiduje również katalog wyłączeń, co do których rozporządzenie nie znajdzie zastosowania. Ze względu na fakt, iż RODO stanowi część prawa unijnego konieczne było właściwe odwołanie do granic kompetencji Unii Europejskiej. Co do zasady UE uprawniona jest wyłącznie do podejmowania działań w granicach kompetencji przyznanych jej przez państwa. Tym samym zrozumiały jest zakaz stosowania rozporządzenia do działalności nieobjętych prawem unijnym[4]. RODO nie znajdzie również zastosowania do operacji przetwarzania podejmowanych przez państwa członkowskie w ramach czynności związanych ze wspólną polityką zagraniczną i bezpieczeństwa. Kolejne wyłączenie poczyniono na rzecz organów prowadzących działalność zmierzającą do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych czy też wykrywania, ścigania czynów zabronionych lub wykonywania kar. Jest ono o tyle uzasadnione, iż ochrona podmiotów danych w związku z przetwarzaniem podejmowanym przez ww. organy regulowana jest przez tzw. dyrektywę policyjną[5]. Zakresem zastosowania RODO nie objęto również

[3] P. Litwiński, P. Barta, M. Kawecki, *Art. 2*, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 141.

[4] Art. 5 Traktatu o Unii Europejskiej, Dz.Urz. UE C 115 z 9.05.2008, s. 13.

[5] 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

przetwarzania podejmowanego przez osoby fizyczne w ramach czynności o charakterze czysto osobistym lub domowym. Praktyka pokazuje jednak, iż interpretacja tego przepisu nie jest zadaniem prostym. Istotne wątpliwości pojawiały się chociażby przy próbie zaklasyfikowania użytkowania portali społecznościowych czy domowego monitoringu wizyjnego[6]. Motyw 18 preambuły posługuje się wyłącznie kilkoma przykładami czynności wyłączonych spod zakresu RODO. Mogą one jednak stanowić cenną wskazówkę przy ocenie konkretnych sytuacji.

Omawiając zagadnienie zakresu zastosowania ogólnego rozporządzenia, nie można pominąć kwestii jego zasięgu terytorialnego. Co do zasady RODO stosuje się do czynności przetwarzania danych podejmowanych przez jednostki organizacyjne prowadzące działalność w Unii Europejskiej[7]. Bez znaczenia pozostaje jednak miejsce samej operacji przetwarzania, gdyż rozporządzenie będzie stosowane również do czynności podejmowanych poza granicami UE. Terytorialny zakres zastosowania RODO zostaje jednak dodatkowo poszerzony przez tzw. koncepcję nakierowania. Zgodnie z nią w określonych sytuacjach przepisy rozporządzenia mogą wiązać także podmioty nieposiadające jednostki organizacyjnej w Unii Europejskiej. Dzieje się tak, gdy do przetwarzania danych osób przebywających w UE dochodzi w związku z oferowaniem im towarów i usług lub monitorowaniem ich zachowania. Należy jednak pamiętać, iż przy ocenie, czy w danym przypadku doszło do nakierowania działalności niewystarczająca jest np. dostępność towarów za pośrednictwem ogólnodostępnej strony internetowej. Motyw 23 doprecyzowuje, iż

przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. UE L 119 z 4.5.2016, s. 60. Dalej jako dyrektywa policyjna lub dyrektywa 2016/680.

[6] P. Litwiński, P. Barta, M. Kawecki, *Art. 2*, [w:] P. Litwiński (red.), *op. cit.,* s. 148–149

[7] Szerzej na temat pojęcia „działalności" oraz „jednostki organizacyjnej": M. Czerniawski, *Artykuł 3*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 148–152.

przy ocenie należy uwzględnić m.in. język komunikacji (stosowany przez sprzedawcę lub usługodawcę), dostępność zamówienia towarów do danego państwa czy możliwość płatności w walucie powszechnie stosowanej w państwie członkowskim.

Praktyczne aspekty terytorialnego zakresu zastosowania RODO są jednak kwestią niezwykle złożoną, co doskonale obrazuje niedawne orzeczenie Trybunału Sprawiedliwości w sprawie *Google LLC przeciwko CNIL*[8]. Przedmiotem sporu stała się realizacja prawa do bycia zapomnianym przez usunięcie wyników wyszukiwania dotyczących podmiotu danych z popularnej wyszukiwarki internetowej. Na gruncie art. 3 pojawiło się jednak pytanie – z których wersji językowych przeglądarki należy usunąć sporne linki. Mimo iż stopień globalizacji usług internetowych (w szczególności tych oferowanych przez przedsiębiorstwa, takie jak Google) mógłby uzasadniać rozszerzenie kompetencji unijnego prawodawcy, to należy pamiętać, iż prawo do ochrony danych osobowych nie jest prawem bezwzględnym. Przy jego realizacji konieczne jest zachowanie właściwej równowagi względem innych praw i wartości (np. wolności informacji internautów). Ponadto należy uwzględnić odmienności występujące w systemach prawnych państw trzecich. Konsekwentnie mimo tego, iż operator wyszukiwarki podlega prawu UE (jako administrator danych[9]), to nie ciąży na nim obowiązek usunięcia linków ze wszystkich wersji językowych strony. Powinien to uczynić wyłącznie względem „unijnych" wersji wyszukiwarki, a jednocześnie uniemożliwić mieszkańcom Unii dostęp do wersji przeznaczonych dla użytkowników z państw trzecich.

Nie ulega wątpliwości, iż najważniejszą definicją wprowadzoną przez unijnego prawodawcę jest definicja danych osobowych. To właśnie ona

[8] Wyrok Trybunału Sprawiedliwości z dnia 24 września 2019 r. w sprawie *Google LLC przeciwko Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, EU:C:2019:772.

[9] Zob. szerzej wyrok Trybunału Sprawiedliwości z dnia 13 maja 2014 r. w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD)*, C-131/12, EU:C:2014:317.

w największym stopniu wpływa na zakres zastosowania całego aktu. Zgodnie z rozumieniem przyjętym przez RODO za dane osobowe należy uznać informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest natomiast osoba fizyczna, którą można bezpośrednio lub bezpośrednio zidentyfikować, m.in. na podstawie imienia, nazwiska, numeru identyfikacyjnego, danych o lokalizacji lub innych czynników określających jej tożsamość fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową bądź społeczną[10]. Przy każdorazowej ocenie, czy osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszystkie zasoby, które najprawdopodobniej zostaną wykorzystane przez administratora lub inny podmiot w tym celu. Należy przy tym uwzględnić ich czas, koszt oraz niezbędną technologię[11]. Podejście to stanowi wyraz tzw. subiektywnego rozumienia przesłanki identyfikowalności przyjętego na gruncie RODO[12]. Odnosząc się do definicji zawartej w dyrektywie 95/46/WE, prawodawca nie wprowadził żadnych znaczących zmian. Rozbudował natomiast katalog przykładów, co zdaje się stanowić odpowiedź na problemy występujące w zakresie interpretacji tego przepisu. Warto jednak zaznaczyć, iż mimo większej liczby przykładów zakres definicji danych osobowych wciąż jest przedmiotem ożywionej dyskusji teoretyków i praktyków. W ostatnich latach szczególnie istotne rozważania dotyczyły m.in. adresu IP czy adresu poczty elektronicznej.

Rozporządzenie wprowadza również pojęcie szczególnej kategorii danych osobowych, zwanych także danymi wrażliwymi. Zalicza się do nich dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane genetyczne, biometryczne oraz dotyczące zdrowia, seksualności lub orientacji seksualnej podmiotu

[10] Art. 4 pkt 1 RODO.
[11] Motyw 26 *ibidem*.
[12] P. Litwiński, P. Barta, M. Kawecki, *Art. 4*, [w:] P. Litwiński (red.), *op. cit.,* s. 186–187.

danych[13]. Łatwo więc dostrzec, iż dane te odnoszą się do szczególnej sfery prywatności osób fizycznych, która zdaniem prawodawcy zasługuje na szczególną ochronę. W tym miejscu warto wspomnieć, iż rozporządzenie wprowadza odmienne podstawy przetwarzania dla tzw. danych zwykłych oraz wrażliwych.

Omawianie jakiegokolwiek modelu ochrony danych osobowych nie jest możliwe bez odniesienia się do lokalnego rozumienia przetwarzania danych. Podobnie jak definicja danych osobowych stanowi ono naturalne uzupełnienie zakresu zastosowania danego aktu prawnego. Zgodnie ze słowniczkiem zawartym w rozporządzeniu za przetwarzanie należy uważać operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Prawodawca wprowadza również katalog przykładów, zawierający następujące operacje przetwarzania: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie oraz niszczenie[14].

W celu stworzenia efektywnych ram systemu ochrony danych osobowych konieczne jest zidentyfikowanie i właściwe zdefiniowanie podmiotów zaangażowanych w czynności przetwarzania. Co oczywiste, poczyniono to również w pracach nad RODO. W pierwszej kolejności należy wspomnieć o osobie, której dane dotyczą, zwanej także podmiotem danych. Warto zaznaczyć, iż może być nią wyłącznie żyjąca osoba fizyczna, gdyż RODO nie znajduje zastosowania do przetwarzania danych osób zmarłych[15]. Równie istotnym podmiotem jest administrator danych, a więc podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych. Może być nim zarówno osoba fizyczna,

[13] Art. 9 ust. 1 RODO.
[14] Art. 4 pkt 2 *ibidem*.
[15] Motyw 27 *ibidem*.

prawna, jak i organ publiczny, jednostka lub inny podmiot. Łatwo więc dostrzec, iż istotnym elementem tej definicji jest sprawowanie faktycznej kontroli nad daną czynnością przetwarzania. Nie jest natomiast istotne faktyczne posiadanie danych[16]. Lektura art. 4 wprost wskazuje na możliwość istnienia współadministratorów danych, których szczególne obowiązki określone zostały w art. 26. Kolejną grupę pomiotów stanowią przetwarzający dane. Zaliczamy do nich wszelkie podmioty dokonujące czynności przetwarzania w imieniu administratora[17]. Pełna zależność od decyzji podjętych przez administratora oznacza nie tylko, iż podmiot przetwarzający nie posiada swobody w zakresie identyfikowania celów, ale także że sama kwestia jego obecności uzależniona jest od wyłącznej decyzji administratora. Choć podmiotem przetwarzającym może być zarówno osoba fizyczna, prawna, jak i organ publiczny, należy pamiętać, iż musi być on odrębnym bytem prawnym od administratora[18]. W praktyce właściwe zidentyfikowanie administratora oraz podmiotów przetwarzających może być nie lada wyzwaniem. Punktem wyjścia każdorazowo powinno być określenie strony, która ma decydującą pozycję w określaniu celów i sposobów przetwarzania. Możliwe jest jednak zaistnienie takich sytuacji, w których relacja między tymi samymi podmiotami oparta na przetwarzaniu dokładnie tego samego zbioru danych zostanie zaklasyfikowana jako dwa różne typy współdziałania (np. administrator-przetwarzający oraz współadministratorzy).

Ogólne rozporządzenie o ochronie danych osobowych dokonało również pewnych zmian w zakresie podstaw przetwarzania danych osobowych. RODO – wzorem dyrektywy – zawiera zamknięty katalog okoliczności uprawniających do przetwarzania danych. Choć prawodawca nie wprowadza hierarchii między poszczególnymi podstawami, to wdraża wyraźne

[16] P. Litwiński, P. Barta, M. Kawecki, *Art. 4*, [w:] P. Litwiński (red.), *op. cit.,* s. 217.

[17] Art. 4 pkt 8 RODO.

[18] K. Witkowska-Nowakowska, *Artykuł 4 pkt 8*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 225.

obostrzenia w wykorzystaniu niektórych z nich. W porównaniu z dyrektywą 95/46/WE największe zmiany wprowadzono w odniesieniu do zgody, która stanowi pierwszą podstawę prawną przetwarzania danych wymienioną w art. 6. Prawodawca zdecydowanie zaostrzył wymogi stawiane poprawnie udzielonej zgodzie. Tym samym oparcie przetwarzania na zgodzie podmiotu danych stało się znacznie bardziej utrudnione, co obrazują już dotychczasowe rozstrzygnięcia organów nadzorczych[19]. Rozporządzenie nie wymaga pisemności zgody, stawia jednak wymóg dobrowolności, konkretności, świadomości oraz jednoznaczności[20]. RODO przewiduje możliwość udzielenia zgody w imieniu innego podmiotu danych wyłącznie w odniesieniu do dziecka poniżej 16. roku życia[21].

Kolejną podstawą prawną wskazaną przez prawodawcę jest przetwarzanie niezbędne do wykonania umowy lub podjęcia działań przed jej zawarciem. Należy jednak wyraźnie zaznaczyć, iż umową uprawniającą do takiego przetwarzania jest wyłącznie umowa, której stroną jest podmiot danych. Tym samym np. umowa zawarta przez pracodawcę z zewnętrznym dostawcą usług nie będzie upoważniać do przetwarzania danych pracowników.

Zgodnie z przepisami rozporządzenia administrator uprawniony jest do przetwarzania danych, gdy jest ono niezbędne do wypełnienia obowiązków prawnych ciążących na nim. W tym miejscu trzeba jednak pamiętać, iż obowiązek musi wynikać z przepisów prawa Unii Europejskiej lub państwa członkowskiego, któremu podlega administrator[22]. Wymóg ten jest szczególnie istotny w przypadku grup przedsiębiorstw, które zwykle związane są licznymi regulacjami, w tym również prawem państw trzecich.

[19] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against Google LLC, https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf [dostęp 20.09.2019].

[20] Art. 7 RODO.

[21] Art. 8 ust. 1 *ibidem*.

[22] Art. 6 ust. 3 *ibidem*.

Przetwarzanie danych uznane będzie za zgodne z RODO także wtedy, gdy zmierza do ochrony żywotnych interesów podmiotu danych. Za takie należy uznać interesy o szczególnie istotnym znaczeniu, jak np. zdrowie, życie czy niektóre interesy majątkowe[23]. Można jednak stwierdzić, iż zakres wykorzystania tej podstawy jest znacząco ograniczony. Jak wskazuje preambuła rozporządzenia, podstawa ta powinna być stosowana wyłącznie w wyjątkowych sytuacjach, które uniemożliwią skorzystanie z innych przesłanek wskazanych w art. 6[24].

Następną podstawę przetwarzania danych stanowi wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podobnie jak w przypadku realizacji obowiązku prawnego, tak i tutaj podstawa prawna powinna wynikać z prawa unijnego lub prawa właściwego państwa członkowskiego.

Ostatnią okolicznością uzasadniającą przetwarzanie danych osobowych na gruncie RODO jest realizacja prawnie uzasadnionych interesów administratora lub strony trzeciej. Posłużenie się tak nieostrym zwrotem rodziło niebezpieczeństwo nadużywania tej instytucji, dlatego prawodawca wprowadził obowiązek przeprowadzania tzw. testu równowagi. Zgodnie bowiem z treścią rozporządzenia zastosowanie tej podstawy możliwe jest wyłącznie wtedy, gdy podstawowe prawa i wolności podmiotu danych nie mają charakteru nadrzędnego nad prawnie uzasadnionym interesem administratora. Prawodawca sugeruje, by każdorazowe oparcie przetwarzania na tej podstawie poprzedzić dogłębną analizą. Powinna ona m.in. uwzględniać ocenę, czy podmiot danych mógłby spodziewać się właśnie takiego przetwarzania[25]. W swej treści RODO przywołuje kilka przykładów prawnie uzasadnionego interesu, w tym m.in. marketing bezpośredni, przeciwdziałanie oszustwom czy zapewnienie

[23] P. Litwiński, P. Barta, M. Kawecki, *Art. 6,* [w:] P. Litwiński (red.), *op. cit.,* s. 301.
[24] Motyw 46 RODO.
[25] Motyw 47 *ibidem.*

bezpieczeństwa sieci i informacji. Należy jednak pamiętać, iż podstawy tej nie mogą stosować organy publiczne w ramach realizacji swoich zadań.

Jak wspomniano powyżej, RODO wyróżnia także szczególną kategorię danych osobowych. Co do zasady ich przetwarzanie jest zabronione. Zakaz ten nie ma jednak charakteru bezwzględnego, gdyż art. 9 wprowadza katalog okoliczności go uchylających. Wydaje się to słusznym rozwiązaniem, gdyż prawo do ochrony danych osobowych należy zawsze odpowiednio ważyć względem innych praw i wolności[26].

Podobnie jak zwykłe dane, tak i dane wrażliwe mogą być przetwarzane na podstawie zgody udzielonej przez podmiot danych. Wszystkie wymogi stawiane „zwykłej" zgodzie obowiązują również w tym wypadku. Rozporządzenie wymaga jednak, aby w tych okolicznościach zgoda udzielona była w sposób wyraźny[27].

Przetwarzanie danych jest możliwe również, gdy jest ono niezbędne do wypełniania obowiązków i wykonywania szczególnych praw przez administratora lub podmiot danych, w dziedzinie prawa pracy, zabezpieczenia społecznego lub ochrony socjalnej oraz gdy jest ono niezbędne do ochrony żywotnych interesów podmiotu danych.

Szczególną podstawę przetwarzania danych wrażliwych zastrzeżono na rzecz fundacji, stowarzyszeń lub innych niezarobkowych podmiotów[28]. W ramach swej uprawnionej działalności mogą one przetwarzać dane sensytywne obecnych i byłych członków oraz osób utrzymujących z nimi stałe kontakty. Prawodawca zastrzega jednak, iż dane nie mogą być ujawniane żadnym podmiotom trzecim, a organizacja zobligowana jest do zastosowania odpowiednich zabezpieczeń. Wprowadzenie takiego rozwiązania wydaje się uzasadnione, gdyż z samej natury podmiotów,

[26] M. Kuba, *Artykuł 9*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 445.

[27] Art. 9 ust. 2 lit. a RODO.

[28] Podmioty te muszą jednak realizować cele polityczne, światopoglądowe, religijne lub związkowe.

takich jak fundacje czy stowarzyszenia, wynika konieczność przetwarzania danych wrażliwych o swoich członkach.

Poza powyższymi okolicznościami przetwarzanie szczególnych kategorii danych dozwolone jest, gdy dane te zostały w sposób oczywisty upublicznione przez podmioty danych lub gdy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń. Wyjątek ten dotyczy także przetwarzania podejmowanego przez sądy w ramach sprawowania wymiaru sprawiedliwości[29].

Kolejne cztery podstawy prawne odwołują się do istotnych interesów publicznych, które w szczególnych okolicznościach mogą przeważać nad prawami jednostki. Ważny interes publiczny może uzasadniać przetwarzanie danych wrażliwych, o ile będzie ono proporcjonalne do wyznaczonego celu i nie będzie naruszać istoty prawa do ochrony danych. Ważny interes publiczny powinien jednak znajdować swą podstawę w prawie unijnym lub prawie państwa członkowskiego. Prawodawca odrębnie odnosi się do przetwarzania niezbędnego do celów profilaktyki zdrowotnej, medycyny pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej, zabezpieczenia społecznego, leczenia oraz zarządzania systemami i usługami opieki zdrowotnej. Rozwiązanie to wydaje się jak najbardziej uzasadnione. Trudno wszakże oczekiwać, aby udzielenie pomocy medycznej uzależnione było od uprzedniego zidentyfikowania właściwej podstawy prawnej przetwarzania danych. Warto jednak zaznaczyć, iż takowe czynności przetwarzania mogą być podejmowane wyłącznie przez pracowników podlegających obowiązkowi zachowania tajemnicy zawodowej (np. lekarzy)[30]. Swoistą konsekwencją dwóch powyższych przesłanek jest ta wyrażona w art. 9 ust. 2 lit. i. Na podstawie tego przepisu przetwarzanie danych wrażliwych możliwe jest ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego. Zalicza się do nich m.in. ochronę przez transgranicznymi zagrożeniami zdrowotnymi (np. epidemie,

[29] Art. 9 ust. 2 lit. e–f RODO.

[30] Art. 9 ust. 3 *ibidem.*

pandemie) czy też zapewnienie wysokiego standardu jakości i bezpieczeństwa opieki zdrowotnej. Ostatnia okoliczność dopuszczona przez prawodawcę unijnego zezwala na przetwarzanie szczególnych kategorii danych osobowych, gdy jest ono niezbędne do celów archiwalnych (podejmowanych wyłącznie w interesie publicznym), badań naukowych, historycznych lub statystycznych. Podobnie jak w innych przypadkach czynności przetwarzania muszą być proporcjonalne do wyznaczonego celu badania.

Powyższe wyliczenie pozwala więc stwierdzić, iż katalog podstaw przetwarzania danych wrażliwych jest stosunkowo szeroki. Warto jednak zauważyć, iż prawodawca unijny pozostawił państwom członkowskim możliwość wprowadzenia dalszych warunków w odniesieniu do przetwarzania danych genetycznych, biometrycznych lub dotyczących zdrowia[31]. Jak słusznie zauważa się w literaturze, przepis ten dopuszcza zarówno wprowadzanie dalszych ograniczeń, jak i okoliczności legalizujących przetwarzanie[32].

Jednym z najistotniejszych założeń europejskiej reformy prawa ochrony danych osobowych było wzmocnienie i doprecyzowanie praw podmiotów danych. Znalazło to swe odzwierciedlenie w preambule do ogólnego rozporządzenia. Prawodawca podkreśla w niej, iż nie można mówić o w pełni skutecznej ochronie danych bez wystarczającej dbałości o prawa osób, których dane dotyczą, oraz obowiązki administratorów i podmiotów przetwarzających. Konsekwentnie prawodawca wprowadził następujące prawa podmiotów danych – prawo dostępu do danych, prawo do sprostowania danych, prawo do usunięcia danych, prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych oraz prawo do sprzeciwu oraz do niepodleganiu decyzjom opartym na zautomatyzowanym przetwarzaniu danych. W tym miejscu nie można również zapomnieć o szczególnym środku ochrony przewidzianym przez rozporządzenie. Zgodnie z art. 77 każdy podmiot danych ma prawo wniesienia skargi

[31] Art. 9 ust. 4 *ibidem*.

[32] M. Kuba, *op. cit.,* s. 454.

do niezależnego organu nadzorczego, jeżeli sądzi, że przetwarzanie danych go dotyczących narusza obowiązujące przepisy. Podstawą do wniesienia skargi może być zarówno działanie, jak i zaniechanie, którego dopuścił się administrator lub podmiot przetwarzający. Organ nadzorczy ochrony danych rozpatrujący skargę ma możliwość nałożenia administracyjnej kary pieniężnej lub kar niepieniężnych przewidzianych przez przepisy rozporządzenia[33]. Warto jednak pamiętać, iż skorzystanie z możliwości wniesienia skargi nie zamyka jednostce drogi do skorzystania z innych administracyjnych lub sądowych środków ochrony prawnej[34].

W celu zapewnienia bieżącej kontroli stosowania prawa ochrony danych osobowych oraz lepszej ochrony interesów jednostek RODO powołuje do życia wyspecjalizowane organy nadzorcze. Europejski system ochrony danych jeszcze pod rządami dyrektywy 95/46/WE wymagał od państw członkowskich utworzenia takowych organów. Jednakże obecnie obowiązujące rozporządzenie dodatkowo umocniło ich pozycję. Mimo iż przepisy rozporządzenia szczegółowo odnoszą się do kompetencji organów, należy stwierdzić, iż prawodawca pozostawił szeroki zakres swobody państwom członkowskim. Realizując tzw. autonomię instytucjonalną, państwa mają prawo uregulować szczegółowe kwestie związane z funkcjonowaniem krajowych organów[35]. Nie ulega jednak wątpliwości, iż najistotniejszą cechą organów nadzorczych, wyraźne sygnalizowaną na poziomie rozporządzenia, jest ich niezależność. To właśnie ona powinna najsilniej definiować pozycję ustrojową organu, a w szczególności jego relacje z innymi organami państwowymi. Niezależność organu powinna być realizowana zarówno w zakresie funkcjonalnym, instytucjonalnym, jak i materialnym. Konsekwencją tego jest chociażby obowiązek odpowiedniego ukształtowania budżetu organu, który nie może stanowić części budżetu innego organu[36].

[33] J. Łuczak, *Artykuł 77*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 1024.
[34] Art. 77 RODO.
[35] P. Barta, P. Litwiński, *Art. 52*, [w:] P. Litwiński (red.), *op. cit.,* s. 668
[36] *Ibidem*, s. 670.

RODO stanowi, iż państwa powinny powołać do życia „co najmniej jeden" organ nadzorczy[37]. Biorąc pod uwagę różnice ustrojowe występujące pomiędzy poszczególnymi państwami członkowskimi, rozwiązanie to szczególnie nie dziwi. Za przykład państwa, które powołało do życia więcej niż jeden organ, mogą posłużyć Niemcy.

Ze względu na ograniczone ramy niniejszego opracowania nie sposób jest szczegółowo omówić wszystkich zadań organów nadzorczych. Samo rozporządzenie formułuje ponad dwadzieścia uprawnień organów, które to dodatkowo mogą zostać poszerzone przez regulacje krajowe. Warto jednak zasygnalizować, iż do najważniejszych zadań organów nadzorczych należy monitorowanie i egzekwowanie stosowania przepisów RODO. Znaczna część ich zadań związana jest jednak ze szczególnymi instytucjami wprowadzonymi przez rozporządzenie. Tym samym organy nadzorcze są uprawnione chociażby do zatwierdzania wiążących reguł korporacyjnych czy przyjmowania standardowych klauzul umownych.

1.2. Transfer danych osobowych do państw trzecich

Model ochrony danych osobowych wprowadzony przez RODO i wdrożony w państwach Unii Europejskiej zakłada również odmienne reguły w zakresie przesyłania (transferu) danych osobowych do państwa trzecich położonych poza Europejskim Obszarem Gospodarczym (EOG). Biorąc pod uwagę daleko posuniętą globalizację i cyfryzację we współczesnym świecie, niemożliwe jest efektywne prowadzenie działalności gospodarczej bez wykorzystania narzędzi, jakie daje Internet.

W motywie 101 RODO podkreślono, że niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej jest przepływ danych osobowych do państw spoza UE i do organizacji międzynarodowych oraz z takich państw i z takich organizacji. Prawodawca

[37] Art. 51 ust. 1 RODO.

unijny zauważa, że wzrost ilości i charakteru omawianego przepływu stworzył nowe wyzwania i problemy w dziedzinie ochrony danych osobowych. Jednocześnie z uwagi na działania na polu gospodarczym nie powinny one prowadzić do obniżenia stopnia ochrony osób fizycznych zapewnianego w Unii niniejszym rozporządzeniem, także w przypadkach dalszego przekazywania danych osobowych: z państwa trzeciego lub organizacji międzynarodowej administratorom lub pomiotom przetwarzającym w tym samym lub w innym państwie trzecim lub tej samej lub innej organizacji międzynarodowej. Jakikolwiek przepływ danych do państw trzecich i organizacji międzynarodowych może się odbywać jedynie na zasadach określonych w RODO i tylko w przypadkach, gdy administrator lub podmiot przetwarzający przestrzegają warunków określonych w przepisach rozporządzenia dotyczących przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym – z zastrzeżeniem pozostałych przepisów RODO.

Istotne jest, aby każde przekazanie danych osobowych do państw trzecich lub organizacji międzynarodowych było dokonywane po wcześniejszym rozważeniu ryzyka, jakie wiąże się z przetwarzaniem danych osobowych poza EOG. Ryzyko to może być związane nie tylko z odmiennym stopniem ochrony danych osobowych, ale również z innymi uprawnieniami lokalnej administracji publicznej w zakresie pozyskiwania przetwarzanych przez podmioty prywatne danych osobowych czy ostatecznie samej czynności przekazywania danych.

W związku z tym, że państwa te mogą charakteryzować się różnym poziomem ochrony danych osobowych, w interesie osób prowadzących działalność gospodarczą w państwach Unii Europejskiej i Europejskiego Obszaru Gospodarczego jest korzystanie z rozwiązań prawnych, które zabezpieczą przetwarzanie tychże danych osobowych w sposób jakościowo co najmniej zbliżony do warunków narzuconych przez RODO[38].

[38] P. Drobek, *Komentarz do artykułu 44 Ogólnego rozporządzenia o ochronie danych,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 859.

Rozdział V RODO zawiera katalog dozwolonych sposobów przekazywania danych osobowych do państw trzecich oraz organizacji międzynarodowych.

Przez pojęcie przekazywania danych do państwa trzeciego lub organizacji międzynarodowej należy rozumieć kwalifikowaną formę przetwarzania[39]. Za przekazywanie danych uznamy każdą operację, w wyniku której dane osobowe zostaną fizycznie przekazane z państwa znajdującego się na terytorium Unii Europejskiej do państwa trzeciego, tj. przekraczają jego granice[40]. Przy kwalifikacji danej czynności jako przekazanie danych do państwa trzeciego lub organizacji międzynarodowej nie ma znaczenia, czy przekazanie danych osobowych ma charakter jednorazowy (incydentalny), czy wielokrotny (*set of transfers)*, sposób przekazywania, okres gromadzenia i przechowywania danych i forma prawna, na podstawie której dochodzi do przekazania[41].

Prawodawca unijny zdecydował się na ustanowienie kilku mechanizmów przekazywania danych osobowych do państw trzecich, biorąc pod uwagę przede wszystkim zapewnienie odpowiedniego poziomu ochrony. Wśród sposobów przekazywania danych uwzględniono:

a) przekazywanie danych na podstawie decyzji stwierdzającej odpowiedni poziom ochrony (art. 45);
b) przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń przez prawnie wiążący i egzekwowalny instrument między organami lub podmiotami publicznymi (art. 46 ust. 2 lit. a);
c) wiążące reguły korporacyjne (art. 46 ust. 2 lit. b);
d) standardowe klauzule ochrony danych przyjęte przez Komisję Europejską zgodnie z procedurą sprawdzającą (art. 46 ust. 2 lit. c);

[39] B. Fischer, *Komentarz do art. 44 Ogólnego rozporządzenia o ochronie danych*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Wrocław 2018, s. 462.

[40] B. Fischer, D. Karwala, *Transfer danych osobowych do państw trzecich (wybrane zagadnienia)*, „Państwo i Prawo" 2007, 1, s. 102.

[41] B. Fischer, *Komentarz do art. 44…*, s. 462.

e) standardowe klauzule ochrony danych przyjęte przez organ nadzorczy i zatwierdzone przez Komisję Europejską zgodnie z procedurą sprawdzającą (art. 46 ust. 2 lit. d);
f) zatwierdzone kodeksy postępowania zgodnie z art. 40 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą (art. 46 ust. 2 lit. e);
g) zatwierdzone mechanizmy certyfikacji zgodnie z art. 42 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą (art. 46 ust. 2 lit. f);
h) klauzule umowne między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej (art. 46 ust. 3 lit. a);
i) postanowienia uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą (art. 46 ust. 3 lit. b).

Przepis art. 45 RODO przyznaje Komisji Europejskiej (KE) kompetencje do uznawania, że państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych osobowych; następuje ono w drodze wydania przez ten organ odpowiedniej decyzji. Jeśli decyzja zostanie przez KE wydana, transfer danych do państwa trzeciego lub organizacji międzynarodowej wskazanej w decyzji nie wymaga spełnienia innych warunków[42]. Metoda ta była dopuszczalna również w poprzednio obowiązującej dyrektywie, jednocześnie pozostawiając pojęcie

[42] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 45*, [w:] P. Litwiński (red.), *op. cit.,* s. 634.

„odpowiedniego stopnia ochrony" jako kluczowe dla całego unijnego modelu regulacji transgranicznego przekazywania danych[43]. Zgodnie z motywem 103 Komisja może stwierdzić ze skutkiem dla całej Unii, że państwo trzecie – lub terytorium czy określony sektor w państwie trzecim – lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych. Ma to na celu zagwarantowanie pewności i jednolitości stosowania prawa w całej Unii w odniesieniu do państw trzecich lub organizacji międzynarodowych, które zostały uznane za zapewniające taki stopień ochrony. Oceniając, czy stopień ochrony jest odpowiedni, Komisja Europejska jest zobowiązana uwzględnić: 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 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

[43] P. Drobek, *Komentarz do artykułu 45 Ogólnego rozporządzenia o ochronie danych* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 863.

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

Jak widać, Komisja – wydając decyzje – nie bierze pod uwagę jedynie kwestii związanych *sensu stricto* z kwestią ochrony danych osobowych w danym państwie trzecim lub organizacji międzynarodowej. Słuszne wydaje się dążenie unijnego ustawodawcy do uznania, że odpowiedni poziom ochrony danych osobowych mogą zagwarantować jedynie państwa trzecie i organizacje międzynarodowe, które w pełni respektują zasady praworządności i prawa człowieka, a także zaciągnięte przez nie zobowiązania międzynarodowe. Istotne jest również, że jednym z warunków wydania decyzji o odpowiednim stopniu ochrony jest ustanowienie w danym kraju niezależnego organu ochrony danych osobowych – brak takiego podmiotu lub jego chociażby częściowa zależność od organów administracji publicznej mogłaby prowadzić do pozorności ochrony praw osoby fizycznej, szczególnie w jej kontaktach z aparatem państwowym.

Warto zauważyć, że decyzja Komisji Europejskiej może dotyczyć państwa, organizacji międzynarodowej bądź określonego sektora lub sektorów w tym państwie czy organizacji. Dotychczas Komisja raczej sporadycznie wydawała tego typu decyzję. Wydawana przez Komisję nie ma jednak charakteru absolutnego – organ może bowiem zdecydować (uprzednio informując o tym państwo trzecie lub organizację międzynarodową i przedstawiając im uzasadnienie) o jej cofnięciu.

Niezależnie od powyższego w przypadku braku uzyskania decyzji Komisji Europejskiej o odpowiednim stopniu ochrony bądź gdy taka decyzja została cofnięta, przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej może odbywać się na pozostałych zasadach określonych w rozdziale V.

Jak wskazuje motyw 108 RODO, w razie braku stwierdzenia odpowiedniego stopnia ochrony danych przez Komisję Europejską, administrator lub podmiot przetwarzający, jeśli chcą nadal przekazywać dane do państw trzecich lub organizacji międzynarodowych, powinni zastosować środki rekomendujące brak ochrony danych, zapewniając osobie, której dane dotyczą, odpowiednie środki zabezpieczenia. Ponieważ adekwatność ochrony nie może być zagwarantowana w sposób generalny, zapewnia się ją indywidualnie przez działania konkretnego podmiotu przetwarzającego dane. Środki te wskazane są w art. 46 RODO i zasadniczo dzielą się na takie, które wywołują skutek bez zezwolenia organu nadzorczego, i takie, które dla swojej skuteczności wymagają zezwolenia organu.

Do tej pierwszej grupy należy między innymi przekazywanie danych z zastrzeżeniem odpowiednich zabezpieczeń przez prawnie wiążący i egzekwowalny instrument między organami lub podmiotami publicznymi. Prawodawca unijny nie sprecyzował charakteru prawnego instrumentu określonego w art. 46 ust. 2 lit. a, Mechanizm prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi powinien być oceniany zarówno z perspektywy prawa międzynarodowego, jak i konstytucyjnego i może przyjmować formę umowy międzynarodowej oraz inne uzgodnienia między państwami, o ile w świetle prawa międzynarodowego mają one charakter wiążący[44].

Kolejnym rozpoznawanym przez RODO sposobem przekazywania danych do państw trzecich są wiążące reguły korporacyjne wspomniane w art. 46 RODO, ale szerzej opisane w art. 47. Aby można było je stosować, konieczne jest ich zatwierdzenie przez krajowy organ nadzorczy zgodnie z mechanizmem spójności określonym w art. 63 RODO.

[44] Warto wskazać, że część autorów widzi konieczność zakotwiczenia prawnie wiążącego i egzekwowalnego instrumentu w prawie krajowym państwa, którego podmiot ze sfery publicznej się na niego powołuje, zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 45*, [w:] P. Litwiński (red.), *op. cit.,* s. 642.

Zatwierdzenie wiążących reguł korporacyjnych przez właściwy organ nadzorczy wymaga łącznego spełnienia trzech przesłanek:

a) są one prawnie wiążące[45] oraz mają zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w tym ich pracowników, i są przez każdego z tych członków egzekwowane[46];
b) wyraźnie przyznają osobom, których dane dotyczą, egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych; oraz
c) spełniają wymogi określone w ust. 2 art. 47.

Uznaje się, że wiążące reguły korporacyjne są środkami prawnymi *sensu largo* o charakterze pośrednim, ich zadaniem jest przede wszystkim rekompensata niskiego stopnia ochrony danych w państwach trzecich, w których występuje część czynności procesu przetwarzania[47]. Ich celem jest umożliwienie przekazywania danych osobowych do państw trzecich w ramach struktur korporacyjnych pomiędzy podmiotami powiązanymi organizacyjnie i kapitałowo. Uznaje się je za jedną z najbardziej elastycznych form gwarancji przekazywania danych do państwa trzeciego przez przedsiębiorców[48].

[45] Charakter tego związania nie wykazuje jednak prawnej doniosłości, istotny jest jedynie skutego w postaci takiego związania, zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 47 Ogólnego rozporządzenia o ochronie danych*, [w:] P. Litwiński (red.), *op. cit.,* s. 649.

[46] Jednocześnie reguły te odnoszą się jedynie do danych przekazywanych do państwa trzeciego i organizacji międzynarodowych, a nie do wszystkich danych przetwarzanych w przedsiębiorstwie lub grupie przedsiębiorstw, zob. Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610136 [dostęp 28.09.2019].

[47] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 47 Ogólnego rozporządzenia o ochronie danych*, [w:] P. Litwiński (red.), *op. cit.,* s. 648; M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych*, Wrocław 2018, s. 137–138.

[48] A. Dmochowska, M. Zadrożny, *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR art. 29, Ustawy o ochronie danych osobowych z 2018 r.*, Warszawa 2018, LEGALIS: 7oeu5fx2.

Wiążące reguły korporacyjne odgrywają szczególną rolę w praktyce obrotu kapitałowego między międzynarodowymi podmiotami. Podstawową funkcją tego mechanizmu certyfikacji jest zrekompensowanie braków w prawie krajowym państwa, do którego przesyłane są dane, które nie pozwalają na przyjęcie adekwatnego poziomu ochrony danych w państwach docelowych[49]. Wydaje się, że wiążące reguły korporacyjne mają charakter regulacji przynależącej do prawa prywatnego – chociaż wiążą swoich adresatów, to ma to charakter wewnętrzny i prywatny[50]. W przeciwieństwie do innych mechanizmów certyfikacji raczej nie powinno się zdarzać, aby wiążące reguły korporacyjne były między sobą szczególnie podobne, gdyż rozwiązania w nich przyjęte w założeniu zdeterminowane są specyfiką poszczególnych przedsiębiorców[51]. Zgodnie z wytycznymi art. 47 reguły powinny przede wszystkim charakteryzować się zapewnieniem ich skuteczności i wiążącego charakteru zarówno w relacjach wewnętrznych i zewnętrznych.

Standardowe klauzule ochrony danych są kolejnymi mechanizmami certyfikacji dozwolonymi przed RODO. Prawodawca unijny wyróżnił dwa ich typy, tzn. standardowe klauzule ochrony danych przyjęte przez Komisję Europejską zgodnie z procedurą sprawdzającą (art. 46 ust. 2 lit. c) oraz standardowe klauzule ochrony danych przyjęte przez organ nadzorczy i zatwierdzone przez Komisję Europejską zgodnie z procedurą sprawdzającą (art. 46 ust. 2 lit. d). Pierwsze ze wspomnianych klauzul były rozpoznawane jako prawnie wiążące już pod rządami poprzednio obowiązującej regulacji. Standardowe klauzule ochrony danych przyjęte przez Komisję Europejską (obecnie obowiązują trzy takie klauzule)

[49] B. Fischer, D. Karwala, *Nowy instrument: wiążące reguły korporacyjny*, cz. 1 i 2, „Rzeczpospolita" 3.01.2006 i 11.01.2006.

[50] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 47,* [w:] P. Litwiński (red.), *op. cit.,* s. 649; D.E. Dukes, E.A. Paine, H.D. Bonyata, *Protection of Privacy in Data International Transfer,* s. 71.

[51] B. Fischer, *Komentarz do art. 47 Ogólnego rozporządzenia o ochronie danych*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 479.

mogą być częścią szerszej umowy o współpracy lub być uzupełnione o inne klauzule czy dodatkowe zabezpieczenia. Ani administrator, ani podmiot przetwarzający nie są uprawnieni do zmiany materialnych elementów standardowych klauzul. Jednocześnie wydaje się pewnym zaniedbaniem, że do dziś (28.09.2019) Komisja nie zaktualizowała omawianych klauzul. Standardowe klauzule ochrony danych mogą być również przyjęte przez organ nadzorczy, jednak w takim przypadku konieczne jest ich zatwierdzenie przez Komisję Europejską zgodnie z procedurą sprawdzającą. Komisja Europejska może zatwierdzić standardowe klauzule ochrony danych określone przez krajowy organ nadzorczy w trybie spójności lub po wydaniu opinii przez Europejską Radę Ochrony Danych. Wydaje się, że ten mechanizm jest głównie stosowany w przypadku sporadycznego przekazywania danych osobowych do państw trzecich, które nie zostały uznane za zapewniające odpowiedni stopień ochrony. W przeciwieństwie do wiążących reguł korporacyjnych, nie są podstawą przekazywania między przedsiębiorcami powiązanymi organizacyjnie i kapitałowo, ale pomiędzy jednostkami gospodarczymi, które łączą jedynie stosunki gospodarcze. Jak wskazano w motywie 109, standardowe klauzule ochrony mogą być częścią szerszej umowy, można je również uzupełnić o np. dodatkowe zabezpieczenia, które jednak nie mogą ani być pośrednio lub bezpośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi czy zatwierdzonymi przez Komisję, ani naruszać podstawowych praw i wolności osób, których dane dotyczą. Ustawodawca unijny wskazuje również na konieczność zachęcania administratorów i podmiotów przetwarzających, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony. Jednocześnie zmiana materialnych elementów klauzul ochrony może prowadzić do utraty ich statusu, a co za tym idzie potencjalnego przekazywania danych do państwa trzeciego niezgodnie z wymaganiami RODO i doprowadzić

do zagrożenia bezpieczeństwa przekazywanych danych i w konsekwencji odpowiedzialności prawnej administratora[52].

Powyższe zabezpieczenia mają na celu zapewnienie przestrzegania w państwie trzecim lub organizacji międzynarodowej zasad ochrony, w tym w szczególności zasady uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych, a także praw osób, których dane dotyczą na co najmniej takim samym poziomie, jaki jest zagwarantowany w Unii Europejskiej[53]. W kontekście zapewnienia bezpiecznego i nieprzerwanego prowadzenia działalności gospodarczej istotne jest, że stosowanie powyższych mechanizmów nie wymagało każdorazowo zgody odpowiedniego organu nadzorczego[54].

Zarówno możliwość skorzystania z kodeksu postępowania, jak i mechanizmu certyfikacji to nowości wprowadzone przez RODO w zakresie transgranicznego przekazywania danych osobowych. Oba mechanizmy muszą być powiązane z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń. Wydaje się, że instrumentem prawnym, który zapewni skuteczność tych rozwiązań, będzie forma umowy. Jednocześnie jednak pojawiają się wątpliwości w zakresie prawidłowego określenia jej stron i treści, ale nie budzi ich to, że rozwiązanie powinno umożliwiać dochodzenie praw przez jednostkę na terytorium Unii Europejskiej[55]. Oba te mechanizmy wymagają każdorazowo zatwierdzenia

[52] Grupa Robocza art. 29 opracowała m.in. zbiór zasad, które należy stosować przy ocenianiu, czy klauzule umowne zawarte między podmiotami gospodarczymi rzeczywiście spełniają wymagania nałożone przez RODO, a co za tym idzie, czy są mechanizmem prawnie dozwolonym przekazywania danych. Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on „Contractual clauses" Considered as compliant with the EC Model Clauses, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf [dostęp 28.09.2019].

[53] P. Drobek, *Komentarz do artykułu 47 Ogólnego rozporządzenia o ochronie danych,* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 871.

[54] *Ibidem,* s. 872.

[55] P. Drobek, *Komentarz do artykułu 46 Ogólnego rozporządzenia o ochronie danych*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 874.

przez organ nadzorczy, a jego brak skutkuje uznaniem przekazania za niespełniające wymagań stawianych przez RODO.

Niezależnie od mechanizmu transferu danych, jaki zostanie zastosowany, ostatecznie do administrator danych osobowych ponosi pełną odpowiedzialność za bezpieczeństwo ich przetwarzania[56]. Powinien on zagwarantować przestrzeganie praw osób fizycznych w tym zakresie i wszelkie środki bezpieczeństwa. Zgodnie z motywem 108 zabezpieczenia te powinny zapewniać, by przestrzegane były wymogi ochrony danych oraz prawa osób, których dane dotyczą, takie same jak w przypadku przetwarzania wewnątrzunijnego, w tym zapewniać dostępność egzekwowalnych praw osoby, której dane dotyczą, i skutecznych środków ochrony prawnej – w tym prawa do skutecznych administracyjnych lub sądowych środków zaskarżenia i do żądania odszkodowania – w UE lub w państwie trzecim.

Obowiązek zapewnienia odpowiedniego stopnia ochrony przetwarzanych danych spoczywający na administratorze nie może ograniczać się jedynie do zapewnienia odpowiednich środków technicznych i organizacyjnych, czy wypełnienia podstawowych obowiązków określonych w art. 4. Zgodnie bowiem z art. 24 RODO administrator jest zobowiązany do uwzględnienia charakteru, zakresu, kontekstu i celu przetwarzania, ale co bardziej istotne – ryzyka naruszenia praw i wolności osób fizycznych. Wydaje się, że szczególnie w przypadku przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych ta ostatnia kwestia powinna być wzięta pod uwagę przez administratora danych. Jednocześnie, zgodnie z motywem 78 RODO, ochrona praw i wolności, o której mowa w przepisie powinna mieć związek z przetwarzaniem danych i wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spójność przepisów rozporządzenia.

[56] *Ibidem*, s. 858.

Pozostaje zatem pytanie, czy w przypadku państw, które nie tyle co jeszcze nie zostały uznane za zapewniające odpowiedni poziom ochrony, ale przede wszystkim są stale i szeroko krytykowane za naruszenia w dziedzinie praw człowieka, powinny być wykorzystywane inne metody przekazywania danych. RODO pozostawia taką furtkę przedsiębiorcom, jednak wydaje się, że w niektórych z państw nie jest możliwe zapewnienie nawet minimalnego poziomu ochrony praw i wolności w związku z przetwarzaniem, z uwagi na odmienne regulacje w tym zakresie. Z drugiej jednak strony, nie sposób ograniczyć współpracy gospodarczej ze wszystkimi podmiotami pochodzącymi z takich państw. W takim przypadku to na administratorze danych osobowych ciąży obowiązek dokładnego zbadania, w jaki sposób kwestia ochrony danych osobowych jest uregulowana w państwie trzecim i jakie środki organizacyjne i techniczne powinny zostać wdrożone, aby z jednej strony zapewnić zgodność z RODO, a z drugiej – nie naruszyć lokalnych regulacji prawnych.

2. Bahrajn

2.1. Wstęp

Królestwo Bahrajnu należy do grupy najbogatszych państw świata arabskiego. Jeszcze do niedawna bahrajńska gospodarka uznawana była za najszybciej rozwijającą się w tamtejszym regionie. Niebagatelny wpływ na to ma położenie państwa w rejonie Zatoki Perskiej, obfitym w złoża ropy naftowej. Przez wiele dekad Bahrajn znajdował się w strefie wpływów brytyjskich. Ostatecznie jednak w 1971 r. państwo uzyskało niepodległość. Zgodnie z przepisami ustawy zasadniczej Bahrajn jest dziedziczną monarchią konstytucyjną, której głową państwa jest król.

Bahrajn to państwo muzułmańskie, w którym istotną rolę odgrywa prawo szariatu. Część autorów wiąże ten fakt z niskim poziomem przestrzegania praw człowieka i obywatela. Rokrocznie największe organizacje pozarządowe wymieniają Bahrajn wśród państw o najniższym poziomie ochrony jednostek[57]. Tym samym dużym zaskoczeniem było przyjęcie w 2018 r. kompleksowej regulacji dotyczącej ochrony danych osobowych. Szczególne zdziwienie może wzbudzać stopień jej surowości.

[57] Zob. szerzej Amnesty International Report 2017/18: The State Of The World's Human Rights. Bahrain, https://www.amnesty.org/en/countries/middle-east-and-north-africa/bahrain/report-bahrain/ [dostęp 1.06.2019].

2.2. Regulacja konstytucyjna

Obecnie obowiązująca konstytucja Królestwa Bahrajnu przyjęta została w 2002 r.[58] Zawiera ona rozdział poświęcony podstawowym prawom i obowiązkom obywateli. Trudno jednak szukać w nim wprost sformułowanego prawa do prywatności. Należy natomiast wskazać, iż niektóre z przepisów odwołują się do kwestii związanych z szeroko pojętą prywatnością. Artykuł 25 wprowadza zasadę nienaruszalności mieszkania. Może być ono przeszukane wyłącznie za zgodą mieszkańców lub w szczególnych uzasadnionych przypadkach, które mają swą podstawę w prawie. Ponadto art. 26 gwarantuje tajemnicę korespondencji obejmującą komunikację listowną, telegraficzną, telefoniczną oraz elektroniczną. Wszelkie wyjątki od tej zasady wymagają wskazania właściwej podstawy prawnej oraz postępowania zgodnego z przepisami prawa stanowionego[59]. W tym miejscu warto również wskazać, iż Bahrajn podpisał oraz ratyfikował Międzynarodowy Pakt Praw Obywatelskich i Politycznych[60], który w art. 17 gwarantuje jednostkom prawo do prywatności.

Nie można również zapomnieć o wpływie prawa szariatu na kwestie związane z prywatnością. Szariat najczęściej określany jest prawem religijnym muzułmanów. Zgodnie z doktryną islamu szariat objawiony został przez Allaha, toteż wyznawcy jego religii są bezwzględnie związani jego nakazami w większości aspektów swojego życia[61]. Znaczenie prawa islamu podkreślone zostało również w ustawie zasadniczej Bahrajnu. Stanowi ona, iż szariat jest głównym źródłem prawa w Królestwie[62]. Pomimo niezwykłej złożoności i skomplikowania szariatu, nie ulega

[58] Konstytucja Królestwa Bahrajnu z 14 lutego 2002 r. Dalej jako: Konstytucja Bahrajnu.

[59] Art. 25–26 *ibidem*.

[60] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. z 1977 r. Nr 38, poz. 167, dalej również MPOiP.

[61] M. Sadowski, *Kontrakt małżeński w prawie islamu*, „Studia Prawno-Ekonomiczne", t. CIII, 2017, s. 97.

[62] Art. 2 Konstytucji Bahrajnu.

wątpliwości, iż zawiera on szereg zasad dotyczących ochrony prywatności. Zgodnie z doktryną każdy aspekt życia należy traktować jako prywatny, chyba że został on ujawniony przez dany podmiot. Szariat podkreśla świętość i nienaruszalność sfery prywatnej[63]. W wielu przypadkach rozważania te stanowią punkt wyjścia do przyjmowania nowych regulacji prawa stanowionego w państwach arabskich[64].

2.3. Regulacje ustawowe

12 lipca 2018 r. Królestwo Bahrajnu przyjęło kompleksową ustawę dotyczącą ochrony danych osobowych, tym samym dołączając do nielicznego grona państw arabskich regulujących te zagadnienia[65]. Ustawa weszła w życie 1 sierpnia 2019 r., uchylając jednocześnie wszelkie wcześniejsze regulacje sprzeczne z PDPL. Dotychczasowe, szczątkowe przepisy z zakresu ochrony danych znajdowały się w szeregu ustaw szczegółowych i aktów wykonawczych. Można było je odnaleźć w prawie telekomunikacyjnym, prawie pracy, prawie ochrony konsumentów czy prawie bankowym. Nie ulega jednak wątpliwości, iż to właśnie kompleksowe regulacje (takie jak PDPL) stanowią lepszą gwarancję ochrony praw i interesów obywateli. Biorąc pod uwagę to, iż wcześniejsze bahrajńskie ustawodawstwo nie przewidywało tak licznych uprawnień dla jednostek, oczekuje się, iż PDPL znacząco wpłynie na sposób prowadzenia działalności gospodarczej[66]. Wśród przyczyn uchwalenia ustawy wymienia się

[63] Y. Khalaileh, N. Kisswani, *The „Right to Privacy" v. telecommunications interception and access: International regulations and implementation in the Arab Region*, „International Review of Law" 2013, Vol. 2, 2014, s. 10–11.

[64] Zob. szerzej: M. Lubis, M. Kartiwi, *Privacy and trust in the Islamic perspective: Implication of the digital age*, [w:] 5th International Conference on Information and Communication Technology for the Muslim World, 2013, s. 1–6.

[65] Law No. 30 of 2018 on the Personal Data Protection Law. Dalej jako: PDPL.

[66] M. Toorani, E. Holley, *Bahrain Publishes Personal Data Protection Law*, https://www.dlapiper.com/en/qatar/insights/publications/2018/09/bahrain-publishes-personal-data-protection-law/ [dostęp 1.06.2019].

przede wszystkim chęć dostosowania krajowego porządku do międzynarodowych standardów ochrony danych. Co oczywiste, takie działanie ma zwiększyć zainteresowanie lokalną gospodarką wśród zagranicznych inwestorów[67].

Zakres przedmiotowy zastosowania ustawy określony został bardzo szeroko. Co do zasady PDPL stosuje się do wszelkich czynności przetwarzania danych, niezależnie od tego, czy wykorzystywane są zautomatyzowane metody przetwarzania czy nie. Artykuł 2 (2) określa natomiast podmiotowy zakres zastosowania ustawy. Zgodnie z nim przepisy stosuje się wobec osób fizycznych mających miejsce zamieszkania lub miejsce prowadzenia działalności gospodarczej na terenie Bahrajnu oraz do osób prawnych posiadających swoją siedzibę w Królestwie. Ponadto ustawa ma zastosowanie do wszelkich podmiotów, które przetwarzają dane z wykorzystaniem środków dostępnych w Bahrajnie, chyba że służą one wyłącznie do przesyłania danych[68]. Tym samym należy stwierdzić, iż PDPL ma zasięg eksterytorialny. Warto jednak zaznaczyć, iż podmioty prowadzące działalność gospodarczą nieposiadające swojej siedziby na terytorium Królestwa zobligowane są do powołania swojego pełnomocnika w Bahrajnie. Będzie on odpowiedzialny za wypełnianie wszelkich obowiązków określonych przez ustawę. Powołanie pełnomocnika wymaga zgłoszenia do lokalnego organu nadzorczego (art. 2 (3)).

PDPL zawiera również skromny katalog wyłączeń. Ustawa nie znajduje zastosowania do czynności przetwarzania danych podejmowanych przez osoby fizyczne w celach osobistych i rodzinnych. Ponadto PDPL

[67] D. Wilkinson, *Five questions you should ask about Bahrain's new data protection law*, https://www.clydeco.com/insight/article/five-questions-you-should-ask-about-bahrains-new-data-protection-law [dostęp 1.06.2019].

[68] Zastrzeżenie to wydaje się o tyle interesujące, iż w ostatnich latach można dostrzec dążenia Bahrajnu do rozwinięcia na swoim terenie tzw. centrów danych dla międzynarodowych przedsiębiorstw, czego przykładem jest m.in. Amazon. Za: A. Jusic, *INSIGHT: Comprehensive Data Protection Comes to Bahrain*, https://news.bloomberglaw.com/privacy-and-data-security/insight-comprehensive-data-protection-comes-to-bahrain [dostęp 1.06.2019].

nie dotyczy czynności przetwarzania podejmowanych w celach związanych z bezpieczeństwem narodowym przez Ministerstwo Obrony, Ministerstwo Spraw Wewnętrznych, Gwardię Narodową, Agencję Bezpieczeństwa Narodowego oraz inne służby bezpieczeństwa (art. 2 (4)). Tym samym katalog ten nie ma charakteru zamkniętego, co może przyczyniać się do potencjalnych nadużyć ze strony władzy publicznej.

Warto zaznaczyć, iż PDPL wyłącza zastosowanie części przepisów w przypadku przetwarzania podejmowanego w związku z działalnością dziennikarską, artystyczną lub literacką. W takiej sytuacji nie znajduje zastosowania wymóg posiadania podstawy prawnej do przetwarzania danych (zarówno tych zwykłych, jak i wrażliwych) oraz ogólne zasady przetwarzania wskazane w art. 3. Ustawa wymaga jednak od właściwego podmiotu zagwarantowania poprawności danych oraz zapewnienia prawa do ich korekty. Zgodnie z art. 6 przetwarzający jest również zobligowany do wdrożenia środków bezpieczeństwa, które uniemożliwią wykorzystanie danych do innych celów.

Naczelnym celem omawianej regulacji jest oczywiście ochrona danych osobowych, których definicja legalna została przyjęta przez PDPL. Przez dane osobowe należy rozumieć informacje (w dowolnej formie) o zidentyfikowanej lub możliwej do zidentyfikowania (pośrednio lub bezpośrednio) osobie fizycznej. Identyfikacja jest możliwa w szczególności za pomocą krajowego numeru identyfikacyjnego oraz dodatkowych informacji odnoszących się do ekonomicznych, fizycznych, formalnych lub społecznych cech danej osoby. W przypadku wątpliwości, czy identyfikacja byłaby możliwa, należy uwzględnić nie tylko środki wykorzystane przez przetwarzającego, ale też takie, które potencjalnie były dla niego dostępne. Wzorem regulacji europejskiej PDPL wprowadza również pojęcie danych wrażliwych. Zgodnie z przyjętą definicją legalną rozumie się przez nie informacje pośrednio lub bezpośrednio ujawniające rasę, pochodzenie etniczne, poglądy polityczne lub światopogląd, przekonania religijne, przynależność do związków zawodowych oraz karalność osoby

fizycznej. Za wrażliwe uznaje się również informacje dotyczące zdrowia oraz orientacji seksualnej (art. 1).

Przetwarzanie danych w rozumieniu bahrajńskiego prawodawcy oznacza operacje lub zestawy operacji wykonywane na danych osobowych w sposób zautomatyzowany lub nie. Obejmuje ono w szczególności zbieranie, utrwalanie, organizowanie, segregowanie, przechowywanie, modyfikowanie, pobieranie, korzystanie, ujawnianie, przesyłanie, udostępnianie, łączenie, usuwanie lub niszczenie. Podobnie jak w przypadku regulacji znanych z innych porządków prawnych, wyliczenie to nie ma charakteru zamkniętego.

W odniesieniu do podmiotów zaangażowanych w czynności przetwarzania PDPL posługuje się nieco inną terminologią niż inne znane regulacje. Osoby, których dane dotyczą, określane zwykle jako podmioty danych, w Bahrajnie nazywane są właścicielami danych (*data owner*). Podmioty odpowiedzialne za ustalenie celów i sposobów przetwarzania danych – w Unii Europejskiej znane pod nazwą administratorów danych – określane są jako zarządcy danych (*data manager*). W sytuacji, gdy cele i sposoby przetwarzania określone są przez prawo, zarządcą jest podmiot odpowiedzialny za wykonanie tego obowiązku. Przetwarzającym określany jest natomiast podmiot dokonujący czynności przetwarzania w imieniu zarządcy danych. W tym wypadku mamy więc do czynienia ze zbieżnością terminologiczną z RODO.

Bahrajńska ustawa o ochronie danych jako generalną przesłankę przetwarzania danych przyjmuje zgodę wyrażoną przez właściciela. PDPL wymaga, by zgoda miała formę pisemną. Ponadto powinna być ona wyraźna, jasna oraz udzielona w konkretnie wskazanym celu. Nie ulega wątpliwości, iż udzielenie jej musi zostać poprzedzone przekazaniem pełnej informacji przez podmiot przetwarzający. Warunkiem koniecznym ważności zgody jest również jej dobrowolność. Ustawa przewiduje prawo do wycofania zgody. Co do zasady właściciel danych może skorzystać z niego na każdym etapie procesu przetwarzania (art. 24).

Zgodnie z brzmieniem ustawy przetwarzanie danych bez zgody właściciela jest zabronione, chyba że znajduje zastosowanie jedna z pozostałych podstaw wskazanych przez PDPL. Przetwarzanie będzie więc uzasadnione, gdy służy realizacji postanowień umowy, której właściciel jest stroną. Odrębną przesłankę stanowią natomiast czynności podejmowane w związku z chęcią zawarcia umowy. Znajdzie ona jednak zastosowanie wyłącznie w sytuacji, gdy właściciel danych zainicjuje te działania. Kolejną okolicznością uzasadniającą przetwarzanie danych z pominięciem wymogu uzyskania zgody właściciela jest wykonanie obowiązku wynikającego z przepisów prawa, który nie pokrywa się z zobowiązaniami kontraktowymi lub nakazem wydanym przez sąd. Katalog przesłanek uzupełnia przetwarzanie w celu ochrony żywotnych interesów właściciela danych oraz realizacja uzasadnionego interesu zarządcy danych lub osoby trzeciej, na rzecz której dane te zostały przekazane. Podobnie jak w przypadku regulacji europejskiej, oparcie danej czynności przetwarzania na przesłance uzasadnionego interesu wymaga przeprowadzenia tzw. testu równowagi. Czynności te nie mogą bowiem doprowadzić do naruszenia fundamentalnych praw lub wolności właściciela danych (art. 4).

Pozytywnie zaskakuje to, że PDPL zawiera odrębny katalog podstaw prawnych przetwarzania danych wrażliwych. Ponownie za punkt wyjścia przyjęto zgodę właściciela danych. Dopiero przy jej braku możliwe jest skorzystanie z jednej z pozostałych ośmiu przesłanek. Przetwarzanie danych wrażliwych następuje zgodnie z prawem, gdy jest ono wymagane do realizacji obowiązków i praw zarządcy związanych ze stosunkiem pracy. Ponadto będzie ono możliwe, gdy jest konieczne do ochrony właściciela w sytuacji, gdy nie jest on zdolny do wyrażenia zgody. W takim przypadku wymagane jest jednak uzyskanie zezwolenia właściwego organu. Dane wrażliwe mogą też być wykorzystane przez zarządcę, gdy są powszechnie dostępne. Kolejną przesłankę stanowi przetwarzanie konieczne do dochodzenia roszczeń prawnych. Obejmuje ona również wszelkie działania przygotowawcze. Dopuszczalne jest także przetwarzanie

podejmowane w kontekście działalności leczniczej przez uprawniony personel medyczny. Przesłanka ta obejmuje czynności związane z zarządzaniem usługami medycznymi, jeżeli podejmowane są przez osoby prawnie zobligowane do zachowania poufności. Dane wrażliwe mogą być również przetwarzane przez stowarzyszenia, związki zawodowe oraz inne organizacje *non-profit*[69]. Wymóg uzyskania zgody nie dotyczy czynności podejmowanych przez kompetentne organy władzy publicznej w sytuacji, gdy są one konieczne do realizacji ich zadań. Ostatnia wskazana przesłanka znajduje zastosowanie wyłącznie do danych dotyczących pochodzenia etnicznego oraz wyznania, jeżeli ich przetwarzanie jest konieczne do zapewnienia równego traktowania (art. 5).

Uzupełniając rozważania dotyczące przetwarzania danych wrażliwych, należy wskazać, iż ustawodawca wprowadził szczególne obostrzenia w zakresie przetwarzania danych dotyczących karalności osoby fizycznej. Zgodnie z wcześniej przytoczoną definicją zaliczane są one do kategorii danych wrażliwych, jednak przesłanki wskazane w art. 5 nie znajdują do nich zastosowania. Co do zasady, przetwarzanie jakichkolwiek informacji dotyczących przeszłości kryminalnej jest zabronione. Zgoda właściciela danych nie jest w tym przypadku wystarczającą podstawą prawną. Katalog wyłączeń tego zakazu zawiera natomiast art. 8.

Wykazanie (oraz właściwe udokumentowanie) podstawy prawnej przetwarzania danych nie jest bynajmniej jedynym wymogiem nałożonym przez bahrajńską regulację. PDPL wzorem innych znaczących aktów wskazuje szereg ogólnych zasad, które powinny znajdować zastosowanie do każdej czynności przetwarzania[70]. W pierwszej kolejności ustawodawca podkreśla, iż dane osobowe muszą być przetwarzane zgodnie z prawem oraz w sposób rzetelny. Dane mogą być zbierane wyłącznie

[69] Skorzystanie z tej przesłanki obwarowane jest dodatkowymi wymogami związanymi z celami danej organizacji. Zob. szerzej: Art. 5 (6)PDPL.

[70] Należy jednak pamiętać o wspomnianym wyżej wyłączeniu dotyczącym przetwarzania danych w ramach działalności dziennikarskiej, artystycznej i literackiej. Zgodnie z art. 6 zasady ogólne (wskazane w art. 3) nie znajdują zastosowania.

w konkretnie wskazanym, prawnie uzasadnionym i wyraźnym celu. Wprowadza się zakaz dalszego przetwarzania, który nie realizuje celu wskazanego na etapie wstępnym. Każda taka operacja powinna być oceniana z punktu widzenia proporcjonalności i celowości, a właściwy podmiot zobligowany jest do zapewnienia prawdziwości danych. W razie potrzeby jednostce należy zapewnić prawo do korekty swoich danych. Od chwili zrealizowania wskazanego celu przetwarzania, dane osobowe powinny być przechowywane w formie niepozwalającej na zidentyfikowanie osoby fizycznej. W przypadku, gdy konieczne jest wydłużenie okresu przechowywania danych (np. do celów naukowych lub statystycznych), należy dokonać ich anonimizacji (art. 3). W sytuacji gdy dane osobowe zostały pozyskane bezpośrednio od właściciela danych, na zarządcy ciąży szereg obowiązków informacyjnych. Jest on m.in. zobligowany do przekazania swoich danych kontaktowych, informacji o celu przetwarzania oraz listy podmiotów otrzymujących dane. Odrębnie ustawa formułuje obowiązki informacyjne w przypadku pozyskania danych od podmiotu trzeciego (art. 17).

W celu zwiększenia kontroli i uprawnień właścicieli danych PDPL przyznaje im kilka istotnych uprawnień. Przede wszystkim mają oni prawo do uzyskania informacji o samym fakcie przetwarzania ich danych. Konsekwentnie przysługuje im również prawo do korekty lub usunięcia swoich danych, aczkolwiek ostatnie z nich obwarowane jest dodatkowymi wymogami. Na mocy PDPL jednostka ma również prawo do sprzeciwu. Obejmuje ono dezaprobatę wobec marketingu bezpośredniego oraz decyzji podejmowanych na podstawie automatycznego przetwarzania danych. Osoba fizyczna może również wyrazić ogólny sprzeciw wobec operacji przetwarzania, jeżeli prawdopodobne jest powstanie szkody po stronie właściciela lub innych osób[71]. W tym miejscu warto podkreślić, iż PDPL wprowadza istotny środek ochrony praw właścicieli danych,

[71] M. Toorani, E. Holley, *op. cit.*

jakim jest skarga do organu nadzorczego. Zgodnie z treścią art. 25 każdy zainteresowany podmiot ma prawo do wystąpienia ze skargą, jeżeli przypuszcza, iż doszło do naruszenia przepisów PDPL.

Podobnie jak w innych państwach posiadających rozwiniętą legislację dotyczącą ochrony danych osobowych, tak i w Bahrajnie obowiązuje generalny zakaz przesyłu danych za granicę. Wychodząc jednak naprzeciw potrzebom współczesnych przedsiębiorstw, ustawodawca wprowadza pewne wyjątki. Wzorem regulacji europejskiej ustawa zastrzega właściwemu organowi prawo do wskazania państw zapewniających odpowiedni poziom ochrony danych osobowych. W przypadku transferu danych do tych państw nie są wymagane żadne dodatkowe działania po stronie zarządcy danych lub przetwarzającego. Mimo iż do dzisiaj nie opublikowano listy państw spełniających powyższe kryteria, oczekuje się, iż będzie ona wskazywać kraje Unii Europejskiej oraz większość państw uznanych przez Komisję Europejską za zapewniające adekwatny poziom ochrony danych[72]. Chęć przesłania danych do kraju nieznajdującego się na takiej liście wiąże się z koniecznością uzyskania pozwolenia. Zarządca danych może również skorzystać z jednego z wyłączeń wskazanych w art. 13. Zgodnie z katalogiem dopuszczalny jest transfer, na który zgodę wyraził właściciel danych, transfer danych z rejestrów publicznych oraz transfer niezbędny do wykonania umowy, ochrony żywotnych interesów właściciela danych, wykonania obowiązku prawnego lub ochrony roszczeń.

Omawiana ustawa powołuje do życia Organ Ochrony Danych Osobowych (*Personal Data Protection Authority*)[73]. Co istotne, PDPL wyraźnie podkreśla niezależność organu, zarówno w wymiarze finansowym, jak i administracyjnym. Zgodnie z art. 27 (1) prawo nadzoru nad jego działalnością przyznano ministrowi właściwemu do spraw wymiaru sprawiedliwości. Organ zobligowany jest do przedkładania ministrowi okresowych

[72] A. Jusic, *op. cit.*

[73] Dalej jako: Organ.

sprawozdań ze swojej działalności. Powinny one wskazywać nie tylko działania podejmowane przez organ, lecz także czynniki uniemożliwiające pełną realizację przepisów dotyczących ochrony danych.

Ustawa zawiera stosunkowo szeroki, ale niewyczerpujący katalog kompetencji przyznanych Organowi (art. 30). Niewątpliwie do jego najważniejszych zadań należy zaliczyć czuwanie nad przestrzeganiem przepisów PDPL oraz wykładnię obowiązków wskazanych w ustawie. Organ uprawniony jest do kontrolowania działalności zarządców danych w zakresie legalności czynności przetwarzania danych. Dodatkowo powinien on zachęcać do przyjmowania wewnętrznej polityki i procedur dotyczących ochrony danych. Organ jest również właściwy do otrzymywania oraz rozpatrywania notyfikacji składanych przez zarządców danych. Zgodnie z przepisami ustawy notyfikacja wymagana jest m.in. przed rozpoczęciem całkowicie lub częściowo zautomatyzowanego przetwarzania danych (art. 14). Ustawa przewiduje także szereg czynności przetwarzania, wymagających uzyskania uprzedniej zgody Organu. Zgodnie z art. 15 zgoda ta jest m.in. konieczna do zautomatyzowanego przetwarzania danych wrażliwych, biometrycznych lub genetycznych. Ponadto Organ rozpatruje skargi składane przez właścicieli danych. Ustawa zastrzega jednak, iż Organ ma również obowiązek przeprowadzenia właściwego dochodzenia w przypadku naruszeń wykrytych i zgłoszonych przez ministra. Podobnie jak w przypadku europejskich organów nadzorczych, do kompetencji bahrajńskiego Organu należy szeroko rozumiana działalność edukacyjna, której celem ma być zwiększanie świadomości konieczności ochrony danych osobowych. Wiąże się z tym obowiązek prowadzenia bieżących badań oraz analiz obowiązującego prawa, czego celem ma być dostosowywanie bahrajńskiego ustawodawstwa do standardów międzynarodowych. Ustawa kładzie duży nacisk na międzynarodową współpracę w zakresie ochrony danych, toteż Organ uprawniony jest do reprezentowania Królestwa na konferencjach międzynarodowych oraz do szeroko pojętej współpracy międzynarodowej.

Należy również podkreślić znaczenie Organu w procesie ustawodawczym. Zgodnie z art. 30 Organ ma możliwość przedkładania opinii na temat zgłoszonych projektów ustaw.

Pracami Organu kieruje siedmioosobowy Zarząd (*Board of Directors*). W jego skład wchodzą członkowie powoływani przez Rząd, Uniwersytet Bahrajnu, Urząd ds. Telekomunikacji, Bank Centralny Bahrajnu oraz Izbę Handlową. Minister właściwy ds. wymiaru sprawiedliwości uprawniony jest do powołania dwóch członków, z czego jeden z nich ma reprezentować środowisko informatyczne, natomiast drugi – sektor finansowy. Powołanie drugiego z nich następuje po konsultacji z Prezesem Banku Centralnego (art. 39). Kadencja członków Zarządu wnosi cztery lata. Głównym zadaniem Zarządu jest kierowanie i nadzorowanie prac Organu.

Na czele Organu stoi Prezes powoływany przez Zarząd na trzyletnią kadencję (art. 43). Do jego obowiązków należy przede wszystkim zarządzanie pracami Organu oraz reprezentowanie go na zewnątrz. Jest on odpowiedzialny za wykonywanie decyzji Zarządu oraz za szeroko pojętą działalność Organu (art. 44).

Jak wspomniano powyżej, PDPL przyznaje jednostkom prawo do wystąpienia ze skargą w przypadku podejrzenia nasuszenia przepisów ustawy. W określonych przypadkach Organ może prowadzić dochodzenie również w sprawach, co do których nie wniesiono skargi. Warto zaznaczyć, iż pracownikom Organu przysługują szerokie uprawnienia, m.in. prawo przeprowadzenia przeszukania w siedzibie podmiotu przetwarzającego dane włącznie z prawem dostępu do wszelkich dokumentów.

Ustawa wprowadza katalog kar administracyjnych, które mogą zostać nałożone przez Zarząd. Zgodnie z art. 55 możliwe jest nałożenie kary finansowej w wysokości 1000 dinarów bahrajńskich za każdy dzień naruszenia[74]. W przypadku stwierdzenia ponownego naruszenia w ciągu trzech lat, stawka ta wzrasta do 2000 dinarów za dzień. Dopuszczalne jest też

[74] Co stanowi równowartość ok. 10 000 zł.

nałożenie jednorazowej kary nieprzekraczającej 20 000 dinarów. Choć kary te mogą wydawać się stosunkowo łagodne (zwłaszcza w porównaniu z tymi przewidzianymi przez przepisy RODO), to szczególną uwagę zagranicznych ekspertów zwraca konstrukcja odpowiedzialności karnej. Ustawa wprowadza bardzo szeroki katalog przestępstw zagrożonych grzywną (w wysokości od 1000 do 20 000 dinarów) lub karą pozbawienia wolności do roku. Zgodnie z art. 58 przestępstwem jest przetwarzanie danych wrażliwych bez podstawy prawnej, transfer danych do państw trzecich z naruszeniem obowiązków wskazanych w ustawie, uchybienie obowiązkowi notyfikacji Organu, przetwarzanie danych bez uprzedniego uzyskania zgody wymaganej prawem, przedłożenie fałszywych lub wprowadzających w błąd informacji właścicielowi danych lub Organowi, utrudnianie lub uniemożliwianie wykonywania obowiązków przez pracowników Organu. W przypadku gdy przestępstwo popełniono w imieniu lub na korzyć osoby prawnej, nakłada się na nią grzywnę w wysokości dwukrotności grzywny wskazanej dla osoby fizycznej (art. 58–59). Łatwo więc można dostrzec, iż naruszenie zdecydowanej większości przepisów ustawy stanowi przestępstwo w rozumieniu prawa bahrajńskiego. I choć kara pozbawienia wolności za złamanie przepisów dotyczących ochrony danych osobowych obecna jest w wielu porządkach prawnych, to tak szeroki katalog przestępstw należy do rzadkości. Z pewnością stanowi to wyzwanie i ostrzeżenie dla podmiotów międzynarodowych chcących prowadzić działalność gospodarczą także na terenie Bahrajnu[75].

2.4. Praktyka

Bahrajński ustawodawca, wychodząc naprzeciw potrzebom sektora prywatnego, zadecydował o wprowadzeniu przeszło rocznego *vacatio*

[75] P. Mennie, *GDPR vs. Bahrain Personal Data Protection Law*, https://www.linkedin.com/pulse/gdpr-vs-bahrain-personal-data-protection-law-phil-mennie/ [dostęp 1.06.2019].

legis. Ustawa o ochronie danych osobowych weszła w życie 1 sierpnia 2019 r. Pomimo wcześniejszych zapowiedzi do dziś nie powołano Organu Ochrony Danych Osobowych, którego rola na etapie wdrażania regulacji byłaby nieoceniona. Skutkiem tego brak jest formalnych poradników lub wytycznych, które znacznie ułatwiłyby dostosowanie się do nowych przepisów. Pojawienie się takich problemów na samym początku nakazuje zastanowić się nad tym, czy omawiana regulacja będzie faktycznie stosowanym prawem. Dodatkowe wątpliwości pojawiają się ze względu na wspomniane na wstępie swobodne podejście do zagadnień związanych z ochroną praw jednostki. Jednym z najgłośniejszych przykładów braku poszanowania prywatności obywateli przez rząd Bahrajnu był zorganizowany proceder inwigilowania i szpiegowania działaczy opozycji oraz aktywistów na rzecz ochrony praw człowieka w latach 2010–2012[76].

Z drugiej jednak strony należy zwrócić uwagę na dużą determinację władz Bahrajnu w zakresie zwiększenia konkurencyjności lokalnego rynku, zwłaszcza w odniesieniu do usług cyfrowych[77]. Trudno jest więc sobie wyobrazić, aby największe przedsiębiorstwa technologiczne zadecydowały o przeniesieniu swojego zaplecza technologicznego do państwa, którego standardy prywatności i poufności budzić będą jakiekolwiek wątpliwości.

2.5. Adekwatność ochrony

Obecnie Bahrajn nie należy do państw uznanych przez Komisję Europejską za zapewniające adekwatny poziom ochrony danych osobowych. Brak jest również jakichkolwiek doniesień co do toczących się

[76] Zob. szerzej: F. Desmukh, *Bahrain Government Hacked Lawyers and Activists with UK Spyware*, https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/ [dostęp 1.06.2019].

[77] K. Al Rumaihi, *A New Law for the Digital Economy: Data Protection in Bahrain*, https://bahrainedb.com/bahrain-pulse/a-new-law-for-the-digital-economy-data-protection-in-bahrain/ [dostęp 1.06.2019].

w tym zakresie rozmów. Biorąc pod uwagę to, iż PDPL dopiero wszedł w życie, fakt ten nie powinien więc szczególnie zastanawiać.

Odnosząc się do kryteriów wskazanych przez art. 45 RODO, wątpliwości co do oceny Bahrajnu pojawiają się już na samym wstępie. Jak podkreślano powyżej, nieprawidłowości w zakresie przestrzegania praw człowieka i obywatela występują w Bahrajnie niemal na porządku dziennym. Liczne uchybienia wskazuje się również w działalności organów ścigania oraz służb bezpieczeństwa, które wielokrotnie nadużywały swojej władzy, stosując przemoc i tortury wobec zatrzymanych. Nie można również zapomnieć, iż w Bahrajnie nadal dopuszczalna i stosowana jest kara śmierci. Pomimo wcześniejszych zapowiedzi jej wycofania oraz kilkuletniego moratorium, w 2017 r. dokonano kolejnej egzekucji skazanego[78].

W obliczu powyższych faktów nieszczególnie dziwi wielowymiarowa dyskryminacja w prawie bahrajńskim. W szczególnie trudnej sytuacji znajdują się kobiety oraz osoby homoseksualne. Brak jest wyraźnych regulacji zakazujących dyskryminacji, a przepisy dotyczące m.in. rozwodów czy karalności przestępstw seksualnych zdają się ją dodatkowo pogłębiać.

Przechodząc do oceny samej regulacji dotyczącej ochrony danych osobowych, trudno oprzeć się wrażeniu, iż PDPL w wielu aspektach stanowi kopię unijnego rozporządzenia. Co oczywiste, uwagę zwracają niewielkie różnice terminologiczne. Warto jednak pamiętać, iż mimo ich istnienia zakres pojęciowy właściciela czy zarządcy danych jest bardzo zbliżony do europejskiego podmiotu i administratora danych. Trudno jest również wskazać na jakiekolwiek istotne różnice w rozumieniu pojęcia danych osobowych czy przetwarzania. Pozytywnie należy oceniać wyróżnienie kategorii wrażliwych danych osobowych oraz wprowadzenie odrębnego katalogu podstaw ich przetwarzania.

Zasady przetwarzania, obowiązki przetwarzających oraz prawa przysługujące właścicielom danych w dużej mierze pozostają spójne ze

[78] Human Rights Watch, *World Report 2019,* Nowy Jork 2019, s. 59–64.

standardami RODO. Warto jednak zaznaczyć, iż PDPL nie wprowadza obowiązku notyfikacji wycieków danych oraz nie gwarantuje jednostkom prawa do przenoszenia danych. Co ciekawe, regulacja bahrajńska powiela instytucję inspektora ochrony danych (*Data Protection Supervisor*) akredytowanego przez Organ. Choć powołanie go co do zasady nie jest obowiązkowe, to Organ może zobligować do tego poszczególne kategorie zarządców danych[79].

PDPL wprowadza mechanizmy ochrony jednostek przed niezgodnym z prawem przetwarzaniem ich danych. Możliwość wystąpienia ze skargą do Organu jest rozwiązaniem zasługującym na uznanie. Analiza przepisów pozwala również przypuszczać, iż kompetencje, jakie przyznano Organowi (oraz Zarządowi), pozwolą mu na skuteczne egzekwowanie PDPL. W tym miejscu nie można jednak zapomnieć, iż ustawa dopiero weszła w życie. Co więcej, jak już wcześniej wspomniano, do dziś nie powołano Organu Ochrony Danych Osobowych, który powinien pełnić kluczową rolę nie tylko na etapie wykonywania przepisów, ale także ich wdrażania. W opinii autorki może stanowić to pierwszy zwiastun dalszych problemów z faktycznym egzekwowaniem przepisów.

2.6. Wnioski

Bahrajńska ustawa o ochronie danych osobowych przyjęta w 2018 r. wydaje się niezwykle kompleksowym i przemyślanym aktem. Nie ulega wątpliwości, iż czerpie on z dorobku unijnego, co zważając na europejski poziom ochrony, powinno być oceniane raczej pozytywnie. Można mieć natomiast pewne wątpliwości co do motywacji lokalnego prawodawcy oraz celów, jakie ma realizować PDPL. Biorąc pod uwagę bahrajńskie podejście do przestrzegania praw i wolności człowieka, trudno jest przypuszczać, iż naczelnym celem ustawy jest troska o dobro obywateli.

[79] M. Toorani, E. Holley, *op. cit.*

Wydaje się raczej, iż przeważają tu cele ekonomiczne i gospodarcze, a przede wszystkim chęć zwiększenia konkurencyjności lokalnego rynku dla zachodnich inwestorów.

Odnosząc się do możliwości uznania Bahrajnu za kraj zapewniający adekwatny poziom ochrony danych osobowych, wydaje się to na razie dość odległe. I choć sama ustawa zdaje się czynić zadość zdecydowanej większości wymogów Komisji Europejskiej, to przeważające znaczenie ma ocena całego porządku prawnego. Bahrajn do dziś boryka się z licznymi problemami o charakterze systemowym, które z punku widzenia Unii Europejskiej będą trudne do przyjęcia. Istnienie rozbudowanego i sprawnego systemu ochrony danych osobowych jest wszakże wątpliwym argumentem przy braku poszanowania zasady praworządności w Królestwie. Warto jednak bliżej przyglądać się dalszym zmianom zachodzącym na Bliskim Wschodzie, zarówno w obszarze ochrony danych osobowych, jak i ogólnych przemian ustrojowych. Niewykluczone jest, iż dążenie do standardów europejskich czy międzynarodowych w jednym aspekcie przełoży się również na pozostałe dziedziny aktywności państwowej.

3. Chiny

3.1. Wstęp

Chińska Republika Ludowa to kraj konstytucyjnie socjalistyczny, w którym władzę, podobnie jak w innych krajach demokracji ludowej, faktycznie sprawuje jedna partia – Komunistyczna Partia Chin. Ogólnochińskie Zgromadzenie Przedstawicieli Ludowych (OZPL) o 5-letniej kadencji jest najwyższym organem władzy ustawodawczej i ustrojodawczej Głową państwa jest przewodniczący wybierany na 5 lat przez OZPL. Przewodniczący mianuje premiera na zlecenie OZPL. Władzę wykonawczą sprawuje Rada Państwowa mianowana przez premiera.

Chiny są państwem o największej populacji na świecie, a co za tym idzie, obywatelom tego kraju oferowana jest olbrzymia liczba usług, do których wykonywania konieczne jest przetwarzanie ogromnej ilości danych osobowych. Brak efektywnych i kompleksowych regulacji może doprowadzić do nieuzasadnionej ingerencji w prawo do prywatności jednostki w niespotykanej nigdzie indziej skali. Co więcej, rząd chiński podejmuje dosyć kontrowersyjne działania, które wymagają zbierania i przetwarzania danych obywateli. Słuszne oburzenie wywołał niedawno wprowadzony masowy program rozpoznawania twarzy. Warto również zauważyć, że chińska konstytucja, jako jeden z niewielu nowożytnych aktów prawnych, dopuszcza istnienie cenzury prewencyjnej, co

w państwach zachodnich w wielu przypadkach niemal tożsame jest z naruszeniem prywatności jednostki[80].

Wszystkie te elementy sprawiają, że świat z zapartym tchem śledzi poczynania chińskich władz w odniesieniu do ochrony prywatności. Niedawny skandal związany z przekazywaniem danych osobowych przez podmiot prywatny podmiotom publicznym w Chinach i zarzuty o szpiegostwo na niespotykaną dotychczas skalę[81] sprawiają, że warto się przyjrzeć poszczególnym regulacjom w Państwie Środka.

3.2. Regulacja konstytucyjna

Tradycyjnie w Chinach pojęcie prywatności związane było z ochroną wstydliwych informacji na temat jednostki, czymś, co należy ukrywać przed opinią publiczną, i z reguły prywatność była przedstawiana w negatywnym świetle. W związku z tym dosyć konserwatywnym podejściem część Chińczyków wciąż uważa, że sprawy prywatne są czymś, o czym wstyd rozmawiać publiczne, a gdy dochodzi do naruszenia ich prywatności, są w stanie bądź to zignorować, bądź sprzeciwić się naruszeniom z wykorzystaniem środków nieprzewidzianych w prawie, zamiast oddać sprawę w ręce sądu tylko po to, aby uniknąć publicznej rozprawy i ewentualnego zainteresowania mediów bądź lokalnej społeczności[82].

Konstytucja Chin w art. 40 gwarantuje każdemu obywatelowi Państwa Środka ochronę wolności oraz tajemnicy korespondencji. Ustrojodawca wskazuje również, że nikt nie może naruszać wolności i tajemnicy

[80] Konstytucja Chińskiej Republiki Ludowej z dnia 4 grudnia 1982 r.

[81] K. O'Flaherty, *Huawei Security Scandal: Everything you need to know,* https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/#10f6aa1e73a5 [dostęp 13.06.2019].

[82] C. Jingchun*, Protecting The Right To Privacy In China, „*Victoria University of Wellington Law Review" 2005, 36, s. 645–664; zob. również: H. Zhao, H.X. Dong, *Research on Personal Privacy Protection of China in the Era of Big Data*, „Open Journal of Social Sciences" 2017, 5, s. 139–145, https://doi.org/10.4236/jss. 2017.56012 [dostęp 14.06.2019].

korespondencji drugiej osoby, poza przypadkami, kiedy jest to konieczne w celu zagwarantowania bezpieczeństwa państwa lub postępowania karnego. Organy administracji publicznej oraz organy ścigania mogą cenzurować wysyłaną korespondencję w przypadkach dozwolonych przepisami ustawy. I chociaż chińska ustawa zasadnicza rozpoznaje prawo do ochrony tajemnicy komunikowania się, nie zawiera postanowień związanych z ochroną prywatności w rozumieniu generalnym ani z ochroną danych osobowych.

Warto również wspomnieć, że chociaż rząd chiński podpisał wiele traktatów i umów międzynarodowych gwarantujących poszanowanie praw człowieka, w tym prawa do prywatności i ochrony danych osobowych, wciąż wielu z tych umów w Chinach nie ratyfikowano (np. Międzynarodowy Pakt Praw Obywatelskich i Politycznych).

Brak odpowiednich regulacji konstytucyjnych i ustawowej definicji prawa do prywatności spowodował wypracowanie i przyjęcie pewnych koncepcji w doktrynie prawa chińskiego, które w dłużej mierze zostały następnie wdrożone przez organy stosujące prawo. W kontekście dalszych rozważań warto przytoczyć jedną z najbardziej popularnych definicji prywatności, zgodnie z którą prywatność to prawo osoby fizycznej, jest ona wolna od publicznej i jakiejkolwiek innej ingerencji w jej sprawy osobiste, odnoszące się jedynie do tej jednostki i informacji na jej temat[83]. Twórcy tej definicji pozycjonują prywatność jako wywodzącą się z równowagi między jednostką a społeczeństwem i pozwalającą jednostce na przeżywanie w spokoju swoich wewnętrznych emocji, ponieważ istnienie prawa do prywatności jest ściśle związane z funkcjonowaniem duchowej sfery życia ludzkiego[84].

Pierwotnie, judykatywa wywodziła prawo do ochrony prywatności z ogólnych zasad prawa cywilnego. Naruszenie prywatności przez wiele

[83] L. Wang, L. Yang, *The Law of the Rights of The Person,* „The Press of Laws", Beijing, 1997, s. 147.

[84] *Ibidem* s. 147.

lat było jednoznaczne ze zniesławieniem w przypadkach, w których ujawniono tajemnice osobiste ustnie lub pisemnie bądź sfabrykowano fakty, aby publicznie oczernić daną osobę, zaszkodzić jej godności lub reputacji, i było klasyfikowane jako naruszenie prawa do dobrego imienia[85].

Warto jednak zauważyć, że mimo aktywności sądów w tym zakresie, rząd chiński zdaje się często pomijać kwestię ochrony prawa do prywatności jako niezbywalnego i przyrodzonego prawa człowieka[86]. Jeszcze w 2012 r., gdy ogłoszono Narodowy Plan Ochrony Praw Człowieka, prawo do prywatności nie było poruszane w żadnym z istotnych kontekstów, rząd zobowiązał się jedynie do niepodejmowania działań, które mogłyby ingerować w prywatność jednostki[87]. Jednocześnie w ostatnich latach przyjęto szereg regulacji, które mają zobowiązać przedsiębiorców do zapewnienia odpowiedniego poziomu ochrony danych osobowych przez nich przetwarzanych.

3.3. Regulacje ustawowe

We wrześniu 2013 r. Ministerstwo Gospodarki i Technologii wydało zbiór zasad dotyczących ochrony informacji na temat jednostki w sektorze telekomunikacyjnym i chociaż zasady te nie są aktem prawnym, to wiążą one dostawców usług telekomunikacyjnych i internetowych[88].

[85] W. Gray, H.R. Zheng, *Opinion of the Supreme People's Court on Questions Concerning the Implementation of the General Principles of Civil Law of the People's Republic of China (Translation)*, s. 79, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2541&context=articles [dostęp 11.06.2019].

[86] The Right to Privacy in China. Submitted by Privacy International, and the Law and Technology Centre of the University of Hong Kong. March 2013. Stakeholder Report Universal Periodic Review, 17th Session – China, https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=142&file=EnglishTranslation [dostęp 13.06.2019].

[87] *Ibidem.*

[88] Revisiting the data protection regime in China, https://deutschland.taylorwessing.com/documents/get/463/revisiting-the-data-protection-regime-in-china.pdf/show_on_screen [dostęp 13.06.2019].

Reguły wydane przez Ministerstwo wskazują, że dane muszą być zbierane i przetwarzane w sposób zgodny z prawem, z poszanowaniem zasady proporcjonalności i tylko wtedy, kiedy jest to absolutnie niezbędne, ponadto konieczne jest wcześniejsze uzyskanie zgody osoby, której dane dotyczą, na ich zbieranie i przetwarzanie[89]. Podmiot przetwarzający dane zobowiązany jest również do powiadomienia podmiotu danych osobowych o celu, metodach i zakresie przetwarzania danych, a wykorzystanie ich jest możliwe tylko wtedy, kiedy jest to niezbędne do dostarczenia zamawianej przez konsumenta usługi[90].

Jednym z aktów prawnych, który reguluje kwestię ochrony danych osobowych konsumentów, jest ustawa o ochronie konsumentów, która weszła w życie 15 marca 2014 r. Zobowiązuje ona podmioty oferujące usługi konsumentom do ochrony informacji na temat jednostki (w zakresie imienia i wizerunku) i ochrony prawa do prywatności[91]. Zbieranie i przetwarzanie danych powinno odbywać się w sposób zgodny z prawem w myśl zasad konieczności i proporcjonalności[92]. Cel, zakres i sposoby przetwarzania danych powinny być ujawnione osobie, której dane dotyczą, przed udzieleniem przez nią zgody na przetwarzanie danych osobowych. Przedsiębiorca zobowiązany jest do pozostawienia danych osobowych w poufności i zastosowania odpowiednich środków bezpieczeństwa, a także powzięcia odpowiednich kroków zabezpieczających w przypadku ich naruszenia. Nie można wykorzystywać danych osobowych do przesyłania niezamówionych informacji handlowych bądź takich, na których otrzymywanie konsument nie wyraził zgody.

Najważniejsze zasady związane z ochroną danych osobowych, które co bardziej istotne mają charakter kompleksowy i odnoszą się do wszystkich gałęzi gospodarki znajdują się w art. 111 prawa cywilnego,

[89] *Ibidem.*
[90] *Ibidem.*
[91] *Ibidem.*
[92] *Ibidem.*

który wszedł w życie 1 października 2017 r.[93] Wskazano w nim, że wszelkie informacje na temat osoby fizycznej powinny być chronione przez prawo, a podmioty przetwarzające dane mogą je pozyskiwać tylko w prawnie dozwolony sposób, uzyskawszy uprzednio zgodę osoby, której dane dotyczą i zapewniając odpowiedni poziom bezpieczeństwa tych informacji[94]. Zabronione jest zbieranie, używanie, przetwarzanie i przenoszenie danych osobowych bez zgody podmiotu, którego dane dotyczą, oraz nie można ich też sprzedawać, kupować, publikować bądź dostarczać, chyba że jest to wyraźnie dozwolone w prawie[95].

1 czerwca 2017 r. weszła w życie ustawa o cyberprzestrzeni, która po raz pierwszy w historii ustawodawstwa chińskiego w tak szeroki sposób reguluje kwestie ochrony danych osobowych[96]. Celem nowej regulacji było przede wszystkim wzmocnienie ochrony w zakresie przetwarzania transgranicznego danych osobowych i wrażliwych. Podmioty przetwarzające zostały zobowiązane do przestrzegania przepisów w tym zakresie w celu ochrony wszystkich kategorii danych, które miałyby być przetwarzane przez podmioty prowadzące działalność gospodarczą w Chinach i chcące przesyłać dane do państw trzecich[97].

Na podmioty, które naruszą przepisy ustawy, mogą być nałożone grzywny, a osobom odpowiedzialnym za naruszenie grozi kara pozbawienia wolności lub zakazu zajmowania określonych stanowisk[98]. Naruszenie

[93] China: Data Protection & Localisation, Cyber Security Law, VPN and Encryption, https://www.beiten-burkhardt.com/sites/default/files/downloads/BB%20BR-Flyer%20A5%20China-Data%20Protection%20en.pdf [dostęp 13.06.2019].

[94] *Ibidem.*

[95] *Ibidem.*

[96] R. Staden ten Brink, J. Wang, D. Veldhoen, A. Arnbak, *China's new cybersecurity law – effective as of 1 June 2017*, „Trade Security Journal" 2017, Issue 2, s. 27.

[97] Whitepaper on Regulatory Implications for Cross-Border Data Transfers from China to the United States, http://sia-partners.com/sites/default/files/sia_partners_whitepaper_mainland_china_data_transfers.pdf [dostęp 11.06.2019].

[98] *The China Cybersecurity Law has been finalized- is your organisation ready to comply with a new law?,* https://www.pwccn.com/en/issues/cybersecurity-and-privacy/china-cybersecurity-law-2017.html [dostęp 11.06.2019].

prawa do prywatności jest penalizowane również na gruncie prawa karnego. Bezprawne przeszukanie zarówno jednostki, jak i miejsca jej przebywania zagrożone jest karą do trzech lat pozbawienia wolności lub ograniczenia wolności, podczas gdy naruszenie tajemnicy korespondencji przez ukrywanie, niszczenie bądź bezprawne otwieranie cudzych wiadomości może skutkować nałożeniem kary do roku pozbawienia wolności lub ograniczenia wolności[99]. Nowelizacja prawa karnego z 2009 r. wprowadziła do zakresu działań penalizowanych przestępstwo naruszenia prawa do ochrony danych osobowych przez wykorzystanie informacji na temat jednostki w innym celu niż zostały ono zebrane w trakcie wykonywania czynności służbowych, zarówno w sektorze prywatnym, jak i publicznym. Czynności te są zagrożone karą do trzech lat pozbawienia wolności, grzywny lub ograniczenia wolności. Odpowiedzialna za naruszenie może być również osoba prawna lub osoba nią zarządzająca[100]. Celem omawianego przepisu jest zarówno wdrożenie odpowiednich środków ochrony danych w działalności podmiotów prywatnych i publicznych, jak i rozbudzenie w pracownikach tych podmiotów świadomości w zakresie ochrony prawa do prywatności[101].

3.4. Praktyka

Ustawa o cyberprzestrzeni wprowadziła przepisy umożliwiające organom nadzoru bezpośrednią kontrolę nad zakresem i sposobami przetwarzania danych osobowych. Już kilka miesięcy po jej wejściu w życie rząd Chin nałożył kilkanaście kar na największe przedsiębiorstwa dostarczające usługi w cyberprzestrzeni z powodu nieprzestrzegania

[99] H. Xue, *Privacy and personal data protection in China: An update for the year end 2009*, „Computer Law & Security Review" 2010, 26, s. 284–289.

[100] Amendment Seven to the Criminal Law, passed by the Standing Committee of the National People's Congress on February 28, 2009.

[101] H. Xue, *op. cit.*

przepisów ustawy w zakresie stosowania narzędzi cenzury przez umieszczanie niedozwolonych treści (takich jak przemoc, seks, używki) przez ich użytkowników na stronach internetowych zarządzanych przez przedsiębiorców[102]. Zapowiedziano również, że będą przeprowadzane okresowe kontrole polityki prywatności dostawców usług w cyberprzestrzeni, a podobne działania już podejmują lokalne przedstawicielstwa Ministerstwa Gospodarki i Technologii Informacyjnej[103].

Bez wątpienia w Chinach wzrasta świadomość obywateli i przedsiębiorców w zakresie ochrony prywatności i danych osobowych. Niestety, wciąż dochodzi do naruszeń praw jednostki w tym zakresie, w wielu przypadkach przez publiczne ujawnienie informacji na temat osoby fizycznej. W styczniu 2008 r. spółka zarządzająca metrem w Szanghaju musiała przeprosić parę, która znalazła się na opublikowanym w internecie nagraniu z kamery CCTV, pokazującym ich całujących się, w tle której dało się słyszeć trzy głosy wulgarnie komentujące zachowanie pokrzywdzonych[104]. W przestrzeni publicznej coraz częściej zdaje się słyszeć głosy o zbyt rozbudowanym systemie monitoringu wizyjnego w miejscach publicznych, co w znaczny sposób narusza prywatność monitorowanych jednostek[105].

Podobny przykład podania do publicznej wiadomości informacji na temat jednostki, czym naruszono jej prawo do prywatności i ochrony danych, odnotowano w 2007 r. Sąd w Pekinie stwierdził, że podanie do publicznej wiadomości wyroku przeciwko jednej z klientek firmy gazociągowej zawierającego w sobie wezwanie do natychmiastowej zapłaty zaległych rachunków jest naruszeniem prawa do ochrony danych osobowych, a tym samym zobowiązał podmiot naruszający do publicznych

[102] *China Cybersecurity Law,* https://www.reedsmith.com/-/media/files/perspectives/2018/chinas-cybersecurity-law-002.pdf [dostęp 13.06.2019].

[103] *Ibidem.*

[104] *Shanghai Metro Apologized to the Lovers Caught on Tape*, „Oriental Morning" January 23, 2008, http://society.people.com.cn/GB/1062/6809132 [dostęp 11.06.2019].

[105] H. Xue, *op. cit.*

przeprosin poszkodowanej[106]. Jednocześnie jest to praktyka, którą stosuje wielu przedsiębiorców w celu wyegzekwowania płatności za dostarczone usługi. Nie zawsze jednak spotyka się to z krytyką ze strony organów publicznych[107].

W 2014 r. rząd ogłosił nowy program, który zakłada stworzenie scentralizowanej bazy danych, której zadaniem jest monitorowanie i dopasowywanie zachowań przedsiębiorców i zwykłych obywateli w celu zwiększenia zaufania do jednostki oraz ułatwienia przedsiębiorcom pozyskiwania wiarygodnych informacji na temat historii kredytowej konsumentów. Od indywidualnego wyniku uzyskanego przez jednostkę zależeć będzie zakres oferowanych jej usług socjalnych i bankowych[108]. Celem programu jest wprowadzenie do bazy danych informacji na temat wszystkich obywateli do 2020 r. i dlatego wymaga się od wszystkich przedsiębiorców dostarczających usługi obywatelom Chin bądź na terytorium państwa współpracy w zakresie zbierania danych ich konsumentów[109]. Rozpoczął się już również projekt pilotażowy, który przyznaje niektóre kary (np. administracyjne, w przypadkach popełnienia określonych wykroczeń bądź innych celów zabronionych itd.) i nagrody w odpowiedzi na zebrane dane, niemniej brak odpowiedniej kontroli nad przetwarzanymi danymi przez jednostkę wzbudza liczne kontrowersje zarówno w Chinach, jak i państwach trzecich[110].

[106] *Court Orders Gas Company to Apologize to a Humiliated Customer*, People's Court Daily, July 16, 2007, http://www.lawtime.cn/info/anli/mfqita/2007071852281.html [dostęp 11.06.2019].

[107] *Bath Posts a Woman's Photo to Chase for the Unpaid Bill, November 23, 2009*, http://news.ifeng.com/society/2/200911/1123_344_1447469.shtml [dostęp 11.06.2019].

[108] K. Munro, *China's social credit system 'could interfere in other nations' sovereignty'*, „The Guardian" June 27, 2018.

[109] J. Karsten, D.M. West, *China's social credit system spreads to more daily transactions,* Brookings, June 18, 2018.

[110] *Data Flows, Online Privacy, and Trade Policy*, March 11, 2019, Congressional Research Service, https://crsreports.congress.gov [dostęp 11.06.2019].

Największe wątpliwości w zakresie odpowiedniego stopnia ochrony danych powoduje jednak rządowy program rozpoznawania twarzy. Praktyczne problemy, jakie on powoduje, można podzielić na dwie kategorie: te wynikające z niewystarczających zabezpieczeń techniczno-organizacyjnych doprowadzających do wycieku danych na niespotykaną dotychczas skalę oraz związane z celem i zakresem przetwarzania danych osobowych. Jednym z najbardziej jaskrawych przykładów naruszeń związanych z brakiem odpowiednich zabezpieczeń jest wyciek danych spowodowanych możliwością pobrania informacji na temat setek tysięcy obywateli ze strony internetowej niezabezpieczonej hasłem[111]. Jednocześnie wydaje się, że tego typu problem można stosunkowo łatwo wyeliminować, a przynajmniej podjąć działania zwiększające bezpieczeństwo danych. Dużo trudniej jednak będzie zmienić nastawienie władz lokalnych i ogólnopaństwowych związane z celem i zakresem przetwarzania danych pochodzących z publicznych rejestrów, w tym przede wszystkim monitoringu wizyjnego. Dotychczas wykorzystuje się je do profilowania osób pochodzących z mniejszości etnicznych[112], monitorowania lokalizacji obywateli i codziennych czynności przez nich wykonywanych (np. tankowania samochodu, kupna biletu na transport publiczny, zużywania energii elektrycznej), wszystko to w zgodzie z przyjętą ideologią kompleksowego zbierania informacji na temat każdej osoby znajdującej się w Państwie Środka[113].

Wydaje się, że mimo iż w Chinach wciąż dochodzi do poważnych ingerencji w prawo do ochrony danych osobowych i prawo do prywatności jednostki, a wielu obywateli nadal pada ofiarą nieuczciwych

[111] Z. Doffman, *China Is Using Facial Recognition To Track Ethnic Minorities, Even In Beijing*, https://www.forbes.com/sites/zakdoffman/2019/05/03/china-new-data-breach-exposes-facial-recognition-and-ethnicity-tracking-in-beijing/#5c7f70e634a7 [dostęp 15.07.2019].

[112] P. Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority,* https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [dostęp 15.07.2019].

[113] Z. Doffman, *op. cit.*

przedsiębiorców, sytuacja jest rozwojowa. Co prawda, rząd wprowadza kontrowersyjne programy i regulacje, jednak wzrasta świadomość prawna nie tylko organów ochrony prawa, ale także – co bardziej istotne – świadomość obywateli[114].

3.5. Adekwatność ochrony

Dotychczas Komisja Europejska nie wydała decyzji stwierdzającej odpowiedni stopień ochrony danych osobowych w Chinach, nie trwają również bardziej zaawansowane rozmowy między zainteresowanymi stronami. Wydaje się, że w ciągu najbliższych lat nie będzie możliwe przekazywanie danych do Chin na podstawie decyzji Komisji Europejskiej, nie tylko dlatego, że podczas gdy regulacje europejskie są w głównej mierze zorganizowane na ochronę prawa do prywatności w jej podstawowych zasadach, regulacje chińskie skupione są przede wszystkim na technicznych i organizacyjnych zabezpieczeniach[115].

Warto zauważyć, że Chiny nie spełniają już pierwszej z przesłanek określonych w art. 45 RODO. Wydaje się bowiem, że z uwagi na specyficzny system polityczny oraz stałe zagrożenie naruszenia praw człowieka nie można uznać, że jest to kraj w pełni praworządny i gwarantujący odpowiedni poziom ochrony przed naruszeniami praw człowieka. Warto podkreślić, że za gwarancjami ustawowymi w zakresie ochrony prywatności i danych osobowych nie zawsze idą efektywne narzędzia ochrony, szczególnie w sektorze publicznym. O ile bowiem sektor prywatny objęty jest dosyć szerokim katalogiem nakazów i zakazów, to jednak nie mają one zastosowania do organów administracji publicznej, która w przypadku Chin najczęściej jest sprawcą działań, które w modelu europejskim uznano by za naruszenie prawa do prywatności i bezpieczeństwa danych osobowych.

[114] M. Dong, *China*, [w:] A.C. Raul (red.), *The Privacy, Data Protection and cybersecurity Law Review,* 2017, s. 105–116.

[115] *Data Flows, Online Privacy…*

Chociaż w Chinach istnieje ustawodawstwo sektorowe w zakresie ochrony danych osobowych, wciąż brak jest porozumienia ogólnego i modelowego aktu prawnego, który w sposób kompleksowy regulowałby tę kwestię. Dotychczasowe regulacje są fragmentaryczne i rozrzucone po wielu aktach prawnych, co powoduje, że system ten nie jest kompleksowy, a co być może bardziej istotne – nieczytelny dla odbiorców zarówno tych, których dane są przetwarzane, jak i tych, którzy dane te przetwarzają. Wpływa to również na efektywność ochrony praw jednostki. Wydaje się, że dopóki Chiny nie przyjmą jednolitego modelu ochrony i odpowiednich ogólnych regulacji w tym zakresie, nie rozpoczną się znaczące rozmowy między Komisją Europejską a Państwem Środka. Brak kompleksowej regulacji sprawia, że nie można mówić o spełnieniu drugiej przesłanki art. 45 RODO.

Warto zauważyć, że chociaż Chiny podpisały szereg umów międzynarodowych w dziedzinie praw człowieka, nie wszystkie z nich zostały ratyfikowane i stały się obowiązującym w Chinach prawem. Konieczne jest również wskazanie, że międzynarodowe organizacje zajmujące się ochroną praw człowieka w swoich raportach podkreślają niski stopień ochrony praw jednostki przyznanej w przepisach krajowych i brak odpowiednich gwarancji zapewniających ich przestrzeganie[116].

Obecnie bardziej prawdopodobne niż wydanie decyzji stwierdzającej odpowiedni stopień ochrony jest zawarcie umowy gospodarczej między Komisją Europejską a Chinami, w myśl której powstanie program certyfikowania przedsiębiorców podobny do funkcjonującego już *Privacy Shield*. By się tak jednak stało, konieczna jest współpraca obu stron i podjęcie przez rząd chiński odpowiednich kroków w celu zagwarantowania pewnego minimum efektywności ochrony danych osobowych w administracji publicznej.

[116] Report of the Working Group on the Universal Periodic Review – China, 26.12.2018.

3.6. Wnioski

Chiny podobnie jak wiele państw azjatyckich wywodzi prawo do prywatności i ochrony danych osobowych z postanowień konstytucji dotyczących wolności słowa i wolności osobistej, nie zawierając jednocześnie regulacji bezpośrednio gwarantujących ochronę tych wartości. Przyjęto jednak szereg ustaw, które mają na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych w sektorze prywatnym.

Wydaje się, że chiński system ochrony danych osobowych i prywatności jest mniej efektywny niż uregulowania przyjęte w Unii Europejskiej czy Stanach Zjednoczonych. Przepisy regulujące te kwestie rozsiane są w wielu aktach prawnych, a zamiast przyjęcia jednej kompleksowej ustawy, zdecydowano się na wprowadzenie poszatkowanych, sektorowych przepisów. Brak niezależnego od rządu organu nadzoru powoduje, że w wielu przypadkach przepisy te nie są przestrzegane. Niepokoi również brak odpowiednich regulacji dotyczących przetwarzania danych osobowych w organach administracji publicznej.

Chiny wciąż nie zdecydowały, jaki model prawnej ochrony danych osobowych chcą przyjąć, czy oparty przede wszystkim na implementacji podstawowych zasad związanych z ochroną danych osobowych i prywatności, tak jak ma to miejsce w Unii Europejskiej, czy powiązać ochronę danych osobowych bezpośrednio z funkcjonowaniem gospodarki, tak jak ma to miejsce w Stanach Zjednoczonych. Wydaje się, że Państwo Środka zmierza do wykształcenia własnego, unikalnego modelu, w którym główną rolę odgrywają potrzeby administracji rządowej. W państwie tym bowiem, nad potrzebę ochrony prywatności i danych osobowych jednostki przekłada się zapewnienie bezpieczeństwa państwa i porządku publicznego, nawet w przypadkach, gdy biorąc za miarę test proporcjonalności, ingerencja w prywatność na gruncie europejskim byłaby uznana za oczywiście bezzasadną. Wytyczne przyjęte przez administrację publiczną o konieczności zbierania wszelkich informacji na temat każdej

osoby znajdującej się w zasięgu publicznej sieci monitoringu nie powodują zwiększenia bezpieczeństwa państwa, doprowadzając jedynie do nieuzasadnionej ingerencji w prawa człowieka.

4. Indie

4.1. Wstęp

Podstawą ustroju Republiki Indii jest konstytucja z 1950 r., według której Indie są demokratyczną republiką federacyjną z prezydentem jako głową państwa. Jednocześnie faktyczna władza pozostaje w rękach premiera, co powoduje, że państwo to charakteryzuje się gabinetową formą rządów. Władzę ustawodawczą sprawuje dwuizbowy parlament obradujący pod przewodnictwem wiceprezydenta. Indie określa się jako największą demokrację świata.

Chociaż indyjska konstytucja nie przyznaje wprost prawa do ochrony prywatności bądź autonomii informacyjnej jednostki, już od lat 70. XX w. indyjski Sąd Najwyższy w swoim orzecznictwie sankcjonuje istnienie tego prawa, opierając je na wynikającej z art. 19 wolności słowa i wolności osobistej przyznanej przez art. 21 konstytucji. Niezależnie od tego dotychczasowe regulacje w tym zakresie rozproszone są w wielu aktach prawnych, a zaprezentowany w 2018 r. projekt ustawy o ochronie danych osobowych[117] wciąż nie został przyjęty przez parlament. W kontekście regulacji wynikających z rozporządzenia o ochronie danych osobowych gwarancje poszanowania autonomii jednostki oraz ochrony

[117] Dalsze rozważania odnoszące się do projektowanej ustawy oparte są na tekście projektu opublikowanym na stronie indyjskiego Parlamentu, https://www.prsindia.org/sites/default/files/bill_files/Draft%20Personal%20Data%20Protection%20Bill%2C%202018%20Draft%20Text.pdf [dostęp 29.05.2019].

danych osobowych w Indiach są niezwykle istotne, biorąc pod uwagę liczbę podmiotów gospodarczych przetwarzających dane obywateli Unii Europejskiej, które korzystają z usług outsourcingu w Indiach. I chociaż wątpliwości co do adekwatności ochrony danych osobowych podniesione przez europejskich przedsiębiorców już w 2007 r. spowodowały nowelizację indyjskich przepisów w tym zakresie, brak odpowiednich gwarancji spowodował, że to raczej sektor prywatny w swoich działaniach doprowadził do podniesienia standardów ochrony danych[118].

4.2. Regulacja konstytucyjna

Prawo do prywatności czy prawo do ochrony danych osobowych nie są wprost w konstytucji przyznane osobom pozostającym pod jurysdykcją Indii. W praktyce stosowania prawa, prawo do prywatności pośrednio odczytuje się z art. 19 ust. 1 lit. a oraz art. 21 indyjskiej konstytucji[119]. Biorąc pod uwagę europejskie standardy, wydaje się, że taka interpretacja postanowień konstytucji Indii jest wykładnią, być może, zbyt daleko idącą. Artykuł 19 ust. 1 lit. a reguluje bowiem kwestię wolności słowa, kreując ją jako uprawnienie wszystkich obywateli Indii. Z kolei art. 21 odnosi się do kwestii wolności osobistej i zakazu jej naruszania w inny sposób niż przewidziany prawem.

Indyjskie sądy, dokonując wykładni rozszerzającej omawianych artykułów, sięgnęły przede wszystkim do regulacji zawartych w międzynarodowych dokumentach chroniących prawa człowieka. Posiłkując się art. 12 Powszechnej Deklaracji Praw Człowieka oraz art. 17 Międzynarodowego Paktu Praw Obywatelski i Politycznych w sprawie *Kharak Singh*,

[118] A. D'Luna Directo, *Data Protection in India: The Legislation of Self-Regulation,* „Northwestern Journal of International Law & Business", 2014, Vol. 35, Nr 1, s. 25A.

[119] V. Singh, *An analysis of personal data protection with special emphasis on current amendments and privacy bill, „*International Journal of Law and Legal Jurisprudence Studies", 2017, vol. 4, issue 1, s. 145.

indyjski Sąd Najwyższy po raz pierwszy wywiódł prawo do prywatności z art. 21 konstytucji[120]. Ogromne znaczenie w dalszej interpretacji prawa do prywatności odegrało złożone przez sędziego Subba Rao zdanie odrębne, który wskazywał, że „Prawo do wolności osobistej zawiera w sobie nie tylko prawo do swobody poruszania się, ale również oznacza, że człowiek jest także wolny od ingerencji w jego życie prywatne. Prawdą jest, że nasza [Indii – aut.] konstytucja nie przyznaje wyraźnie prawa do prywatności jako prawa podstawowego, ale wspomniane prawo jest podstawowym składnikiem wolności osobistej. Każde demokratyczne państwo szanuje życie wewnętrzne jednostki: oczekuje się od niej odpoczynku, szczęścia, spokoju i bezpieczeństwa. Dom to «forteca» każdego, naruszenie jego spokoju to ingerencja w wolność osobistą jednostki".

Podobnej interpretacji dokonano w sprawie stowarzyszenia Narodów Unii na Rzecz Swobód Obywatelskich przeciwko Indiom[121]. Gdy w 1975 r. Sąd Najwyższy ponownie rozpatrywał kwestię istnienia bądź nieistnienia gwarancji prawa do prywatności w indyjskiej konstytucji, posiłkował się anglosaską koncepcją prawa do prywatności jako prawa do bycia pozostawionemu samemu sobie (*right to be alone)*[122]. Rozpatrywana skarga Jeevan Reddy J. dotyczyła zbyt dokuczliwych środków nadzoru, co zdaniem skarżącego naruszyło jego prawo do prywatności wynikające z art. 21 konstytucji Indii[123]. W tym samym roku Sąd Najwyższy stwierdził jednak,

[120] *Right to privacy under art. 21 and related conflicts,* http://www.legalservicesindia.com/article/1630/Right-To-Privacy-Under-Article-21-and-the-Related-Conflicts.html [dostęp 28.05.2019]; warto w tym miejscu zauważyć, że posiłkowanie się uniwersalnymi aktami ustanawiającymi ochronę praw człowieka jest powszechną praktyką w indyjskich sądach, a Sąd Najwyższy w swoich orzeczeniach wskazuje, że interpretacja przepisów krajowych powinna zawsze przebiegać zgodnie z i w celu osiągnięcia standardów wynikających z aktów prawa międzynarodowego regulujących kwestię praw i wolności jednostki, zob. J. Panday, *India's Supreme Court Uphold Right to Privacy – as a Fundamental Right – and It's about Time,* https://www.eff.org/pl/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time [dostęp 28.05.2019].

[121] People's Union for Civil Liberties (PUCL) v Union of India, (1997) 1 SCC 301.

[122] *Right to privacy under…*

[123] *Ibidem.*

że chociaż zakłada, że prawo do prywatności jest prawem podstawowym, to podlega ono ograniczeniom z uwagi na ochronę interesu publicznego[124]. Prawo to może zostać ograniczone ustawą, która powinna spełniać przesłanki sprawiedliwości, uczciwości i rozsądności[125]. Uzasadnione ograniczenia mogą zostać nałożone na prawo do prywatności w interesie suwerenności i integralności Indii, bezpieczeństwa państwa, przyjaznych stosunków z obcymi państwami, porządku publicznego, przyzwoitości lub moralności, lub w związku z obrazą sądu, zniesławieniem lub podżeganiem do przestępstwa. Prawo do prywatności może być ograniczone również w przypadku istnienia dobra prawnego o wyższym znaczeniu[126] oraz może w ogóle nie dotyczyć osoby, która dobrowolnie podejmuje kontrowersyjne działania[127].

Jednocześnie prawa przyznane (lub domniemane) obywatelom w konstytucji mogą być przedmiotem skarg jedynie w relacjach jednostka–państwo, zatem nawet wzmożony aktywizm sędziowski w zakresie ochrony prywatności i danych osobowych nie jest w stanie zapewnić bezpieczeństwa tychże w relacjach między podmiotami prywatnymi[128].

W marcu 2002 r. Komisja Konstytucyjna w swoim raporcie zaleciła nowelizację konstytucji w celu dodania art. 21-B bezpośrednio gwarantującego prawo do prywatności[129]. Projektowany przepis zakłada prawo do ochrony życia rodzinnego, miru domowego i korespondencji każdego, z jednoczesnym zastrzeżeniem, że organy państwa mogą ograniczyć korzystanie z prawa do prywatności z uwagi na bezpieczeństwo

[124] Wyrok Sądu Najwyższego z dnia 18 czerwca 1975 r. *Govind vs State Of Madhya Pradesh & Anr*.

[125] Wyrok Sądu Najwyższego z dnia 25 stycznia 1978 r. *Maneka Gandhi vs Union Of India*

[126] Wyrok Sądu Najwyższego z dnia 18 marca 1975 r. *Gobind vs State Of Madhya Pradesh And Anr*.

[127] Wyrok Sądu Najwyższego z dnia 7 października 1994 r. *R. Rajagopal vs State Of T.N.*

[128] V. Singh, *op. cit.,* s. 147.

[129] Centrum Internetu i Społeczeństwa, *Privacy in India. Country Report, October 2011,* https://cis-india.org/internet-governance/country-report.pdf [dostęp 5.06.2019].

państwa, bezpieczeństwa publicznego, w celu zapobiegania lub wykrywania przestępstw, ochrony zdrowia publicznego i moralności publicznej bądź ochrony praw i wolności innych osób[130]. Projektowana nowelizacja wciąż nie została przyjęta przez parlament.

Chociaż indyjska konstytucja nie reguluje kwestii ochrony danych osobowych, a prawo do prywatności wywiedzione zostało z niej przez interpretację organów stosujących prawo, ochrona zarówno prywatności, jak i danych osobowych była gwarantowana przez akty prawne niższego rzędu. Przez wiele lat regulacja ta była szczątkowa, fragmentaryczna i rozsiana po różnych aktach prawnych.

4.3. Regulacje ustawowe

Aktem prawnym, który w najszerszym zakresie (chociaż jak wspomniano wyżej nie w sposób całościowy) reguluje kwestię ochrony prywatności, jest Ustawa o technologii informacyjnej z 2000 r. Jej nowelizacja przyjęta w 2006 r. wprowadziła do indyjskiego porządku prawnego odpowiedzialność karną i cywilną podmiotu za niewłaściwą ochronę danych osobowych[131].

Kary te mają jednak zastosowanie tylko w bardzo wąskim katalogu przypadków. Art. 43A ustawy o technologii informacyjnej wskazuje, że aby narazić się na odpowiedzialność cywilną, dany podmiot musiałby przetwarzać dane wrażliwe w systemach, które w pełni samodzielnie kontroluje, w sposób niedbały wprowadzać i zarządzać środki bezpieczeństwa i działając w złej wierze, osiągać zyski z przetwarzania danych. Zagrożone karą więzienia do lat trzech bądź grzywną jest ujawnienie danych osobowych bez zgody osoby, której one dotyczą, bądź naruszenia wiążącej umowy powstałe w wyniku działania w złej wierze.

[130] *Ibidem*.

[131] A. D'Luna Directo, *Data Protection in India…*.

W 2011 r. Minister Komunikacji i Technologii Informacyjnych Indii ogłosił do publicznej wiadomości Reguły IT dotyczące bezpieczeństwa informacji i danych osobowych[132]. W notatce prasowej wskazał, że mają one zastosowanie do wszystkich podmiotów prywatnych oraz osób przebywających na terenie Indii, których dane zostały zagrożone[133]. Jest to zbiór reguł i zaleceń dotyczących przetwarzania danych i ich ujawniania, przesyłania danych osobowych poza terytorium Indii, ochrony prywatności oraz polityki bezpieczeństwa, które w myśl Reguł IT powinny obowiązywać w każdym przedsiębiorstwie. Twórcy Reguł IT podjęli próbę skodyfikowania dotychczasowych zaleceń sądów powszechnych w zakresie ochrony danych osobowych. Jednocześnie wydaje się, że jest to dopiero pierwszy krok w zakresie zapewnienia pełnego bezpieczeństwa przetwarzanych danych osobowych.

Dopiero w 2017 r. Minister Elektroniki i Technik Informacyjnych powołał zespół do opracowania ustawy o ochronie danych osobowych, którego naczelnym celem było zapewnienie rozwoju gospodarki cyfrowej przy jednoczesnej ochronie danych osobowych obywateli[134]. Niedługo po tym Sąd Najwyższy podtrzymał swoje stanowisko w zakresie ochrony prywatności jednostki, rekomendując rządowi podjęcie kroków w celu powszechnego uregulowania kwestii ochrony danych osobowych w sposób, który weźmie pod uwagę nie tylko ochronę prywatności jednostki, ale również uzasadnione interesy państwa w tym zakresie, tworząc rozwiązania przyjazne globalnym przedsiębiorstwom[135]. Sąd Najwyższy wskazał również, że jedną ze sfer prawa do prywatności jest ochrona

[132] *Reasonable Security Practices and Procedures.*

[133] Khaitan and Co., *Data Privacy and protection law in India: Understanding the regime*, http://www.lexology.com/library/detail.aspx?g=5e567142-bd88-4c00-a1ea-71203e02614d [dostęp 4.06.2019].

[134] Trilegal, *The personal data protection bill, 2018,* https://www.trilegal.com/pdf/create.php?publication_id=15&publication_title=the-personal-data-protection-bill-2018 [dostęp 29.05.2019].

[135] Wyrok Sądu Najwyższego z dnia 24 sierpnia 2017 r. *K.S. Puttaswamy and Anr. v. Union of India and Ors.*

tożsamości jednostki, z której to wywiedziono konieczność ochrony danych osobowych jednostki. W momencie pisania niniejszego opracowania (wrzesień 2019 r.) zaprezentowana 27 lipca 2018 r. ustawa o ochronie danych osobowych nie została jeszcze przyjęta przez parlament, jednak jej projekt jest szeroko komentowany przez teoretyków i praktyków prawa.

Przyjmuje się, że nowa, kompleksowa regulacja w zakresie ochrony danych osobowych w znacznej części wzorowana jest na modelu wdrożonym przez RODO[136], zachowując pewne odrębności charakterystyczne dla Indii[137]. Twórcy projektu w swoim raporcie wskazują przede wszystkim, że w odróżnieniu od powszechnego na świecie założenia o nieszkodliwości przepływu transgranicznego danych, w Indiach przyjęto koncepcję, wedle której przepływ ten może wywołać znaczne szkody[138]. Skrytykowano również stawianie interesów globalnych przedsiębiorstw ponad interesem jednostki, którego przykładem miałyby być używane powszechnie pojęcia podmiotu danych osobowych oraz administratora danych[139].

[136] P. Anand, V. Luniya, *Understanding the Personal Data Protection Bill, 2018 and Bracing for Impact,* https://www.livelaw.in/law-firms/understanding-the-personal-data-protection-bill-2018-and-bracing-for-impact-142034 [dostęp 29.05.2019]; Nishith Dessai Associates, *New Data Protection Law Proposed in India! Flavors of GDPR*, http://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA_Summary.pdf [dostęp 29.05.2019].

[137] Np. do kategorii wrażliwych danych osobowych zalicza się informacje na temat przynależności kastowej lub plemiennej, status transpłciowy czy status międzypłciowy.

[138] 58.60.Committee of Experts under the Chairmanship of Justice B.N. SrikrishnaKomitet Ekspertów pod przewodnictwem sędziego B.N. Srikrishna, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018.pdf [dostęp 29.05.2019].

[139] W projekcie ustawy posłużono się terminami *data principal* oraz *data fiduciary*. O ile przeniesienie na grunt polski tego drugiego pojęcia nie przysparza większych trudności i wydaje się, że z powodzeniem można używać pojęcia „powiernika danych", to w przypadku znanego w Polsce określenia podmiotu danych osobowych sprawa nie jest taka prosta. W uzasadnieniu do projektu ustawy jej twórcy w sposób wyraźny i krytyczny odnieśli się do pojęcia *data subject*, które to w Polsce tłumaczymy jako podmiot danych osobowych, zatem niezasadne byłoby posługiwanie się nim w niniejszym opracowaniu. Inspirując się lemowskim słowotwórstwem, biorąc pod uwagę stosunek prawny powierzenia (łac. *Fiducia*), wydaje się, że najtrafniejsze byłoby używanie pojęcia „podmiotu powierzającego dane" i tak też czynimy w niniejszym opracowaniu.

Przetwarzanie danych przez powierników danych powinno być dozwolone jedynie wtedy, gdy służy to zrealizowaniu oczekiwań podmiotów powierzających dane w sposób służący dobru publicznemu oraz wolnej gospodarce cyfrowej. Zdaniem twórców projektu wdrożenie tej zasady umocni autonomię jednostki oraz pozwoli na pełne wykorzystywanie przepływu danych. Jednym z przepisów projektu ustawy, które mają dążyć do zrealizowania tego celu, jest prawo podmiotu powierzającego dane do przeniesienia danych od jednego powiernika do drugiego w przypadkach określonych w projekcie ustawy. Głównym założeniem projektu jest zachowanie równowagi między interesami jednostki, podmiotów gospodarczych i państwa, co zdaniem autorów w znacznym stopniu różni się od koncepcji wypracowanych w Stanach Zjednoczonych, Unii Europejskiej, Chinach i może być podstawą do stworzenia własnego, centroazjatyckiego modelu ochrony danych osobowych.

Projektowana ustawa dotyczy danych osobowych, które zostały zebrane, ujawnione, współdzielone bądź w inny sposób przetwarzane na terytorium Indii, bądź danych, które przetwarzane są przez rząd, obywateli Indii lub jakichkolwiek podmiotów prywatnych albo publicznych powstałych zgodnie z przepisami indyjskiego prawa. Zakres terytorialny stosowania ustawy jest zatem dosyć szeroki – dotyczy bowiem nie tylko podmiotów mających siedzibę w Indiach, ale również każdego, kto przetwarza dane na terytorium państwa, oraz podmiotów, które, co prawda, mają siedzibę w Indiach, ale dane przetwarzają w innych jurysdykcjach.

W myśl projektowanej ustawy przetwarzanie danych osobowych obywateli Indii może odbywać się jedynie za ich zgodą, chyba że przetwarzanie jest niezbędne do realizacji funkcji pełnionych przez organy ustawodawcze bądź wykonawcze w celu realizacji potrzeb obywateli; lub gdy wymaga tego zdrowie jednostki, zagrożenie zdrowia publicznego lub naruszenie porządku publicznego; lub gdy jest to niezbędne w celu realizacji obowiązków wynikających ustawy bądź orzeczenia sądu; lub

w innych celach określonych przez inspektora ochrony danych osobowych w celu przeciwdziałania oszustwom bądź ściągnięcia długów. Przetwarzanie danych wrażliwych dozwolone jest jedynie w przypadku wyraźnej zgody podmiotu powierzającego dane, gdy jest to niezbędne do wykonania zadań władzy ustawodawczej bądź wykonawczej w celu odpowiedzi na potrzeby obywateli lub gdy jest to niezbędne do wywiązania się z obowiązku wynikającego z ustawy bądź orzeczenia sądu.

Przesyłanie danych osobowych poza teren Indii jest dozwolone jedynie w przypadku, gdy rząd uzna transfer do danego kraju za dozwolony lub gdy inspektor ochrony danych osobowych wyda zgodę na transfer danych w przypadku zaistnienia stanu wyższej konieczności.

Projekt ustawy zakłada również powołanie centralnego organu (inspektora ochrony danych osobowych) składającego się z przewodniczącego oraz sześciu członków, którzy powinni wyróżniać się co najmniej 10-letnim doświadczeniem w zakresie ochrony danych osobowych i technologii informacyjnych. Ten nowy w indyjskim systemie prawnym organ będzie zobowiązany do monitorowania przestrzegania obowiązków związanych z ochroną danych osobowych i ich egzekwowania, prowadzenia badań i budowania świadomości społecznej, tworzenia standardów i rekomendacji oraz rozpatrywania skarg podmiotów powierzających dane. Naruszenie przepisów projektowanej ustawy ma być zagrożone karą finansową w wysokości do 5% globalnego obrotu podmiotu gospodarczego.

Na marginesie można tylko dodać, że już w 2006 r. pod głosowanie parlamentu Indii została poddana ustawa o ochronie danych osobowych, która w znaczny sposób nawiązywała do ówcześnie obowiązującej w Unii Europejskiej dyrektywy, jednak do dzisiaj nie została ona przyjęta. Pozostaje więc pytanie, czy nowy projekt ustawy o ochronie danych osobowych podzieli los swojej poprzedniczki i czy indyjski parlament gotowy jest na zmiany w tym zakresie.

4.4. Praktyka

Chociaż wciąż brak jest pełnej kodyfikacji prawa ochrony danych osobowych, rząd indyjski coraz częściej podejmuje działania w celu zwiększenia bezpieczeństwa przetwarzanych danych, chociażby przez nowelizację wspomnianej już ustawy o technologiach informacyjnych. Bez wątpienia jednak to orzecznictwo sądów powszechnych ma największy wpływ na bezpieczeństwo danych osobowych przetwarzanych przez podmioty prowadzące działalność gospodarczą w Indiach. Warto zauważyć, że nie tylko sądy wpływają na efektywność prawa do ochrony danych osobowych, ale również rozmaite organy ochrony praw obywateli, które na co dzień zapewniają odpowiednią ochronę przez nakładanie kar na podmioty publiczne i prywatne. Przykładem takich działań jest nałożenie przez komisję ds. sporów konsumenckich kary na Airtel – Stowarzyszenie Operatorów Komórkowych kary w wysokości Rs. 75 lakhs (blisko 100 tysięcy euro) w związku ze skargami konsumentów na prześladowanie przez agresywne i natarczywe telefony i SMS-y telemarketingowe[140]. Sąd Najwyższy nakazał Bankowi Rezerw Indii wdrożenie odpowiednich procedur w celu wyeliminowania połączeń telefonicznych z ofertami telemarketingowymi na podstawie stwierdzenia naruszenia prawa do prywatności[141].

Przez wiele lat dużym problemem w Indiach (który wciąż występuje, chociaż zostały podjęte działania w celu jego zminimalizowania) były przestępstwa związane z kradzieżą tożsamości. Przykładowo w grudniu 2004 r. czterech pracowników *call center* wykradło dane i hasła do kont bankowych czterech klientów CitiGroup. Otworzyli oni nowe konta w indyjskim banku i dopuścili się kradzieży blisko 250 tysięcy

[140] S. Ardhapurkar, T. Srivastava, S. Sharma, V. Chaurasiya, A. Vaish, *Privacy and Data Protection in Cyberspace in Indian Environment, „I*nternational Journal of Engineering Science and Technology" 2010, Vol. 2(5), s. 945.

[141] V. Sharma, *White Paper on Privacy Protection in India,* http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf [dostęp 4.06.2019].

dolarów[142]. W 2005 r. policja odzyskała 230 tysięcy, a sprawcy zostali ukarani. W 2010 r. nałożono na ICICI Bank karę w wysokości 18,5 tysiąca dolarów za dopuszczenie do przecieku danych, który w konsekwencji doprowadził do kradzieży środków znajdujących się na kontach ich klientów[143]. Sąd wskazał na brak wdrożenia odpowiednich procedur, w tym przede wszystkim dwustopniowej autoryzacji, które to doprowadziły do finansowej straty powodów. Rok później na ten sam bank z tych samych powodów nałożono karę finansową w wysokości 35 tysięcy dolarów[144].

Niepokojący jest jednak fakt, że w incydentach naruszenia prywatności biorą również udział organy administracji publicznej. W połowie listopada 2010 r. dwie czołowe gazety opublikowały podsłuch telefoniczny rozmowy między Nirą Radią, znaną lobbystką korporacyjną, a kilkoma wpływowymi Indusami, w tym szefami kilku potężnych firm medialnych i korporacji[145]. Rozmowy te zostały nagrane w trakcie dochodzenia prowadzonego przez Departament Podatku Dochodowego i są powszechnie znane jako dowód obnażający nieetyczne związki między biznesem, mediami i polityką w Indiach. Jeden z przedsiębiorców nagranych na taśmach złożył skargę do sądu, domagając się wydania tychże taśm z powodu naruszenia jego prawa do prywatności. Sprawa wywołała głośną dyskusję w całych Indiach na temat granic inwigilacji obywateli i warunków, jakie muszą zostać spełnione, żeby była ona dozwolona.

W ostatnich latach wzrosła nie tylko świadomość społeczna, ale również mediów w tym zakresie. Poszczególni nadawcy do swoich reguł

[142] Anon, *The MphasiS Scandal – And How it Concerns U.S. Companies Considering Offshore BPO*, http://www.carretek.com/main/news/articles/MphasiS_scandal.htm [dostęp 6.06.2019], zob. również: *idem*, *MphasiS case: BPOs feel need to tighten security. Indian Express,* http://www.expressindia.com/news/fullstory.php?newsid=44856 [dostęp 6.06.2019].

[143] *Umashankar v. ICICI Bank, Tuticorin*, (2010), http://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf [dostęp 6.06.2019].

[144] *Thomas Raju v. ICICI Bank, Anna Nagar*, (2011), http://www.naavi.org/cl_editorial_11/civil_jurisdiction_3_16052011.pdf [dostęp 6.06.2019].

[145] Privacy In India – Country Report – October 2011, https://cis-india.org/internet-governance/country-report.pdf [dostęp 6.06.2019].

i polityk dodają postanowienia związane z ochroną prywatności swoich odbiorców oraz podejmowaniem działań edukacyjnych na rzecz bezpieczeństwa danych osobowych[146]. W 2011 r. jeden z publicznych nadawców został ukarany karą w wysokości blisko 1500 dolarów za naruszenie prywatności odbiorców przez podżeganie ich na wizji do ujawnienia swojej orientacji i tożsamości seksualnej. Nadawca dzwonił pod numery telefonów osób zarejestrowanych na portalu dla homoseksualistów, a prezenterzy prowadzili rozmowę telefoniczną w sposób, który miał zapewnić publiczne ujawnienie swojej tożsamości na żywo w telewizji[147].

W ostatnich latach kontrowersje wzbudza również projekt Aadhaar, którego celem jest zbieranie informacji na temat obywateli w jednym miejscu oraz nadawanie obywatelom i osobom przebywającym na terytorium Indii indywidualnego numeru, który miałby być przez nich używany każdorazowo w kontaktach z administracją publiczną. Numer Aadhaar, co prawda, nie jest wystarczający, żeby w pełni zidentyfikować określoną osobę, ale jest on połączony z numerem telefonu, konta bankowego czy prawa jazdy[148]. Program ten wzbudził również wątpliwości Międzynarodowego Komitetu Praw Człowieka, który wezwał w sierpniu 2019 r. władze Indii do odpowiedzenia w raporcie okresowym w 2020 r. na zarzuty organizacji społecznych związanych z jego funkcjonowaniem[149]. Przede wszystkim Komitet wskazuje na liczbę naruszeń w zakresie ochrony danych przetwarzanych w ramach projektu Aadhaar, które prowadziły do wycieku ogromnej ilości danych. Komitet zażądał również wyjaśnień

[146] *Ibidem*.

[147] P. Iyengar, *News Broadcasting Standards Authority Censures Tv9 Over Privacy Violations! Privacy india*, http://privacyindia.org/2011/03/25/news-broadcasting-standards-authority-censures-tv9- over-privacy-violations [dostęp 6.06.2019].

[148] V. Sridhar, T.K. Srikanth, *As Aadhaar project enters a critical year, here are the worries that still remain*, //economictimes.indiatimes.com/articleshow/62656100.cms?-from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst [dostęp 28.09.2019].

[149] List of issues prior to submission of the fourth periodic report of India, 22.08.2019.

w związku z możliwością dostępu do nagrań z kamer przemysłowych bez zgody odpowiedniego organu.

Niezależnie od działań podejmowanych przez sądy i inne organy publiczne, szczególne znaczenie w zakresie ochrony danych osobowych mają podmioty prywatne. W 2017 r. rynek usług outsourcingowych w Indiach był wart 170 bilionów dolarów[150]. Stanowi on jedną z największy sił napędowych indyjskiej gospodarki. Wśród kluczowych korzyści związanych z przenoszeniem części działalności przedsiębiorstwa do Indii wymienia się redukcję kosztów[151]. Jednocześnie od lat zachodnie przedsiębiorstwa zwracają uwagę nie tylko na potencjalne oszczędności, ale również na odpowiedni stopień zabezpieczeń, których wymagają od swoich kontrahentów[152]. Brak całościowej regulacji prawnej w tym zakresie w Indiach stanowi poważny problem, który obok różnic kulturowych[153] jest jedną z głównych przyczyn złej prasy, która dotyka tę gałąź gospodarki[154], a co za tym idzie – powolnego wycofywania się zachodnich przedsiębiorstw z indyjskiej jurysdykcji[155].

Dostrzegając te zagrożenia, indyjskie przedsiębiorstwa zajmujące się outsourcingiem, działając wspólnie, podjęły działania samoregulacyjne w celu zapewnienia odpowiedniego poziomu ochrony danych

[150] R. Sachitanand, *India's $150 billion outsourcing industry stares at an uncertain future,* https://economictimes.indiatimes.com/articleshow/56543653.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst [dostęp 29.05.2019].

[151] S.Z. Haque, *IT Outsourcing Services in India and the Lesson It Teaches Us,* https://www.indusnet.co.in/it-outsourcing-services-in-india-and-its-lessons/ [dostęp 29.05.2019].

[152] A. D'Luna Directo, *Data Protection in India…,* s. 21.

[153] K. Wartburton, *5 Key Cultural Issues when Outsourcing to India*, https://www.linkedin.com/pulse/5-key-cultural-issues-when-outsourcing-india-keith-warburton/ [dostęp 29.05.2019].

[154] S. Overby, *Eight reasons why Outsourcing to India Could Hurt Your Business*, https://www.cio.com/article/2437890/eight-reasons-why-outsourcing-to-india-could-hurt-your-business.html [dostęp 29.05.2019].

[155] *On the Turn: India is No Longer the Automatic Choice for IT Services and Back-Office Work*, ECONOMIST (Jan. 17, 2013), http://www.economist.com/news/special-report/21569571-india-no-longerautomatic-choice-it-services-and-back-office-work-turn?zid=292&ah=165a5788fdb0726c01b137 4d8e1ea285 [dostęp 30.05.2019].

osobowych. Inicjatywa NASSCOM[156] obejmuje stworzenie pozarządowego stowarzyszenia Bezpieczeństwa Danych Indii (*Data Security of India – DSCI),* które zajmuje się tworzeniem zaleceń, przewodników, rekomendacji, prowadzeniem działań edukacyjnych w celu zwiększenia bezpieczeństwa cyberprzestrzeni, świadomości w zakresie bezpieczeństwa informacji i danych osobowych oraz ochrony prywatności[157]. Organizacja współpracuje z organami administracji publicznej, agencjami rządowymi, związkami przedsiębiorców oraz innymi organizacji pozarządowymi. Oczywiste jest, że ich działania nie mają mocy prawnej, a co za tym idzie w praktyce nie mogą być w pełni egzekwowane, zatem od wielu lat sami przedsiębiorcy postulują wprowadzenie zmian ustawowych w tym zakresie.

Bez wątpienia, największą przeszkodą dla indyjskich przedsiębiorców przed pełnym wykorzystaniem potencjału gospodarczego rynku Unii Europejskiej jest kwestia przepływu danych między dwoma kontynentami. Dotychczas nie udało się wypracować kompromisu w tym zakresie przez Unię Europejską i rząd Indii, a Indie wciąż nie zostały uznane przez Komisję Europejską za kraj zapewniający odpowiednią ochronę danych osobowych.

4.5. Adekwatność ochrony

Zmiany w dziedzinie prawa do prywatności w Indiach w ostatnich latach oraz wciąż rozwijający się rynek usług zachęcają europejskich przedsiębiorców do prowadzenia chociaż części interesów w tym kraju. Jednocześnie, jak już zostało wspomniane, brak kompleksowych regulacji w tej

[156] Indyjskie stowarzyszenie branżowe technologii informatycznych i oprogramowania komputerowego. Powstało w 1988 r. z siedzibą w New Delhi. Działa na zasadach *non-profit*, a finansowane jest przez przemysł IT. Zrzesza 1500 członków, którymi głównie są firmy stanowiące 95% przychodów branży informatycznej.

[157] https://www.dsci.in/content/about-us#about_section [dostęp 30.05.2019].

dziedzinie powoduje uzasadnione obawy związane z bezpieczeństwem danych osobowych przetwarzanych w Indiach. Sytuację komplikuje fakt, że dotychczas Komisja Europejska nie wydała odpowiedniej decyzji stwierdzającej adekwatność ochrony danych osobowych w Indiach i zezwalającej na w miarę swobodny przepływ danych między krajami. Oczywiście, przedsiębiorcy mogą korzystać z innych narzędzi dozwolonych przez rozporządzenie ogólne o ochronie danych osobowych, jednak stwierdzenie adekwatności ochrony przez Komisję Europejską jest zdecydowanie najprostszym i najbezpieczniejszym sposobem transferu danych.

W 2010 r. Unia Europejska opublikowała raport dotyczący adekwatności ochrony danych osobowych w Indiach, który następnie został w bardzo obszerny sposób skomentowany przez NASSCOM. Unia Europejska stwierdziła już wtedy brak możliwości uznania Indii za kraj posiadający adekwatny stopień ochrony danych osobowych z uwagi na wielorakie odrębności w tym zakresie[158]. W raporcie z 2010 r. podkreślono, co prawda, wysiłki sądów powszechnych w celu zagwarantowania ochrony prawa do prywatności w drodze wykładni prawa, ale jednocześnie podkreślono, że prawo to nie jest *per se* chronione na gruncie konstytucyjnym. Wskazano również brak obowiązku przetwarzania danych z poszanowaniem zasady proporcjonalności, niemożność skutecznego egzekwowania praw przed podmioty danych osobowych (o ile te prawa w ogóle zostały przyznane), brak gwarancji odpowiednich zabezpieczeń technicznych i organizacyjnych, niejasne regulacje związane z przetwarzaniem danych wrażliwych i niedostateczny stopień ich ochrony, brak kompletnych regulacji w zakresie wykorzystywania danych w celach marketingowych oraz brak odpowiednich organów nadzorujących i egzekwujących przepisy związane z ochroną danych osobowych. W konkluzji wskazano, że Indie obecnie nie zapewniają odpowiedniej ochrony danych osobowych zarówno w sektorze publicznym, jak i prywatnym oraz nie spełniają

[158] NASSCOM, *Whitepaper EU Adequacy Assessment of India*, https://www.dsci.in/sites/default/files/White_Paper_EU_Adequacy_Assessment_of_India.pdf [dostęp 5.06.2019].

przesłanek określonych przez Grupę roboczą art. 29. Bardziej pozytywnie oceniono niektóre aspekty niezależności organów i dostępne środki zaradcze. Jednocześnie Indie wciąż nie przyjęły kompleksowej regulacji w tym zakresie i chociaż odpowiednie kroki zostały podjęte, wciąż nie gwarantuje się odpowiedniej ochrony danych osobowych[159].

Trzeba wskazać, że działania w celu wzmocnienia współpracy gospodarczej, w tym osiągnięcia porozumienia w zakresie przepływu danych osobowych między Unią Europejską a Indiami są podejmowane przez obie zainteresowane strony. W 2019 r. Ministerstwo Elektroniki i Technologii Informacyjnej powołało grupę ekspertów ds. bezpieczeństwa w celu rozwiązania problemów związanych z technologiami informatycznymi i technologiami informatycznymi dotyczącymi adekwatności bezpieczeństwa danych w Unii Europejskiej i ułatwienia dostępu do rynku UE dla indyjskich przedsiębiorców z branży informatycznej[160]. Już rok wcześniej odbyły się spotkania wspólnej grupy roboczej ds. wspólnych technologii informacyjnych i komunikacyjnych Indii i UE (ICT), która jest również kierowana przez Ministerstwo Elektroniki i Technologii Informacyjnej, w ramach której zorganizowane zostały szkolenia i warsztaty na temat rozporządzenia ogólnego o ochronie danych osobowych[161]. Warto odnotować, że indyjska Rada Ochrony Danych Osobowych we współpracy z NASSCOM stworzyła specjalną linię telefoniczną, gdzie konsultanci odpowiadają na pytania przedsiębiorców związane z ochroną danych w Unii Europejskiej[162].

[159] *Ibidem.*

[160] Press Information Bureau Government of India Ministry of Commerce & Industry, *Data-Adequacy Status for Indian Companies,* http://www.pib.nic.in/Pressreleaseshare.aspx?PRID=1562523 [dostęp 5.06.2019].

[161] *Ibidem.*

[162] S. Agarwal, *Europe's data protection law may have severe implications for India's IT industry,* https://economictimes.indiatimes.com/articleshow/63741020.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst [dostęp 5.06.2019].

4.6. Wnioski

Analizując dokonane powyżej rozważania, można stwierdzić, że Indie nie zapewniają adekwatnego poziomu ochrony danych osobowych w rozumieniu rozporządzenia ogólnego o ochronie danych osobowych. Brak gwarancji konstytucyjnych oraz kompleksowego uregulowania w aktach prawnych niższego rzędu powoduje niepewność prawa po stronie obywateli państwa. Jednocześnie, jak pokazuje dotychczasowa praktyka, judykatywa z powodzeniem wywodzi prawo do ochrony prywatności i danych osobowych z dotychczas istniejących przepisów.

Charakterystyczny dla Indii ogromny rynek usług outsourcingowych powoduje, że prywatni przedsiębiorcy sami wymuszają odpowiednie zmiany w tym zakresie. Silne związki gospodarcze z przedsiębiorstwami zarejestrowanymi w krajach Unii Europejskiej powodują, że nawet w przypadku braku regulacji ustawowej, związki przedsiębiorców indyjskich dokonują swoistej samoregulacji. Nie można również zapominać o wpływie umów gospodarczych zawieranych między przedsiębiorcami z Indii i Unii Europejskiej – często to właśnie europejskie podmioty zamawiające w swoich umowach wymuszają zmiany w zakresie zabezpieczeń technicznych i organizacyjnych danych osobowych, tak aby przetwarzać dane zgodnie z wytycznymi RODO.

Wydaje się, że to właśnie podmioty gospodarcze będą siłą napędową zmian, które czekają Indie w tym zakresie. Jednocześnie można obawiać się braku tożsamego poziomu ochrony różnych kategorii danych. I chociaż trudno spodziewać się wydania przez Komisję Europejską decyzji stwierdzającej adekwatny poziom ochrony danych osobowych (głównie z powodu opieszałości parlamentu indyjskiego w pracach nad kompleksową regulacją), to dane osobowe są i będą przetwarzane na terytorium Indii z wykorzystaniem innych mechanizmów transferu.

5. Japonia

5.1. Wstęp

Japonia jest monarchią parlamentarną, z dwuizbowym parlamentem ukształtowanym w czasach okupacji amerykańskiej. Warto zauważyć, że jest to jeden z nielicznych krajów na świecie, który utrzymał konstytucję narzuconą przez okupanta. Gabinet jest wybierany przez zgromadzenie narodowe i to jego członkowie faktycznie pełnią władzę wykonawczą, podczas gdy cesarzowi przysługują jedynie funkcje reprezentacyjne. Japonia na całym świecie słynie z wysokiej kultury służby cywilnej, opartej na merytokracji i apolityczności. Jej członkowie stanowią urzędniczą elitę państwową, która gwarantuje ciągłość jego działania.

Specyfika społeczno-kulturowa Japonii sprawia, że obywatele Kraju Kwitnącej Wiśni przez wiele lat nie byli szczególnie zainteresowani ochroną ich prawa do prywatności w rozumieniu europejskim. Co więcej, nadmierna dbałość o zakres informacji udostępnianych publicznie może być przez resztę społeczeństwa uznawana za wyraz nieufności. Biorąc jednak pod uwagę, że obecnie obowiązująca konstytucja Japonii została uchwalona podczas okupacji amerykańskiej, uwarunkowanie kulturowe nie miało zbytniego wpływu na fakt nieumiejscowienia prawa do prywatności w katalogu praw podstawowych ustawy zasadniczej.

Chociaż japońska konstytucja nie zawiera postanowień wprost przyznających jednostce prawa do prywatności lub prawa do ochrony danych osobowych, Japonia była jednym z pierwszych państw Azji,

które dokonało pełnej kodyfikacji w tym zakresie. Model wykształcony w tym państwie jest w wielu aspektach niemal tożsamy z modelem przyjętym w Unii Europejskiej. Nie powinno więc dziwić, że to właśnie to państwo jako pierwsze od wejścia w życie rozporządzenia ogólnego o ochronie danych osobowych zostało uznane za kraj zapewniający adekwatny stopień ochrony danych osobowych. Co więcej, po raz pierwszy w historii decyzja Komisji Europejskiej była poparta dwustronną umową między Japonią a Unią Europejską, w której to strony wzajemnie uznały adekwatność regulacji dotyczącej ochrony danych osobowych.

5.2. Regulacja konstytucyjna

Ukształtowanie społeczno-kulturowe Japonii wpływa znacząco na rozumienie prawa do prywatności w tym państwie. Specyficzne dla tej kultury silne związki między członkami danej społeczności odrzucają zachodnie i europejskie rozumienie prawa do prywatności jako prawa do pozostawania w samotności jako wskazujące na brak współpracy i niezdolność komunikowania się z innymi[163]. Prawo do prywatności jako prawo do kontrolowania obiegu informacji na swój temat uważane jest zarówno za nadmiar nieufności wobec społeczeństwa, jak i podmiotów zbierających, przetwarzających oraz przechowujących dane[164]. W związku z tym poczucie prywatności w społeczeństwie japońskim nie jest tak istotne jak dla obywateli Starego Kontynentu[165]. Jednocześnie wskazuje się, że wraz z rozwojem nowych technologii i znaczenia społeczeństwa informacyjnego, stosunek do prawa do prywatności wśród obywateli

[163] Y. Orito, K. Murata, *Privacy Protection in Japan: Cultural Influence on the Universal Value,* http://www.kisc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf [dostęp 6.06.2019].

[164] *Ibidem.*

[165] *Ibidem.*

Japonii ewoluuje i z każdym rokiem coraz bardziej zależy im na ochronie informacji na swój temat[166].

Konstytucja Japonii nie odnosi się wprost do ochrony prawa do prywatności bądź ochrony danych osobowych. Dotychczasowe orzecznictwo sądów powszechnych poszukuje tych praw w art. 13 ustawy zasadniczej, który stanowi: „Wszystkich obywateli szanuje się jako jednostki ludzkie. Ich prawa do życia, wolności i dążenia do szczęścia, o ile nie pozostają w sprzeczności z dobrem publicznym, brane są w najwyższym stopniu pod uwagę w działalności ustawodawczej i innych poczynaniach państwa". Już w 1964 r. wskazywano na ochronę prywatności jako prawa wynikającego z konstytucji Japonii, wskazując że podanie informacji na temat osoby fizycznej do publicznej wiadomości stanowi naruszenie jej prywatności[167]. Ponadto, już wtedy wskazano, że nawet osoby publiczne, takie jak politycy, zachowują prawo do prywatności życia rodzinnego i prywatnego, wolnego od sfery publicznej[168].

W wyroku z 1969 r. Sąd Najwyższy Japonii uznał prawo do prywatności i ochrony danych osobowych za prawo konstytucyjne[169]. W 1965 r. studenci Uniwersytetu Ritsumeikan w Kioto zorganizowali marsz protestacyjny bez odpowiednich zezwoleń. Podczas demonstracji policjant zrobił zdjęcia uczniów zaangażowanych bezpośrednio w demonstrację oraz zgromadzonych wokół niej. Pomimo protestów jednego z fotografowanych, policjant nie zaprzestał robienia zdjęć, co doprowadziło ostatecznie do złożenia pozwu przez potencjalnie pokrzywdzonego. Sąd orzekł

[166] A.A. Adams, K. Murata, Y. Orito, *The Japanese Sense of Information Privacy*, http://www.a-cubed.info/Publications/The_Japanese_Sense_of_Information_Privacy.pdf [dostęp 6.06.2019].

[167] Wyrok Sądu Okręgowego w Tokio z dnia 28 września 1964 r. (Showa 36), (Wa) No. 1882.

[168] Warto wspomnieć, że wyrok został wydany w wyniku pozwu złożonego przez Hachiro Arita, który bez swojej zgody został głównym bohaterem książki *Utage no ato/After the Banquet* wydanej w 1961 r. przez Yukio Mishima.

[169] Sąd Najwyższy, wyrok Wielkiej Ławy z dnia 24 grudnia 1969 r., Keishu, tom 23, nr 12, s. 1625.

przeciwko twierdzeniom protestujących o naruszeniu prywatności, wskazując na brak odpowiedniego zezwolenia na zorganizowanie manifestacji, wskazując jednocześnie, że w innych okolicznościach robienie zdjęć bez zgody fotografowanej osoby narusza jej prawo do prywatności. Sąd uznał również prawo każdej osoby fizycznej do ochrony dotyczących jej informacji osobowych przed ich ujawnieniem osobie trzeciej lub podaniem do wiadomości publicznej bez ważnego powodu.

Kilkanaście lat później do katalogu orzeczeń sankcjonujących istnienie prawa do prywatności w Japonii dodano uznanie prawa do nieudostępniania informacji na temat przeszłości kryminalnej jednostki do publicznej wiadomości[170]. Z kolei w 1984 r. sąd w Tokio stwierdził, że każdy ma prawo do sprawdzania i poprawiania danych osobowych zbieranych na swój temat[171].

Na początku XXI w. ten sam sąd wskazał, że „wolność obywateli w życiu prywatnym jest chroniona przed sprawowaniem władzy publicznej i może być ona postrzegana jako jedna z wolności osoby fizycznej w życiu prywatnym, a każda osoba fizyczna ma prawo do ochrony dotyczących jej informacji osobowych przed ich ujawnieniem osobie trzeciej lub podaniem do wiadomości publicznej bez ważnego powodu"[172].

Pomimo jednolitej linii orzeczniczej, komisja konstytucyjna Japonii wskazuje na konieczność nowelizacji ustawy zasadniczej w taki sposób, aby wprost przyznawała osobom fizycznym prawo do prywatności rozumianego jako prawo decydowania, jakie informacje na jej temat powinny być podane do wiadomości publicznej[173]. Członkowie komisji konstytucyjnej zwracają również uwagę na ogromną rolę mediów w ochronie

[170] 14th April 1981 (Showa 56), Third Petty Bench of the Supreme Court Adjudication.

[171] Tokyo District Court, 1982 (Showa 57), (Wa) No. 3.

[172] Sąd Najwyższy, wyrok z dnia 6 marca 2008 r., Minshu, t. 62, nr 3, s. 665.

[173] *Handbook on the Research Report on the Constitution of Japan*, Research Commission on the Constitution House of Councillors JAPAN 2005, http://www.sangiin.go.jp/eng/report/ehb/ehb.pdf [dostęp 7.06.2019].

prawa do prywatności oraz duże skutki społeczne jej naruszenia przez *mass media*.

Należy również wspomnieć, że chociaż konstytucja Japonii nie przyznaje wprost prawa do prywatności ani swoim obywatelom, ani innym osobom fizycznym, państwo to jest stroną wielu umów i paktów międzynarodowych, które nakładają na nie obowiązek poszanowania prywatności jednostki. Wśród nich dość wymienić Powszechną Deklarację Praw Człowieka czy Międzynarodowy Pakt Praw Obywatelskich i Politycznych.

5.3. Regulacje ustawowe

Japonia jako jedno z pierwszych państw azjatyckich, pomimo braku regulacji konstytucyjnoprawnych, przyjęła przepisy mające zagwarantować efektywne prawo ochrony danych osobowych[174]. Obecnie w Japonii obowiązują trzy ustawy w zakresie ochrony danych osobowych, wszystkie przyjęte w maju 2003 r. i kilkukrotnie nowelizowane. Są to: ustawa o ochronie informacji osobowych[175], ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji[176] i ustawa o ochronie informacji osobowych znajdujących się w posiadaniu niezależnych agencji administracyjnych[177].

Dwa ostatnie akty (zmienione w 2016 r.) zawierają przepisy mające zastosowanie do ochrony danych osobowych przez podmioty sektora publicznego i nie mają do nich zastosowania postanowienia decyzji

[174] *Asia Pacific Data Protection and Cyber Security Guide 2018. Shifting landscapes across the Asia-Pacific region,* https://www.jdsupra.com/legalnews/asia-pacific-data-protection-and-cyber-77787/ [dostęp 6.06.2019].

[175] Act on the Protection of Personal Information Act No. 57 of (2003).

[176] Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003).

[177] Act on the Protection of Personal Information Held by Administrative Organs, Act No. 58 of May 30, 2003.

Komisji Europejskiej w sprawie uznania adekwatności ochrony[178]. Ostatnia nowelizacja ustawy o ochronie informacji osobowych weszła w życie 30 maja 2017 r. Do definicji danych osobowych dodano bowiem numery identyfikacyjne, którymi posługują się osoby pozostające na terytorium Japonii, wprowadzono obostrzenie w stosunku do małych przedsiębiorców (zatrudniających do 5 tysięcy pracowników), przetwarzających dane osobowe swoich pracowników, zobowiązano przedsiębiorców przetwarzających dane osobowe poza terytorium Japonii do uzyskania wyraźnej zgody podmiotu danych osobowych na przetwarzanie poza granicami państwa danych wrażliwych, wprowadzono obowiązek prowadzenia rejestrów przetwarzania danych osobowych oraz zgłaszania wszelkich naruszeń i potencjalnych naruszeń bezpieczeństwa danych osobowych[179]. Regulacje te są łudząco podobne do przepisów ogólnego rozporządzenia o ochronie danych osobowych.

Decyzją Rady Ministrów przyjętą 12 czerwca 2018 r., rząd japoński zmienił politykę podstawową. W celu ułatwienia międzynarodowych transferów danych przekazuje się inspektorowi danych osobowych, jako organowi kompetentnemu w administrowaniu i wdrażaniu APPI, „uprawnienia do podjęcia niezbędnych działań w celu zminimalizowania różnic między systemami i operacjami pomiędzy Japonią a danym państwem trzecim na podstawie ustawy w celu zapewnienia odpowiedniego postępowania

[178] 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, OJ L 76, 19.3.2019, p. 1–58.

[179] *Protecting personal information in the age of Big Data – Japan's new regime,* https://www.aplaw.jp/clientalert-en-dataprotection-december2017.pdf [dostęp 6.06.2019], zob. również: N. Higashizawa, Y. Aihara, *Data Privacy Protection of Personal Information versus Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)*, http://www.city-yuwa.com/english/publication/shared/PDF/DCJ201784_cy_1-15.pdf [dostęp 6.06.2019]; *Japan's New Data Privacy Regime and How it Will Enable Cross-Border Data Flows, Innovation and Privacy Protections in the Modern Information Age,* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_japan_workshop_slide_deck_10_may_2017-cc.pdf [dostęp 6.06.2019].

z danymi osobowymi otrzymanymi od takiego kraju". Decyzja Rady Ministrów stanowi, że obejmuje to uprawnienia do ustanowienia wzmocnionej ochrony poprzez przyjęcie przez organ surowszych zasad uzupełniających i wykraczających poza te określone w ustawie o ochronie informacji osobowych i zarządzeniu gabinetu.

Na podstawie art. 6 ustawy o ochronie informacji osobowych i decyzji Rady Ministrów inspektor danych osobowych w dniu 15 czerwca 2018 r. przyjął „Zasady uzupełniające na mocy ustawy o ochronie danych osobowych do przetwarzania danych osobowych przeniesionych z UE w oparciu o decyzję w sprawie adekwatności" w celu zwiększenia ochrony danych osobowych przekazywanych z Unii Europejskiej do Japonii w oparciu o decyzję o adekwatności. Te dodatkowe zasady są prawnie wiążące dla japońskich podmiotów gospodarczych i egzekwowane zarówno przez sądy, w taki sam sposób, jak przepisy ustawy, którą uzupełniają.

Mimo że ustawodawca Japonii w bardzo szerokim zakresie uregulował kwestię ochrony danych osobowych, wciąż istnieją sektory, w których te regulacje mogą nie być wystarczające. Dla przykładu, w Japonii nie ma szczegółowych regulacji prawnych dedykowanych *cookies* i innym narzędziom związanym z przetwarzaniem informacji o użytkowniku w Internecie. Jednocześnie, gdy informacje te są uznawane za dane osobowe, obowiązują odpowiednie regulacje dotyczące ochrony prywatności i danych osobowych[180].

5.4. Praktyka

Wydaje się, że Japonia zapewnia nie tylko wysokie standardy ustawowe w zakresie ochrony danych osobowych, ale co bardziej istotne, idzie za tym efektywność prawa.

[180] *Data Protection Laws of the World. Japan*, https://www.dlapiperdataprotection.com/index.html?t=law&c=JP [dostęp 6.06.2019].

Działania, takie jak *phishing, hacking* czy kradzież tożsamości, są penalizowane i zagrożone karą grzywny lub pozbawienia wolności do lat pięciu[181]. Prokuratura oraz inne organy podejmujące działania w celu wykrycia i schwytania sprawców przestępstw są zobowiązane do poszanowania prywatności wszystkich uczestników postępowania. Nie mogą dokonać przeszukania, konfiskaty czy nagrywania rozmów bez zezwolenia sądu[182].

Oprócz odpowiedzialności karnej, osoby, które w niewłaściwy sposób przetwarzają dane osobowe bądź dopuszczają się uchybień w zakresie wprowadzenia odpowiednich stopni zabezpieczeń, muszą liczyć się z ewentualnością wystąpienia przeciwko nim z powództwem cywilnym. Sąd w Tokio w 2014 r. nałożył na dostawcę systemów teleinformatycznych karę w wysokości niemal 185 tysięcy dolarów w związku z niezapewnieniem odpowiedniego poziomu zabezpieczeń w oprogramowaniu dostarczanym podmiotowi zamawiającemu, co w ostateczności doprowadziło do wycieku danych na temat kart kredytowych klientów tego ostatniego[183]. Sąd uwzględnił jednocześnie, że pomimo że dostawca usług proponował wprowadzenie usprawnień, podmiot zamawiający odmówił skorzystania z niego, co doprowadziło do obniżenia o 80% żądań powoda[184].

W ostatnich latach znacząco spadła liczba postępowań wynikłych z naruszenia prawa do prywatności i ochrony danych osobowych. Jednym z największych naruszeń w historii był wyciek danych blisko 50 milionów użytkowników serwisu internetowego obsługiwanego przez firmę Benesse w 2014 r. Stwierdzając brak odpowiednich zabezpieczeń, Minister Ekonomii, Handlu i Gospodarki zobowiązał dostawcę usług do wzięcia

[181] M. Hamada & Matsumoto, *Japan*, [w:] *The International Comparative Legal Guide to: A practical cross-border insight into cybersecurity work*, https://www.acc.com/sites/default/files/resources/20190314/1492582_1.pdf [dostęp 06.06.2019].

[182] M. Hamada & Matsumoto, *Data Protection & Cyber Security*, Chambers. Global Practice Guides, s. 10.

[183] *Ibidem.*

[184] *Ibidem.*

odpowiedzialności za naruszenie bezpieczeństwa danych, zwiększenia wysiłków w zakresie ochrony danych osobowych oraz zapewnienia stosowania odpowiednich procedur. Nie została jednocześnie nałożona żadna kara finansowa na Benesse[185].

Rząd Japonii zachęca przedsiębiorców i osoby fizyczne do rozwiązywania sporów dotyczących ochrony prawa do prywatności i danych osobowych w drodze mediacji i porozumień, bez zaangażowania organów administracji publicznej oraz rezygnując z nakładania wysokich kar, chyba że naruszenie jest na tyle duże, że zawiadomienie organu nadzoru jest konieczne w celu zapewnienia przestrzegania prawa[186].

W ostatnich latach największe kontrowersje wzbudziło wprowadzenie przez rząd globalnego programu identyfikacji obywateli „Mój numer" (*My number*)[187]. Każdej osobie przebywającej na terytorium Japonii (włączając w to cudzoziemców i dzieci) został nadany indywidualny 12-cyfrowy numer, którym to jednostka może się posługiwać w kontaktach z sektorem prywatnym i publicznym[188]. Celem programu jest usprawnienie i ujednolicenie procedur administracyjnych między agencjami rządowymi w takich kwestiach, jak podatki i ubezpieczenia społeczne, ułatwiając życie zarówno urzędnikom, jak i ogółowi społeczeństwa[189]. Innym celem jest pomoc w zapobieganiu przestępstwom, takim jak uchylanie się od opodatkowania i bezprawne otrzymywanie świadczeń socjalnych. Jednak wiele osób wyraziło obawy dotyczące nowego systemu, w tym kwestii takich jak podstawowa prywatność i bezpieczeństwo ich danych osobowych[190]. W maju 2019 r. tylko 13% populacji wyraziło zainteresowanie

[185] *A Look at New Trends: Privacy Laws in East, Central, and South Asia and the Pacific*, https://media2.mofo.com/documents/170602-privacy-laws-asia-pacific.pdf [dostęp 6.06.2019].

[186] *Ibidem.*

[187] M. Homada & Matsumoto, *Data Protection…,* s. 11.

[188] L.G. Kittaka, *11 things you need to know about my number*, https://blog.gaijinpot.com/japan-my-number-system [dostęp 6.06.2019].

[189] *Ibidem.*

[190] *Ibidem.*

otrzymaniem specjalnej karty, która służy do obsługi systemu „Mój numer" i pozwala na wykorzystywanie jego możliwości w kontaktach z administracją publiczną[191]. Rząd zapewnia, że program ten gwarantuje pełne bezpieczeństwo danych osobowych, jest regularnie monitorowany, a samo podanie numeru identyfikacyjnego nie umożliwi kradzieży tożsamości[192]. Pracodawcy mogą prosić pracowników o podanie numeru identyfikacyjnego, jednak ich dostęp do danych osobowych do niego przypisanych jest ograniczony jedynie do wąskiej kategorii danych i nie obejmuje informacji na temat stanu zdrowia czy zakresu pozyskiwanej pomocy społecznej[193]. Pomimo licznych kontrowersji rząd japoński jest zdeterminowany, aby nadal wdrażać program, w tym również w tak wrażliwych obszarach, jak służba zdrowia czy pomoc społeczna[194].

Jednocześnie, biorąc pod uwagę obecny stan ochrony danych osobowych w Japonii, wydaje się, że nawet kontrowersyjne programy wprowadzane przez rząd japoński są stosunkowo bezpieczne, przynajmniej z perspektywy europejskiego prawa ochrony danych osobowych.

5.5. Adekwatność ochrony

Japonia jest pierwszym azjatyckim krajem, co do którego Komisja Europejska wydała decyzję o adekwatności ochrony danych osobowych[195]. I chociaż pod rządami poprzednio obowiązującej dyrektywy Komisja Europejska rozpoznawała niektóre kraje jako zapewniające odpowiedni

[191] Japan's government plans for My Number ID cards to be used for health insurance by 2023, https://www.japantimes.co.jp/news/2019/06/05/national/japanese-government-seeks-number-ids-double-health-cards-starting-2021/#.XPlZCIgzY2w [dostęp 6.06.2019].

[192] L.G. Kittaka, *op. cit.*

[193] *Ibidem.*

[194] *Japan's government plans…*

[195] 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, OJ L 76, 19.3.2019, p. 1–58.

poziom ochrony, to po raz pierwszy w historii zawarto umowę bilateralną o wzajemnym uznaniu adekwatnej ochrony danych osobowych[196].

Dane osobowe przetwarzane przez podmioty gospodarcze na podstawie RODO na terytorium Japonii podlegają tym samym gwarancjom co w Unii Europejskiej. Żeby zapewnić odpowiedni poziom ochrony, Japonia zgodziła się znowelizować dotychczas obowiązujące prawo, aby przystosować je do bardziej restrykcyjnych reguł związanych z przetwarzaniem w Japonii danych osobowych pochodzących z Unii Europejskiej. Zmiany dotyczyły włączenia informacji na temat orientacji seksualnej i seksualności jednostki oraz przynależności do związków zawodowych do kategorii danych wrażliwych, przyznania podmiotom danych osobowych prawa do uzyskania kopii przetwarzanych danych, przetwarzania danych wyłącznie w celu, w jakim zostały zebrane, anonimizacji oraz przesyłania danych pochodzących z Unii Europejskiej poza terytorium Japonii[197]. Ponadto wprowadzono narzędzia umożliwiające obywatelom Unii dochodzenie swych praw na terytorium państwa. Osoba, która uważa, że jej prawo do ochrony danych osobowych zostało naruszone, może skorzystać z środków ochrony prawnej dostępnych w Japonii, takich jak: skarga do organu nadzoru, podjęcie mediacji z podmiotem naruszającym bądź wytoczenie powództwa w związku z naruszeniem prawa do prywatności lub prawa do ochrony danych osobowych[198].

Jednocześnie podmioty, które chcą przetwarzać dane osobowe w Japonii, muszą dostosować się do obowiązującego tam prawa. Największe różnice dotyczą uzyskania wcześniejszej zgody na przetwarzanie danych wrażliwych (pod rządami rozporządzenia ogólnego co do zasady ich przetwarzanie jest niedozwolone), uprawnienia podmiotu danych osobowych

[196] M. Nishi, *Data Protection in Japan to Align With GDPR,* https://webcache.googleusercontent.com/search?q=cache:YBzeg3bxPr4J:https://www.skadden.com/-/media/files/publications/2018/09/quarterly-insights/data_protection_in_japan_to_align_with_gdpr.pdf+&cd=2&hl=pl&ct=clnk&gl=pl [dostęp 6.06.2019].

[197] *Ibidem*.

[198] V. Jourová, *EU Japan Adequacy Decision. Fact Sheet*, styczeń 2019.

do otrzymania jedynie kopii przetwarzanych danych (podczas gdy w RODO uprawnienia te są zdecydowanie szersze i obejmują również prawo do zmiany oraz usunięcia przetwarzanych danych), obowiązek prowadzenia rejestrów przetwarzania danych jedynie w przypadku ich przekazywania podmiotom trzecim (RODO zakłada, że obowiązek ten dotyczy wszystkich podmiotów przetwarzających dane), obowiązek podjęcia odpowiednich kroków w zgłoszenia odpowiednim organom nadzorczym przypadku naruszenia bądź potencjalnego naruszenia bezpieczeństwa przetwarzanych danych (w RODO zgłoszenie naruszenia jest obligatoryjne)[199]. Ponadto, zgodnie z japońskim prawem, obowiązek wyznaczenia inspektora ochrony danych osobowych nie jest bezwzględny, ale konieczne jest monitorowanie przetwarzania danych osobowych pracowników[200].

5.6. Wnioski

Japonia z pewnością jest pionierem w dziedzinie ochrony danych osobowych w państwach azjatyckich, mimo braku tradycji ochrony prywatności przez członków społeczeństwa. Chociaż podobnie jak w innych państwach azjatyckich, brak jest gwarancji konstytucyjnych, judykatywa z powodzeniem wywodzi prawo do ochrony danych osobowych z pozostałych postanowień ustawy zasadniczej, sięgając również po akty prawa międzynarodowego, które to prawo przyznają.

Obecne regulacje prawne są zbieżne, żeby nie powiedzieć tożsame z rozporządzeniem europejskim. Ułatwia to nie tylko prowadzenie działalności gospodarczej w tym kraju przez podmioty pochodzące z Unii Europejskiej, ale świadczy również o przyjęciu modelu, który przy założeniu efektywności wprowadzonych rozwiązań zapewnia poszanowanie prywatności jednostki. Koncepcja ta wydaje się pionierska w krajach

[199] M. Nishi, *op. cit.*
[200] *Ibidem*.

azjatyckich – jak pokazują pozostałe rozważania poczynione w niniejszym opracowaniu nie jest to szczególnie popularne podejście.

Dosyć wysoki poziom ochrony danych osobowych w tym kraju to zasługa również rozwoju technologicznego i gospodarczego. Japonia w celu utrzymania gospodarki na wysokim poziomie musi stale utrzymywać rynki zbytu swoich usług, a jednym z największych z nich z pewnością są kraje Unii Europejskiej. Wydaje się zatem, że kraj ten nie miał zbyt wielkiego wyboru czy dostosować swoje ustawodawstwo do wymogów Unii czy też nie. Jednocześnie wydaje się, że wzrastający poziom świadomości wśród obywateli z biegiem czasu wymusiłby te same zmiany.

6. Malezja

6.1. Wstęp

Malezja to kolejny przykład państwa pełnego kontrastów. Jedna z najdynamiczniej rozwijających się gospodarek Azji Wschodniej, nadal boryka się z licznymi problemami wynikającymi z dużego rozwarstwienia społecznego, trudnej historii, a nawet konfliktów wewnętrznych.

Malezja jest monarchią konstytucyjną, na czele której stoi król wybierany na pięcioletnią kadencję. Od czasu uzyskania niepodległości władze silnie rozwijały lokalną gospodarkę, która początkowo opierała się na rolnictwie i przemyśle wydobywczym. Obecnie znacznie większe znaczenie ma dla niej przemysł elektroniczny oraz szeroko pojęty sektor usługowy. Na przestrzeni ostatnich lat rząd Malezji starał się tworzyć warunki jak najbardziej sprzyjające zagranicznym inwestorom. Działania te obejmują nie tylko prowadzenie atrakcyjnej polityki podatkowej, lecz także tworzenie solidnego i godnego zaufania systemu prawnego. Wydaje się, iż politycy odnieśli w tym zakresie sukces, gdyż Malezja od kilku lat wymieniana jest wśród państw z najwyższym wskaźnikiem łatwości prowadzenia działalności gospodarczej[201]. Niewątpliwie jednym z kolejnych działań zwiększających zaufanie do malezyjskiego rynku było stopniowe wdrażanie kolejnych regulacji z zakresu prywatności i ochrony danych osobowych[202].

[201] Zob. szerzej: https://www.doingbusiness.org [dostęp 20.06.2019].

[202] S. Jawahitha, M. Ishak, M. Mazahir, *E-Data Privacy and the Personal Data Protection Bill of Malaysia*, „Journal of Applied Sciences" 2007, vol. 7 (5), s. 734.

6.2. Regulacja konstytucyjna

Obecnie obowiązująca ustawa zasadnicza Malezji pochodzi z 1957 r., aczkolwiek na przestrzeni lat poddawano ją licznym nowelizacjom. Rozdział II zawiera skromny katalog podstawowych wolności, z którego można wyinterpretować również prawo do prywatności. Zgodnie z treścią art. 5 (1) „Nikogo nie można pozbawić życia lub wolności osobistej, za wyjątkiem przypadków określonych w prawie”[203]. Pomimo tego, iż literalna wykładnia wspomnianego przepisu nie daje podstawy do potwierdzenia konstytucyjnego charakteru prawa do prywatności, to z pomocą przychodzi orzecznictwo. Wyrok w sprawie *Sivarasa* to jedno z przełomowych rozstrzygnięć w najnowszej historii Malezji[204]. Rozstrzygając kwestie konstytucyjności ustawy o nabywaniu nieruchomości, Sąd Federalny odniósł się do rozumienia wspomnianego powyżej przepisu ustawy zasadniczej. W uzasadnieniu wskazano, iż oczywiste jest, że z pojęcia wolności osobistej możliwe jest wyinterpretowanie prawa do prywatności. Obecnie przyjmuje się, iż wyrok w tej sprawie stał się punktem wyjścia do dalszego dynamicznego rozwoju krajowej legislacji z zakresu ochrony prywatności[205].

6.3. Regulacja ustawowa

Malezyjski reżim ochrony danych osobowych oparty jest na ustawie z 2010 r., która weszła w życie w 15 listopada 2013 r.[206] Przyjęcie PDPAM stanowiło istotny krok na drodze do jak najlepszej ochrony danych osób

[203] „No person shall be deprived of his life or personal liberty save in accordance with law”. Za: Konstytucja Malezji z dnia 31.08.1957 r.

[204] Wyrok Sądu Federalnego z dnia 17 listopada 2009 r. w sprawie *Sivarasa Rasiah v. Badan Peguam Malaysia & Anor* [2010] 3 CLJ 507.

[205] Z.M. Yusoff, *Protection of privacy in Malaysia: A law for the future*, Wellington 2014, s. 88.

[206] Personal Data Protection Act 2010, act 709. Dalej jako: PDPAM lub Ustawa.

fizycznych, gdyż dotychczasowa regulacja była niezwykle rozdrobniona[207]. Ustawa znajduje zastosowanie do podmiotów przetwarzających oraz posiadających kontrolę nad procesami przetwarzania danych osobowych w związku z transakcjami handlowymi. Dalsze przepisy zawężają jednak zakres podmiotowy ustawy stanowiąc, iż PDPAM ma zastosowanie do podmiotów założonych w Malezji[208] lub podmiotów, które wykorzystują do przetwarzania danych infrastrukturę znajdującą się na jej terytorium. Korzystanie to nie może jednak ograniczać się wyłącznie do przesyłu danych. Podmioty nieposiadające swej siedziby w Malezji zobligowane są do wyznaczenia lokalnego pełnomocnika[209]. Ustawa zawiera również niewielki katalog wyłączeń, zgodnie z którym nie ma ona zastosowania do władzy federalnej i stanowej. Ponadto czynności przetwarzania podejmowane poza granicami Malezji nie znajdują się w zakresie zastosowania aktu, chyba że planowane jest ich późniejsze przetwarzanie w kraju[210].

Jak wspomniano powyżej, PDPAM przyjmuje dość nietypową definicję danych osobowych. W pierwszej kolejności zastrzega ona, iż danymi osobowymi są wyłącznie informacje związane z podejmowanymi transakcjami handlowymi, które bezpośrednio lub pośrednio odnoszą się do zidentyfikowanego lub możliwego do zidentyfikowania podmiotu danych. Jako przykłady wspomnianych w definicji transakcji handlowych wymienia się wszelkie dostawy dóbr, świadczenia usług, ubezpieczenia, umowy agencyjne czy pożyczki. Pojawiają się natomiast wątpliwości co do tego, czy odpłatność takiej umowy jest warunkiem koniecznym[211].

[207] S. Kandiah, *The Privacy, Data Protection and Cybersecurity Law Review. Malaysia*, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175635/malaysia [dostęp 15.06.2019].

[208] Ustawa precyzuje, iż pod tym pojęciem należy rozumieć m.in. osoby fizyczne przebywające na terenie Malezji przez co najmniej 180 dni w roku kalendarzowym, spółki i innego rodzaju stowarzyszenia założone zgodnie z prawem Malezji oraz podmioty prowadzące regularną działalność w Malezji. Za: art. 2 (4) PDPAM.

[209] Art. 2 (1)–(3) *ibidem*.

[210] Art. 3 *ibidem.*

[211] S. Kandiah, *op. cit.*

Ustawodawca zastrzega również, iż wyrażenie opinii o podmiocie danych także powinno być traktowane jako dane osobowe. Poza zakresem definicji znajdują się natomiast informacje przetwarzane w celu sprawozdawczości kredytowej podejmowanej przez właściwe agencje rządowe. Należy jednak podkreślić, iż konkretne informacje powinno się traktować jako dane osobowe w rozumieniu PDPAM, tylko jeżeli przetwarzane są z wykorzystaniem zautomatyzowanych metod, utrwalane w celu późniejszego przetwarzania lub utrwalane w zorganizowanym zbiorze danych. Jak można więc zauważyć, definicja ta ma charakter mieszany i niezwykle złożony. Jednak rezultatem przyjęcia takiego rozumienia danych jest znaczne zawężenie zakresu zastosowania omawianego aktu.

Malezyjska regulacja wyróżnia również szczególną kategorię danych, jakimi są dane wrażliwe. Zgodnie z definicją ustawową przez dane wrażliwe rozumie się wszelkie dane osobowe zawierające informacje na temat zdrowia fizycznego lub psychicznego, poglądów politycznych, wyznania, światopoglądu lub przeszłości kryminalnej osoby fizycznej. Dodatkowo katalog ten może być rozszerzony w formie rozporządzenia właściwego ministra[212].

Pomimo dość rozbudowanego opisu zakresu zastosowania ustawy, który częściowo odnosi się do samego pojęcia przetwarzania, prawodawca wprowadza odrębną, legalną definicję przetwarzania. Oznacza ono zbieranie, utrwalanie, przechowywanie, organizowanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie, łączenie, poprawianie, usuwanie lub niszczenie danych osobowych. Definicja ta pozostaje więc spójna z tym, co powszechnie przyjęto w innych jurysdykcjach.

Art. 4 PDPAM wyróżnia trzy kategorie podmiotów związanych z procesami przetwarzania danych – podmiot danych, użytkownika

[212] Art. 4 PDPAM.

danych oraz przetwarzającego. Co nie zaskakuje, przez podmiot danych rozumie się osobę fizyczną, której dane dotyczą. Pojęciem niestosowanym w innych regulacjach jest natomiast użytkownik danych. Zgodnie z definicją legalną jest nim każdy podmiot, który samodzielnie lub wspólnie z innymi przetwarza jakiekolwiek dane osobowe, ma kontrolę lub zezwala na ich przetwarzanie. Można więc stwierdzić, iż rozumienie tego pojęcia znacząco pokrywa się z europejskim administratorem danych. Ostatnim wyróżnionym podmiotem jest przetwarzający, czyli każdy podmiot dokonujący operacji przetwarzania w imieniu użytkownika danych, który nie czyni tego we własnym celu. Ustawa zastrzega jednak, iż przetwarzającym nie może być pracownik użytkownika danych.

Nie ulega większej wątpliwości, iż malezyjski reżim ochrony danych oparty jest w dużej mierze na zgodzie podmiotu danych. PDPAM przyjmuje jako generalną zasadę obowiązek posiadania zgody na przetwarzanie danych. Pomimo tak znaczącej roli zgody, ustawodawca nie wprowadził jej definicji legalnej lub katalogu obowiązkowych elementów. Tym samym nie zadecydowano o wprowadzeniu jej wymaganej formy. Jednakże biorąc pod uwagę obowiązek prowadzenia rejestru udzielonych zgód nałożony na użytkownika, najbardziej wskazane byłoby zastosowanie formy pisemnej[213]. Ustawodawca wymaga natomiast, by zgoda wyraźnie wskazywała cel przetwarzania. W przypadku braku zgody udzielonej przez podmiot danych użytkownik może polegać na jednej z podstaw wskazanych w art. 6 (2). Zalicza się do nich wykonanie umowy, której stroną jest podmiot danych, podejmowanie czynności zmierzających do zawarcia umowy, wykonanie obowiązku prawnego ciążącego na użytkowniku danych oraz ochronę żywotnych interesów podmiotu danych. Ponadto przetwarzanie wypełnia kryteria legalności, gdy podejmowane jest w celach administrowania wymiarem sprawiedliwości lub wykonywania funkcji powierzonej przez prawo.

[213] S. Kandiah, *op. cit.*

PDPAM wprowadza również kilka dodatkowych podstaw prawnych uprawniających do ujawnienia danych. Jest ono możliwe przy przeciwdziałaniu lub ujawnieniu popełnienia przestępstwa oraz przy prowadzeniu dochodzenia. Ujawnienie danych będzie możliwe również, gdy wymaga tego lub zezwala na to prawo, bądź nakaz sądowy. Uprawnione jest również udostępnienie danych przez użytkownika, który pozostawał w uzasadnionym przekonaniu, iż obowiązujące prawo na to zezwala. Podobnie, możliwe jest ujawnienie danych osobowych przez użytkownika, który pozostawał w uzasadnionym przekonaniu, iż podmiot danych udzieliłby na nie zgody, gdyby o nim wiedział. Uzupełnienie tego katalogu stanowi udostępnienie danych konieczne z punktu widzenia interesu publicznego[214].

Odrębnie przewidziano katalog przesłanek legalizujących przetwarzanie wrażliwych danych osobowych. Ponownie jako regułę prawodawca przyjął przetwarzanie na podstawie zgody. Jednakże zgodnie z art. 40 (1) przetwarzanie danych wrażliwych wymaga zgody wyraźniej. W przypadku jej braku użytkownik może wskazać, iż przetwarzanie jest konieczne do wykonania obowiązku prawnego związanego ze stosunkiem zatrudnienia. Inną okolicznością uzasadniającą przetwarzanie jest ochrona żywotnych interesów podmiotu danych lub innej osoby. Podstawa ta znajdzie zastosowanie wyłącznie wtedy, gdy podmiot danych (lub osoba działająca w jego imieniu) nie może udzielić zgody lub zachodzi uzasadnione podejrzenie, iż uzyskanie jej nie byłoby możliwe. Podobnie jak w innych porządkach prawnych, tak i w Malezji przetwarzanie danych wrażliwych dopuszczalne jest przy świadczeniu usług medycznych lub w związku z prowadzonymi postępowaniami sądowymi. Dodatkowo zgoda nie będzie wymagana na potrzeby udzielenia porady prawnej, dochodzenia swoich praw na drodze sądowej lub zarządzania wymiarem sprawiedliwości. Zgoda na przetwarzanie danych wrażliwych nie jest

[214] Art. 8 oraz 39 PDPAM.

potrzebna, gdy dane te zostały ujawnione przez podmiot danych. PDPAM upoważnia również właściwego ministra do wskazania dodatkowych podstaw prawnych przetwarzania danych wrażliwych[215].

Przetwarzanie danych osobowych w zgodzie z PDPAM wymaga od użytkownika danych przestrzegania siedmiu zasad sformułowanych przez ustawodawcę. Tzw. zasada generalna stanowi odpowiednik unijnej zasady legalności przetwarzania. Zgodnie z nią użytkownik danych zobligowany jest każdorazowo do posiadania odpowiedniej podstawy prawnej przetwarzania[216]. Zgodnie z kolejną zasadą podmiot danych powinien być poinformowany w formie pisemnej o najistotniejszych aspektach prowadzonego przewarzania. PDPAM obliguje użytkownika danych m.in. do przekazania informacji o celu przetwarzania, kategoriach danych oraz podmiotach trzecich otrzymujących dane[217]. Ponadto ustawa zakazuje udostępniania danych w celach sprzecznych z pierwotnie określonym oraz udostępnienia na rzecz podmiotów pierwotnie niewskazanych w informacji przekazanej osobie fizycznej[218]. Co oczywiste, dane osobowe powinny być przetwarzane w sposób bezpieczny, a użytkownik odpowiedzialny jest za wdrożenie odpowiednich zabezpieczeń[219]. PDPAM wprowadza również zasadę ograniczenia przechowywania danych, prawidłowości danych oraz dostępu do nich[220].

Zwiększając ochronę praw i wolności jednostek, ustawodawca malezyjski przewidział szereg praw przysługujących podmiotom danych w związku z przetwarzaniem ich danych. Nie odbiegają one znacznie od standardów przyjętych w Unii Europejskiej czy innych państwach o uznanym poziomie ochrony danych osobowych. Katalog uprawnień obejmuje prawo dostępu do danych, prawo do sprostowania danych oraz prawo

[215] Art. 40 *ibidem.*
[216] Art. 6 *ibidem.*
[217] Art. 7 *ibidem.*
[218] Art. 8 *ibidem.*
[219] Art. 9 *ibidem*
[220] Art. 10–12 *ibidem.*

wycofania udzielonej zgody. Dodatkowo osoby fizyczne posiadają prawo sprzeciwu wobec przetwarzania, które z dużym prawdopodobieństwem mogłoby wyrządzić im szkodę oraz prawo sprzeciwu wobec marketingu bezpośredniego.

W zakresie transgranicznego przesyłu danych osobowych PDPAM posiłkuje się rozwiązaniami przyjętymi w innych systemach prawnych. Co do zasady transfer poza granice Malezji jest zabroniony, chyba że dany kraj uznany został przez Komisarza za zapewniający podobny poziom ochrony danych[221]. Pomimo opublikowania projektu rozporządzenia w tej sprawie w 2017 r. do dziś nie weszło ono w życie[222]. Ustawa przewiduje jednak inne okoliczności umożliwiające przesył danych do państw trzecich. Zgodnie z art. 123 (3) transfer dozwolony jest za zgodą podmiotu danych oraz gdy jest wymagany do zawarcia lub wykonania umowy. Ustawodawca umożliwia również przesyłanie danych do celów prowadzenia postępowań sądowych, uzyskania porady prawnej lub ochrony przysługujących praw. Co interesujące, transfer transgraniczny jest zgodny z przepisami PDPAM, gdy użytkownik danych posiada uzasadnione podstawy, by uznać, iż jest on konieczny do ochrony podmiotu danych przed niekorzystnymi działaniami, a niepraktyczne byłoby uzyskanie zgody podmiotu danych. Wystarczającą podstawą transferu jest również powzięcie przez użytkownika odpowiednich środków bezpieczeństwa, które zagwarantują ochronę na poziomie nie niższym od tego, który zapewniony jest w Malezji. Dodatkowo przesył danych uzasadnia ochrona żywotnych interesów podmiotów danych oraz interesu publicznego Malezji.

[221] Art. 129 (1)–(2) *ibidem*.

[222] Projekt wskazywał następujące państwa: kraje członkowskie Europejskiego Obszaru Gospodarczego, Wielką Brytanię, USA, Kanadę, Szwajcarię, Nową Zelandię, Argentynę, Urugwaj, Andorę, Wyspy Owcze, Guernsey, Izrael, Wyspę Man, Australię, Japonię, Koreę Południową, Chiny, Hong Kong, Tajwan, Singapur, Filipiny oraz DIFC. Za: Public consultation paper No. 1/2017, Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017.

PDPAM powołuje do życia Komisarza ds. Ochrony Danych Osobowych (*Personal Data Protection Commissioner*)[223]. Powoływany jest on na trzyletnią kadencję przez właściwego ministra. Do jego najważniejszych kompetencji należy dbałość o wdrożenie i wykonywanie PDPAM, działalnie jako organ doradczy ministra w kwestiach związanych z ochroną danych oraz zachęcanie do przyjmowania kodeksów dobrych praktyk. Komisarz powinien czuwać nad przestrzeganiem przepisów ustawy, wydawać okólniki, promować świadomość i konieczność ochrony danych osobowych. Do jego zadań należy również szeroko pojęta współpraca międzynarodowa, w szczególności z innymi organami nadzoru.

W celu zapewnienia odpowiedniego wykonania przepisów ustawy, przewiduje ona szereg przepisów penalizujących poszczególne działania użytkowników danych lub przetwarzających. W większości przypadków ustawa zastrzega karę grzywny lub pozbawienia wolności. Naruszenie którejkolwiek z zasad przetwarzania wskazanych w art. 5(1) stanowi przestępstwo zagrożone grzywną nieprzekraczającą 300 tysięcy ringgit lub karą pozbawienia wolności do lat dwóch. Możliwe jest również orzeczenie obydwu kar łącznie[224]. Taką samą karą zagrożony jest niezgodny z prawem transgraniczny przesył danych[225]. Warto jednak zaznaczyć, iż PDPAM nie formułuje wprost prawa do odszkodowania. Jednostki mogą dochodzić swych praw wyłącznie nie podstawie ogólnych przepisów prawa cywilnego[226].

6.4. Praktyka

Pierwsze działania w zakresie egzekwowania przepisów PDPAM podjęto dopiero w połowie 2017 r. Dotyczyły one czynności przetwarzania

[223] Dalej jako: Komisarz.
[224] Art. 5 (2) PDPAM.
[225] Art. 129 (5) *ibidem.*
[226] S. Kandiah, *op. cit*.

danych osobowych podejmowanych przez prywatną szkołę wyższą. W toku postępowania wykazano, iż przetwarzała ona dane byłych pracowników bez wymaganej prawem rejestracji. Co ciekawe, wszystkie dotychczasowe rozstrzygnięcia odnosiły się dokładnie do tego samego obowiązku. Zgodnie z art. 15 (1) określone grupy użytkowników danych zobligowane są do zarejestrowania swojej działalności w rejestrze prowadzonym przez Komisarza ds. Ochrony Danych Osobowych[227]. Niedopełnienie obowiązku zagrożone jest karą grzywny do 500 tysięcy ringgit lub karą pozbawienia wolności do lat trzech[228]. W 2017 r. stwierdzono cztery naruszenia w tym obszarze, natomiast w 2018 r. tylko jedno[229]. Malezyjski regulator nie publikuje szczegółów dotyczących danej sprawy lub podmiotu odpowiedzialnego za naruszenie. Wskazany jest wyłącznie sektor działalności użytkownika danych. Dotychczasowe działania podejmowano wobec podmiotów działających w obszarze edukacji, turystyki oraz wobec agencji pracy.

Wejście w życie RODO również w Malezji przyczyniło się do rozpoczęcia dyskusji nad koniecznością nowelizacji obowiązującego prawa. Przedstawiciele rządu, zdając sobie sprawę z wpływu unijnej regulacji na rynek międzynarodowy, wyrazili konieczność prac nad przyjęciem nowych rozwiązań legislacyjnych[230]. Do dziś nie podjęto jednak dalszych działań w tym zakresie, trudno jest więc ocenić, jaki zakres obejmą planowane zmiany.

[227] Zgodnie z rozporządzeniem rejestracji powinny dokonać m.in. banki, firmy inwestycyjne, firmy ubezpieczeniowe, prywatne przychodnie, agencje turystyczne, wskazane linie lotnicze, szkoły wyższe, deweloperzy nieruchomości oraz spółki prowadzące działalność z zakresu prawa, audytu, księgowości lub architektury. Za: Personal Data Protection (Class of data users) Order 2013, P.U. (A) 336.

[228] Art. 16 (4) PDPAM.

[229] http://www.pdp.gov.my/index.php/en/pusat-media/berita/989-pengguna-data-yang-telah-dikenakan-tindakan-di-bawah-akta-perlindungan-data-peribadi-2010-akta-709 [dostęp 15.07.2019].

[230] https://gdpr.report/news/2019/03/19/malaysia-reviews-data-protection-laws/ [dostęp 15.06.2019].

6.5. Adekwatność ochrony

Odnosząc się do trzech kategorii czynników branych pod uwagę przez Komisję Europejską w czasie oceny adekwatności zagranicznych systemów, należy przyznać, iż ewaluacja Malezji nie jest zadaniem prostym. Pierwsze wątpliwości pojawiają się już na etapie oceny praworządności oraz poszanowania praw człowieka i podstawowych wolności. Pomimo gwarancji wskazanych w obowiązujących przepisach, poziom ochrony praw i wolności jednostki nadal pozostawia wiele do życzenia. Znane są liczne przypadki naruszania wolności słowa, zwłaszcza w odniesieniu do wszelkiej działalności opozycyjnej. Podobne problemy występują w zakresie realizacji wolności zgromadzeń oraz prawa do zrzeszania się. W tym miejscu należy również wskazać na nieprawidłowości w funkcjonowaniu wymiaru sprawiedliwości. Szerokie uprawnienia organów ścigania pozwalają na długotrwałe aresztowania bez wyroku sądowego lub jakiejkolwiek możliwości zaskarżenia aresztu. Poważnym problemem pozostaje nadal nadużywanie przemocy przez funkcjonariuszy publicznych względem osób zatrzymanych i aresztowanych[231].

Odnosząc się do istniejącej legislacji z zakresu ochrony danych osobowych, należy pozytywnie ocenić przyjęcie kompleksowej regulacji przez malezyjskiego ustawodawcę. Zasady przetwarzania danych oraz prawa przyznane podmiotom danych w dużej mierze pozostają spójne z rozwiązaniami europejskimi. Pewne wątpliwości pojawiają się w odniesieniu do katalogu podstaw przetwarzania danych wrażliwych oraz transgranicznego transferu danych. W wielu przypadkach prawodawca pozwala użytkownikowi na oparcie swojego działania na przypuszczeniu, iż podmiot danych wyraziłby na nie zgodę. Ponadto istotną wadą PDPAM jest brak możliwości ubiegania się o odszkodowanie lub wystąpienia ze skargą do organu nadzoru. Dochodzenie swoich praw na drodze cywilnej

[231] Human Rights Watch, *World Report 2019,* Nowy Jork 2019, s. 366–371.

wydaje się rozwiązaniem niewystarczającym, które z pewnością nie gwarantuje jednostce odpowiedniej ochrony.

W zakresie istnienia oraz działalności niezależnego organu nadzorczego należy wskazać na instytucję Komisarza ds. Ochrony Danych Osobowych. Choć jest on organem odpowiedzialnym za czuwanie nad przestrzeganiem przepisów dotyczących ochrony danych, jego niezależność budzi pewne wątpliwości. Powoływany jest on przez właściwego ministra bez konieczności angażowania jakichkolwiek dodatkowych organów. Pozwala to na dość łatwe powiązanie decyzji o wyborze ze względami politycznymi. Co równie istotne, minister ma niemal nieograniczoną możliwość odwołania Komisarza, gdyż ustawa nie precyzuje okoliczności uzasadniających jego dymisję[232]. Ponadto minister ma możliwość wydawania Komisarzowi poleceń i wytycznych, które (tak długo jak nie są sprzeczne z postanowieniami PDPAM) powinny być przez niego właściwie realizowane. W związku z powyższym należy stwierdzić, iż niezależność malezyjskiego organu nadzorczego budzi duże wątpliwości.

Odnosząc się do ostatniego kryterium wskazanego przez RODO (zobowiązań zaciągniętych na arenie międzynarodowej), warto zauważyć, iż Malezja nie ratyfikowała najważniejszych umów międzynarodowych z zakresu ochrony prawa do prywatności, w tym Międzynarodowego Paktu Praw Obywatelskich i Politycznych, czy Konwencji o prawach dziecka. Malezja jest jednak członkiem Stowarzyszenia Narodów Azji Południowo-Wschodniej, które podejmuje stopniowe działania w obszarze ochrony danych osobowych. Pomimo braku charakteru wiążącego, Stowarzyszenie przyjmuje dokumenty mające promować zintensyfikowane działania w zakresie ochrony danych[233].

[232] G. Greenleaf, *Limitations of Malaysia's data protection Bill,* „Privacy Laws & Business International Newsletter" 2010, No. 104, s. 2.

[233] Zob. szerzej: ASEAN Framework on Personal Data Protection oraz ASEAN Framework on Digital Data Governance.

6.6. Wnioski

Analiza obowiązującego ustawodawstwa w Malezji nie daje prostej odpowiedzi co do poziomu ochrony danych osobowych. Choć punktem wyjścia do przyjęcia PDPAM była regulacja europejska, lokalny ustawodawca wprowadził w niej wiele modyfikacji. W rezultacie ustawa jest niezwykle złożonym i skomplikowanym aktem, którego interpretacja przysparza wiele trudności, nawet w odniesieniu do podstawowych definicji. Zapowiadana nowelizacja malezyjskiej ustawy w szczególności powinna wziąć pod uwagę poszerzenie zakresu obowiązywania ustawy. Zawężanie zakresu wyłącznie do przetwarzania w kontekście transakcji handlowych zdaje się nadmierne, zwłaszcza w obliczu trudności w definiowaniu tego pojęcia.

Dotychczasowa praktyka wskazuje jednak na to, iż ustawa spełnia swoją rolę, a organy powołane do jej egzekwowania wywiązują się ze swoich obowiązków. Można mieć jednak pewne wątpliwości, czy jest to wystarczające dla uznania Malezji za kraj zapewniający adekwatny poziom ochrony w rozumieniu RODO. Z pewnością obecnie obowiązująca regulacja stanowi solidną podstawę do dalszego rozwoju ochrony danych osobowych w tym państwie.

7. Międzynarodowe Centrum Finansowe Dubaju (*Dubai International Financial Centre*)

7.1. Wstęp

Dynamiczny rozwój gospodarczy i ekonomiczny państw na Bliskim Wchodzie oraz chęć zwiększenia atrakcyjności rodzimych rynków dla zachodnich inwestorów przyczyniły się do wdrożenia nietypowych rozwiązań prawnoustrojowych. Choć pojęcie specjalnych stref ekonomicznych znane jest niemal na całym świecie, to ich forma, jaką przyjęto w niektórych państwach Zatoki Perskiej zdecydowanie odbiega od standardowych rozwiązań. Specjalna strefa ekonomiczna Dubaju – Międzynarodowe Centrum Finansowe Dubaju (*Dubai International Financial Centre*[234]) powstało w 2004 r. jako jeden z głównych ośrodków sektora finansowego i bankowego na Bliskim Wschodzie[235]. DIFC posiada odrębne od reszty państwa ustawodawstwo, organy regulacyjne, system wymiaru sprawiedliwości oraz reżim prawny. Wszystko to przyjęto w celu, wyjścia naprzeciw oczekiwaniom potencjalnych inwestorów, w szczególności tych, którzy na co dzień funkcjonują w krajach systemu *common law*. Przykładem rozwiązań szczególnie atrakcyjnych dla inwestorów jest

[234] Dalej jako: DIFC lub Strefa.

[235] Federal Decree Number 35 for the year 2004 to Establish Financial Free Zone in Dubai oraz Dubai Law No. 9 of 2004 in respect of The Dubai International Financial Centre.

np. dopuszczalność posiadania 100% udziałów w lokalnych spółkach przez obcokrajowców[236]. Jednak co najistotniejsze, odrębna jurysdykcja Strefy oznacza, iż regulacje Zjednoczonych Emiratów Arabskich (ZEA) z zakresu prawa cywilnego i handlowego nie obowiązują na terenie DIFC[237]. Właściwym organom przysługuje prawo stworzenia własnych regulacji, które w przypadku DIFC tworzone są w języku angielskim, a nie arabskim.

7.2. Regulacja konstytucyjna

Zgodnie z regulacją dotyczącą prawnego reżimu stref ekonomicznych, mają one prawo do tworzenia własnych przepisów z zakresu prawa cywilnego i handlowego. Oznacza to jednak, iż nie posiadają one pełnej niezależności w zakresie ustawodawstwa, a część prawa federalnego nadal znajdzie zastosowanie na terytorium DIFC. Właśnie dlatego rozważania dotyczące ochrony danych osobowych należy rozpocząć od federalnej ustawy zasadniczej. Obecnie obowiązująca konstytucja Zjednoczonych Emiratów Arabskich pochodzi z 1971 r. Późniejsza nowelizacja art. 121 przyznała wprost władzy federalnej możliwość tworzenia szczególnych stref ekonomicznych oraz określania ich jurysdykcji (w tym wyłączenia spod przepisów prawa federalnego)[238].

Katalog praw i wolności jednostki zawarty w konstytucji ZEA nie formułuje wprost prawa do prywatności. Warto jednak zauważyć, iż art. 31 konstytucji ZEA gwarantuje tajemnicę korespondencji. Ustawa zasadnicza wyłącznie przykładowo wymienia tu pocztę czy telegraf jako formy komunikowania objęte zakresem tego przepisu. Jednak katalog ten ma charakter otwarty. Wskazuje się, iż zakres zastosowania tego przepisu jest

[236] A. Tarbuck, Ch. Lester, *Dubai's legal system. Creating a legal and regulatory framework for a modern society*, Dubaj 2009, s. 9.

[237] Art. 3 (2) Federal Law No. 8 of 2004 Regarding The Financial Free Zones.

[238] Art. 121 Konstytucji Zjednoczonych Emiratów Arabskich z dnia 2 grudnia 1971 r. Dalej jako: Konstytucja ZEA.

znaczenie szerszy, niż wskazuje na to jego wykładnia literalna. Przyjmuje się wszakże, iż celem art. 31 jest szeroko pojęta ochrona prywatności[239]. Warto również zauważyć, iż zupełnie odrębnie ustawa zasadnicza ZEA wprowadza również gwarancje dotyczące nienaruszalności mieszkania[240].

Należy także pamiętać, iż Zjednoczone Emiraty Arabskie są państwem muzułmańskim, w którym prawo szariatu odgrywa znaczącą rolę. Zgodnie z art. 7 to właśnie szariat stanowi główne źródło prawa w państwie. Niewątpliwie wywiera to istotny wpływ na zagadnienia związane z prywatnością jednostek. Zagadnienie to zostało omówione szerzej w rozdziale dotyczącym Bahrajnu.

7.3. Regulacja ustawowa

Zjednoczone Emiraty Arabskie nie posiadają kompleksowej, federalnej regulacji dotyczącej ochrony danych osobowych. Częściowo powiązane z tym zagadnieniem są natomiast ustawy dotyczące transakcji elektronicznych[241] oraz cyberprzestępczości[242]. Dodatkowo federalny kodeks karny penalizuje różnorodne naruszenia prywatności osób fizycznych, które polegają m.in. na udostępnieniu wizerunku osoby, ujawnieniu szczegółów prywatnej rozmowy, ujawnieniu informacji poufnych pozyskanych w związku z wykonywanym zawodem lub pełnioną funkcją oraz na naruszeniu tajemnicy korespondencji[243].

Nie ulega jednak wątpliwości, iż szczegółowe uregulowanie kwestii ochrony danych osobowych stanowi w dzisiejszych czasach jeden z warunków *sine qua non* konkurencyjnej gospodarki. Toteż nie dziwi, iż

[239] V. Woods, *Privacy and data protection in The UAE*, http://www.hadefpartners.com/News/329/Privacy-and-data-protection-in-the-UAE [dostęp 15.06.2019].

[240] Art. 36 Konstytucji ZEA.

[241] Federal Law No. 1 of 2006 on Electronic Commerce and Transactions.

[242] Federal Law No. 5 of 2012 on Combating Cybercrimes.

[243] Art. 378–380 Federal Law No. 3 of 1987 The Penal Code.

specjalne strefy ekonomiczne, których głównym założeniem jest prowadzenie międzynarodowej wymiany handlowej, postanowiły o przyjęciu własnych regulacji z tego zakresu. W odpowiedzi na brak prawa federalnego czy lokalnego szczegółowa ustawa przyjęta została nie tylko w DIFC, lecz także w *Abu Dhabi Global Market*.

Ustawa o ochronie danych osobowych została przyjęta w DIFC w 2007 r., a następnie znowelizowana w styczniu 2018 r.[244] Władze Strefy wyraźnie podkreślają, iż regulacja w pełni realizuje wytyczne OECD z zakresu ochrony prywatności, a także jest spójna z prawem Unii Europejskiej. Podobnie jak w innych państwach, naczelnym celem ustawy jest właściwe zrównoważenie praw jednostek oraz interesów różnorodnych podmiotów gospodarczych przetwarzających ich dane. Uzupełnienie powyższej ustawy stanowi rozporządzenie wydane 15 lutego 2007 r.[245]

Na wstępie należy ponowie i wyraźnie zaznaczyć, iż zakres zastosowania DPL ograniczony jest wyłącznie do Międzynarodowego Centrum Finansowego Dubaju, a nie całego emiratu. Ustawa znajduje zastosowanie do przetwarzania danych, przez które rozumie się wszelkie operacje lub zestawy operacji wykonywane na danych osobowych, niezależnie od tego, czy wykorzystywane są zautomatyzowane metody. Przetwarzanie w szczególności obejmuje zbieranie, utrwalanie, organizowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, używanie, ujawnianie, rozpowszechnianie, segregowanie, łączenie, blokowanie, usuwanie lub niszczenie[246]. Wyliczenie to nie ma jednak charakteru zamkniętego. Ustawa nie zawiera generalnego katalogu wyłączeń, jednak przyznaje *DIFC Authority's Board of Directors* prawo do uchylenia DPL (lub jego części) w odniesieniu do konkretnego administratora danych[247]. Ponadto określone przepisy (dotyczące przesyłu danych do państw trzecich, obowiązków

[244] Data Protection Law DIFC Law No. 1 of 2007. Dalej jako: DPL lub Ustawa.
[245] Data Protection Regulations, Consolidated Version No.3. Dalej jako: Rozporządzenie.
[246] Art. 3 Załącznika nr 1 do DPL.
[247] Art. 39 (1) DPL.

informacyjnych oraz prawa dostępu, korekty i usunięcia danych) nie znajdują zastosowania do *Dubai Financial Services Authority*, *DIFC Authority* oraz *Registrar of Companies*, czyli najważniejszych organów Strefy. Wyłączenie to będzie uzasadnione tylko w przypadku, gdy wypełnienie obowiązków wskazanych w prawie najprawdopodobniej naruszyłoby przepisy DPL[248].

Podmioty zaangażowane w procesy przetwarzania definiowane są w DPL w sposób zbieżny z RODO. Osoba, której dotyczą dane osobowe, określana jest mianem podmiotu danych. Podmiot, który samodzielnie lub wspólnie z innymi określa cele i środki operacji przetwarzania, określany jest natomiast administratorem danych. Warto natomiast zwrócić uwagę, iż definicja wskazuje, iż administratorem może być wyłącznie podmiot znajdujący się lub działający w DIFC. Tym samym definicja wprowadza swoiste ograniczenie podmiotowe zakresu zastosowania omawianej ustawy. DPL definiuje również trzecią kategorię podmiotów, jakimi są przetwarzający. Ustawa wskazuje, iż należy przez nich rozumieć wszelkie podmioty przetwarzające dane w imieniu administratora. W tym przypadku prawodawca nie dokonuje żadnego zawężenia podmiotowego[249].

Ustawa wprowadza bardzo lakoniczną definicję legalną danych osobowych. Zgodnie z DPL przez dane osobowe rozumie się wszelkie dane odnoszące się do możliwej do zidentyfikowania osoby fizycznej. Prawodawca wprowadził natomiast znacznie bardziej szczegółową definicję tejże osoby. Możliwa do zidentyfikowania (pośrednio i bezpośrednio) jest każda żyjąca osoba fizyczna, co do której ujawniono numer identyfikacyjny oraz inne informacje dotyczące jej cech biologicznych, fizycznych, biometrycznych, fizjologicznych, psychicznych, ekonomicznych, kulturowych lub społecznych[250]. Łatwo więc zauważyć, iż ostatecznie połączenie

[248] Art. 39 (2) *ibidem*.
[249] Art. 3 Załącznika nr 1 do DPL.
[250] *Ibidem*.

tych dwóch definicji skutkuje rozumieniem danych osobowych spójnym z tym, jakie przyjęto w innych regulacjach.

PDL wyróżnia również szczególną kategorię danych, jakimi są dane wrażliwe. Zgodnie z definicją ustawową uznaje się za nie dane osobowe ujawniające lub dotyczące (pośrednio lub bezpośrednio) rasy, pochodzenia etnicznego, przynależności lub poglądów politycznych, wyznania, karalności, przynależności do związków zawodowych, zdrowia lub seksualności.

Co oczywiste, PDL wymaga, aby dane osobowe przetwarzane były wyłącznie w sposób zgodny z prawem, co w praktyce oznacza wykazanie odpowiedniej podstawy prawnej dla przetwarzania. Ustawa zawiera dwa katalogi przesłanek – jeden dla danych „zwykłych" oraz drugi dla danych wrażliwych. Art. 9 wyszczególnia pięć podstaw uprawniających do przetwarzania danych osobowych, jednak ustawodawca wydaje się nie przyznawać pierwszeństwa żadnej z nich. Administrator może polegać na pisemnej zgodzie udzielonej przez podmiot danych lub wykazać, iż przetwarzanie jest niezbędne do celów wykonania umowy, której podmiot danych jest stroną[251]. Kolejną przesłanką jest wykonanie obowiązku prawnego ciążącego na administratorze danych. Prawodawca za odrębną podstawę przyjmuje konieczność wykonywania zadań w interesie DIFC lub realizowania władzy w imieniu *DIFC Authority*, *Dubai Financial Services Authority*, *Registrar of Companies* lub sądu. Ostatecznie ustawa zezwala również na przetwarzanie danych ze względu na uzasadniony interes administratora danych lub podmiotów trzecich, na rzecz których udostępniono dane. Przesłanka ta nie znajdzie jednak zastosowania, gdy uzasadniony interes podmiotów danych będzie przeważał[252].

Przetwarzanie danych wrażliwych jest co do zasady zabronione w DIFC, natomiast ustawa wskazuje kilkanaście okoliczności uchylających

[251] Przesłanka ta uzasadnia również podejmowanie czynności przetwarzania zmierzających do zawarcia umowy. Za: art. 9 (b) DPL.

[252] Art. 9 *ibidem*.

ten zakaz. Pierwszą z nich jest udzielenie pisemnej zgody przez podmiot danych. Wykonywanie obowiązków nałożonych prawem na administratora oraz ochrona żywotnych interesów podmioty danych również uzasadniają przetwarzanie. W przypadku danych wrażliwych członków fundacji, stowarzyszeń lub innych organizacji *non-profit* przetwarzanie będzie dopuszczalne, gdy służy podejmowaniu uzasadnionych działań przez te podmioty. Przetwarzanie to musi jednak ograniczać się wyłącznie do osób mających regularny kontakt z organizacją oraz mieć związek z jej celami. PDL dopuszcza przetwarzanie danych wrażliwych, które w sposób wyraźny zostały upublicznione przez podmiot danych lub gdy przetwarzanie jest niezbędne do dochodzenia lub ochrony roszczeń prawnych. Jako odrębną podstawę ustawodawca wskazuje czynności, których podjęcie konieczne jest do przestrzegania prawa wiążącego administratora. Co ciekawe, osobno wyszczególniono czynności wiążące się z koniecznością przestrzegania wytycznych i wymogów dotyczących audytu, rachunkowości, przeciwdziałania praniu brudnych pieniędzy lub finansowania terroryzmu oraz zapobiegania przestępczości. Wydaje się, iż przy drobnej zmianie brzmienia przepisów przesłanka ta zawierałaby się w zakresie podstawy wskazanej wcześniej, aczkolwiek widać tu wyraźnie położony nacisk na wymogi o szczególnym znaczeniu dla sektora finansowego. To samo widoczne jest przy kolejnej podstawie, zgodnie z którą dane wrażliwe mogą być przetwarzane, gdy przyczynia się to do zachowania uzasadnionych interesów administratora uznanego na międzynarodowym rynku finansowym. Zgodnie z ustawą zezwala się również na przetwarzanie szczególnej kategorii danych, gdy jest to konieczne do świadczenia usług medycznych lub ochrony ludności przed stratami finansowymi wynikłymi z działań niezgodnych z prawem lub przestępstwami popełnionymi przez osoby świadczące usługi bankowe, ubezpieczeniowe, inwestycyjne lub inne. Finalnie należy wskazać, iż wykazanie żadnej z wyżej przytoczonych podstaw prawnych nie będzie konieczne w sytuacji uzyskania pisemnej zgody Komisarza ds. Ochrony

Danych (*Commissioner of Data Protection*). Ustawa nie wskazuje na żadne szczegółowe okoliczności, które powinny być wzięte pod uwagę przy udzielaniu takowej zgody, jednak zastrzega, iż administrator zobligowany jest do zastosowania adekwatnych środków bezpieczeństwa[253]. Odmowa udzielenia wspomnianej zgody podlega zaskarżeniu do właściwego sądu.

Wykazanie przez administratora jednej z wyżej wymienionych podstaw przetwarzania danych czyni zadość zasadzie zgodnego z prawem przetwarzania. DPL wskazuje ponadto, iż każdorazowo dane muszą być przetwarzane rzetelnie i w sposób bezpieczny. Każda operacja winna być podejmowana w sposób proporcjonalny w wyraźnie określonym i uzasadnionym celu. To na administratorze ciąży również obowiązek dbałości o aktualność i prawdziwość danych. Powinien on również zadbać, aby dane były przetwarzane tylko tak długo, jak to jest niezbędne do realizacji wskazanego celu[254]. Co interesujące, podobnie jak w przypadku europejskiej regulacji DPL nakłada obowiązek prowadzenia rejestru przetwarzania danych. Powinien on zawierać informacje na temat wszystkich podejmowanych operacji przetwarzania, włączając jej opis, cel, typ podmiotów danych oraz typ przetwarzanych danych[255].

Wzorem innych istotnych regulacji, DPL przyznaje podmiotom danych prawa, które mają zapewniać im lepszą ochronę ich interesów. Na żądanie podmiotu danych administrator ma obowiązek udzielić jej na piśmie informacji na temat kategorii danych przetwarzanych przez niego oraz celu przetwarzania. W przypadku, gdy jest to robione w sposób niezgodny z przepisami DPL, jednostka ma prawo do wystąpienia z wnioskiem o sprostowanie lub usunięcie danych[256]. Ponadto podmiotom danych przysługuje prawo sprzeciwu wobec prowadzonego przetwarzania[257].

[253] Art. 10 (1)–(2) *ibidem*.
[254] Art. 8 (1) *ibidem*.
[255] Art. 6.1.1 Rozporządzenia.
[256] Art. 17 DPL.
[257] Art. 18 *ibidem*.

W przypadku uzasadnionego przypuszczania, iż było ono niezgodne z prawem i miało negatywny wpływ na prawa lub interesy podmiotu danych, ma on prawo do wystąpienia ze skargą do Komisarza ds. Ochrony Danych[258].

Pomimo iż DPL nie dotyczy terytorium całego państwa, a wyłącznie niewielkiej strefy ekonomicznej, prawodawca mimo wszystko postanowił o uregulowaniu kwestii zagranicznego transferu danych. Ze względów oczywistych, w tym przypadku do transferu poza granice DIFC będzie dochodzić nawet w sytuacji przesyłu danych do innych emiratów zrzeszonych w ramach Zjednoczonych Emiratów Arabskich. Wzorem innych regulacji prawodawca nie wymaga spełnienia żadnych dodatkowych wymogów w przypadku transferu danych do państw o ekwiwalentnym poziomie ochrony danych osobowych. Pomiotem odpowiedzialnym za stworzenie listy wyżej wymienionych państw jest Komisarz ds. Ochrony Danych. Obecnie lista ta obejmuje wszystkie państwa członkowskie Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego, a także Andorę, Argentynę, Guernsey, Japonię, Jersey, Kanadę, Nową Zelandię, Szwajcarię, Urugwaj, Wyspy Owcze oraz Wyspę Man[259]. W przypadku przesyłu danych osobowych do innych państw konieczne jest spełnienie jednego z warunków wskazanych w art. 12 (1). Administrator może ubiegać się o zgodę Komisarza przy jednoczesnym zapewnieniu odpowiednich środków bezpieczeństwa. Inną możliwością jest uzyskanie pisemnej zgody podmiotu danych. Okolicznością uzasadniającą transfer danych może być również wykonanie umowy zawartej między administratorem i podmiotem danych lub administratorem i podmiotem trzecim na rzecz podmiotu danych. Przesył danych poza granice DIFC jest możliwy także wtedy, gdy służy on ochronie żywotnych interesów podmiotu danych lub

[258] Art. 34 (1) *ibidem.*

[259] Dubai International Financial Centre, Adequate Data Protection Regimes, https://www.difc.ae/business/operating/data-protection/adequate-data-protection-regimes/ [dostęp 15.06.2019].

gdy jest niezbędny, lub wymagany prawem ze względu na interesy DIFC. Transfer danych pochodzących z publicznych rejestrów podlega wyłączeniu spod generalnego zakazu. Podobnie jak w przypadku przetwarzania danych wrażliwych, przesył danych poza granice DIFC jest zgodny z obowiązującą ustawą, jeżeli jest niezbędny do celów przestrzegania obowiązków prawnych nałożonych na administratora, gdy przyczynia się do zachowania uzasadnionych interesów administratora uznanego na międzynarodowym rynku finansowym lub gdy jest konieczny do przestrzegania określonych wymogów regulacyjnych[260].

Obecnie trudno jest sobie wyobrazić funkcjonowanie efektywnego systemu ochrony danych osobowych bez powołania do życia kompetentnego organu nadzorczego. Ustawodawca czyni to również w przypadku regulacji obowiązującej w Strefie. Zgodnie z art. 22 ustawy Prezes DIFC (*The President*) ma obowiązek powołać na stanowisko Komisarza ds. Ochrony Danych osobę o odpowiednim doświadczeniu i kwalifikacjach. Wybór ten powinien być zaopiniowany przez *DIFC Authority's Board of Directors*, a kadencja Komisarza trwa trzy lata. DPL wskazuje, iż głównym celem działalności Komisarza jest promowanie dobrych praktyk oraz szerzenie świadomości w zakresie konieczności ochrony danych osobowych. Ustawa formułuje również bardziej szczegółowe kompetencje. Zgodnie z nimi Komisarz jest uprawniony do oceniania poprawności operacji przetwarzania podejmowanych przez administratorów i przetwarzających, wydawania ostrzeżeń, upomnień i rekomendacji, inicjowania postępowań w sprawie naruszenia przepisów DPL przez sądami, nakładania kar administracyjnych oraz inicjowania postępowań w sprawie odszkodowań w imieniu podmiotów danych. Ponadto Komisarz jest odpowiedzialny za przygotowywanie projektów rozporządzeń, kodeksów postępowania czy wytycznych oraz przedkładanie ich do *DIFC Authority's Board of Directors*[261]. Co istotne, ustawa podkreśla niezależność

[260] Art. 12 DPL.

[261] Art. 26 *ibidem*.

Komisarza w wykonywaniu swoich obowiązków, aczkolwiek pewne wątpliwości może rodzić tryb odwoływania go ze stanowiska. Zgodnie z art. 24 Prezes DIFC ma prawo odwołać Komisarza w dowolnym momencie i bez zachowania dodatkowych terminów wypowiedzenia, w przypadku niezdolności do pełnienia funkcji lub niewłaściwego zachowania. Tak szerokie określenie podstaw odwołania oraz brak jakichkolwiek dodatkowych wymogów formalnych może potencjalnie sprzyjać nadużyciom i wpłynąć na niezależność organu.

Jak wspomniano powyżej Komisarz ma prawo przeprowadzać dochodzenia w przypadku podejrzenia naruszenia przepisów DPL. W sytuacji stwierdzenia naruszenia ma on prawo wydać decyzję zobowiązującą administratora do zaprzestania dalszych operacji przetwarzania danych osobowych[262]. Ponadto przysługuje mu prawo do nałożenia administracyjnej kary pieniężnej. Ustawa wprowadza maksymalne stawki kar dla każdego z rodzajów naruszenia. Ich wysokość waha się od 5 tysięcy do 25 tysięcy dolarów. Co ciekawe, najsurowsza kara przewidziana jest za niedopełnienie obowiązku notyfikacji Komisarza w przypadkach, gdy jest ona wymagana przez prawo[263]. Oznacza to, iż czynność czysto formalna, niewymagająca nawet odpowiedzi lub decyzji ze strony regulatora uznawana jest za istotniejszą niż zgodne z prawem przetwarzanie danych. Administratorom danych przysługuje prawo do odwołania się od decyzji Komisarza do właściwego sądu w terminie 30 dni[264].

7.4. Praktyka

Pomimo rozwiniętej regulacji dotyczącej ochrony danych osobowych zaskakujący jest brak jakichkolwiek powszechnie dostępnych informacji na temat egzekwowania prawa w DIFC. Ustawa nie obliguje Komisarza

[262] Art. 33 *ibidem.*
[263] Załącznik nr 2 do DPL.
[264] Art. 37 *ibidem.*

ds. Ochrony Danych do publikowania okresowych sprawozdań ze swojej działalności. Próżno też szukać szczegółów rozstrzygnięć wydawanych przez niego. W jednej z niedawnych wypowiedzi Komisarz powiedział, iż dotychczas nie wszczęto żadnych dochodzeń oraz nie wydano żadnych decyzji odnośnie do egzekwowania przepisów DPL w praktyce. Zaznaczył jednak, iż planowane jest powzięcie dodatkowych działań w tym zakresie w najbliższych miesiącach[265].

Obecnie obowiązująca ustawa o ochronie danych osobowych jest w dużej mierze oparta na europejskiej dyrektywie 95/46/EC. Jednak w związku z wejściem w życie RODO w 2018 r. pojawiła się pilna potrzeba zrewidowania przepisów obowiązujących w DIFC. Obecnie toczą się więc prace nad odpowiednią nowelizacją DPL. Projekt nowej ustawy przedłożony został do konsultacji społecznych[266]. Prawodawca w uzasadnieniu do projektu wyraźnie wskazuje, iż projekt w dużej mierze oparty został na zasadach i rozwiązaniach przyjętych przez ustawodawcę unijnego. Lektura projektu faktycznie nasuwa liczne skojarzenia z RODO. Zakłada on m.in. wprowadzenie instytucji inspektora ochrony danych osobowych oraz zwiększenie wymogów dotyczących udzielania zgody na przetwarzanie danych.

Wydaje się więc, iż mimo niewielkiej aktywności organu nadzorczego DIFC nadal kładzie duży nacisk na kwestie ochrony danych. Należy mieć nadzieję, iż nowelizacja prawa nie pozostanie wyłącznie deklaracją, lecz faktycznie przyczyni się do zwiększenia ochrony jednostek.

7.5. Adekwatność ochrony

Na wstępie należy zaznaczyć, iż zgodnie z art. 45 RODO Komisja Europejska jest uprawniona do wydania decyzji o adekwatności nie tylko

[265] Allen & Overy, *Cross-border Data Transfer. Data Protection, United Arab Emirates (DIFC)*, Dubai 2018, s. 81.

[266] https://www.difc.ae/files/8515/6093/1994/Consultation_Paper_No._6_June_2019_Annex_1.pdf [dostęp 15.06.2019].

w odniesieniu do państwa trzeciego lub organizacji międzynarodowej, lecz także danego terytorium lub określonego sektora w tym państwie. Tym samym wydaje się, iż na gruncie rozporządzenia unijnego byłoby możliwe uwzględnienie *Dubai International Financial Centre* na liście państw i terytoriów o odpowiednim poziomie ochrony danych osobowych. Nie można jednak zapomnieć, iż przepisy prawa federalnego oraz polityka prowadzona przez władzę państwową nadal wywierają znaczący wpływ na sytuację prawną i faktyczną w Strefie. Toteż rozważania dotyczące potencjalnej adekwatności ochrony uwzględniać będą zarówno te dotyczące całego państwa, emiratu, jak i specjalnej strefy ekonomicznej.

Konstytucja Zjednoczonych Emiratów Arabskich zawiera dość obszerny katalog praw i wolności człowieka. Niestety, podobnie jak w przypadku innych państw Bliskiego Wschodu, nadal występują liczne problemy w ich realizacji. Zgodnie z doniesieniami organizacji zajmujących się ochroną praw człowieka, obecnie największym problemem jest przestrzeganie wolności słowa. Jest to szczególnie widoczne w przypadku aktywistów i dziennikarzy krytykujących działania władzy. Równie istotną kwestią jest dyskryminacja kobiet. Według obecnie obowiązującego prawa różnicowanie sytuacji jednostek ze względu na płeć nie mieści się w legalnej definicji dyskryminacji. Z podobnymi problemami borykają się osoby homoseksualne.

W zakresie realizacji zasady praworządności Zjednoczone Emiraty Arabskie zdają się przodować wśród państw arabskich. Niestety, lokalne sytuacje nadal znacząco odbiegają od zachodnich standardów. Wpływa na to przede wszystkim brak transparentności w działaniach rządu, ograniczone możliwości udziału obywateli w sprawowaniu władzy oraz utrudniona działalność organizacji pozarządowych[267]. Uczciwie należy jednak przyznać, iż pod względem niezależności wymiaru sprawiedliwości oraz

[267] The World Justice Project, *Rule of Law Index 2019*, Waszyngton 2019, s. 150.

jego efektywności kraj ten należy do światowej czołówki[268]. Sytuacja ta wygląda jeszcze lepiej w odniesieniu do DIFC, która odrębnie kształtuje swój wymiar sprawiedliwości w zgodzie z zachodnimi wymogami.

Przechodząc do kwestii ustawodawstwa z zakresu ochrony danych osobowych, należy oczywiście docenić fakt przyjęcia jednej, kompleksowej regulacji. Nie ulega wątpliwości, iż DPL jest znacząco inspirowana regulacją unijną. Ustawodawca zadecydował wyłącznie o wprowadzeniu niewielkich zmian odzwierciedlających charakterystykę lokalnej gospodarki. I to właśnie te nieliczne odmienności wydają się kluczowe z punktu widzenia oceny adekwatności.

W zakresie definiowania danych, przetwarzania czy też podmiotów zaangażowanych w procesy przetwarzania (administrator, podmiot danych, przetwarzający) trudno jest odnaleźć jakiekolwiek odmienności od rozwiązań europejskich. Zakres zastosowania DPL jest na tyle szeroki, iż trudno cokolwiek zarzucić ustawodawcy. Powstrzymano się od wprowadzania nadmiernych wyłączeń, które mogłyby podawać w wątpliwość faktyczny cel wdrożenia ustawy. O ile katalog przesłanek przetwarzania danych osobowych nie budzi większych wątpliwości, to pewne zastrzeżenia można mieć do wyliczenia podstaw przetwarzania danych wrażliwych. Łatwo dostrzec, iż jest on bardzo obszerny (jedenaście przesłanek) oraz czyni pewne ustępstwa na rzecz szeroko pojętego sektora finansowego. Dla przykładu wystarczy wskazać przetwarzanie konieczne ze względu na uzasadniony interes administratora uznanego na międzynarodowym rynku finansowym[269]. Niemal identyczne wątpliwości budzi katalog okoliczności uzasadniających transgraniczny przesył danych osobowych.

Katalog praw jednostek w dużej mierze pozostaje spójny ze standardami europejskimi, nie można jednak pominąć braku prawa do

[268] World Economic Forum, *The Global Competitiveness Report 2018*, Genewa 2018, s. 581.

[269] Art. 10 (1) (g) DPL.

wycofania zgody. Biorąc pod uwagę znaczenie zgody w lokalnym systemie, zaskakuje tego typu pominięcie ustawodawcy. Warto również zaznaczyć, iż DPL nie wprowadza instytucji inspektora ochrony danych osobowych lub innej równoważnej.

Pomimo wskazanych powyżej odmienności, nie wydaje się, by miały one kluczowe znaczenie z punktu widzenia oceny adekwatności. Czynnikiem, który trzeba natomiast wziąć pod uwagę, jest znikoma aktywność lokalnego organu nadzorczego. Trudno uwierzyć, aby kilkanaście lat obowiązywania ustawy nie przyczyniło się do ujawnienia choć jednego przypadku nieprawidłowości w przetwarzaniu danych. I chociaż ustawowy katalog kompetencji Komisarza ds. Ochrony Danych pozwala przypuszczać, iż wypełniałby on wymogi stawiane przez RODO, to w obliczu jego bierności trudno jest ocenić jego skuteczność.

7.6. Wnioski

Aktywność prawodawcy Międzynarodowego Centrum Finansowego Dubaju należy z pewnością do jednych z najciekawszych przykładów dbałości o ochronę danych osobowych. I choć sama regulacja zdaje się w dużej mierze powieleniem prawa unijnego, to szczególnie zaskakuje determinacja DIFC do unormowania tej kwestii, pomimo braku federalnej legislacji w tym zakresie. Trudno przypuszczać, aby główną motywacją prawodawcy była szczególna dbałość o prawa jednostek. Wszakże celem i sensem istnienia całej Strefy jest przekonanie zagranicznych inwestorów do prowadzenia działalności na terenie Zjednoczonych Emiratów Arabskich. Niezależnie od motywacji, wydaje się jednak, iż każdy progres w dziedzinie ochrony danych osobowych należy oceniać pozytywnie.

Do dziś Komisja Europejska nie zabrała stanowiska co do ochrony danych osobowych na wydzielonym terytorium państwa, choć przepisy RODO zdają się dopuszczać taką możliwość. Dokonując racjonalnej

oceny, trzeba jednak przyznać, iż ogólnopaństwowe problemy w zakresie praworządności Zjednoczonych Emiratów Arabskich mogą negatywnie wpłynąć na ocenę DIFC. To samo odnosi się do swoistych przywilejów nadawanych przez prawodawstwo DIFC na rzecz instytucji finansowych. Strefa niewątpliwie posiada regulację stanowiącą doskonały punkt wyjścia do dalszego rozwoju systemu ochrony danych. Jednakże wydanie decyzji o adekwatności przez Komisję Europejską wymaga dalszych działań, które być może zostaną podjęte podczas toczących się prac nad nowelizacją ustawy.

8. Rosja

8.1. Wstęp

Dla wielu krajów Unii Europejskiej Federacja Rosyjska wciąż pozostaje znaczącym partnerem gospodarczym, a współpraca między podmiotami europejskimi i rosyjskimi często wymaga wymiany przetwarzanych przez nie danych osobowych. Jednocześnie głośno się mówi o naruszeniach w sferze ochrony danych osobowych w tym państwie. Ciekawe jest, że w tym przypadku mowa jest o naruszeniach ze strony państwa, a nie podmiotów gospodarczych.

I chociaż niemal od upadku Związku Radzieckiego rosyjska konstytucja gwarantuje ochronę prywatności, danych osobowych czy tajemnicy komunikowania się, rzeczywistość często w znacznym stopniu odbiega od przepisów ustawy zasadniczej. Sytuację komplikuje fakt, że Rosja zmaga się od lat z poważną liczbą cyberataków i zagrożeniem cyberbezpieczeństwa państwa. Niezbędne zatem było wprowadzenie dosyć rygorystycznych przepisów w zakresie przetwarzania danych osobowych, które w niektórych aspektach w sposób kontrowersyjny regulują te kwestie. Niezależnie od tego ogólne zasady przetwarzania danych osobowych są podobne do tych, które znamy z RODO. W ustawie zagwarantowane są często tożsame uprawnienia jednostki, obowiązki podmiotów, które dane przetwarzają, a także podobne regulacje dotyczące zabezpieczeń technicznych czy organizacyjnych.

Jednocześnie największą różnicą jest to, że głównym beneficjentem przepisów o ochronie danych osobowych nie jest jednostka, a państwo. W połączeniu z oskarżeniami o autorytarne formy rządów w Federacji Rosyjskiej pod znakiem zapytania stoi uznanie tego państwa przez Komisję Europejską za zapewniające adekwatny poziom ochrony.

8.2. Regulacja konstytucyjna

Kwestia ochrony prywatności i danych osobowych była obca sowieckiemu rozumieniu społeczeństwa, państwa i praw człowieka[270]. Dopiero w 1993 r. uregulowano to zagadnienie w konstytucji demokratycznej Federacji Rosyjskiej.

Ustrojodawca rosyjski poświęcił kwestii prywatności aż trzy niezależne artykuły ustawy zasadniczej. Umieszczone zostały one w rozdziale drugim konstytucji poświęconym prawom i wolnościom człowieka i obywatela. W art. 23 gwarantuje się nienaruszalność życia prywatnego, ochronę tajemnicy osobistej i rodzinnej oraz obronę czci i dobrego imienia. W ust. 2 gwarantuje się każdemu, a więc również cudzoziemcom przebywającym czasowo lub stale na terytorium Federacji Rosyjskiej, prawo do tajemnicy korespondencji, rozmów telefonicznych oraz informacji przekazywanych drogą pocztową, telegraficzną i inną. Wszelkie ograniczenia tego prawa są dopuszczalne jedynie w przypadku prawomocnego postanowienia sądowego.

Ustawa zasadnicza odnosi się również do kwestii informacji na temat osoby, zabraniając zbierania, przechowywania, wykorzystywania i rozpowszechniania informacji na temat życia prywatnego osoby zainteresowanej bez jej zgody. Wraz ze wzrostem świadomości na temat zagrożeń związanych z nieuprawnionym przetwarzaniem danych osobowych, do

[270] N. Dorryakova, *Privacy in the Russian Legislation,* https://www.law.uw.edu/media/1304/russia-intermediary-liability-of-isps-privacy.pdf [dostęp 9.07.2019].

katalogu wskazanego w art. 24, na poziomie ustawowym dodano informacje na temat stanu zdrowia, transakcji finansowych, tajemnic handlowych, *cookies*, fotografie oraz informacje zawarte na profilach w mediach społecznościowych[271]. Ustawa zasadnicza nakłada również obowiązek na organy władzy państwowej i samorządu terytorialnego oraz ich funkcjonariuszy zapewnienia każdemu zainteresowanemu możliwości zapoznania się z dokumentami i materiałami bezpośrednio dotyczącymi jego praw i wolności, o ile ustawa nie stanowi inaczej. Konstytucja Federacji Rosyjskiej zapewnia również nienaruszalność mieszkania, zabraniając każdemu wkraczania do niego wbrew woli zamieszkujących w nim osób, z wyjątkiem przypadków przewidzianych przez ustawę federalną lub na podstawie postanowienia sądu.

Nie można również zapominać, że zgodnie z art. 15 konstytucji, częścią składową systemu prawnego Federacji Rosyjskiej są ogólnie uznane zasady i normy prawa międzynarodowego oraz porozumienia międzynarodowe zawarte przez Federację Rosyjską. W przypadku konfliktu między porozumieniem międzynarodowym a prawem krajowym, pierwszeństwo przyznaje się prawu międzynarodowemu. Oznacza to, że gwarancje dotyczące ochrony prawa do prywatności zawarte w Europejskiej Konwencji Praw Człowieka[272] czy MPOiP. W przypadku zatem, gdy okaże się, że wewnętrzne ustawodawstwo w sposób niewystarczający chroni prywatność i dane osobowe jednostki bądź gdy jednostka nie może wyegzekwować przyznanych jej w porozumieniach międzynarodowych praw, może ona złożyć skargę zgodnie z procedurą opisaną w poszczególnych aktach prawa międzynarodowego. Warto zauważyć, że obywatele Rosji oraz osoby, które uznają, że organy rosyjskie naruszyły jej uprawnienia w tym zakresie bądź nie zapewniły odpowiednich gwarancji, skrupulatnie

[271] D. Garrie, I. Byhovsky, *Privacy and Data Protection in Russia, „*Journal of Law and Cyber Welfare" 2017, s. 237.

[272] 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.

korzystają z przyznanych im w aktach prawa międzynarodowego uprawnień, a Federacja Rosyjska wielokrotnie była stroną postępowań prowadzonych np. przez Europejski Trybunał Praw Człowieka[273].

8.3. Regulacja ustawowa

Dopiero w 2006 r. rosyjski ustawodawca pochylił się nad kwestią prywatności i ochrony danych osobowych, uchwalając ustawę o ochronie danych osobowych[274] oraz ustawę o lokalizacji danych[275]. Przepisy ustawy o ochronie danych osobowych były zbliżone do regulacji Unii Europejskiej zawartych w dyrektywie 95/46/WE. Celem ustawy było wzmocnienie praw jednostki w zakresie przetwarzania jej danych osobowych, w tym także prawa do prywatności życia rodzinnego i osobistego oraz nienaruszalności prywatności jednostki. Przepisów omawianej ustawy nie stosuje się jednak do danych zanonimizowanych, powszechnie dostępnych informacji, danych niezbędnych do funkcjonowania sądownictwa oraz wymaganych w związku z wypełnianiem przez Federację Rosyjską jej obowiązków wynikających z prawa międzynarodowego.

Na podstawie omawianej ustawy zostało wydane rozporządzenie wykonawcze dotyczące zaakceptowanych przez rząd środków organizacyjnych i technicznych oraz metod ochrony danych osobowych, które mają przeciwdziałać naruszeniom.

Jedną z cech charakterystycznych dla rosyjskiego prawa ochrony danych osobowych jest brak rozróżnienia między podmiotem administrującym a przetwarzającym dane, zastąpionych ogólnym pojęciem

[273] Wyrok ETPCz z dnia 16 października 2010 r. w sprawie *Nazarenko v Russia* (ECtHR) No 34938/13.

[274] Federal Law FZ-152.

[275] Federal Law FZ-242

operatora danych, którego działania podlegają omawianym ustawom[276]. W związku z tym, niezależnie od tego, jaką rolę pełni dany podmiot i jakie czynności wykonuje w odniesieniu do danych osobowych, podlega tym samym rygorystycznym przepisom.

Podmioty prywatne, które chcą przetwarzać dane osobowe obywateli rosyjskich, muszą spełnić szereg warunków. Konieczne jest uzyskanie przez nie zgody podmiotu danych osobowych na przetwarzanie jego danych, zobowiązane są do przestrzegania prawa stanowionego w tym zakresie, powinny powołać inspektora ochrony danych osobowych, wdrożyć odpowiednie środki techniczne i organizacyjne w celu przeciwdziałania naruszeniom oraz są zobowiązane do powiadamiania podmiotów, których dane dotyczą, o wszelkich zaistniałych naruszeniach.

22 lipca 2014 r. uchwalono nowelizację ustawy o ochronie danych osobowych, która weszła w życie 1 września 2015 r. Zgodnie z jej brzmieniem wszyscy operatorzy danych osobowych powinni gromadzić i przetwarzać dane osobowe obywateli Rosji jedynie na terytorium Federacji Rosyjskiej (z poszanowaniem pewnych wyjątków)[277]. Karą za nieprzestrzeganie tego obowiązku jest blokada strony internetowej podmiotu naruszającego oraz rejestracja naruszenia w Rejestrze Naruszeń Praw Podmiotów Danych Osobowych prowadzonym przez Roskomnadzor. W praktyce nowelizacja wymusza na dostawcach internetowych treści posiadanie serwerów na terytorium Rosji oraz przetwarzanie danych pochodzących z Federacji tylko w tym państwie[278]. Dotyczy to wszystkich dostawców usług, którzy przetwarzają jakiekolwiek dane osobowe,

[276] V. Khayryuzov, *The Privacy, Data Protection and Cybersecurity Law Review – Edition 5. Russia,* https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175638/russia [dostęp 10.07.2019].

[277] *Data Protection Laws of the World. Russia.,* https://www.dlapiperdataprotection.com/index.html?t=law&c=RU [dostęp 9.07.2019].

[278] J. Priebe, J. Tomaszewski, *Fortress Russia – The Russian Data Localization Law*, https://www.globalprivacywatch.com/2015/05/fortress-russia-the-russian-data-localization-law/ [dostęp 10.07.2019].

chociażby adres e-mail (którego podanie jest niezbędne w celu korzystania niemal ze wszystkich usług oferowanych przez Internet)[279].

Mimo dosyć wysokiego zagrożenia cyberprzestępczością, która ponadto generuje olbrzymie koszty w Federacji Rosyjskiej, ustawodawca dotychczas dosyć powoli wprowadzał wymagane zmiany w prawie, które w sposób całościowy odnosiłyby się do problemu ochrony danych osobowych w Rosji[280]. Jednocześnie, gdy zdecydowano się na zmiany, przybrały one inny kierunek niż spodziewany i pożądany zarówno przez obywateli rosyjskich oraz organizacje międzynarodowe zajmujące się ochroną praw człowieka.

W lipcu 2016 r. Vladimir Putin podpisał jedną z najbardziej kontrowersyjnych nowelizacji w zakresie danych osobowych – prawo Yarovaya[281].

[279] Na marginesie można wskazać, że kontrowersyjna nowelizacja jednoznacznie wskazała, że blogerzy, których strony odwiedza dziennie więcej niż 3 tysięcy użytkowników, są poddani takim samym restrykcjom jak tradycyjne redakcje oraz zobowiązani są do wpisania się do publicznego rejestru blogerów pod groźbą zakazu dalszej publikacji. Zob. M. S. Zhuravlev, T.A. Brazhnik, *Problems for Internet Business and Users Caused by New Russian Legislation*, „Information Law Journal" 2014, Vol. 5, Issue 4, s. 26, *Complying with Russia's New Privacy law,* https://www.gartner.com/smarterwithgartner/complying-with-russias-new-privacy-law/ [dostęp 10.07.2019].

[280] D. Garrie, I. Byhovsky, *op. cit.*, s. 236.

[281] Russian Federal Law # 375--ФЗ dated July 6, 2016 On Making Changes into the Criminal Code of the Russian Federation and into the Criminal Procedural Code of the Russian Federation in Part Establishing Additional Measures On Counteracting Terrorism and Ensuring Public Safety introduced changes to 1) the Criminal Code, 2) the Criminal Procedural Code of the Russian Federation and 3) the Federal Law dated July 27, 2006 # 153--ФЗOn Introducing Changes into Separate Legislative Acts of the Russian Federation in Relating to Adoption of the Federal Law On Ratification of Convention of the Council of Europe On Prevention of Terrorism and On Federal Law On Counteracting Terrorism. Russian Federal Law# 374--ФЗ dated July 6, 2016 On Making Changes into the Federal Law on Counteracting Terrorism and Separate Legal Acts of the Russian Federation in Part Establishing Additional Measures On Counteracting Terrorism and Ensuring Public Safety introduced changes into 18 laws, including: 1) Federal Law On Counteracting Terrorism; 2) Federal Law On Federal Security Service; 3) Federal Law On Executive Investigative Activity; 4) Federal Law On External Intelligence; 5) Federal Law on Procedure of Exiting the Russian Federation and Entering into the Russian Federation; 6) Federal Law On Weapons; 7) Air Code of the Russian Federation; 8) Federal Law On Freedom of Conscience and on Religious Associations; 8) Federal Law On Post Communication; 10) Federal Law On

Pakiet składa się z szeregu regulacji zmieniających dotychczas obowiązujące prawo, nakładając na podmioty dostarczające usługi telekomunikacyjne, w tym sieć komputerową, obowiązek gromadzenia przez 6 miesięcy kopii zapasowych wszelkich rozmów, zarówno wiadomości głosowych, jak i tekstowych, niezależnie, czy zostały one wyrażone w piśmie czy np. w formie zdjęcia bądź internetowego mema[282]. Ponadto podmioty te są zobowiązywane do gromadzenia przez co najmniej rok od powzięcia aktywności przez użytkownika informacji na temat otrzymywania bądź przesyłania zarówno jakichkolwiek wiadomości głosowych, tekstowych, obrazkowych, dźwięków lub w formie filmów przez rzeczonych użytkowników, jak i informacji na temat ich samych[283]. Dostawcy usług telekomunikacyjnych zobowiązani są do dostarczania kopii wskazanych powyżej informacji organom nadzoru oraz haseł i kluczy niezbędnych do odkodowania informacji w przypadku stosowania tego rodzaju zabezpieczeń.

Nowelizacja sprecyzowała i rozszerzyła zakres danych, które w przypadku ich przetwarzania powinny pozostać na terytorium Federacji Rosyjskiej. Zakaz przetwarzania danych poza terytorium Rosji obejmuje wszystkie wiadomości elektroniczne, które spełniają jedno z następujących kryteriów i dotyczą: 1) użytkowników zarejestrowanych lub zalogowanych pod adresem IP przypisanym do dostawcy usług internetowych zarejestrowanego Rosji; 2) użytkowników, którzy podpisując umowę na dostawę

Counteracting Legalization (Laundering) of Income, Received by Illegal Means, and of Financing of Terrorism; 11) Code of the Russian Federation On Administrative Offenses; 12) Federal Law On Transport--Expedition Activity; 13) Federal Law On Communication; 14) Housing Code of the Russian Federation; 15) Federal Law on Information, Informational Technologies, and On Protection of Information; 16) Federal Law On Transport Safety; 17) Federal Law On the Territorial Jurisdiction of District (Naval) Military Courts; and 18) Federal Law On the Security of the Fuel and Energy Complex. Dalej jako „prawo Yarovaya".

[282] Gorodissky & Partneres, *Yarovaya Law and new data storage requirements for online data distributors*, https://www.lexology.com/library/detail.aspx?g=8029c37f-5a1c-4025-ac3f-8b3ede9c42e8 [dostęp 9.07.2019].

[283] *Ibidem.*

usług telekomunikacyjnych posługiwali się paszportem rosyjskim bądź innym dokumentem wydanym przez rosyjskie organy administracji publicznej; 3) użytkowników, którzy korzystali z narzędzi bądź oprogramowania, które zostało w tym czasie zlokalizowane czasowo lub stale w Rosji (co stwierdza się przez użycie narzędzi geolokalizacyjnych); 4) użytkowników, którzy podali numer telefonu przypisany do rosyjskiego dostawcy usług telekomunikacyjnych w trakcie podpisywania umowy o dostarczenie usług telekomunikacyjnych; 5) użytkowników, których dostawcy danych internetowych znajdują się na terytorium Rosji bądź zostali za takich uznani przez organy administracji publicznej Federacji.

Prawo Yarovaya obejmuje zatem swoim zakresem praktycznie każdego użytkownika Internetu, który znajduje się na terytorium Rosji bądź w jakikolwiek sposób jest związany z Federacją, chociażby przez umowę z operatorem tam zarejestrowanym. Stwarza to ogromne ryzyko nieakceptowalnej przez kraje Unii Europejskiej inwigilacji i stanowi naruszenie bezpieczeństwa danych osobowych. Rosyjskie sądy dotychczas nie badały zgodności znowelizowanych przepisów z art. 23 konstytucji Federacji Rosyjskiej, który jak już zostało wspomniane zapewnia wolność i ochronę tajemnicy korespondencji. Nałożony na dostawców usług sieciowych obowiązek nie tylko przetrzymywania wszelkiej korespondencji (jak też informacji o prowadzeniu korespondencji), ale również przekazywania treści wiadomości wraz z kluczem do ich odkodowania organom państwowym stanowi oczywiste naruszenie tajemnicy korespondencji. Warto zauważyć, że żądanie udostępnienia określonych wiadomości nie musi być poparte postanowieniem sądu.

Wydaje się, że zakres i forma wprowadzonych przepisów stoi w oczywistej sprzeczności z europejskim rozumieniem prawa do prywatności i ochrony danych osobowych. Legislacja, która według jej twórców miała służyć przede wszystkim ochronie państwa i obywateli przed cyberterroryzmem i cyberprzestępczością, według jej przeciwników będzie

służyć wyłącznie uciszaniu opozycji politycznej i przejęciu przez rząd całkowitej kontroli nad użytkownikami Internetu w Rosji[284].

8.4. Praktyka

Federacja Rosyjska, podobnie jak omówiona już Chińska Republika Ludowa, charakteryzuje się specyficznym systemem prawnym, który w znacznym stopniu dopuszcza autorytarne działania władzy, które istotnie manipulują i kontrolują stosowanie prawa w praktyce[285].

Nad przestrzeganiem zawartych w ustawach gwarancji ochrony danych osobowych czuwa Prokurator Generalny, Roskomnadzor (Federalne Biuro Kontroli nad Komunikacją, Technologiami Informacyjnymi i Prasą) i Federalne Biuro Kontroli Technicznej i Eksportu. Główny ciężar badania i penalizowania naruszeń został nałożony jednak na Roskomnadzor, który jest uprawniony do wysyłania zapytań w zakresie przetwarzania danych osobowych zarówno do osób fizycznych jako podmiotów danych osobowych, jak i osób prawnych, które te dane przetwarzają; przeprowadzania kontroli oraz sprawdzania poprawności informacji przekazywanych przez operatorów danych i podmiotów przetwarzających na temat przetwarzania danych przekazywanych osobom fizycznym. Ponadto do zadań organu należy rozpatrywanie skarg podmiotów prywatnych, podejmowanie działań konsultacyjnych i opiniodawczych, analiza publikacji prasowych związanych z przetwarzaniem danych osobowych oraz współpraca międzynarodowa w tym zakresie.

Kontrole przeprowadzane przez organ mogą ograniczać się jedynie do sprawdzenia dokumentów związanych z przetwarzaniem danych bądź być przeprowadzone w miejscu prowadzenia działalności i obejmować

[284] *Russia's 'Big Brother' Law Enters Into Force,* https://www.themoscowtimes.com/2018/07/01/russias-big-brother-law-enters-into-force-a62066 [dostęp 9.07.2019].

[285] A.J. Cornell, *Right to Privacy*, https://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156 [dostęp 9.07.2019].

zarówno kontrolę infrastruktury informatycznej, jak i zabezpieczeń techniczno-organizacyjnych[286]. Niezależnie od tego Roskomnadzor stale monitoruje sieć internetową w celu zapobiegania naruszeniom prawa. Przeprowadzane kontrole mogą być zaplanowane i ważne przez rok (co oznacza, że nie powinno w tym czasie dochodzić do ponownych audytów) bądź zapowiedziane jedynie z 24-godzinnym uprzedzeniem w przypadku złożenia skargi na działalność podmiotu[287].

Mimo że Roskomnadzor jest uprawniony do blokowania stron internetowych oraz rozwiązywania podmiotów, które przetwarzają dane osobowe z naruszeniem prawa, dotychczas w przypadku stwierdzonych naruszeń nakładał na nie kary finansowe i administracyjne, niewykluczone jednak, że w przyszłości zmieni dotychczasową praktykę[288]. Jednocześnie, w przypadku sprzeciwu organizacji wobec nałożonej kary, sądy często nie tylko podtrzymują decyzję Rostkomnadzoru, ale również zakazują prowadzenia działalności na terytorium Rosji i wygaszają ich strony internetowe. Do najczęstszych przewinień odnotowanych przez rosyjskie sądu należy bez wątpienia niedopełnienie obowiązku powiadomienia wobec organu bądź jednostki. Można je podzielić na następujące grupy: 1) niedopełnienie obowiązku informacyjnego bądź opóźnienie w poinformowaniu Roskomnadzoru o przetwarzaniu danych; 2) niedopełnienie obowiązku informacyjnego bądź opóźnienie w odpowiedzi na zapytanie przesłane przez Roskomnadzor; 3) przesłanie niekompletnych bądź nieprawidłowych informacji o przetwarzaniu danych do Roskomnadzoru; 4) niedopełnienie obowiązku poinformowania o zmianach w przetwarzaniu danych osobowych[289].

[286] A. Savelye, *Russia's new personal data localization regulations: A step forward or a self-imposed sanction?*, „Computer Law & Security Review" 2016, 32, s. 128–145.

[287] *Ibidem.*

[288] D. Garrie, I. Byhovsky, *op. cit.*, s. 246.

[289] *Judicial Practice of 2008-2009 Involving Roskomnadzor in regard to Violations of the Federal Law No. 152 On Personal Data,* http://eng.pd.rkn.gov.ru/legislation_of_the_russian_federation/judicial_practice/ [dostęp 11.07.2019].

Na kary szczególnie narażone są podmioty międzynarodowe, takie jak Google, Facebook, czy już zamknięty w Rosji LinkedIn[290]. Warto jednocześnie zauważyć, że część podmiotów międzynarodowych niemal natychmiast po nowelizacji z 2015 r. przeniosło dane rosyjskich użytkowników na serwery zlokalizowane w Federacji, aby uniknąć naruszenia ustawy[291]. Większy opór wśród korporacji międzynarodowych bez wątpienia powodują przepisy prawa Yarovai – tylko w czerwcu 2019 r. rosyjskie agencje rządowe wystąpiły do Google z żądaniem usunięcia ponad 19 tysięcy wyników znajdujących się na stronach internetowych giganta[292].

20 marca 2018 r. Sąd Najwyższy w Rosji oddalił skargę spółki Telegram, które żądała unieważnienia zarządzenia rządowej Agencji Bezpieczeństwa nakładającego na spółkę obowiązek dostarczenia kluczy kodujących umożliwiających Agencji odczytywanie wiadomości przesyłanych przez użytkowników platformy społecznościowej Telegram[293]. Ta ostatnia stoi na stanowisku, że użyte przez nich narzędzia zabezpieczające uniemożliwiają odczytanie i przekazanie kluczy anonimizujących, podczas gdy zdaniem Agencji jest to technicznie możliwe[294]. Ostatecznie Telegram odmówił wydania kluczy, co poskutkowało wydaniem przez sąd okręgowy w Moskwie wyroku podtrzymującego blokadę serwisu. Roskomnadzor w kwietniu 2018 r. nakazał wszystkim operatorom internetowym i telefonicznym blokadę platformy społecznościowej Telegram[295].

[290] O. Razumovskaya, L. Mills, *Court Upholds Decision to Ban LinkedIn in Russia*, https://www.wsj.com/articles/court-upholds-decision-to-ban-linkedin-in-russia-1478791726 [dostęp 9.07.2019]; L. Goasduff, *Complying with Russia's New Privacy Law*, https://www.gartner.com/smarterwithgartner/complying-with-russias-new-privacy-law/ [dostęp 11.07.2019].

[291] *Uber agreed to move the personal data or Russians to Russia*, https://lenta.ru/news/2015/07/10/uber/ [dostęp 10.07.2019], *Viber moved its servers to Russia*, http://izvestia.ru/news/593438 [dostęp 10.07.2019].

[292] *Government requests to remove the content*, https://transparencyreport.google.com/government-removals/by-country/RU?hl=en&country_item_amount=group_by:totals;authority:%20RU%20&%20lu%20=%20country_item_amount [dostęp 10.07.2019].

[293] V. Khayryuzov, *op. cit.*

[294] *Ibidem.*

[295] *Ibidem.*

Organ próbował zablokować również samą platformę, jednak właściciele spółki skutecznie to uniemożliwiają, stale zmieniając adres IP. Działania Roskomnadzoru doprowadziły do zakłóceń w funkcjonowaniu innych stron internetowych, co natychmiast poskutkowało masową krytyką organu, a także do wszczęcia postępowania sądowego przeciwko Roskomnadzorowi, którego działania uniemożliwiły funkcjonowanie skarżącego[296]. Do dzisiaj organowi nie udało się całkowicie zablokować dostępu do serwisu Telegram[297].

W badaniach przeprowadzonych przez Instytut Ponemon, w latach 2014–2015 koszt poniesiony przez państwo w związku z cyberprzestępczością wzrósł o 29%[298]. Jednocześnie już od 2012 r. Roskomnadzor zauważał coraz większe zagrożenie cyberprzestępczością, wskazując jednakże na brak odpowiedniej reakcji władzy centralnej na cyberataki i brak odpowiednich regulacji w tym zakresie[299]. W swoich raportach organ wskazuje nawet na „systematyczne" naruszenia prawa ochrony danych osobowych w Rosji. W 2018 r. po przeprowadzeniu 728 inspekcji Roskomnadzor stwierdził niemal dwa tysiące naruszeń[300]. Średnia kara administracyjna nałożona na podmiot nieprzestrzegający przepisów ustaw rzadko kiedy przekraczała tysiąc dolarów (najwyższe kary były nakładane w przypadkach nieuzyskania zgody podmiotu danych osobowych na przetwarzanie danych)[301].

Podmioty prywatne, których dane są przetwarzane z naruszeniem prawa, mają prawo wystąpić z pozwem przeciwko naruszającemu o naprawienie szkody, w tym również szkody niemajątkowej, jednak takie

[296] *Ibidem.*

[297] *Ibidem.*

[298] D. Garrie, I. Byhovsky, *op. cit.*, s. 236.

[299] Report. Activity of the Competent Authority for Protecting the Rights of Personal Data Subjects, http://eng.pd.rkn.gov.ru/docs/report2012.pdf [dostęp 10.07.2019].

[300] K. Andreeva, A. Dergacheva, V. Striz, *Hot Topics In Data Privacy Regulation In Russia*, https://www.morganlewis.com/-/media/files/publication/presentation/webinar/2018/hot-topics-in-personal-data-regulation-in-russia_27nov18.ashx [dostęp 11.07.2019].

[301] *Ibidem.*

skargi mogą być składane w ramach postępowania sądowego, co sprawia, że jest to niezbyt popularny środek dochodzenia sprawiedliwości[302]. Konieczność przedstawienia dowodów wystąpienia szkody, nawet niematerialnej, a także skomplikowana procedura sądowa oraz stosunkowo niskie odszkodowania sprawiają, że jednostka chętniej składa zawiadomienie do organu nadzoru, jakim jest Roskomnadzor niż skargę indywidualną[303].

Skala naruszeń oraz brak efektywnych środków kontroli realizacji praw jednostki sprawiają, że trudno mówić o skutecznych gwarancjach ochrony prawa do prywatności w Rosji. Kontrowersyjne regulacje prawne oraz sposób ich wprowadzania, a także wyraźne nastawienie na ochronę interesów państwa, a nie jednostki pokazują, że Federacja Rosyjska przyjęła różny od europejskiego system ochrony danych osobowych. Warto również zwrócić uwagę, że rokrocznie przed Europejskim Trybunałem Praw Człowieka są rozpatrywane skargi przeciwko Rosji w zakresie naruszenia prawa do prywatności i ochrony danych osobowych przez władze rosyjskie.

8.5. Adekwatność ochrony

Federacja Rosyjska dotychczas nie została uznana przez Komisję Europejską za kraj zapewniający odpowiedni poziom ochrony w rozumieniu RODO. Nieprowadzone są również w tym momencie rozmowy, w celu zawarcia czy to umowy gospodarczej, czy innej formy współpracy. Mimo bliskiego położenia geograficznego, wydaje się, że Unia Europejska i Federacja Rosyjska są obecnie na przeciwległych biegunach ochrony danych osobowych.

Biorąc pod uwagę najbardziej kontrowersyjne przepisy prawa Yarovai, należy zaznaczyć, że przetwarzanie danych osobowych w Rosji nie odpowiada zasadom konieczności i niezbędności. Są one przetwarzane

[302] V. Khayryuzov, *op. cit.*
[303] *Ibidem.*

dłużej niż jest to wymagane do osiągnięcia celu, z uwagi na konieczność pozostawienia kopii zapasowych lub oryginałów dokumentów zawierających te informacje. Co prawda, ustawa o ochronie danych osobowych przewiduje konieczność zaprzestania przetwarzania i usunięcia ich w ciągu trzydziestu dni od osiągnięcia celu, dla którego zostały przetwarzane, bądź cofnięcia zgody podmiotu danych, jednak w wielu przypadkach opisanych w prawie Yarovai podmioty przetwarzające dane są zobowiązane do zachowania kopii informacji przez 6 lub 12 miesięcy w celu dostarczenia ich na żądanie organów administracji publicznej.

Wątpliwości budzi również brak rozróżnienia między administratorem danych osobowych i podmiotem przetwarzającym. Powoduje to nie tylko jednakowy zakres kompetencji obu podmiotów, ale co za tym idzie podaje w wątpliwość możliwość zapewnienia odpowiedniego stopnia ochrony. Może to również prowadzić do nierównomiernego obciążenia podmiotów przetwarzających obowiązkami wynikającymi z ustawy, biorąc pod uwagę korzyści ekonomiczne uzyskiwane z przetwarzania danych i sam zakres przetwarzania.

Mimo wyposażenia podmiotów danych osobowych w niemal tożsamy zakres praw, jak ten wynikający z RODO, wątpliwości budzi brak efektywnych narzędzi gwarantujących ochronę danych osobowych. Nieefektywne są bowiem procedury sądowe mające na celu przyznanie podmiotom poszkodowanym słusznego odszkodowania i przeciwdziałanie naruszeniom. Przypadek portalu Telegram pokazuje, że rosyjski organ nadzoru nie jest w stanie wyegzekwować nakładanych kar i zapewnić zgodności przetwarzania z przepisami prawa krajowego (abstrahując od samej oceny tego prawa). Dodatkowo w praktyce nie istnieją żadne gwarancje, które miałyby chronić jednostkę przed nadmierną ingerencją organów publicznych w jej prawo do prywatności, czego przykładem jest możliwość odczytywania korespondencji użytkowników Internetu, nawet gdy jest ona zakodowana.

Oczywiste jest, że poważne zastrzeżenia budzi również to, że w znacznym zakresie dane osobowe muszą być przetwarzane w Rosji, niezależnie od miejsca zarejestrowania podmiotu gospodarczego, który prowadzi działalność w tym państwie. Powoduje to komplikacje przede wszystkim zagranicznym podmiotom i może prowadzić do nieusprawiedliwionego uprzywilejowania podmiotów krajowych.

Federacja Rosyjska spełnia wymagania stawiane przez RODO w zakresie obowiązku informacyjnego względem podmiotu, którego dane dotyczą, uzyskania zgody tegoż podmiotu na przetwarzanie danych, powoływania inspektora ochrony danych osobowych, wprowadzenia ograniczeń w transgranicznym przesyłaniu danych czy obowiązków związanych z powiadamianiem o wystąpieniu naruszenia w ochronie danych osobowych. Warto zauważyć, że chociaż rosyjska legislacja nie zna koncepcji danych wrażliwych, prawodawca posługuje się pojęciem specjalnej kategorii danych osobowych oraz pojęciem danych biometrycznych, które odpowiadają pojęciu danych wrażliwych.

W kontekście Federacji Rosyjskiej warto również zwrócić uwagę, że samo uznanie tego państwa za kraj zapewniający adekwatny poziom ochrony nie umożliwi dwustronnego przekazywania danych osobowych. Przesyłanie danych osobowych z Rosji do państw trzecich, w tym również państw Unii Europejskiej podlega również wewnętrznym regulacjom państwa. Zgodnie z art. 12 ustawy o ochronie danych osobowych podmioty przetwarzające dane mogą przesyłać je do innych podmiotów znajdujących się na terytorium państwa trzeciego, jeśli jest ono uznane za zapewniające odpowiedni stopień ochrony. Za takie uznaje się państwa – strony konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[304]. Spełnia ten warunek większość państw – członków Unii Europejskiej. Ponadto Roskomnadzor może uznać

[304] Konwencja Nr 108 Rady Europy z 1981 r. 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).

poszczególne państwa za takie, które gwarantują adekwatny stopień ochrony[305]. Jednocześnie przesyłanie danych jest możliwie również przy wystąpieniu innych przesłanek, takich jak zgoda podmiotu, którego dane dotyczą, konieczność transferu danych w celu realizacji postanowień umowy między operatorem a podmiotem, którego dane dotyczą, a także żywotne interesy obu podmiotów. Nieznana jest w Rosji koncepcja transferu danych osobowych przez podmioty należące do jednej grupy kapitałowej w oparciu o wiążące reguły korporacyjne.

Niezależnie od powyższych zastrzeżeń, warto również zwrócić uwagę na wątpliwości w zakresie praworządności w działaniach władzy publicznej, poszanowania praw człowieka i obywatela oraz urzeczywistniania zasad demokratycznego państwa prawnego. Wszystkie te elementy są niezbędne do uznania, że państwo zapewnia odpowiedni stopień ochrony. Wydaje się nawet, że nawet jeśli nastąpi pełna harmonizacja rosyjskiego prawa ochrony danych osobowych z RODO, nie sprawi to, że Federacja Rosyjska automatycznie zostanie uznana za kraj zapewniający odpowiedni stopień ochrony. Harmonizacja będzie zatem stanowić ułatwienie dla międzynarodowych podmiotów gospodarczych, które nie będą musiały dostosowywać standardów ochrony danych osobowych[306]. Jednakże, wydaje się, że dopóki formy rządów, które noszą cechy autorytaryzmu, nie przekształcą się w rozwiązania w pełni demokratyczne, nie będzie możliwe wydanie decyzji o adekwatności przez Komisję Europejską.

[305] Za takie dotychczas uznano: Australię, Argentynę, Izrael, Kanadę, Maroko, Malezję, Meksyk, Mongolię, Nową Zelandię, Angolę, Benin, Cape Verde, Koreę, Peru, Tunezję, Chile, Kosta Ryke, Katar, Mali, Singapur, RPA, Gabon i Kazachstan.

[306] *Russia: Harmonising Data Protection Laws With The Eu,* http://www.gorodissky.com/publications/articles/russia-harmonising-data-protection-laws-with-the-eu/ [dostęp 11.07.2019].

8.6. Wnioski

Bez wątpienia z uwagi na rozwój współpracy gospodarczej między Unią Europejską a Federacją Rosyjską pożądany jest taki stan rzeczy, w którym podmioty międzynarodowe prowadzące działalność gospodarczą w Rosji i UE w sposób względnie swobodny i harmonijny mogłyby wzajemnie przekazywać sobie dane osobowe. Jednocześnie dążenia ekonomiczne nie powinny przysłaniać konieczności zapewnienia elementarnych gwarancji w zakresie ochrony tychże danych. Obecnie pomimo bliskości terytorialnej ochrona danych osobowych w obu systemach pozostaje na przeciwległych biegunach. Wydaje się, że nie jest możliwe w najbliższym czasie uznanie Federacji Rosyjskiej za państwo zapewniające odpowiedni poziom ochrony.

Brak odpowiednich gwarancji poszanowania praw człowieka, w tym również prawa do ochrony prywatności i danych osobowych, a także niezrozumiały obowiązek przetwarzania danych osobowych na terytorium Federacji Rosyjskiej przez podmioty oferujące tam usługi, zwiększa nieufność wobec rządzących i stawia pod znakiem zapytania kwestię uznania tego państwa za praworządne i demokratyczne, co jest warunkiem niezbędnym do wydania decyzji o adekwatności.

Kolejnym aspektem, nad którym należy się poważnie zastanowić, jest ocena efektywności rozwiązań prawnych i skuteczność gwarancji w nich zawartych. Wydaje się, że nie można za takie uznać rozwiązań, które uniemożliwiają podmiotom prywatnym uchylanie się od wykonania decyzji organu nadzoru i sądu, niezależnie od oceny zasadności prawomocnego orzeczenia sądu czy przyjętych rozwiązań prawnych. Szczególnie niepokojące jest to wtedy, kiedy organ nadzoru w istocie charakteryzuje się dosyć rozległymi kompetencjami, które w innych krajach mogłyby być nawet uznane za nadmierne. Praktyka nieprzyznawania adekwatnych odszkodowań w przypadku skarg podmiotów prywatnych, a także długotrwałe i skomplikowane procedury, które *de facto* czynią je

nieużytecznymi i w konsekwencji nieużywanymi przez obywateli pokazuje martwość przyjętych regulacji prawnych. Jednak najbardziej niepokojący jest fakt, że w starciu z aparatem państwa jednostka nie ma żadnej możliwości zapobiegania naruszeniom w ochronie danych osobowych i prywatności dokonywanymi przez organy publiczne.

Oczywiste jest, że decyzja o uznaniu danego państwa za zapewniające odpowiedni poziom ochrony jest ułatwieniem w obrocie gospodarczym, ale nie warunkiem niezbędnym do przesyłania danych do Rosji. Jednocześnie, biorąc pod uwagę regulacje prawne w tym zakresie obowiązujące w Federacji Rosyjskiej, a także egzekwowalność przepisów, podmioty które decydują się skorzystać z innych możliwych sposobów transferu danych, powinny poważnie rozważyć wdrożenie dodatkowych narzędzi technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych, a także wziąć pod uwagę stopień inwigilacji, jakiego państwo dopuszcza się względem podmiotów znajdujących się pod jego jurysdykcją.

9. Singapur

9.1. Wstęp

Singapur powszechnie uznawany jest za jedno z najważniejszych centrów finansowych. Nieprawdopodobnie dynamiczny i owocny rozwój tamtejszej gospodarki uczynił z tego niewielkiego państwa drugi najbogatszy kraj Azji oraz jeden z najlepiej rozwiniętych krajów na świecie. Jednak Singapur kojarzony jest również z niezwykle surowym ustawodawstwem. Wystarczy wspomnieć, iż kara śmierci jest tam nadal dopuszczalna i stosowana.

Rozważania dotyczące szeroko pojętej prywatności i poufności w przypadku Singapuru należy poprzedzić informacją dotyczącą tajemnicy bankowej. Nie ulega bowiem wątpliwości, iż jednym z filarów singapurskiej gospodarki jest sektor bankowy i finansowy[307]. Znajduje to swe odzwierciedlenie w lokalnych przepisach prawa bankowego, które definiują jeden z najsurowszych reżimów tajemnicy bankowej na świecie.

9.2. Regulacja konstytucyjna

Republika Singapuru uzyskała niepodległość 9 sierpnia 1965 r. Wtedy też uchwalono konstytucję, która obowiązuje do dziś. Pomimo licznych nowelizacji ustawy zasadniczej katalog zawartych w niej praw i wolności

[307] Polska Agencja Inwestycji i Handlu, *Singapur. Przewodnik po rynku*, Warszawa 2017, s. 4.

człowieka nadal pozostaje stosunkowo skromny. Rozdział IV konstytucji zatytułowany „Podstawowe wolności" zawiera zaledwie osiem artykułów, które formułują m.in. zakaz dyskryminacji[308], wolność słowa i zgromadzeń[309], wolność wyznania[310] oraz prawo do edukacji[311]. Próżno w nim jednak szukać jakichkolwiek odniesień do gwarancji dotyczących prywatności.

Pomimo dość czytelnej regulacji konstytucyjnej przedstawiciele doktryny podejmują próby wyinterpretowania prawa do prywatności z innych przepisów ustawy zasadniczej. W szczególności rozważania te dotyczą art. 9 (1), który gwarantuje wolność osobistą[312]. W literaturze wskazuje się, iż podobną wykładnię stosuje się w Indiach, a zbieżność przepisów obydwu konstytucji pozwala przypuszczać, iż takie rozwiązanie byłoby możliwe również w Singapurze[313]. Co ciekawe, dyskusja dotycząca art. 9 (1) przeniesiona została z rozważań doktrynalnych i znalazła swe odzwierciedlenie w lokalnym orzecznictwie. Pierwszym zwiastunem zmian było orzeczenie w sprawie *Ong Ah Chuan v Public Prosecutor*[314]. W wyroku wskazano, iż należy przychylić się do postulatu szerokiej wykładni konstytucji w celu zapewnienia jednostkom jak najpełniejszej realizacji zasady sprawiedliwości. Mimo iż podobne stanowisko zostało podtrzymane również w wyroku w sprawie *Haw Tua Tau v Public Prosecutor*, późniejsza linia orzecznicza *Judicial Committee of the Privy Council* wskazywała raczej na literalną i wąską interpretację art. 9 (1). Utrzymała się ona, aż to zmian w ustroju singapurskiej władzy

[308] Art. 12 Konstytucji Singapuru.

[309] Art. 14 *ibidem*.

[310] Art. 15 *ibidem*.

[311] Art. 16 *ibidem*.

[312] „Art. 9(1) Nikt nie może być pozbawiony życia lub wolności osobistej z wyjątkiem sytuacji określonych w prawie" [tłum. M. Abu Gholeh].

[313] S. Wee Choong Sian, *Privacy law: a case for the protection of informational privacy in Singapore*, „Singapore Law Review" 2013, vol. 31, s. 145.

[314] Wyrok Judicial Committee of the Privy Council z dnia 15 października 1980 w sprawie *Ong Ah Chuan and another v. Public Prosecutor*, UKPC 32.

sądowniczej. W 1994 r. zniesiono możliwość wnoszenia apelacji w sprawach karnych do *Judicial Committee of the Privy Council* i przekazano tę kompetencję Sądowi Apelacyjnemu Republiki Singapuru[315]. Sąd ten kilkukrotnie potwierdzał konieczność szerokiej interpretacji wspomnianego artykułu. W szczególności odnosił się on do rozumienia słów „sytuacji określonych w prawie"[316], które (zdaniem Sądu) mogą obejmować także fundamentalne zasady naturalnej sprawiedliwości (*natural justice*)[317]. Powyższe wskazuje na to, iż wyinterpretowanie prawa do prywatności z art. 9 (1) konstytucji jest wykładnią dominującą. Tym samym mimo faktu, iż prawo do prywatności nie jest *expressis verbis* wyrażone w ustawie zasadniczej, można wskazać na pewien stopień konstytucyjnej ochrony prywatności[318]. I choć obecna linia orzecznicza wydaje się ugruntowana, to nadal obecne są głosy nawołujące do wyraźnego uregulowania tej kwestii w konstytucyjnym katalogu praw i wolności[319].

9.3. Regulacje ustawowe

Na poziomie aktów podkonstytucyjnych można wskazać na kilka istotnych regulacji odnoszących się do tematyki szeroko pojętej prywatności oraz ochrony danych osobowych. Z punktu widzenia niniejszych rozważań za najistotniejszą regulację należy uznać lokalną ustawę o ochronie danych osobowych, przyjętą w 2012 r.[320] Nie bez znaczenia pozostaje jednak ustawa o zagrożeniach komputerowych i cyberbezpieczeństwie

[315] A.K. Cieśniewski, *Kodeks karny Singapuru*, „Prokuratura i Prawo" 2016/3, s. 121.

[316] *In accordance with law*.

[317] Wyrok Sądu Apelacyjnego Republiki Singapuru z dnia 20 października 2004 w *sprawie Nguyen Tuong Van v Public Prosecutor* [2005] 1 SLR 103.

[318] S. Wee Choong Sian, *op. cit.*, s. 147.

[319] Privacy International, *The Right to Privacy in Singapore. Stakeholder Report Universal Periotic Review,* https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf [dostęp 1.06.2019].

[320] Personal Data Protection Act 2012. Dalej jako: PDPA.

z 2017 r., która penalizuje nieuprawniony dostęp do danych[321]. Istotne przepisy wprowadza również lokalne prawo telekomunikacyjne[322] oraz bankowe[323]. W tym miejscu warto wskazać, iż Singapur jest jednym z ostatnich państw, które do dziś nie przystąpiły do Międzynarodowego Paktu Praw Obywatelskich i Politycznych[324]. Fakt ten jest o tyle istotny, iż Pakt w art. 17 przewiduje prawo do prywatności.

Trzonem singapurskiego reżimu ochrony danych osobowych jest wspomniana wyżej regulacja PDPA. Pomimo dynamicznego rozwoju prawa ochrony danych w krajach azjatyckich PDPA pozostaje jedną z pierwszych kompleksowych regulacji w tym regionie. Ustawa weszła w życie 2 stycznia 2013 r., implementując zdecydowaną większość wytycznych OECD dotyczących prywatności[325]. Jak wskazano na wstępie, celem PDPA jest wprowadzenie zasad dotyczących zbierania, korzystania i udostępniania danych osobowych z poszanowaniem praw i interesów podmiotów danych oraz podmiotów przetwarzających[326]. Ustawa nie znajduje jednak zastosowania do organów władzy publicznej oraz innych podmiotów działających w ich imieniu. Co interesujące (i zaskakujące), zakresem obowiązywania PDPA nie objęto również czynności przetwarzania danych wynikających ze stosunku pracy. Podobnie natomiast do rozwiązań przyjętych w innych państwach, ustawa nie dotyczy czynności przetwarzania o charakterze osobistym lub domowym[327]. Dodatkowe wyłączenia przewidziano na rzecz danych zawartych w zbiorach danych

[321] Computer Misuse And Cybersecurity (Amendment) Act, No. 22 of 2017.

[322] Telecomunications Act, No. 43 of 1999.

[323] Banking Act, No. 41 of 1970.

[324] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. z 1977 r. Nr 38, poz. 167.

[325] The OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [dostęp 1.06.2019].

[326] Art. 3 PDPA.

[327] Art. 4 (1) *ibidem.*

przez okres dłuższy niż 100 lat[328], danych osobowych osób zmarłych[329] oraz biznesowych danych kontaktowych[330,331].

Powyższe rozważania pozwalają na zdefiniowanie zakresu podmiotowego oraz terytorialnego stosowania PDPA. Nie ulega wątpliwości, iż ustawa znajdzie zastosowanie wyłącznie do podmiotów prywatnych. Przez podmioty (określane w akcie jako *organizations*) należy rozumieć zarówno osoby fizyczne, jak i prawne, niezależnie od tego, czy zostały utworzone na podstawie prawa singapurskiego oraz czy posiadają miejsce zamieszkania (siedzibę) na terenie państwa[332]. Tym samym należy stwierdzić, iż PDPA ma charakter eksterytorialny i znajduje zastosowanie do każdego podmiotu przetwarzającego tamtejsze dane osobowe, niezależenie od tego, gdzie dojdzie do czynności przetwarzania.

Co oczywiste, PDPA odnosi się do danych osobowych, które zostały zdefiniowane w dość zwięzły sposób. Zgodnie z definicją ustawową za dane osobowe należy uznać wszelkie dane dotyczące osoby (niezależnie od tego, czy są zgodne z prawdą czy nie), która na ich podstawie może być zidentyfikowana. Za dane osobowe należy również uznać takie informacje, które samoistnie nie identyfikują konkretnej osoby, jednak w połączeniu z innymi posiadanymi przez podmiot przetwarzający jest to wysoce prawdopodobne[333]. Według PDPA, dane osobowe mogą dotyczyć wyłącznie osoby fizycznej (również zmarłej). Definicja ta pozostaje spójna z najważniejszymi regulacjami na świecie, jednak, jak wiadomo, właściwy jej zakres ujawnia się zazwyczaj dopiero w praktyce stosowania

[328] Art. 4 (4a) *ibidem.*

[329] Z zastrzeżeniem, iż przepisy dotyczące udostępniania danych osobowych oraz ogólna reguła ochrony danych osobowych (art. 24) znajdują zastosowania przez 10 lat od momentu śmierci osoby. Art. 4 (4b) *ibidem*.

[330] Zgodnie z definicją legalną dane te obejmują imię, stanowisko, numer telefonu służbowego, służbowy adres korespondencyjny oraz mailowy oraz inne zbliżone informacje, które nie są udostępniane wyłącznie w celach osobistych.

[331] Poza wyjątkami wprost wskazanymi w ustawie. Art. 4 (5) PDPA.

[332] Art. 2 *ibidem*.

[333] *Ibidem.*

ustawy. Singapurska Komisja Ochrony Danych Osobowych (*Personal Data Protection Commission*)[334] w swoich wytycznych wskazuje przykłady danych osobowych. Wymienia wśród nich m.in. numer telefonu komórkowego, utrwalony obraz twarzy, utrwalony zapis głosu, odciski palców, obraz tęczówki oka, czy profil DNA[335]. Warto jednak zaznaczyć, iż PDPA nie przewiduje specjalnych kategorii danych, np. danych wrażliwych, które wyróżnione są w innych porządkach prawnych. Pomimo tego naruszenie zasad przetwarzania w odniesieniu do danych powszechnie uznawanych za wrażliwe może stanowić podstawę do zaostrzenia nałożonej kary.

Ustawodawca wprowadził również legalną definicję przetwarzania, tym samym określając katalog czynności objętych zakresem omawianego aktu. Zgodnie z brzmieniem art. 2 przetwarzanie obejmuje wszelkie operacje lub zestawy operacji wykonywane na danych osobowych, w szczególności takie jak utrwalanie, przechowywanie, organizowanie, adaptowanie, modyfikowanie, pobieranie, łączenie, przesyłanie, usuwanie lub niszczenie. Przytoczony katalog nie ma jednak charakteru zamkniętego. Dość łatwo można więc dostrzec zbieżność z europejskim rozumieniem przetwarzania wprowadzonym przez przepisy RODO[336].

W przeciwieństwie do rozwiązań przyjętych w państwach Unii Europejskiej PDPA wprowadza bardzo skromny katalog podstaw przetwarzania danych. Singapur należy do państw, które niemal w całości opierają swój system na zgodzie wyrażonej przez podmiot danych. Inną okolicznością dopuszczoną przez PDPA jest przetwarzanie danych wymagane lub dopuszczone przez przepisy ustawy lub jakiegokolwiek innego prawa stanowionego[337]. W przypadku zastosowania tej podstawy

[334] Dalej jako: PDPCS lub Komisja.

[335] Advisory guidelines on key concepts in the Personal Data Protection Act, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf [dostęp 1.06.2019].

[336] Art. 4 pkt 2 RODO.

[337] Art. 13 PDPA.

obowiązują odrębne zasady dotyczące utrwalania, korzystania oraz udostępniania danych. Określone one zostały w załącznikach do ustawy. Każdy z nich zawiera katalog kilkunastu okoliczności, w których poszczególne operacje na danych osobowych mogą być wykonywane bez konieczności uzyskania zgody. Ze względu na obszerność tych wyliczeń niemożliwe jest przytoczenie ich w całości. Niemniej jednak warto wskazać, iż ustawodawca dopuszcza zarówno utrwalanie, korzystanie, jak i udostępnianie w sytuacji, gdy dane osobowe są już publicznie dostępne (np. udostępnione w mediach społecznościowych), gdy przetwarzanie jest konieczne z punktu widzenia interesu państwa lub w celu dokonania oceny (np. w stosunku zatrudnienia, w przypadku naboru, konkursów)[338].

Ze względu na znaczenie zgody w omawianym reżimie prawnym ustawodawca poświęca dużo uwagi jej konstrukcji prawnej. PDPA wprost wskazuje, iż poprawnie udzielona zgoda musi być świadoma, konkretna i dobrowolna. Świadomość podmiotu danych wiąże się z obowiązkiem udzielenia wymaganych informacji przez przetwarzającego. Ustawa obliguje przede wszystkim do przekazania wyczerpujących informacji co do celu przetwarzania. W przypadku zmiany celu w trakcie operacji przetwarzania informacja ta powinna być również przekazana jednostce. Dodatkowo na żądanie zgłoszone przed udzieleniem zgody należy udostępnić dane kontaktowe osoby wyznaczonej do udzielania informacji na temat przetwarzania danych w imieniu przetwarzającego[339]. Ustawa wprost zakazuje udzielania nieprawdziwych lub mylących informacji o podejmowanych czynnościach przetwarzania. Stosowanie niedozwolonych praktyk przez przetwarzającego prowadzi do nieważności zgody. Jak wskazano powyżej, poprawnie udzielona zgoda powinna być konkretna, a więc jasno określać cel przetwarzania. Ostatecznie musi ona spełniać również wymóg dobrowolności. Tym samym przetwarzający

[338] Art. 1 Drugiego załącznika do PDPA, art. 1 Trzeciego załącznika do PDPA, art. 1 Czwartego załącznika do PDPA.

[339] Art. 20 (1) PDPA.

nie może uzależniać przystąpienia do umowy (np. sprzedaży, świadczenia usług) od udzielenia zgody przez jednostkę, jeżeli wykracza ona poza rozsądnie wymagany zakres danych[340].

PDPA nie wprowadza żadnych wytycznych co do formy zgody, tym samym może być ona udzielona w dowolnej formie. Lokalny regulator zachęca jednak do pozyskiwania zgody w formie pisemnej lub innej udokumentowanej. Wytyczne te mają wyłącznie charakter dobrych praktyk, jednak nie można odmówić im słuszności. W teorii dopuszczalne jest pozyskanie zgody np. w formie ustnej. Należy jednak liczyć się z późniejszymi trudnościami w udowodnieniu, iż zgoda została faktycznie pozyskana.

Ustawa obok tradycyjnej konstrukcji zgody wprowadza również pojęcie czynności równoznacznej z udzieleniem zgody (*deemed consent*). Zgodnie z brzmieniem art. 15 sytuacja, w której jednostka dobrowolnie udostępnia swoje dane w celu ich przetwarzania, powinna być traktowana tak jak udzielenie zgody. Ustawodawca wprowadza jednak zastrzeżenie, iż okoliczności powinny wskazywać na uzasadnione przypuszczenie, iż jednostka faktycznie chciała dobrowolnie udostępnić swoje dane[341].

Zważając na fakt, iż singapurski system ochrony danych osobowych oparty jest w dużej mierze na zgodzie jako przesłance przetwarzania, za uzasadnione należy uznać wprowadzenie prawa do wycofania zgody przez jednostkę. PDPA stanowi, iż podmiot danych może z niego skorzystać w każdej chwili, jednak z zachowaniem odpowiedniego okresu wypowiedzenia. Uprawnienie to dotyczy zarówno „tradycyjnej" zgody, jak i czynności jednoznacznych z udzieleniem zgody. Oceniając, czy termin wskazany przez jednostkę spełnia ustawowe kryteria, należy przede wszystkim wziąć pod uwagę czas konieczny na podjęcie działań zmierzających do zaprzestania przetwarzania. PDPCS podkreśla, iż trudno

[340] Art. 20 (2) *ibidem*.

[341] W.B. Chik, *The Singapore Personal Data Protection Act and an assessment of future trends in data privacy*, „Computer Law and Security Review" 2013, 29(5), s. 562.

jest tu wskazać sztywny termin, który miałby zastosowanie do wszystkich sytuacji. Sugeruje jednak, iż termin ten nie powinien być krótszy niż dziesięć dni roboczych od momentu otrzymania informacji przez przetwarzającego. W przypadku, gdy nie jest on w stanie dochować wyznaczonego terminu, Komisja zaleca poinformowanie jednostki[342]. Co oczywiste, podmioty przetwarzające dane nie mogą odmawiać jednostkom skorzystania z przysługującego im prawa do wycofania zgody. Jednakże przetwarzający zobligowany jest do poinformowania podmiotu danych o potencjalnych konsekwencjach takiej czynności. Co istotne, wypowiedzenie zgody powinno jasno wskazywać swój zakres, a w szczególności cele, dla których dane nie powinny być dłużej przetwarzane[343].

Poza prawem do wycofania zgody jednostkom przysługuje również prawo dostępu do danych[344] oraz prawo do sprostowania danych[345]. Ustawodawca nie przewiduje natomiast, znanego z porządku europejskiego, prawa do bycia zapomnianym, co przez niektórych przedstawicieli doktryny poczytywane jest za swoiste niedopatrzenie[346].

Dbając o zachowanie właściwych standardów ochrony danych osobowych PDPA jako zasadę ogólną przyjmuje zakaz przesyłania danych poza terytorium Singapuru. Zakaz ten podlega jednak licznym wyłączeniom określonym przez przepisy ustawy. Co do zasady, transfer ten będzie możliwy, jeżeli przetwarzający jest w stanie udowodnić, iż standardy wprowadzone przez PDPA zostaną zachowane również poza graniami państwa[347]. W takiej sytuacji podmiot otrzymujący dane powinien być związany obowiązkiem prawnym, wynikającym np. z przepisów prawa, umowy lub wiążących reguł korporacyjnych. Wprowadzenie takiego wyłączenia wydaje się absolutnie konieczne we współczesnym, zdigitalizowanym świecie.

[342] Advisory guidelines on key…, s. 46–47.
[343] Art. 16 PDPA.
[344] Art. 21 *ibidem*.
[345] Art. 22 *ibidem*.
[346] W.B. Chik, *op.cit*. s. 570 i n.
[347] Art. 26 PDPA.

Ustawodawca, wychodząc więc naprzeciw oczekiwaniom lokalnych przedsiębiorców, umożliwia im ubieganie się o wyłączenie wspomnianego wyżej zakazu. Decyzja Komisji każdorazowo wymaga opublikowania w dzienniku urzędowym. Ponadto może ona wskazywać dodatkowe wymogi, jakie podmiot przetwarzający zobligowany jest podjąć.

Rozważając możliwość zniesieniu zakazu transferu danych poza granice Singapuru, należy również pamiętać o generalnym uprawnieniu Komisji do zwolnienia z obowiązków wynikających z ustawy. Na mocy art. 62 Komisja za zgodą ministra ma prawo uchylić dowolne (również i wszystkie) przepisy ustawy w odniesieniu do konkretnego podmiotu lub kategorii podmiotów. Zwolnienie to może podlegać dodatkowym warunkom lub obowiązkom nałożonym przez Komisję.

Na mocy PDPA powołana została do życia Komisja ds. Ochrony Danych Osobowych (*The Personal Data Protection Commission*)[348]. Jej pozycja wydaje się w dużej mierze zbliżona do organów nadzorczych powoływanych w państwach Unii Europejskiej. Do zadań Komisji należy zwiększanie świadomości dotyczącej ochrony danych osobowych oraz udzielanie szeroko pojętego doradztwa z tego zakresu. Pełni ona również funkcję organu doradczego przy singapurskim rządzie. Komisja uprawniona jest to reprezentowania Rządu w stosunkach międzynarodowych. Należy również wspomnieć, iż to właśnie PDPCS odpowiada za wykonanie ustawy[349]. Na czele Komisji stoi wyłaniany przez nią Komisarz (*Commissioner for Personal Data Protection*)[350]. Możliwe jest powołanie jego zastępców, aczkolwiek ustawa nie określa ich liczby[351].

Omawiając rolę Komisji w krajowym systemie ochrony danych osobowych, nie można jednak zapomnieć o jej uprawnieniu do wydawania

[348] Art. 5 *ibidem*.
[349] Art. 6 *ibidem*.
[350] Art. 8 *ibidem*.
[351] Obecnie powołano wyłącznie jednego zastępcę Komisarza. Za: https://www.pdpc.gov.sg/About-Us/Who-We-Are [dostęp 1.06.2019].

poleceń (*directions*) dotyczących stosowania przepisów ustawy[352]. Mogą one zobowiązywać przetwarzającego do zaprzestania działań sprzecznych z przepisami ustawy (takich jak zbieranie, korzystanie, udostępnianie danych) lub usunięcia danych pozyskanych w niewłaściwy sposób. Komisja może również nałożyć na podmiot przetwarzający karę finansową w wysokości nieprzekraczającej miliona dolarów. Ustawa zastrzega jednak, iż zastosowanie tego środka nie jest możliwe w odniesieniu do działań stanowiących przestępstwo w rozumieniu PDPA. Warto zaznaczyć, iż istnieje procedura sądowej rejestracji poleceń wydawanych przez Komisję. Czynność ta nadaje im moc równą orzeczeniom sądowym. Właściwy sąd może także zapewnić poleceniom ich odpowiednie wykonanie[353].

Poza wskazaną powyżej możliwością nakładania kar o charakterze administracyjnym, należy pamiętać, iż PDPA wprowadza również przepisy karne. W pierwszej kolejności ustawa sankcjonuje nieuzasadnione korzystanie z prawa dostępu do danych oraz prawa do sprostowania danych. Za nieuprawnione uznaje się czynności dotyczące danych osób trzecich podejmowane bez właściwego umocowania. Przestępstwo to zagrożone jest grzywną w wysokości nieprzekraczającej 5 tysięcy dolarów lub karą pozbawienia wolności do 12 miesięcy. Ustawa przewiduje możliwość jednoczesnego orzeczenia obydwu kar[354]. Odrębnie PDPA penalizuje czynność polegającą na usunięciu, zmianie, sfałszowaniu, ukryciu lub zniszczeniu danych (lub poleceniu dokonania tych działań) w celu uchylenia się od wniosku złożonego przez podmiot danych przy realizacji przysługującego mu prawa dostępu oraz sprostowania danych. W tej sytuacji ustawa przewiduje wyłącznie grzywnę. Jej wysokość uzależniona jest od podmiotu dokonującego naruszenia[355]. Kolejnym przestępstwem wskazanym w PDPA jest utrudnianie lub uniemożliwianie

[352] Art. 29 PDPA.

[353] Art. 30 *ibidem.*

[354] Art. 51 (1)–(2) *ibidem.*

[355] Do 5 tysięcy dolarów w odniesieniu do osób fizycznych oraz do 50 tysięcy dolarów w przypadku innych podmiotów. Za: art. 51 (3a), (4) *ibidem*.

wykonywania obowiązków osobom działającym w imieniu Komisji oraz przekazywanie nieprawdziwych informacji Komisji. Czyny te zagrożone są taką samą karą. W przypadku osoby fizycznej obejmuje ona grzywnę do 10 tysięcy dolarów lub karę pozbawienia wolności do 12 miesięcy[356]. W sytuacji popełnienia wyżej wymienionego czynu przez inny podmiot orzeczona grzywna nie może przekroczyć 100 tysięcy dolarów[357].

9.4. Praktyka

PDPA z powodzeniem obowiązuje w Singapurze od 2013 r. W tym czasie Komisja wykazywała się stosunkowo dużą aktywnością, zarówno w zakresie edukacyjnym (m.in. przez publikację wytycznych oraz poradników), jak i wykonawczym przez wydawanie rozstrzygnięć. W zagranicznych komentarzach wskazuje się na dużą ostrożność PDPCS, której naczelnym celem wydaje się odpowiednie wyważenie interesów przetwarzających oraz podmiotów danych. Choć podmioty zachęcane są do samodzielnego rozwiązywania zaistniałych konfliktów, Komisja chętnie podejmuje działania w sprawach wskazujących na zaniechania systemowe lub takich, które zagrażają interesom większej liczby osób[358].

W 2018 r. Komisja wydała 25 rozstrzygnięć, w których zidentyfikowała naruszenie przepisów ustawy. Do połowy 2019 r. stwierdzono natomiast 17 uchybień. W tym roku PDPCS nałożyła również jedną z najwyższych kar finansowych w historii. Zgodnie z rozstrzygnięciem wydanym 14 stycznia 2019 r. dwie spółki – SingHealth oraz IHiS – zobligowano łącznie do zapłaty miliona dolarów[359]. Sprawa ta dotyczyła cyberataku na

[356] Ustawa wprowadza możliwość orzeczenia obydwu kar łącznie.

[357] Art. 51 (5) PDPA.

[358] W. Chang, *Singapore: Data Protection 2018*, https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore [dostęp 1.06.2019].

[359] Decyzja Komisarza ds. Ochrony Danych Osobowych w sprawie *Singapore Health Services Pte. Ltd. i inni*, DP-1807-B2435.

bazę danych zawierającą dane prawie półtora miliona pacjentów. W samym rozstrzygnięciu określono to zdarzenie mianem najgorszego ataku w historii Singapuru. Po przeprowadzeniu szczegółowego dochodzenia, Komisarz stwierdził naruszenie art. 24 PDPA obligującego podmioty do ochrony przetwarzanych danych przez wdrożenie odpowiednich środków bezpieczeństwa zabezpieczających przed nieuprawnionym dostępem do danych. W uzasadnieniu do tego przełomowego rozstrzygnięcia wskazano czynniki, które przyczyniły się do wymierzenia tak surowej kary. Wśród nich wskazano m.in. objętość bazy danych, ilość ujawnionych danych, szczególny charakter danych.

Odnosząc się do innych istotnych rozstrzygnięć, warto przywołać m.in. sprawę *Spring College International*, w której szkoła wyższa posługiwała się wizerunkiem i innymi danymi osobowymi studentów na portalach społecznościowych bez ważnej zgody na przetwarzanie ich danych w celach marketingowych[360].

9.5. Adekwatność ochrony w rozumieniu RODO

Singapur pomimo rozbudowanego i stosunkowo ugruntowanego systemu ochrony danych do dziś nie został uznany przez Komisję Europejską za zapewniający adekwatny poziom ochrony. Brak jest również informacji na temat toczących się w tym zakresie rozmów.

Odnosząc się do kryteriów oceny wskazanych w art. 45 RODO, należy stwierdzić, iż obecna sytuacja prawa i faktyczna Singapuru nie budzi większych zastrzeżeń z punktu widzenia praworządności czy niezależności władzy sądowniczej. Konstytucja Singapuru wprowadza katalog podstawowych wolności jednostek. Pomimo tego nadal utrzymywane są surowe regulacje dotyczące wolności zgromadzeń obligujące obywateli do każdorazowego uzyskania zezwolenia policji. Liczne

[360] W. Chang, *op. cit.*

wątpliwości pojawiają się również w zakresie realizacji wolności słowa w Singapurze. Poza przypadkami karania osób krytykujących bieżącą politykę rządu, szczególnie niepokojące są regulacje wprowadzające cenzurę prewencyjną wszystkich filmów[361].

Przechodząc do kwestii samego prawa ochrony danych osobowych, pozytywnie należy oceniać przyjęcie kompleksowej i spójnej regulacji. Pomimo jej szerokiego zakresu zastosowania, dwie kwestie mogą budzić zastrzeżenia z unijnego punktu widzenia. Po pierwsze trudno jest dostrzec zasadność ograniczenia zastosowania ustawy do czynności przetwarzania wynikających ze stosunku zatrudnienia. Wyłączenie to znacznie utrudnia sytuację pracownika, który i bez tego zwykle znajduje się w gorszej sytuacji niż prawodawca. Singapurski prawodawca zdaje się więc bardziej dbać o interesy pracodawców, co wskazuje na zupełnie inny kierunek niż w Unii Europejskiej[362]. RODO, dostrzegając brak równowagi między sytuacją pracodawcy i pracowników, stara się chronić tych drugich, co można dostrzec chociażby w wysoce ograniczonej możliwości uzyskiwania zgody na przetwarzania. Po drugie należy zwrócić uwagę na możliwość wprowadzania dodatkowych wyłączeń podmiotowych przez Komisje za zgodą ministra[363]. Ustawodawca nie wskazuje na okoliczności uzasadniające przyjęcie takich wyłączeń, ani nie zastrzega żadnych dodatkowych wymogów. Tym samym, tak długo, jak między ministrem a Komisją panuje zgoda, możliwości ograniczania zastosowania PDPA są właściwie nieograniczone. Trudno jest oceniać pozytywnie takie rozwiązane, gdyż z pewnością nie sprzyja ono pewności prawa oraz ochronie prawa obywateli.

Choć w zakresie definiowania ustawodawca singapurski pozostaje spójny z prawodawcą europejskim, to z pewnością uwagę zwraca brak

[361] Human Rights Watch, *World Report 2019,* Nowy Jork 2019, s. 514-517.

[362] Warto również pamiętać, iż przetwarzanie w celu dokonania oceny nie wymaga od podmiotu przetwarzającego uzyskania zgody. Ustawodawca wprost wskazuje, iż w większości przypadków „dokonywanie oceny" wiąże się z relacjami wynikającymi ze stosunku pracy, np. zatrudnienie, awans czy zwolnienie. Za: art. 2 (1) PDPA.

[363] Art. 62 *ibidem*.

wyróżnienia danych wrażliwych. Mimo iż źródła nienormatywne pośrednio odnoszą się do koncepcji szczególnych kategorii danych osobowych, to PDPA nie wprowadza w tym zakresie żadnego rozróżnienia. Trudno jest przypuszczać, czy wynika to ze zwykłego przeoczenia ustawodawcy czy celowego działania. Jednakże z całą pewnością należy uznać to za wadę lokalnego systemu.

Zgodnie z kryteriami oceny adekwatności wprowadzonymi przez art. 45 RODO należy stwierdzić, iż singapurski system ochrony danych osobowych przewiduje istnienie niezależnego organu nadzorczego odpowiedzialnego za egzekwowanie przepisów. Uprawnienia przyznane Komisji przez PDPA pozwalają jej na skuteczne funkcjonowanie, co obrazuje m.in. liczba wydawanych rozstrzygnięć. Na gruncie obowiązujących przepisów posiada ona również odpowiednie upoważnienie do działania na arenie międzynarodowej oraz podejmowania działań o charakterze doradczym na szeroką skalę.

Ze względu na niewielką liczbę inicjatyw międzynarodowych z zakresu ochrony danych osobowych trudno powiedzieć, aby był to istotny aspekt oceny danego systemu. Jak wskazano we wcześniejszym podrozdziale, Singapur nie przystąpił do Międzynarodowego Paktu Praw Obywatelskich i Politycznych, który gwarantuje prawo do prywatności. Warto jednak zaznaczyć, iż Singapur jest członkiem Stowarzyszenia Narodów Azji Południowo-Wschodniej, które podejmuje stopniowe działania na rzecz zwiększania standardów ochrony danych osobowych. Z całą pewnością nie mają one takiej intensywności działalność Unii Europejskiej.

9.6. Wnioski

Analiza obowiązującego prawodawstwa singapurskiego oraz bieżącej praktyki z zakresu ochrony danych osobowych pozwala stwierdzić, iż jest to jeden z najlepiej rozwiniętych systemów azjatyckich. Szczegółowa

i kompleksowa ustawa wskazuje na wiele punktów stycznych z regulacją europejską, zarówno w zakresie praw jednostek, jak i uprawnień organów nadzorczych. PDPA potwierdza jednak, iż jedną z najważniejszych wartości Singapuru jest ochrona interesu państwa oraz szerokie uprawnienia władzy. Ustawa wszakże nie znajduje zastosowania do organów władzy państwowej, a jednostki nie posiadają skutecznych narzędzi ochrony przed nadmiernym lub nieuzasadnionym przetwarzaniem przez nie danych. Prawodawca pozwala również władzy na niemal dowolne kształtowanie zakresu zastosowania ustawy w zależności od bieżącej sytuacji. To właśnie te elementy należy uznać za najsłabsze punkty lokalnej regulacji.

Choć obecny system ochrony danych zdaje się realizować swoje cele w wielu aspektach (np. działalność edukacyjna i doradcza Komisji, mnogość rozstrzygnięć dotyczących przestrzegania prawa), to wydaje się, iż zakres zastosowania ustawy jest obecnie największą przeszkodą do uznania Singapuru za kraj zapewniający adekwatny poziom ochrony. Obecnie trudno jest oceniać, czy sytuacja ta ulegnie zmianie w najbliższym czasie. Jednakże należy pamiętać, jak duże znaczenie dla Singapuru ma międzynarodowa współpraca gospodarcza, dla której decyzja o adekwatności byłaby dużym ułatwieniem. Pozostaje więc mieć nadzieję, iż względy ekonomiczne zmotywują prawodawcę do dalszego rozwoju lokalnego systemu ochrony danych osobowych.

Bibliografia

Akty prawne i projekty

1. Act on the Protection of Personal Information Held by Administrative Organs, Act No. 58 of May 30, 2003.
2. Amendment Seven to the Criminal Law, passed by the Standing Committee of the National People's Congress on February 28, 2009.
3. Banking Act, No. 41 of 1970.
4. Computer Misuse And Cybersecurity (Amendment) Act, No. 22 of 2017.
5. Data Protection Law DIFC Law No. 1 of 2007.
6. 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, OJ L 76, 19.3.2019, p. 1–58.
7. Dubai Law No. 9 of 2004 in respect of The Dubai International Financial Centre.
8. 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. WE L 281 z 23.11.1995, s. 31–50.
9. Federal Decree Number 35 for the year 2004 to Establish Financial Free Zone in Dubai.
10. Federal Law FZ-152.
11. Federal Law FZ-242.
12. Federal Law No. 1 of 2006 on Electronic Commerce and Transactions.

13. Federal Law No. 3 of 1987 The Penal Code.
14. Federal Law No. 5 of 2012 on Combating Cybercrimes.
15. Federal Law No. 8 of 2004 Regarding The Financial Free Zones.
16. Konstytucja Królestwa Bahrajnu z 14 lutego 2002 r.
17. Konstytucja Singapuru z dnia 9 sierpnia 1965 r.
18. Konstytucja Zjednoczonych Emiratów Arabskich z dnia 2 grudnia 1971 r.
19. Konwencja Nr 108 Rady Europy z 1981 r. 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.
20. 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.
21. Law No. 30 of 2018 on the Personal Data Protection Law.
22. Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. z 1977 r. Nr 38, poz. 167.
23. Personal Data Protection (Class of data users) Order 2013, P.U. (A) 336.
24. Personal Data Protection Act 2010, act 709.
25. Personal Data Protection Act 2012.
26. Public consultation paper No. 1/2017, Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017.
27. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. U. UE L 119 z 4.05.2016, s. 1–88.
28. Telecomunications Act, No. 43 of 1999.
29. Yarovaya Law 374-FZ i 375-FZ

Publikacje

1. *A Look at New Trends: Privacy Laws in East, Central, and South Asia and the Pacific*, https://media2.mofo.com/documents/170602-privacy-laws-asia-pacific.pdf [dostęp 6.06.2019].

2. Adams A.A., Murata K., Orito Y., *The Japanese Sense of Information Privacy*, http://www.a-cubed.info/Publications/The_Japanese_Sense_of_Information_Privacy.pdf [dostęp 6.06.2019].
3. Agarwal S., *Europe's data protection law may have severe implications for India's IT industry,* https://economictimes.indiatimes.com/articleshow/63741020.cms?utm_source=contentofinterest&utm_medium=-text&utm_campaign=cppst [dostęp 5.06.2019].
4. Al Rumaihi K., *A New Law for the Digital Economy: Data Protection in Bahrain*, https://bahrainedb.com/bahrain-pulse/a-new-law-for-the-digital-economy-data-protection-in-bahrain/ [dostęp 1.06.2019].
5. Allen & Overy, *Cross-border Data Transfer. Data Protection, United Arab Emirates (DIFC)*, Dubai 2018.
6. Anand P., Luniya V., *Understanding the Personal Data Protection Bill, 2018 and Bracing for Impact,* https://www.livelaw.in/law-firms/understanding-the-personal-data-protection-bill-2018-and-bracing-for-impact-142034 [dostęp 29.05.2019].
7. Andreeva K., Dergacheva A., Striz V., *Hot Topics In Data Privacy Regulation In Russia*, https://www.morganlewis.com/-/media/files/publication/presentation/webinar/2018/hot-topics-in-personal-data-regulation-in-russia_27nov18.ashx [dostęp 11.07.2019].
8. Anon, *MphasiS case: BPOs feel need to tighten security. Indian Express,* http://www.expressindia.com/news/fullstory.php?newsid=44856 [dostęp 6.06.2019].
9. Anon, *The MphasiS Scandal – And How it Concerns U.S. Companies Considering Offshore BPO*, http://www.carretek.com/main/news/articles/MphasiS_scandal.htm [dostęp 6.06.2019].
10. Ardhapurkar S., Srivastava T., Sharma S., Chaurasiya V., Vaish A., *Privacy and Data Protection in Cyberspace in Indian Environment,* „International Journal of Engineering Science and Technology" 2010, Vol. 2(5).
11. *Asia Pacific Data Protection and Cyber Security Guide 2018. Shifting landscapes across the Asia-Pacific region,* https://www.jdsupra.com/legalnews/asia-pacific-data-protection-and-cyber-77787/ [dostęp 6.06.2019].
12. *Bath Posts a Woman's Photo to Chase for the Unpaid Bill, November 23, 2009*, http://news.ifeng.com/society/2/200911/1123_344_1447469.shtml [dostęp 11.06.2019].

13. Bielak-Jomaa E., Lubasz D. (red.), *RODO Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.
14. Błażewski M., Behr J., *Środki prawne ochrony danych osobowych*, Wrocław 2018.
15. Centrum Internetu i Społeczeństwa, *Privacy in India. Country Report, October 2011,* https://cis-india.org/internet-governance/country-report.pdf [dostęp 5.06.2019].
16. Chang W., *Singapore: Data Protection 2018*, https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore [dostęp 1.06.2019].
17. Chik W.B., *The Singapore Personal Data Protection Act and an assessment of future trends in data privacy*, „Computer Law and Security Review" 2013, 29(5).
18. *China Cybersecurity Law,* https://www.reedsmith.com/-/media/files/perspectives/2018/chinas-cybersecurity-law-002.pdf [dostęp 13.06.2019].
19. China: Data Protection & Localisation, Cyber Security Law, VPN and Encryption, https://www.beiten-burkhardt.com/sites/default/files/downloads/BB%20BR-Flyer%20A5%20China-Data%20Protection%20en.pdf [dostęp 13.06.2019].
20. Cieśniewski A.K., *Kodeks karny Singapuru*, „Prokuratura i Prawo" 2016/3.
21. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018.pdf [dostęp 29.05.2019].
22. Cornell A.J., *Right to Privacy*, https://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156 [dostęp 9.07.2019].
23. *Court Orders Gas Company to Apologize to a Humiliated Customer*, People's Court Daily, July 16, 2007, http://www.lawtime.cn/info/anli/mfqita/2007071852281.html [dostęp 11.06.2019].
24. D'Luna Directo A., *Data Protection in India: The Legislation of Self-Regulation,* „Northwestern Journal of International Law & Business", 2014, Vol. 35, Nr 1.
25. *Data Flows, Online Privacy, and Trade Policy*, Congressional Research Service, March 11, 2019, https://crsreports.congress.gov [dostęp 11.06.2019].

26. *Data Protection Laws of the World. Japan*, https://www.dlapiperdataprotection.com/index.html?t=law&c=JP [dostęp 6.06.2019].
27. *Data Protection Laws of the World. Russia,* https://www.dlapiperdataprotection.com/index.html?t=law&c=RU [dostęp 9.07.2019].
28. Desmukh F., *Bahrain Government Hacked Lawyers and Activists with UK Spyware*, https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/ [dostęp 1.06.2019].
29. Dmochowska A., Zadrożny M., *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR art. 29, Ustawy o ochronie danych osobowych z 2018 r.*, Warszawa 2018, LEGALIS: 7oeu5fx2.
30. Doffman Z., *China Is Using Facial Recognition To Track Ethnic Minorities, Even In Beijing*, https://www.forbes.com/sites/zakdoffman/2019/05/03/china-new-data-breach-exposes-facial-recognition-and-ethnicity-tracking-in-beijing/#5c7f70e634a7 [dostęp 15.07.2019].
31. Dong M., *China*, [w:] A.C. Raul (red.), *The Privacy, Data Protection and cybersecurity Law Review,* 2017.
32. Dorryakova N., *Privacy in the Russian Legislation,* https://www.law.uw.edu/media/1304/russia-intermediary-liability-of-isps-privacy.pdf [dostęp 9.07.2019].
33. Dukes D.E., Paine E.A., Bonyata H.D., *Protection of Privacy in Data International Transfer.*
34. Fischer B., Karwala D., *Nowy instrument: wiążące reguły korporacyjny,* cz. 1 i 2, „Rzeczpospolita" 3.01.2006 i 11.01.2006.
35. Fischer B., Karwala D., *Transfer danych osobowych do państw trzecich (wybrane zagadnienia)*, „Państwo i Prawo" 2007, 1.
36. Garrie D., Byhovsky I., *Privacy and Data Protection in Russia, „*Journal of Law and Cyber Welfare" 2017.
37. Goasduff L., *Complying with Russia's New Privacy Law*, https://www.gartner.com/smarterwithgartner/complying-with-russias-new-privacy-law/ [dostęp 11.07.2019].
38. Gorodissky & Partneres, *Yarovaya Law and new data storage requirements for online data distributors*, https://www.lexology.com/library/detail.aspx?g=8029c37f-5a1c-4025-ac3f-8b3ede9c42e8 [dostęp 9.07.2019].

39. *Goverment requests to remove the content*, https://transparencyreport.google.com/government-removals/by-country/RU?hl=en&country_item_amount=group_by:totals;authority:%20RU%20&%20lu%20=%20country_item_amount [dostęp 10.07.2019].
40. Gray W., Zheng H. R., *Opinion of the Supreme People's Court on Questions Concerning the Implementation of the General Principles of Civil Law of the People's Republic of China (Translation),* "Law & Contemp. Probs." 1989, vol. 52, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2541&context=articles [dostęp 11.06.2019].
41. Greenleaf G., *Limitations of Malaysia's data protection Bill,* „Privacy Laws & Business International Newsletter" 2010, 104.
42. Hamada M., Matsumoto, *Data Protection & Cyber Security*, Chambers. Global Practice Guides, https://practiceguides.chambers.com/practice-guides/data-protection-cybersecurity-2019/japan [dostęp 15.07.2019].
43. Hamada H., Matsumoto, *Japan*, [w:] *The International Comparative Legal Guide to: A practical cross-border insight into cybersecurity work*, https://www.acc.com/sites/default/files/resources/20190314/1492582_1.pdf [dostęp 6.06.2019].
44. *Handbook on the Research Report on the Constitution of Japan*, Research Commission on the Constitution House of Councillors, Tokio 2005, http://www.sangiin.go.jp/eng/report/ehb/ehb.pdf [dostęp 7.06.2019].
45. Haque S.Z., *IT Outsourcing Services in India and the Lesson It Teaches Us,* https://www.indusnet.co.in/it-outsourcing-services-in-india-and-its-lessons/ [dostęp 29.05.2019].
46. Higashizawa N., Aihara Y., *Data Privacy Protection of Personal Information versus Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)*, http://www.city-yuwa.com/english/publication/shared/PDF/DCJ201784_cy_1-15.pdf [dostęp 6.06.2019].
47. Iyengar P., *News Broadcasting Standards Authority Censures Tv9 Over Privacy Violations! Privacyindia*, http://privacyindia.org/2011/03/25/news-broadcasting-standards-authority-censures-tv9-over-privacy-violations [dostęp 6.06.2019].
48. *Japan's New Data Privacy Regime and How it Will Enable Cross-Border Data Flows, Innovation and Privacy Protections in the Modern Information Age,* https://www.informationpolicycentre.com/uploads/5/7/

1/0/57104281/final_cipl_japan_workshop_slide_deck_10_may_2017-cc.pdf [dostęp 6.06.2019].

49. *Japan's government plans for My Number ID cards to be used for health insurance by 2023*, https://www.japantimes.co.jp/news/2019/06/05/national/japanese-government-seeks-number-ids-double-health-cards-starting-2021/#.XPlZCIgzY2w [dostęp 6.06.2019].
50. Jawahitha S., Ishak M., Mazahir M., *E-Data Privacy and the Personal Data Protection Bill of Malaysia*, „Journal of Applied Sciences" 2007, vol. 7 (5).
51. Jingchun C*., Protecting The Right To Privacy In China,* „Victoria University of Wellington Law Review" 2005, 36.
52. Jourová V., *EU Japan Adequacy Decision. Fact Sheet*, 2019.
53. *Judicial Practice of 2008–2009 Involving Roskomnadzor in regard to Violations of the Federal Law No. 152 On Personal Data,* http://eng.pd.rkn.gov.ru/legislation_of_the_russian_federation/judicial_practice/ [dostęp 11.07.2019].
54. Jusic A*., INSIGHT: Comprehensive Data Protection Comes to Bahrain*, https://news.bloomberglaw.com/privacy-and-data-security/insight-comprehensive-data-protection-comes-to-bahrain [dostęp 1.06.2019].
55. Kandiah S., *The Privacy, Data Protection and Cybersecurity Law Review. Malaysia*, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175635/malaysia [dostęp 15.06.2019].
56. Karsten J., West D.M., *China's social credit system spreads to more daily transactions,* Brookings, June 18, 2018.
57. Khaitan and Co., *Data Privacy and protection law in India: Understanding the regime*,
58. Khalaileh Y., Kisswani N., *The „Right to Privacy" v. telecommunications interception and access: International regulations and implementation in the Arab Region*, „International Review of Law" 2013, Vol. 2, 2014.
59. Khayryuzov V., *The Privacy, Data Protection and Cybersecurity Law Review – Edition 5. Russia,* https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175638/russia [dostęp 10.07.2019].

60. Kittaka L.G., *11 things you need to know about my number*, https://blog.gaijinpot.com/japan-my-number-system/ [dostęp 6.06.2019].

61. Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.

62. Lubis M., Kartiwi M., *Privacy and trust in the Islamic perspective: Implication of the digital age*, [w:] 5th International Conference on Information and Communication Technology for the Muslim World, 2013.

63. Mennie P., *GDPR vs. Bahrain Personal Data Protection Law*, https://www.linkedin.com/pulse/gdpr-vs-bahrain-personal-data-protection-law-phil-mennie/ [dostęp 1.06.2019].

64. Mozur P., *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority,* https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [dostęp 15.07.2019].

65. Munro K., *China's social credit system 'could interfere in other nations' sovereignty'*, „The Guardian" June 27, 2018.

66. NASSCOM, *Whitepaper EU Adequacy Assessment of India*, https://www.dsci.in/sites/default/files/White_Paper_EU_Adequacy_Assessment_of_India.pdf [dostęp 5.06.2019].

67. Nishi M., *Data Protection in Japan to Align With GDPR,* https://webcache.googleusercontent.com/search?q=cache:YBzeg3bxPr4J:https://www.skadden.com/-/media/files/publications/2018/09/quarterly-insights/data_protection_in_japan_to_align_with_gdpr.pdf+&cd=2&hl=pl&ct=clnk&gl=pl [dostęp 6.06.2019].

68. Nishith Dessai Associates, *New Data Protection Law Proposed in India! Flavors of GDPR*, http://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA_Summary.pdf [dostęp 29.05.2019].

69. O'Flaherty K., *Huawei Security Scandal: Everything you need to know,* https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/#10f6aa1e73a5 [dostęp 13.06.2019].

70. *On the Turn: India is No Longer the Automatic Choice for IT Services and Back-Office Work*, http://www.economist.com/news/special-report/21569571-india-no-longerautomatic-choice-it-services-and-back-of

fice-work-turn?zid=292&ah=165a5788fdb0726c01b1374d8e1ea285 [dostęp 30.05.2019].

71. Orito Y., Murata K., *Privacy Protection in Japan: Cultural Influence on the Universal Value,* http://www.kisc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf, [dostęp 6.06.2019].
72. Overby S., *Eight reasons why Outsourcing to India Could Hurt Your Business*, https://www.cio.com/article/2437890/eight-reasons-why-outsourcing-to-india-could-hurt-your-business.html [dostęp 29.05.2019].
73. Panday J., *India's Supreme Court Uphold Right to Privacy as a Fundamental Right – and It's about Time,* https://www.eff.org/pl/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time [dostęp 28.05.2019].
74. Polska Agencja Inwestycji i Handlu, *Singapur. Przewodnik po rynku*, Warszawa 2017.
75. Press Information Bureau Government of India Ministry of Commerce & Industry, *Data-Adequacy Status for Indian Companies,* http://www.pib.nic.in/Pressreleaseshare.aspx?PRID=1562523 [dostęp 5.06.2019].
76. Priebe J., Tomaszewski J., *Fortress Russia – The Russian Data Localization Law*, https://www.globalprivacywatch.com/2015/05/fortress-russia-the-russian-data-localization-law/ [dostęp 10.07.2019].
77. Privacy In India – Country Report – October 2011, https://cis-india.org/internet-governance/country-report.pdf [dostęp 6.06.2019].
78. Privacy International, *The Right to Privacy in Singapore*. *Stakeholder Report Universal Periotic Review,* https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf [dostęp 1.06.2019].
79. *Protecting personal information in the age of Big Data – Japan's new regime,* https://www.aplaw.jp/clientalert-en-dataprotection-december2017.pdf [dostęp 6.06.2019]
80. Razumovskaya O., Mills L., *Court Upholds Decision to Ban LinkedIn in Russia*, https://www.wsj.com/articles/court-upholds-decision-to-ban-linkedin-in-russia-1478791726 [dostęp 9.07.2019].
81. Revisiting the data protection regime in China, https://deutschland.taylorwessing.com/documents/get/463/revisiting-the-data-protection-regime-in-china.pdf/show_on_screen [dostęp 13.06.2019].

82. *Right to privacy under art. 21 and related conflicts,* http://www.legalservicesindia.com/article/1630/Right-To-Privacy-Under-Article-21-and-the-Related-Conflicts.html [dostęp 28.05.2019].
83. *Russia: Harmonising Data Protection Laws With The Eu,* http://www.gorodissky.com/publications/articles/russia-harmonising-data-protection-laws-with-the-eu/ [dostęp 11.07.2019].
84. *Russia's 'Big Brother' Law Enters Into Force,* https://www.themoscowtimes.com/2018/07/01/russias-big-brother-law-enters-into-force-a62066 [dostęp 9.07.2019].
85. Sachitanand R., *India's $150 billion outsourcing industry stares at an uncertain future, https:*//economictimes.indiatimes.com/articleshow/56543653.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst [dostęp 29.05.2019].
86. Sadowski M., *Kontrakt małżeński w prawie islamu*, „Studia Prawno-Ekonomiczne", t. CIII, 2017.
87. Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Wrocław 2018.
88. Savelye A., *Russia's new personal data localization regulations: A step forward or a self-imposed sanction?*, „Computer Law & Security Review" 2016, 32.
89. *Shanghai Metro Apologized to the Lovers Caught on Tape*, „Oriental Morning" January 23, 2008, http://society.people.com.cn/GB/1062/6809132 [dostęp 11.06.2019].
90. Sharma V., *White Paper on Privacy Protection in India,* http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf [dostęp 4.06.2019].
91. Singh V., *An analysis of personal data protection with special emphasis on current amendments and privacy bill,* „International Journal of Law and Legal Jurisprudence Studies" 2017, vol. 4, issue 1.
92. Staden ten Brink R., Wang J., Veldhoen D., Arnbak A., *China's new cybersecurity law – effective as of 1 June 2017*, „Trade Security Journal" 2017, Issue 2.
93. Sridhar V., Srikanth T.K., *As Aadhaar project enters a critical year, here are the worries that still remain*, https://economictimes.indiatimes.com/

articleshow/62656100.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst [dostęp 28.09.2019].

94. Tarbuck A., Lester Ch., *Dubai's legal system. Creating a legal and regulatory framework for a modern society*, Dubaj 2009.
95. *The China Cybersecurity Law has been finalized- is your organisation ready to comply with a new law?,* https://www.pwccn.com/en/issues/cybersecurity-and-privacy/china-cybersecurity-law-2017.html [dostęp 11.06.2019].
96. *The Right to Privacy in China. Submitted by Privacy International, and the Law and Technology Centre of the University of Hong Kong. March 2013. Stakeholder Report Universal Periodic Review, 17th Session – China*, https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=142&file=EnglishTranslation [dostęp 13.06.2019]
97. Toorani M., Holley E., *Bahrain Publishes Personal Data Protection Law*, https://www.dlapiper.com/en/qatar/insights/publications/2018/09/bahrain-publishes-personal-data-protection-law/ [dostęp 1.06.2019].
98. Trilegal, *The personal data protection bill, 2018,* https://www.trilegal.com/pdf/create.php?publication_id=15&publication_title=the-personal-data-protection-bill-2018 [dostęp 29.05.2019].
99. *Uber agreed to move the personal data or Russians to Russia*, https://lenta.ru/news/2015/07/10/uber/ [dostęp 10.07.2019].
100. *Viber moved its servers to Russia*, http://izvestia.ru/news/593438 [dostęp 10.07.2019].
101. Wang L., Yang L., *The Law of the Rights of The Person,* „The Press of Laws", Beijing, 1997.
102. Wartburton K., *5 Key Cultural Issues when Outsourcing to India*, https://www.linkedin.com/pulse/5-key-cultural-issues-when-outsourcing-india-keith-warburton/ [dostęp 29.05.2019].
103. Wee Choong Sian S., *Privacy law: a case for the protection of informational privacy in Singapore*, „Singapore Law Review" 2013, vol. 31.
104. *Whitepaper on Regulatory Implications for Cross-Border Data Transfers from China to the United States*, http://sia-partners.com/sites/default/files/sia_partners_whitepaper_mainland_china_data_transfers.pdf [dostęp 11.06.2019].

105. Wilkinson D., *Five questions you should ask about Bahrain's new data protection law*, https://www.clydeco.com/insight/article/five-questions-you-should-ask-about-bahrains-new-data-protection-law [dostęp 1.06.2019].
106. Woods V., *Privacy and data protection in The UAE*, http://www.hadefpartners.com/News/329/Privacy-and-data-protection-in-the-UAE [dostęp 15.06.2019].
107. Xue H., *Privacy and personal data protection in China: An update for the year end 2009*, „Computer Law & Security Review" 2010, 26.
108. Yusoff Z.M., *Protection of privacy in Malaysia: A law for the future*, Wellington 2014.
109. Zhao H., Dong H.X., *Research on Personal Privacy Protection of China in the Era of Big Data*. „Open Journal of Social Sciences" 2017, 5, https://doi.org/10.4236/jss.2017.56012 [dostęp 14.06.2019].
110. Zhuravlev M.S., Brazhnik T.A., *Problems for Internet Business and Users Caused by New Russian Legislation*, „Information Law Journal" 2014, Vol. 5, Issue 4.
111. *Complying with Russia's New Privacy law,* https://www.gartner.com/smarterwithgartner/complying-with-russias-new-privacy-law/ [dostęp 10.07.2019].

Orzeczenia i decyzje

1. Decyzja Komisarza ds. Ochrony Danych Osobowych w sprawie *Singapore Health Services Pte. Ltd. i inni*, nr sprawy DP-1807-B2435.
2. Wyrok Judicial Committee of the Privy Council z dnia 15 października 1980 r. w sprawie *Ong Ah Chuan and another v. Public Prosecutor*, UKPC 32.
3. Wyrok Sądu Apelacyjnego Republiki Singapuru z dnia 20 października 2004 r. w sprawie *Nguyen Tuong Van v Public Prosecutor*, [2005] 1 SLR 103.
4. Wyrok Sądu Federalnego z dnia 17 listopada 2009 r. w sprawie *Sivarasa Rasiah v. Badan Peguam Malaysia & Anor* [2010] 3 CLJ 507.
5. Wyrok Sądu Najwyższego Indii z 24.08.2017 r. w sprawie *K.S. Puttaswamy and Anr. v. Union of India and Ors.*

6. Wyrok Sądu Najwyższego Indii z dnia 18 marca 1975 r. w sprawie *Govind vs State Of Madhya Pradesh & Anr*.
7. Wyrok Sądu Najwyższego Japonii z dnia 6 marca 2008 r., Minshu, tom 62, nr 3, s. 665.
8. Wyrok Sądu Okręgowego w Tokio z dnia 28 września 1964 r. (Showa 36), (Wa) No. 1882
9. Wyrok Tokyo District Court, 1982 (Showa 57), (Wa) No. 3.
10. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r. w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD)*, C-131/12, EU:C:2014:317.
11. Wyrok Trybunału Sprawiedliwości z dnia 24 września 2019 r. w sprawie *Google LLC przeciwko Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, ECLI:EU:C:2019:772.
12. Wyrok Sądu Najwyższego Indii z dnia 18 marca 1975 r. w sprawie *Gobind vs State Of Madhya Pradesh And Anr.*
13. Wyrok Sądu Najwyższego Indii z dnia 25 stycznia 1978 r. w sprawie *Maneka Gandhi vs Union Of India.*
14. Wyrok Europejskiego Trybunału Praw Człowieka z 16 października 2010 r. w sprawie *Nazarenko v Russia* (ECtHR) No 34938/13.
15. Wyrok Sądu Najwyższego Indii w sprawie *People's Union for Civil Liberties (PUCL) v Union of India*, (1997) 1 SCC 301.
16. Wyrok Sądu Najwyższego Indii z dnia 7 października 1994 r. w sprawie *Rajagopal vs State Of T.N.*
17. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 grudnia 2015 r. w sprawie *Roman Zakharov v Russia* (ECtHR) No 47143/06.
18. Wyrok Sądu Najwyższego Indii w sprawie *Thomas Raju v. ICICI Bank, Anna Nagar*, (2011), http://www.naavi.org/cl_editorial_11/civil_jurisdiction_3_16052011.pdf [dostęp 6.06.2019].
19. Wyrok Sądu Najwyższego Indii w sprawie *Umashankar v. ICICI Bank, Tuticorin*, (2010), http://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf [dostęp 6.06.2019].
20. Wyrok Sądu Najwyższego Japonii z dnia 24 grudnia 1969 r., Keishu, tom 23, nr 12, s. 1625.

21. Wyrok Sądu Najwyższego Japonii z dnia 14 kwietnia 1981 r. (Showa 56), *Third Petty Bench of the Supreme Court Adjudication.*

Raporty, publikacje rządowe i dokumenty organów publicznych

1. Advisory guidelines on key concepts in the Personal Data Protection Act, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf [dostęp 1.06.2019].
2. Amnesty International Report 2017/18: The State Of The World's Human Rights. Bahrain, https://www.amnesty.org/en/countries/middle-east-and-north-africa/bahrain/report-bahrain/ [dostęp 1.06.2019].
3. ASEAN Framework on Digital Data Governance.
4. ASEAN Framework on Personal Data Protection.
5. Human Rights Watch, *World Report 2019,* Nowy Jork 2019.
6. Report of the Working Group on the Universal Periodic Review – China, 26.12.2018.
7. Report. Activity of the Competent Authority for Protecting the Rights of Personal Data Subjects, http://eng.pd.rkn.gov.ru/docs/report2012.pdf [dostęp 10.07.2019].
8. The OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [dostęp 1.06.2019].
9. The World Justice Project, *Rule of Law Index 2019*, Waszyngton 2019.
10. World Economic Forum, The Global Competitiveness Report 2018, Genewa 2018.
11. Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610136 [dostęp 28.09.2019].
12. Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on „Contractual clauses" Considered as compliant with the EC Model Clauses https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf [dostęp 28.09.2019].

Publikacje z dyscypliny nauki prawne – prawo konstytucyjne, które ukazały się w e-Wydawnictwie WPAE UWr

Justyna Węgrzyn, *Prawo konsumenta do informacji w Konstytucji RP i w prawie unijnym*, Wrocław 2013
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/40651

Współczesne koncepcje ochrony wolności i praw podstawowych, red. Andrzej Bator, Mariusz Jabłoński, Marek Maciejewski, Krzysztof Wójtowicz, Wrocław 2013
Dostęp online: http://bibliotekacyfrowa.pl/publication/42456

Małgorzata Masternak-Kubiak, *Odesłania do prawa międzynarodowego w Konstytucji RP,* Wrocław 2013
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/41352

Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym, red. Mariusz Jabłoński, Wrocław 2014
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/51986

Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi, red. Mariusz Jabłoński i Sylwia Jarosz-Żukowska, Wrocław 2014
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/56032

Krzysztof Wójtowicz, *Constitutional Courts and European Union Law,* Wrocław 2014
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/54527

*Zasada pierwszeństwa prawa Unii Europejskiej w praktyce działania organów władzy publicznej RP***,** red. Mariusz Jabłoński, Sylwia Jarosz-Żukowska, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/64552

Artur Ławniczak, *Geneza Konstytucji,* Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/65468

*Teoretyczne i praktyczne aspekty realizacji prawa petycji***,** red. Ryszard Balicki i Mariusz Jabłoński, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/66901

Ewolucja państwowości w Brazylii, Polsce i Eurazji. Evolução do estado no Brasil, Polônia e Eurásia, red. Marcos A. Maliska, Krystian Complak, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/64761

Międzynarodowa ochrona praw człowieka – współczesne problemy na świecie, red. Mariusz Jabłoński, Tomasz Jurczyk, Patryk Gutierrez, Wrocław 2015
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/67621

Identyfikacja granic wolności i praw jednostki. Prawnoporównawcza analiza tożsamego przypadku pod kątem praktyki stosowania prawa amerykańskiego i polskiego, red. Mariusz Jabłoński, Wrocław 2016
Dostęp online: http://www.bibliotekacyfrowa.pl/dlibra/publication/79781

Instytucje demokracji bezpośredniej w praktyce, red. Olga Hałub, Mariusz Jabłoński, Mateusz Radajewski, Wrocław 2016
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/80567

Aktualne problemy ochrony wolności i praw mniejszości w Polsce i na świecie, red. Joanna Beata Banach-Gutierrez, Mariusz Jabłoński, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/84127

Współczesne polityczno-prawne systemy państw Europy, Azji i Ameryki Łacińskiej, red. Krystian Complak, Patryk Gutierrez, Jolanta Rosiak, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/dlibra/publication/84639

Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne, red. Mariusz Jabłoński, Kinga Flaga-Gieruszyńska, Krzysztof Wygoda, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/92803

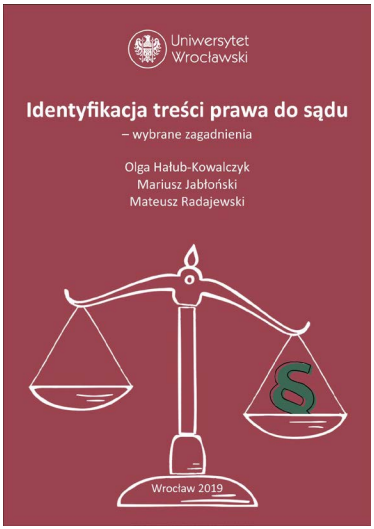
Magdalena Bainczyk, *Polski i niemiecki Trybunał Konstytucyjny wobec członkostwa państwa w Unii Europejskiej*, Wrocław 2017
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/84085

Dookoła Wojtek... Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi, red. Ryszard Balicki, Mariusz Jabłoński, Wrocław 2018
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/95368

Ryszard Balicki, *Funkcja europejska Sejmu RP,* Wrocław 2019
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/101626

Specyfika organizacji i funkcjonowania organów władzy publicznej. Analiza porządków prawnych państw współczesnych, red. Mariusz Jabłoński, Magdalena Abu Gholeh, Wrocław 2019
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/101490

Anna Śledzińska-Simon, *Analiza proporcjonalności ograniczeń konstytucyjnych praw i wolności. Teoria i praktyka*, Wrocław 2019
Dostęp online: http://www.bibliotekacyfrowa.pl/publication/102713



Olga Hałub-Kowalczyk, Mariusz Jabłoński, Mateusz Radajewski, *Identyfikacja treści prawa do sądu – wybrane zagadnienia*, Wrocław 2019
Dostęp online: https://www.bibliotekacyfrowa.pl/publication/104603

w przygotowaniu

Osobowość prawna jako przesłanka wykonywania konstytucyjnych wolności i praw, pod redakcją Michała Bernaczyka i Mariusza Jabłońskiego,
Dostęp online: https://www.bibliotekacyfrowa.pl/publication/108539

[...] książka jest bez wątpienia dziełem nowatorskim i potrzebnym. Autorki zwróciły uwagę na problematykę, która nie była dotąd szeroko analizowana w polskim piśmiennictwie, co w sposób znaczący podnosi wartość recenzowanej pracy. [...] Autorki z podjętego zadania badawczego wywiązały się bardzo dobrze, a monografia może przyczynić się do wielu dyskusji naukowych w gronie konstytucjonalistów i specjalistów z zakresu problematyki ochrony danych osobowych i prawa do prywatności.

z recenzji wydawniczej dr. hab. Pawła Kuczmy,
prof. Uniwersytetu Zielonogórskiego

ISBN 978-83-66066-87-8 (druk)
ISBN 978-83-66066-88-5 (online)