Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, 155–173

DOI: 10.17951/teka.2018.13.2.155-173

PRAWNE DYLEMATY REGULACJI CYBERPRZESTRZENI: KONFLIKT POMIĘDZY BEZPIECZEŃSTWEM NARODOWYM A PRAWEM DO PRYWATNOŚCI Z PERSPEKTYWY PRAWODAWSTWA UE I USA

Marcin Rojszczak

Wydział Prawa i Administracji
Uniwersytet Warszawski
ORCID ID: https://orcid.org/0000-0003-2037-4301
e-mail: marcin.rojszczak@gmail.com

Streszczenie: Unijny model ochrony prywatności jest powszechnie uznawany za najbardziej rozbudowany i kompleksowy, zarówno pod względem zakresu ochrony praw osób, których dane dotyczą, jak i spójności obowiązków nałożonych na podmioty zobowiązane. Coraz wyraźniej dostrzegalna jest jednak niespójność unijnych przepisów z regulacjami stosowanymi przez Stany Zjednoczone Ameryki, a więc jednego z głównych partnerów handlowych UE. Zarówno amerykańskie przepisy federalne, jak i normy konstytucyjne nie wprowadzają równie silnego reżimu w zakresie ochrony prywatności. Co więcej, prawodawca amerykański inaczej wyważa znaczenie ochrony praw podstawowych z uwagi na potrzeby związane z zapewnieniem bezpieczeństwa narodowego. Niezgodność przepisów UE i USA dotyczących różnych relacji między prawem do prywatności a celami bezpieczeństwa ogólnego jest praktycznym i aktualnym problemem w budowaniu partnerstwa transatlantyckiego. Celem artykułu jest przedstawienie rozważań dotyczących potencjalnego konfliktu między prawami jednostek a celami bezpieczeństwa narodowego, wraz z przedstawieniem najważniejszych przepisów UE i USA w tej dziedzinie oraz wyjaśnieniem przyczyn ich wzajemnej niezgodności.

Słowa kluczowe: prawo do prywatności, bezpieczeństwo narodowe, prawa człowieka, cyberprzestrzeń, prawo międzynarodowe

WPROWADZENIE[1]

Problem potencjalnej kolizji pomiędzy prawami i wolnościami osobistymi a uprawnieniami państwa, związanymi z zapewnieniem bezpieczeństwa ogólnego może być analizowany z różnych perspektyw: uwzględniając dorobek nauk praw-

[1] Stan prawny oraz odnośniki internetowe aktualne na dzień 15.10.2018 r.

nych, np. skuteczność systemów ochrony praw człowieka [Skrzydło 1995], nauk o bezpieczeństwie, np. elastyczność gwarancji konstytucyjnych w sytuacjach zagrożenia bezpieczeństwa państwa [Szuniewicz 2016] czy badań dotyczących stosunków międzynarodowych, np. współpraca w zakresie zapobiegania i przeciwdziałania najpoważniejszym przestępstwom [Laskowski 2015].

Zakresem niniejszego artykułu jest analiza relacji pomiędzy prawami jednostki (w szczególności prawem do prywatności) a celami bezpieczeństwa ogólnego w państwach demokratycznych. Punktem wyjścia dla dalszych rozważań będzie zatem termin „bezpieczeństwo narodowe", obejmujący z definicji także ochronę wartości i potrzeb jednostki.

W nauce o bezpieczeństwie wprowadza się wiele systematyk pozwalających na podział obszaru badawczego. Piotr Majer [2012: 11], jako elementarny wskazuje podział podmiotowy, zgodnie z którym można wyróżnić bezpieczeństwo narodowe i międzynarodowe. W takim ujęciu „bezpieczeństwo międzynarodowe" obejmuje przestrzeń relacji zewnętrznych (niekoniecznie oddziałujących na dane państwo), podczas gdy pojęcie „bezpieczeństwo narodowe" należy wiązać z wewnętrzną działalnością państwa[2]. Istotnym zagadnieniem jest także relacja pomiędzy bezpieczeństwem narodowym a bezpieczeństwem państwa. Polska konstytucja operuje wyłącznie terminem „bezpieczeństwo państwa", podczas gdy akty prawne UE oraz prawodawstwo amerykańskie posługuje się obydwoma terminami. Jak wskazuje się w literaturze przedmiotu, bezpieczeństwo państwa należy wiązać z ochroną przed zagrożeniami wewnętrznymi i zewnętrznymi, a więc jest pojęciem bliskim obronności [Czuryk et al. 2016: 20]. Z kolei bezpieczeństwo narodowe jest szersze i obejmuje także ochronę potrzeb i wartości, które są bliskie jednostce. W efekcie ochrona bezpieczeństwa narodowego jest charakterystyczna dla działania państwa demokratycznego, podczas gdy ochrona bezpieczeństwa państwowego jest realizowana przez każde państwo, także totalitarne.

Uwzględniając rozwój techniki, skutkujący postępującą cyfryzacją wielu obszarów życia, coraz większa część aktywności społecznych przenosi się do cyberprzestrzeni. Uniwersalny, ponadnarodowy charakter cyberprzestrzeni z jednej strony tworzy nowe możliwości budowy relacji społecznych, z drugiej jednak może stanowić skuteczne narzędzie dla propagowania ekstremizmów czy działań naruszających prawo. Techniki i środki służące identyfikowaniu takich działań mogą służyć zarówno wykrywaniu zagrożeń dla bezpieczeństwa, ale również nadzorowaniu i kontrolowaniu jednostki lub całych społeczeństw.

Przedstawiony problem badawczy ma jeszcze jeden, równie istotny aspekt. Upowszechnienie usług świadczonych elektroniczne oraz nowych form prze-

[2] Należy pamiętać, że podział na bezpieczeństwo międzynarodowe i narodowe nie jest podziałem dychotomicznym – można bez trudu wyróżnić działania oddziałujące na obie sfery. Dla przykładu w dokumentach doktrynalnych armii Stanów Zjednoczonych Ameryki bezpieczeństwo narodowe jest definiowane łącznie przez sferę działalności wewnętrznej i zewnętrznej państwa [por. *DoD Dictionary*… 2017: 168].

twarzania danych (np. przetwarzanie w chmurze obliczeniowej, analizy dużych zbiorów danych – *big data*) doprowadziło do globalizacji rynku przetwarzania informacji. Obserwacja ta ma istotne konsekwencje także przy analizie problemu ewentualnej kolizji pomiędzy prawami jednostki a uprawnieniami władzy publicznej. Tradycyjnie zakres dopuszczalnej ingerencji w prawa podstawowe w systemach prawnych państw demokratycznych jest regulowany normami konstytucyjnymi. Zgodnie z zasadą rządów prawa, normy ochronne stanowione w ustawie zasadniczej służą do określenia warunków wprowadzenia ograniczeń (limitacji) praw podstawowych. Globalizacja rynku przetwarzania danych powoduje, że ustanowienie regulacji ochronnych wyłącznie na poziomie prawa krajowego jest rozwiązaniem o ograniczonej skuteczności. Według danych z września 2017 roku, sześć z dziesięciu największych[3] operatorów serwisów społecznościowych to przedsiębiorcy podlegający prawu Stanów Zjednoczonych Ameryki, podczas gdy pozostałe cztery e-usługi należą do przedsiębiorców chińskich [*Most famous*…]. Dostęp do danych użytkowników europejskich korzystających z usług świadczonych przez dostawców zagranicznych nie podlega ochronie przewidzianej przez krajowe przepisy konstytucyjne właściwego państwa członkowskiego lub prawodawstwo UE. Także zbiory danych, gromadzone i zarządzane przez profesjonalne podmioty zajmujące się usługami z zakresu profilowania użytkowników – tzw. brokerów danych (ang. *data brokers*) – mogą stanowić źródło informacji o jednostkach, łatwo dostępne dla organów ścigania państw trzecich. Warto przy tym zaznaczyć, że niektórzy z brokerów danych prowadzący działalności na terenie Stanów Zjednoczonych Ameryki zarządzają bazami danych zawierającymi profile ponad 500 mln użytkowników internetu, a więc zbiorem większym niż liczba mieszkańców UE.

Dlatego słuszny jest pogląd, że płaszczyzna międzynarodowa jest właściwa do analizy relacji pomiędzy obszarem bezpieczeństwa narodowego a prawami podstawowymi. W dalszych rozważaniach analizowane będą relacje zachodzące w czasach pokoju. Obszar badawczy nie obejmuje zatem środków nadzwyczajnych, funkcjonujących w systemach prawnych na wypadek wystąpienia sytuacji zagrażających bezpieczeństwu państwa. Stąd też pominięte zostaną rozważania dotyczące klauzul derogacyjnych wynikających z przepisów zarówno konstytucyjnych, jak i prawnomiędzynarodowych.

Do zaprezentowania i omówienia różnych sposobów uregulowania wskazanej problematyki zostanie wykorzystany przykład prawodawstwa Unii Europejskiej oraz Stanów Zjednoczonych Ameryki. W literaturze przedmiotu europejski model ochrony prywatności i danych osobowych powszechnie uznaje się za najbardziej zaawansowany, stanowiący punkt odniesienia dla innych prawodawców na świecie [Schwartz 2013, 1968]. System prawny Stanów Zjednoczonych Ameryki cechuje się znacząco odmiennym podejściem, przy jednocześnie silniejszych uprawnieniach władzy w realizacji szeroko rozumianych zadań z zakresu bezpie-

[3] Według liczby zarejestrowanych użytkowników.

czeństwa narodowego. Niedopasowanie obu systemów skutkuje praktycznymi trudnościami w rozwijaniu transatlantyckiej współpracy gospodarczej i budowie wspólnej, bezpiecznej przestrzeni przetwarzania danych. Celem niniejszego artykułu będzie zatem przybliżenie przyczyn leżących u podstaw obserwowanych obecnie problemów we współpracy UE–USA w zakresie ochrony prywatności, jak również wskazanie możliwych rozwiązań. Porównywanie systemu prawnego organizacji międzynarodowej (Unia Europejska) z prawodawstwem państwa (Stany Zjednoczone Ameryki) w naturalny sposób może prowadzić do przekłamań czy nieporozumień. Dlatego pod pojęciem dorobku prawnego UE należy rozumieć nie tylko prawo pierwotne czy wtórne samej organizacji, ale również normy konstytucyjne i prawnomiędzynarodowe wspólne dla państw członkowskich i rozpoznawalne przez instytucje unijne jako tzw. ogólne zasady prawa [TSUE, 11/70, p. 2 sentencji].

ŹRÓDŁA PRAWNEJ OCHRONY PRYWATNOŚCI

Prawo do prywatności po raz pierwszy zostało wymienione w katalogu praw podstawowych w Powszechnej Deklaracji Praw Człowieka (dalej: PDPC). Chociaż akt ten nie miał charakteru prawnie wiążącego, w istotny sposób wpłynął na kształtowanie norm konstytucyjnych oraz prawnomiędzynarodowych w kolejnych dziesięcioleciach. Uwzględnienie prywatności w katalogu praw człowieka skutkowało przeniesieniem na państwa odpowiedzialności za wprowadzenie odpowiednich środków ochronnych, zarówno w relacjach horyzontalnych, jak i wertykalnych.

Wzmacnianie znaczenia ochrony praw podstawowych w państwach europejskich było związane z prawotwórczą działalnością organizacji międzynarodowych – takich jak Rada Europy czy Europejska Wspólnota Gospodarcza. Pod auspicjami każdej z tych organizacji wypracowano normy i standardy postępowania o różnym charakterze prawnym, z czasem prowadzące do przyjęcia wiążących aktów prawnomiędzynarodowych. Europejski model ochrony praw człowieka tradycyjnie jest wiązany z Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności [Dz.U. 1993 Nr 61 poz. 284, dalej: EKPC] oraz dorobkiem Europejskiego Trybunału Praw Człowieka [ETPC]. Uzupełnieniem Konwencji w gronie państw członkowskich UE była przyjęta w 2001 roku Karta Praw Podstawowych [Dz. Urz. UE 2010/C 83/389, dalej: KPP]. Dokument ten początkowo miał charakter prawnie wiążący wyłącznie dla instytucji UE. Stan ten uległ zmianie po przeprowadzeniu reformy lizbońskiej i nadaniu – zgodnie z art. 6 ust. 1 Traktatu o Unii Europejskiej [Dz. Urz. UE 2016/C 202/13, dalej: TUE] – KPP mocy równej traktatom. O ile zatem we wcześniejszym stanie prawnym ochrona praw podstawowych (w tym prywatności) była wywodzona przez TSUE z ogólnych zasad prawa, to po przyjęciu Traktatu z Lizbony wynika wprost z norm prawa pierwotnego UE.

W systemie prawnym państw członkowskich UE normy EKPC oraz KPP (czy szerzej – prawa UE) są usytuowane powyżej ustaw zwykłych. Chociaż kwestia pierwszeństwa prawa UE przed normami konstytucyjnymi jest nadal obszarem dyskusyjnym[4], to w niektórych z państw członkowskich pierwszeństwo to wynika wprost z przepisów konstytucyjnych[5]. Uogólniając, można zatem przyjąć, że w odniesieniu do wszystkich państw członkowskich UE ochrona prywatności jest w obecnym stanie prawnym gwarantowana normami prawnopublicznymi o znaczeniu ponadustawowym. W przypadku Polski ochrona ta wynika wprost z art. 47 (prawo do prywatności) oraz art. 51 (ochrona danych osobowych) konstytucji.

Zgodnie z art. 7 KPP, każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. Prawo to przynależy więc wszystkim jednostkom, niezależnie od posiadanego obywatelstwa czy spełniania innych, dodatkowych warunków[6]. W ten sposób prawodawca unijny wyraził jedną z cech tradycyjnie wiązanych z prawami człowieka – jaką jest ich przyrodzony charakter. W europejskim dorobku prawnym prywatność jest nierozerwalnie związana z godnością człowieka, a ta z kolei z wolnością jednostki[7].

Odmienne podejście do rozumienia prywatności oraz definiowania prawnych granic jej ochrony dominuje w doktrynie amerykańskiej. Amerykańska konstytucja nie definiuje wprost gwarancji związanych z ochroną prywatności. Prawo do prywatności zostało sformułowane przez Sąd Najwyższy USA w drodze precedensowych orzeczeń wydanych na tle stosowania Czwartej Poprawki[8], dotyczącej nietykalności osobistej oraz zakazującej przeprowadzania nieuzasadnionych rewizji oraz zatrzymań. Dopiero w 1965 roku Sąd Najwyższy w sprawie *Griswold* v. *Connecticut* potwierdził, że Czwarta Poprawka obejmuje także prawo jednostki do ochrony swojej prywatności [Motyka 2006: 88–94].

W przypadku USA braki we właściwych standardach konstytucyjnych nie mogą być uzupełnione normami prawnomiędzynarodowymi. Dzieje się tak pomimo faktu, że Stany Zjednoczone Ameryki przystąpiły i ratyfikowały Międzynarodowy Pakt Praw Obywatelskich i Politycznych [Dz.U. 1977 Nr 38 poz. 167, dalej: MPPOP]. Traktat ten został opracowany pod auspicjami ONZ i miał służyć przeniesieniu norm PDPC na grunt wiążących zobowiązań prawnomię-

[4] Chociaż TSUE uznał w szeregu orzeczeń prymat prawa UE także nad normami konstytucyjnymi państw członkowskich (np. TSUE, C-399/11, p. 59), wniosek ten jest kwestionowany w orzecznictwie sądów krajowych (np. TK, K 18/04) oraz doktrynie [por. Banaszak 2015].

[5] Dotyczy na przykład Estonii, w której prymat prawa UE nad przepisami konstytucji wynika z przepisów Aktu Konstytucyjnego o Członkowstwie w Unii Europejskiej [Safjan, Bosek 2016, art. 91 nb 26].

[6] Analogicznie treść prawa sformułowano w krajowych przepisach konstytucyjnych [por. art. 47 Konstytucji] oraz europejskiej konwencji [por. art. 8 ust. 1 EKPC].

[7] Por. np. art. 30 Konstytucji: „Przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych".

[8] Polskie tłumaczenie Czwartej Poprawki: http://libr.sejm.gov.pl/tek01/txt/konst/usa.html.

dzynarodowych[9]. Na skutek zastrzeżeń zgłoszonych przez Stany Zjednoczone Ameryki w trakcie procedury ratyfikacyjnej przepisy MPPOP nie mają jednak bezpośredniego skutku w prawodawstwie wewnętrznym. Konsekwencją jest brak możliwości powołania się przez jednostki na normy traktatu jako wzorzec kontroli w sporach prowadzonych przed sądami amerykańskimi. W efekcie praktyczne znaczenie przepisów Paktu z perspektywy jednostki jest niewielkie i nie prowadzi do wzmocnienia gwarancji czy rozszerzenia praw i obowiązków ponad obowiązujący standard konstytucyjny.

Oparcie treści oraz granic prawa do prywatności w amerykańskim systemie prawnym wyłącznie na precedensach prowadzi do wielu ograniczeń. Po pierwsze, ze swojej natury precedensy mają charakter kazuistyczny – a więc dotyczą konkretnej sprawy lub typów spraw. Dopóki zatem SN nie potwierdzi prawidłowości oceny nowego stanu faktycznego, nie ma pewności czy dokonywana interpretacja jest prawidłowa. Precedensy SN nie definiują nowego prawa, a tylko wskazują, że już istniejące normy prawne są wystarczające, aby wywieźć określone gwarancje. Orzeczenia SN nie mogą zatem wprowadzić rozstrzygnięcia niezgodnego z przepisami konstytucji. Problem „kreacji prawa"[10] przez Sąd Najwyższy USA znalazł szerokie omówienie w literaturze przedmiotu [Jaskiernia 1994]. Jak zauważył A. Pułło, cały złożony proces wykładni przepisów ustawy zasadniczej przez Sąd Najwyższy USA doprowadził do tego, że niektóre z praw – takie jak prawo do prywatności – pojawiły się w orzecznictwie bez wyraźnych konstytucyjnych podstaw [Pułło 1997: 36].

Model ochrony prywatności oparty na Czwartej Poprawce charakteryzuje się także ograniczeniami w zakresie kręgu osób uprawnionych oraz podmiotów zobowiązanych. Funkcją ochronną obejmuje wyłącznie obywateli oraz rezydentów Stanów Zjednoczonych Ameryki [por. SN USA, 494 U.S. 259 1990], ma skutek wyłącznie wertykalny [Johnson 2017: 878] oraz ma ograniczone zastosowanie w odniesieniu do działań organów władzy publicznej poza obszarem Stanów Zjednoczonych Ameryki [Corradino 1989: 618–619]. W rezultacie postanowienia Czwartej Poprawki muszą być w pełni stosowane przez organy władzy publicznej wyłącznie na terytorium USA i tylko w odniesieniu do osób stale tam przebywających.

[9] Stronami MPPOP są także państwa członkowskie UE, jednak w ich przypadku większe znaczenie posiada EKPC oraz bezpośrednio prawo UE. Prawo do prywatności zostało zagwarantowane w art. 17 traktatu, a jego treść i zakres ochronny jest zbliżony do wynikającego z EKPC.

[10] Pod pojęciem kreacji prawa należy rozumieć interpretowanie lub doprecyzowanie przepisów w sposób wykraczający poza literalne brzmienie pierwotnego aktu. Uwzględniając szerokie kompetencje Sądu Najwyższego USA w tym zakresie (wynikające z tzw. klauzuli supremacyjnej), dokonana wykładnia niejednokrotnie prowadziła do wniosków sprzecznych z analizowanym przepisem. W doktrynie amerykańskiej dominuje jednak pogląd, że to prawodawca – stanowiąc normy – może odrzucić jurydyczną interpretację przez nowelizację przepisów. Brak takiej nowelizacji lub przyjęcie w nowej ustawie dyskutowanych regulacji w niezmienionym kształcie jest interpretowane jako aprobata dla kierunku orzecznictwa [Jaskiernia 1994: 28–29].

Należy zauważyć, że konsekwencją braku uwzględnienia w przepisach konstytucyjnych *expresis verbis* prawa do prywatności jest także brak gwarancji związanych z ochroną danych osobowych. W modelu europejskim ochrona danych osobowych jest prawem wywodzonym wprost z prawa do prywatności (ma to miejsce np. na gruncie przepisów EKPC, w której nie zdefiniowano wprost prawa do ochrony danych osobowych) lub definiowanym jako oddzielne prawo (np. w KPP[11] lub polskiej konstytucji[12]). Sposób sformułowania prawa do prywatności – przez wyliczenie przykładowego katalogu dóbr chronionych (*vide*: wcześniejsza treść prawa wynikająca z art. 7 KPP) – pozwala na rozszerzanie zakresu przedmiotowego w sposób odzwierciedlający przemiany społeczne oraz postęp techniki. Dlatego w modelu europejskim rozszerzenie zakresu ochronnego nie wymaga zmiany przepisów materialnych[13]. Tej elastyczności jest pozbawiona amerykańska konstytucja. Analiza orzecznictwa SN prowadzi do wniosku, że treść prawa do prywatności wynikająca z Czwartej Poprawki jest przedmiotowo znacząco węższa niż wynikająca z norm europejskich. W szczególności nie obejmuje w ogóle obszaru ochrony danych osobowych.

Odmienne normy konstytucyjne w UE i USA skutkują także wprowadzeniem innych przepisów ustawowych oraz ukształtowaniem odmiennych obowiązków władzy publicznej w zakresie ochrony prywatności. W Unii Europejskiej regulacje ustawowe służą uzupełnieniu i doprecyzowaniu gwarancji konstytucyjnych. Europejski model ochrony danych – którego podstawę obecnie stanowi dyrektywa 95/46 oraz zastępujące ją rozporządzenie 2016/679 (tzw. ogólne rozporządzenie o ochronie danych) – przewiduje wprowadzenie identycznych obowiązków prawnopublicznych dla wszystkich podmiotów przetwarzających informacje, niezależnie czy należą do sektora prywatnego czy publicznego. Ponieważ prawo do prywatności jest prawem podstawowym, jego ochrona wynika z regulacji prawnopublicznych. W tym celu przepisy UE wymagają utworzenia organu nadzoru, którego nieodłączną cechą jest niezależność od władzy wykonawczej[14]. Niezależny organ nadzoru stoi na straży ochrony praw jednostki, jednocześnie odpowiada za nadzorowanie przestrzegania standardów przetwarzania danych.

Z kolei w Stanach Zjednoczonych Ameryki przepisy ochronne dotyczące prywatności są wprowadzane sektorowo i fragmentarycznie. W prawodawstwie amerykańskim najbliższym odpowiednikiem europejskiego ogólnego rozporządzenia jest ustawa o prywatności (88 Stat. 1896, dalej: Privacy Act), która jednak reguluje wyłącznie czynności gromadzenia i przetwarzania danych przez organy federalne. Przepisy Privacy Act zawierają wiele wyłączeń, m.in. w zakresie podmiotów zobowiązanych, jak również celu przetwarzania – np. wyłączone

[11] Por. art. 7 KPP.

[12] Por. art. 47 Konstytucji.

[13] Przykładem może być uznanie przez EKPC, że przepis art. 8 ust. 1 stanowi wystarczającą podstawę dla objęcia ochroną także treści wiadomości elektronicznych. Por. ETPC, 62617/00.

[14] Por. art. 16 ust. 2 TFUE, art. 8 ust. 3 KPP, a także wyroki ETPC w sprawach C-518/07, C-614/10 oraz C-288/12.

spod przepisów ustawy jest przetwarzanie prowadzone przez organy ścigania w związku z prowadzonymi dochodzeniami[15]. Brak konstytucyjnych gwarancji związanych z ochroną prywatności powoduje, że państwo nie jest zobowiązane do wprowadzenia właściwych przepisów regulujących relacje horyzontalne. Także prawo stanowe w różny sposób definiuje treść i zakres ochrony prywatności.

Konsekwencją rozproszonych norm prawnych jest także brak powołania jednego organu odpowiedzialnego za nadzór nad przestrzeganiem przepisów dotyczących ochrony prywatności i danych osobowych. Funkcje nadzorcze są realizowane sektorowo, przy czym najbardziej zbliżone zadania do europejskich organów nadzoru pełni Federalna Komisja Handlu (FTH).

Podsumowując dotychczasowe rozważania – ochrona prywatności została odmiennie uregulowana w systemie prawnym Unii Europejskiej oraz Stanów Zjednoczonych Ameryki. W modelu europejskim przyjęto, że prawo do prywatności należy do katalogu praw podstawowych, jego ochrona jest realizowana przez przepisy konstytucyjne uzupełniane normami prawnomiędzynarodowymi. Prawna ochrona przysługuje wszystkim jednostkom, a jej zakres obejmuje wszystkie obszary aktywności. Z kolei w Stanach Zjednoczonych Ameryki treść prawa wynika z orzeczeń Sądu Najwyższego i ma charakter kazuistyczny. Ochrona nie przysługuje wszystkim jednostkom, a krąg podmiotów zobowiązanych obejmuje wyłącznie organy władzy publicznej. Na płaszczyźnie horyzontalnej (pomiędzy jednostkami) ochrona jest realizowana przez regulacje prywatnoprawne (zobowiązania umowne, polityki prywatności itp.), a więc nie ma charakteru zobowiązań *erga omnes*.

OGRANICZENIA I LIMITACJA

Przed przedstawieniem szczegółowych rozważań dotyczących obszaru bezpieczeństwa narodowego konieczne jest omówienie istniejących środków prawnych skutkujących ograniczeniem praw i wolności osobistych. Gdyby bowiem przyjąć, że prawa jednostki – takie jak prawo do prywatności – mają charakter absolutny i nadrzędny względem praw zbiorowych (np. bezpieczeństwa publicznego), żadne ograniczenia – niezależne od swojego charakteru i realizowanego celu – nie mogłyby zostać uznane za legalne[16].

W systemach prawnych państw demokratycznych przyjmuje się, że wszelkie ograniczenia wolności i praw jednostki powinny wynikać z przepisów rangi ustawowej, być zgodne z zasadą rządów prawa oraz być konieczne z uwagi na ważny interes społeczny. W polskim porządku prawnym ustanawianie ograniczeń

[15] Por. 5 U.S.C. §552a(a)(8)(B)(iii).

[16] Por. np. opinia 1/15 TSUE z 26.07.2017, p. 136: „Prawa gwarantowane w art. 7 i 8 karty nie stanowią prerogatyw o charakterze absolutnym, lecz powinny być oceniane w świetle ich funkcji społecznej".

w korzystaniu z wolności i praw zostało uregulowane w art. 31 ust. 3 konstytucji. Warunek „konieczności w demokratycznym państwie" został powiązany z realizacją celu bezpieczeństwa lub porządku publicznego, ochrony środowiska, zdrowia lub moralności publicznej. Jest to katalog zbieżny z wymienionym w EKPC (por. treść art. 8 ust. 2). Z kolei w redakcji art. 52 ust. 1 KPP podkreślono znaczenie zasady proporcjonalności oraz konieczności jako niezbędnych przesłanek warunkujących wprowadzenie ograniczeń w przestrzeni praw i wolności osobistych.

Zachowanie proporcjonalności wprowadzanych środków było wielokrotnie akcentowane zarówno w orzecznictwie krajowych sądów konstytucyjnych, jak i trybunałów międzynarodowych. Brak zachowania zasady proporcjonalności było bezpośrednim powodem stwierdzenia przez ETPC naruszenia przepisów konwencji (np. wyrok 37138/14), jak również uznania przez TSUE niezgodności badanych dokumentów normatywnych z prawem UE (np. wyrok C-239/12). Zasada proporcjonalności jest zachowana, jeżeli wprowadzane środki są adekwatne (nie prowadzą do nadmiernego, nieuzasadnionego naruszenia praw podstawowych) oraz konieczne (oczekiwane rezultaty nie mogą być osiągnięte w inny, mniej inwazyjny sposób). W orzecznictwie ETPC wypracowano wiele kryteriów pozwalających na weryfikację, czy analizowane przepisy krajowe ograniczające prawa podstawowe nie prowadzą do ich naruszenia, a więc czy wprowadzana ingerencja jest uzasadniona, uwzględniając cele i normy ustrojowe wspólne dla państw demokratycznych (ETPC, 54934/00, §95).

Konstytucja Stanów Zjednoczonych Ameryki jest pozbawiona jasnej i precyzyjnej klauzuli limitacyjnej. Ponieważ treść wielu praw i wolności (w tym prawa do prywatności) określonych w federalnej karcie praw (ang. *United States Bill of Rights*)[17] została ukształtowana w drodze precedensów, także dyskusja związana z dopuszczalnym zakresem ingerencji wymaga odniesienia do dorobku judykatury.

Na tym tle omówienia wymagają dwie istotne doktryny prawne – uzasadnionego oczekiwania prywatności (ang. *reasonable expectation of privacy*) oraz zasada trzeciej strony (ang. *third party doctrine*). Pierwsza służy ocenie przez sąd, czy w określonej sytuacji jednostka może oczekiwać prawnej ochrony prywatności. Jej istotą jest nie tylko ustalenie, czy w subiektywnym odbiorze jednostki dane zdarzenie ingerowało w sferę prywatności, ale również próba zobiektywizowania tej oceny dzięki uwzględnieniu obowiązujących norm społecznych [Czubik 2013: 155–156]. Z kolei doktryna trzeciej strony prowadzi do wyłączenia spod ochrony informacji, które jednostka sama ujawniła osobom trzecim. W szczególności zgodnie z zasadą trzeciej strony, informacje powierzone zewnętrznym podmiotom w celu dalszego przetwarzania w ramach prowadzonej działalności gospodarczej nie mogą korzystać z ochrony przewidzianej Czwartą Poprawką[18].

[17] W literaturze terminem tym określa się pierwsze dziesięć poprawek do konstytucji USA.

[18] Obowiązująca treść zasady trzeciej strony była kształtowana w wielu wyrokach SN, przy czym warunki pozwalające na jej zastosowane wynikają z wyroku Sądu Najwyższego w sprawie *Couch v. United States*.

Zgodnie z zasadą trzeciej strony dane zawarte na bilingach telekomunikacyjnych, zestawieniach sald bankowych, rozliczeniach kart kredytowych itp. nie podlegają ochronie, a dostęp do nich przez organy władzy publicznej (np. organy ścigania) nie wymaga zastosowania procedury wynikającej z Czwartej Poprawki.

Należy pamiętać, że Czwarta Poprawka chroni wyłącznie obywateli i rezydentów Stanów Zjednoczonych Ameryki oraz że wiąże wyłącznie działania władzy publicznej (nie ma zastosowania w relacjach horyzontalnych). Jednocześnie – z uwagi na wąski zakres stosowania – nie może być ona podstawą do wywodzenia gwarancji konstytucyjnych dotyczących ochrony danych osobowych. Dlatego – inaczej niż w demokracjach europejskich – w Stanach Zjednoczonych Ameryki konflikt pomiędzy prawami podstawowymi a bezpieczeństwem narodowym częściej ogniskuje się wokół gwarancji nietykalności i wolności osobistej, zakazu stosowania tortur w trakcie czynności śledczych czy prawa do sądu. Wynika to z faktu, że gwarancje te znajdują silniejsze zaakcentowanie w amerykańskiej konstytucji niż prawo do prywatności. Dość powiedzieć, że w zapoczątkowanej na nowo po wydarzeniach z 11.09.2001 roku dyskusji nad legalnością stosowania przemocy przez agentów federalnych także wybitni przedstawiciele amerykańskiej nauki prawa, tacy jak R. Posner, rozważali możliwość zaakceptowania faktu stosowania tortur wobec podejrzanych [Kuisz 2013].

Bez wątpienia przepisy europejskie pozostawiają władzy wykonawczej oraz judykaturze zdecydowanie mniejszy margines uznania, pozwalający na kształtowanie lub wpływanie na rozszerzenie katalogu okoliczności uzasadniających ingerencję w prawa podstawowe. Należy pamiętać, że bezpośrednią przyczyną tej różnicy nie są wyłącznie bardziej precyzyjne i restrykcyjne przepisy konstytucyjne i prawnomiędzynarodowe, ale także odmienne doświadczenia związane z totalitaryzmami w XX wieku. Ideą leżącą u podstaw przyjęcia PDPC, a później wypracowania EKPC, jak również wprowadzenia do porządków konstytucyjnych państw europejskich silnych gwarancji dotyczących praw człowieka było wzmocnienie rządów prawa, pozwalające na uniknięcie sytuacji, w której duży luz decyzyjny pozostawiony rządzącym pozwala na erozję mechanizmów ochrony praw, a w konsekwencji na przyjęcie rozwiązań prowadzących do wypaczenia idei państwa demokratycznego.

ROZUMIENIE I ZAKRES BEZPIECZEŃSTWA NARODOWEGO

Aprobując fakt, że prawo do prywatności nie należy do praw absolutnych, należy przeanalizować, czy wystarczającym powodem jego limitacji jest realizacja zadań z obszaru bezpieczeństwa narodowego.

O ile komparastyka systemów prawnych UE i USA może być stosunkowo ławo przeprowadzona, jeżeli chodzi o prawne mechanizmy ochrony prywatności, to już w przypadku bezpieczeństwa narodowego pojawiają się dwie zasadnicze trudności. Pierwszą jest brak powszechnie wypracowanej legalnej definicji tego

pojęcia, natomiast drugą – ograniczona stosowalność prawa UE w obszarze bezpieczeństwa państwa.

Zgodnie z art. 4 ust. 2 TSUE, ochrona bezpieczeństwa narodowego pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego. Ponieważ w traktatach nie zdefiniowano pojęcia bezpieczeństwa narodowego, a konsekwencją stosowania art. 4 ust. 2 jest wyłączenie tego obszaru spod zakresu stosowania prawa UE, realne byłoby ryzyko, że poszczególne państwa członkowskie mogłyby dowolnie swobodnie interpretować zakres tego pojęcia, a w konsekwencji uniemożliwić kontrolę własnych działań przez instytucje Unii. Dlatego TSUE orzekł, że spójność prawa UE oraz rynku wewnętrznego wymaga, aby rozumienie pojęć, takich jak „bezpieczeństwo publiczne" – które nie znajdują rozwinięcia w postanowieniach traktatowych – podlegało wykładni i ocenie sądu [Wyrok TSUE 41/74]. Dotychczasowe orzecznictwo wskazuje, że w przypadkach, w których państwa sygnalizowały możliwość zastosowania wyłączenia przedmiotowego z przepisów dotyczących ochrony prywatności, Trybunał uznawał możliwość zastosowania prawa UE. Nie zmienia to faktu, że w przypadku uznania, że dane działanie mieści się w definicji celów bezpieczeństwa narodowego, jest ono wyłączone spod stosowania prawa UE – a w efekcie nie mają zastosowania także gwarancje wynikające z KPP [Rojszczak 2017: 164–167].

Odmiennie sytuacja wygląda w przypadku EKPC, która nie zawiera ogólnej klauzuli wyłączającej przedmiotowo stosowanie konwencji w zakresie celów bezpieczeństwa ogólnego. Jak wielokrotnie uznał ETPC, ochrona porządku publicznego jest celem uzasadniającym zastosowanie środków ingerujących w zakres prawa do prywatności. Ingerencja ta, aby była jednak uzasadniona, musi być proporcjonalna – a więc adekwatna i konieczna. Dotychczasowe doświadczenia związane z kontrolą tzw. ustaw antyterrorystycznych czy nadzwyczajnych uprawnień organów ścigania prowadzą do wniosku, że ogólne regulacje skutkujące ograniczeniem praw całego lub dużej części społeczeństwa nie mogą zostać uznane za konieczne z uwagi na brak ich proporcjonalności [zob. np. TSUE, C-203/15: 116]. A zatem z perspektywy prawodawstwa europejskiego prawo do prywatności jednostki może być ograniczone, jeżeli jest to konieczne z uwagi na dobro ogólne. Ograniczenie to musi być jednak uzasadnione konkretną potrzebą związaną z toczącym się dochodzeniem lub postępowaniem karnym. Zarówno TSUE, jak i ETPC wypowiadały się negatywnie o możliwości stosowania działań prewencyjnych, nieznajdujących uzasadnienia w innym materiale dowodowym, a skutkujących ingerencją w sferę prywatności jednostek.

W amerykańskim systemie prawnym uprawnienia władzy wykonawczej do wprowadzania środków ingerujących w prawa podstawowe są bardziej rozbudowane niż analogiczne regulacje funkcjonujące w państwach europejskich. Konstytucja USA nadaje prezydentowi prerogatywy związane z utrzymaniem bezpieczeństwa publicznego. Ich wykonywanie nie może być skutecznie ograniczone aktami stanowionymi przez Kongres. Dodatkowo w wielu ustawach Kongres delegował władzy wykonawczej kompetencje do stanowienia regulacji

mających wpływ na bezpieczeństwo państwa[19]. Z połączenia nieprecyzyjnych standardów konstytucyjnych, fragmentarycznych przepisów ustawowych oraz rozbudowanych uprawnień rządu federalnego powstał system prawny, w którym cele bezpieczeństwa narodowego w wielu przypadkach przeważają nad prawami i wolnościami osobistymi[20].

Niedawna dyskusja na temat koniecznej nowelizacji przepisów ustawy o nadzorze nad wywiadem obcym [92 Stat. 1783, dalej: FISA] może posłużyć do zobrazowania różnic pomiędzy europejskim a amerykańskim modelem ochrony prywatności. W Stanach Zjednoczonych Ameryki od 1978 roku funkcjonują przepisy pozwalające na wydawanie niejawnych – i w praktyce niezaskarżalnych – wyroków przez specjalny, tajny sąd, skutkujących objęciem inwigilacją milionów obywateli. Kolejne nowelizacje ustawy FISA prowadziły do dalszego rozszerzenia uprawnień służb specjalnych[21]. Pomimo licznych działań prowadzonych przez stowarzyszenia obrony praw człowieka, legalność środków wynikających z FISA nie została skutecznie zakwestionowana na drodze sądowej. Chociaż uprawnienia wynikające z ustawy FISA są wątpliwe prawnie, nawet uwzględniając nieprecyzyjne w tym zakresie normy konstytucyjne USA, to i tak – pomimo trwającej wiele lat dyskusji na ten temat – problem ten nie został rozwiązany przez federalnego prawodawcę.

Judykatura amerykańska nie wypracowała przy tym własnych standardów pozwalających na ocenę zakresu dopuszczalnej ingerencji w prawa osobiste uzasadnianej celami bezpieczeństwa ogólnego. Nie mając wystarczającego oparcia w normach konstytucyjnych czy w przepisach prawa stanowionego, sądy fe-

[19] Błędem byłoby jednak wskazywanie wyłącznie jednej przyczyny tego, dlaczego w systemie ustrojowym Stanów Zjednoczonych Ameryki uprawnienia egzekutywy zaczynają dominować nad pozostałymi władzami. Dla przykładu W. Marshall wymienił 11 głównych powodów i każdy z nich poddał analizie [Marshall 2008].

[20] Przykładem może być sprawa *ACLU v NSA*, sygn. 493 F.3d 644 [6th Cir. 2007]. Amerykańska Unia Swobód Obywatelskich (*American Civil Liberties Union*, ACLU) wytoczyła powództwo przeciwko Agencji Bezpieczeństwa Wewnętrznego (*National Security Agency*, NSA), kwestionując legalność prowadzonych przez nią programów wywiadu elektronicznego, w ramach których była przechwytywana łączność elektroniczna na masową skalę. Pozew ACLU został oddalony z uwagi na brak wykazania interesu prawnego, tj. udowodnienia, że działania NSA obejmowały osoby, w imieniu których występował powód. W praktyce wykazanie objęcia danej osoby tajnym programem inwigilacji jest niemożliwe z uwagi na niejawność podejmowanych działań. Wniosek ten prowadzi do znacznego ograniczenia w Stanach Zjednoczonych Ameryki możliwości dochodzenia sądowej ochrony prawa do prywatności przez osoby objęte działaniami inwigilacyjnymi przez władze państwowe. Szersze omówienie wyroku w „Harvard Law Review" 2008, t. 121, s. 922–929. Szerzej na temat orzecznictwa SN USA w sprawach dotyczących bezpieczeństwa narodowego i praw podstawowych w: [Stone 2007].

[21] Przykładem mogą być kontrowersje związane z przyjęciem ustawy z 25.10.2001 o zjednoczeniu i wzmocnieniu USA dzięki dostarczeniu właściwych narzędzi potrzebnych do wykrywania i zapobiegania aktom terrorystycznym (znanej w literaturze jako *Patriot Act*) lub ustawy z 10.07.2008 r. o zmianie ustawy o nadzorze nad wywiadem obcym (*Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*). Omówienie Privacy Act w: [Czubik 2013: 203–205].

deralne nie stosują zasady proporcjonalności czy konieczności jako warunku koniecznego dla wprowadzanych ograniczeń.

Praktycznym przykładem funkcjonowania podziału kompetencji w prawodawstwie amerykańskim jest wydane w styczniu 2017 roku przez prezydenta Donalda Trumpa rozporządzenie wykonawcze 13768 (82 FR 8799), zgodnie z którym organy rządu federalnego zobowiązano do niestosowania w odniesieniu do obcokrajowców praw wynikających z ustawy Privacy Act[22]. Niezależnie od innych kontrowersji związanych ze wskazanym rozporządzeniem uwagę zwraca wprowadzenie środków limitacyjnych względem praw podstawowych w akcie innym niż ustawowy.

Podsumowując tę część rozważań, należy zauważyć, że prawodawstwo europejskie oraz amerykańskie różni się nie tylko odmienną treścią i zakresem prawa do prywatności, ale również odmiennym wyważeniem celów bezpieczeństwa państwowego względem praw i wolności osobistych.

KONSEKWENCJE NIEDOPASOWANIA SYSTEMÓW PRAWNYCH

Przedstawione różnice w prawodawstwie UE i USA skutkują wieloma praktycznymi trudnościami w budowaniu transatlantyckiego partnerstwa w zakresie swobodnego przepływu danych. W literaturze przedmiotu wskazuje się na ograniczoną skuteczność praw i gwarancji obywateli UE w odniesieniu do danych przetwarzanych na terenie Stanów Zjednoczonych Ameryki lub przez podmioty podlegające prawu UE (*The US legal system*…: 5). Uwzględniając znaczenie współpracy UE–USA, także w zakresie usług społeczeństwa informacyjnego, jest to przeszkoda, która coraz częściej stoi na przeszkodzie dalszemu zacieśnianiu współpracy dwustronnej. W ostatnich latach można wskazać co najmniej trzy obszary, w których niedopasowanie systemów prawnych stanowiło istotne utrudnienie we wzajemnych relacjach UE–USA – są to: współpraca handlowa, współpraca w obszarze wymiarów sprawiedliwości oraz wymiana danych dotyczących pasażerów.

Elementem, który coraz częściej warunkuje rozwój współpracy handlowej, zwłaszcza w obszarze e-usług, jest swobodna wymiana danych osobowych. Podstawę dla tej wymiany przez wiele lat stanowiła decyzja KE 2000/520 o adekwatności zabezpieczeń i wynikający z niej program Bezpieczna przystań [Dz. Urz. WE z 2000/L 215/7]. W 2014 roku TSUE w wyroku *Schrems* stwierdził, że amerykańskie prawodawstwo nie gwarantuje ochrony praw podstawowych na poziomie porównywalnym do wynikającego z prawa UE, m.in. z uwagi na nadrzędność przepisów dotyczących bezpieczeństwa narodowego nad prawami podstawowymi [TSUE, C-362/14]. W konsekwencji uznał, że Komisja przekro-

[22] Zob. art. 14 rozporządzenia wykonawczego 13768.

czyła swoje kompetencje, i unieważnił decyzję, co doprowadziło do znacznego utrudnienia transatlantyckiej wymiany danych [Rojszczak 2018].

Także w obszarach współpracy dotyczącej bezpieczeństwa publicznego niedopasowanie systemów prawnych prowadzi do negatywnych skutków. Przykładem może być wymiana informacji o pasażerach (ang. *Passenger Name Record*, PNR), które na podstawie amerykańskich przepisów muszą być przekazywane przez linie lotnicze wykonujące połączenia do Stanów Zjednoczonych Ameryki. Unia Europejska, rozpoznając potrzebę ochrony przed zagrożeniami terrorystycznymi i poważną przestępczością, wynegocjowała i zawarła umowę międzynarodową ze Stanami Zjednoczonymi Ameryki, na podstawie której dane PNR mogą być przekazywane przez europejskich przewoźników bez naruszania obowiązujących ich przepisów o ochronie danych. Podobna umowa została zawarta z Australią oraz uzgodniona z Kanadą. Projekt umowy UE–Kanada został skierowany przez PE do Trybunału w trybie wynikającym z art. 218 ust. 11 Traktatu o Funkcjonowaniu Unii Europejskiej [Dz. Urz. UE 2016/C 202/47, dalej: TFUE] celem wyrażenia opinii o zgodności projektowanego rozwiązania z prawem UE. Trybunał w opinii z dnia 26.07.2017 wskazał, że środki zastosowane w przedłożonym projekcie w wielu miejscach nie mogą być pogodzone z prawem UE, w szczególności z przepisami dotyczącymi ochrony prywatności i danych osobowych. Jak zauważył TSUE, realizacja celu związanego z porządkiem publicznym czy bezpieczeństwem narodowym nie uzasadnia podejmowania działań skutkujących nieproporcjonalną ingerencją w obszar praw jednostek. Opinia Trybunału oznacza brak możliwości zawarcia umowy z Kanadą w bieżącym kształcie, nie prowadzi jednak do automatycznego unieważnienia umowy ze Stanami Zjednoczonymi Ameryki. Biorąc pod uwagę, że umowa UE–USA zawierała mniej restrykcyjne zapisy niż projekt umowy z Kanadą, należy oczekiwać, że w przypadku sądowej kontroli traktatu zawartego ze Stanami Zjednoczonymi Ameryki także ta umowa zostanie uznana za niezgodną z prawem UE.

KONKLUZJE

Problematyka odmiennego wyważenia relacji pomiędzy bezpieczeństwem narodowym a prawami jednostki w prawodawstwie Unii Europejskiej oraz Stanów Zjednoczonych Ameryki będzie coraz częściej tematem intensywnej dyskusji w nauce prawa. Postępująca globalizacja, dynamiczny rozwój e-usług świadczonych transgranicznie, ale także rosnące znaczenie świadomości społeczeństwa w zakresie roli i ochrony prywatności przyczynia się do zwiększenia presji na prawodawców w zakresie wypracowania wspólnych standardów ochrony praw podstawowych w cyberprzestrzeni. Jednocześnie brakuje podstaw, aby oczekiwać, że partner amerykański doprowadzi do znaczącego ograniczenia kompetencji i uprawnień organów władzy publicznej w obszarze bezpieczeństwa narodowego. Istnieją co najmniej dwa istotne argumenty wspierające ten pogląd.

Pierwszy, związany *stricte* z systemem prawnym, dotyczy słabości norm konstytucyjnych Stanów Zjednoczonych Ameryki w obszarze ochrony prywatności. Ponieważ zmiana konstytucji w warunkach amerykańskiego systemu politycznego jest rozwiązaniem nierealnym, pozostaje możliwość wypracowania odmiennej linii orzeczniczej przez Sąd Najwyższy (a więc zastosowanie rozszerzającej interpretacji Czwartej Poprawki) – jednak biorąc pod uwagę dotychczasowe orzecznictwo, nie ma powodów sądzić, aby scenariusz taki był możliwy.

Drugi powód jest natury politycznej. Obecna administracja amerykańska, w szczególności prezydent D. Trump, akcentują w swojej polityce wewnętrznej i zewnętrznej doktrynę „Najpierw Ameryka" (ang. *America First*). Jednym z jej elementów jest rosnące znaczenie kompetencji służb specjalnych oraz wprowadzanie regulacji ograniczających prawa osobiste. Obecna administracja nie poszukuje porozumienia ani konsensusu z partnerami zagranicznymi w zakresie budowania wspólnej płaszczyzny ochrony praw jednostek w cyberprzestrzeni. Liczne dowody wspierające ten pogląd można odnaleźć w zaktualizowanej strategii bezpieczeństwa narodowego USA, opublikowanej 22.12.2017 roku. Autorzy doktryny wskazują, że „Internet jest wynalazkiem amerykańskim i powinien odzwierciedlać nasze wartości w trakcie dalszego rozwoju i transformacji dla następnych pokoleń i wszystkich narodów" [*National Security*… 2017: 13].

Nie należy oczekiwać, że państwa europejskie podejmą kroki prowadzące do osłabiania mechanizmów ochrony praw podstawowych. Unia Europejska podejmuje kolejne działania wzmacniające środki ochrony prywatności w cyberprzestrzeni, jednocześnie realizuje działania prowadzące do budowy wspólnych unijnych ram zapobiegania i wykrywania najpoważniejszych przestępstw.

W piśmiennictwie wyrażane jest przekonanie o możliwości szukania porozumienia pomiędzy UE i USA na płaszczyźnie aktów prawnomiędzynarodowych [por. Kowalik-Bańczyk 2015: 409]. Wskazuje się w tym zakresie na możliwość wypracowania nowego protokołu dodatkowego do MPPOP [*Rezolucja*… 2013: 1] czy przystąpienia obu partnerów do funkcjonującej już obecnie Konwencji 108 [Greenleaf 2015: 4]. Oba rozwiązania, jakkolwiek interesujące intelektualnie, również wydają się mało prawdopodobne. Stany Zjednoczone Ameryki dotąd nie sygnalizowały chęci poddania swojego systemu prawnego zewnętrznej kontroli, a jak pokazuje doświadczenie związane z MPPOP – bez skutecznego mechanizmu kontrolnego traktat międzynarodowy ustanowiony w obszarze praw podstawowych posiada ograniczoną skuteczność.

Przedstawione rozważania stanowią jedynie wstęp do szerszej dyskusji na temat adekwatności systemów ochrony praw człowieka w erze powszechnej cyfryzacji. Problemy, które uwidaczniają się w przestrzeni transnarodowej, każą od nowa zastanowić się nad legalną definicją państwa i granic jego imperium, sposobem formułowania uniwersalnych praw jednostki, a także nadmiernie elastycznym definiowaniem kluczowych pojęć, takich jak bezpieczeństwo narodowe.

Konkludując powyższe refleksje, warto pamiętać, że w istocie wolności i prawa jednostki nigdy nie mogą być przeciwstawiane prawom zbiorowym – postrze-

ganie praw podstawowych jako „przeszkody" czy utrudnienia w realizacji zadań z zakresu bezpieczeństwa ogólnego jest błędem. Jak słusznie zauważył Aaron Barak, wieloletni prezes Sądu Najwyższego Izraela, „prawa człowieka nie są narzędziem zniszczenia państwa; ich ochrona nie może stać się usprawiedliwieniem dla podważania bezpieczeństwa narodowego w każdym przypadku, niezależnie od okoliczności […]. Z drugiej strony musimy wziąć pod uwagę wartości i zasady dotyczące ludzkiej godności i wolności […]. Bezpieczeństwo narodowe nie jest nieograniczonym uprawnieniem do krzywdzenia jednostek. Demokratyczne państwa muszą znaleźć równowagę między tymi sprzecznymi wartościami i zasadami. Żadna z nich nie powinna zdominować drugiej" [Barak 2002: 153].

Title: Legal Dilemmas of Cyberspace Regulation: Conflict Between National Security and the Right to Privacy from the Perspective of EU and US Legal Systems

Summary: The model of protection of privacy in cyberspace implemented in the European Union is widely recognized as the most sophisticated, both in terms of protection of data subjects' rights and consistency of obligations imposed on data processors. The current regulations – including the broadly discussed new general data protection regulation – are the results of more than twenty years of evolution, initiated by the EC in 1990 by submitting projects of the first Community regulations. Information security professionals point on the issue of inevitable collision of EU regulations with the regulations applied by one of its main trade partners – the United States. The US laws, including constitutional norms, lead to significantly different level of privacy protection. The most noticeable difference is the scope of permissible interference from the public authorities, taking the form of extensive electronic surveillance programs. Programs of this type are oriented on collecting bulk data, including – inevitably – also information about EU citizens. Mass surveillance raises serious constitutional objections in many European countries, and its conduct has also become one of the reasons for the invalidation of the Safe Harbor program by the CJEU. This program was the main method of transferring personal data from the EU to US-based processors. The incompatibility of EU and US laws regarding the different relations between right to privacy and national security is a practical and current problem in building mutual relations. Cyberspace has no boundaries, so this problem has an additional dimension – related to the attempt to determine to what extent territorial standards can be effectively applied in the supranational space. The purpose of the article is to present considerations regarding the potential conflict between rights of the individuals and national security objectives, together with the presentation of the most important EU and US laws in this area and with explanation of the causes of their mutual incompatibility.

Keywords: right to privacy, national security, human rights, cyberspace, international law

BLIBLIOGRAFIA

1. Banaszak B. (2015), *Zasada nadrzędności Konstytucji w polskim porządku prawnym*, [w:] *Zasada pierwszeństwa prawa Unii Europejskiej w praktyce działania organów władzy publicznej RP*, M. Jabłoński, S. Jarosz-Żukowska (red.), Wrocław, s. 41–54.
2. Barak A. (2002), *Foreword: A Judge On Judging: The Role of a Supreme Court in a Democracy*, "Harvard Law Review", t. 116, s. 19–162.

3. Corradino E. (1989), *The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far?*, "Fordham Law Review", t. 57, s. 617–635.
4. Czubik A. (2013), *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Kraków, s. 155–156.
5. Czuryk M. et al. (2016), *Bezpieczeństwo państwa: zagadnienia prawne i administracyjne*, Olsztyn.
6. Decyzja Komisji z 26.07.2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz.Urz. WE z 2000 nr L 215).
7. *DOD Dictionary of Military and Associated Terms*, US Department of Defence 2017, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
8. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE z 1995 Nr L 281, s. 31).
9. Executive Order 13768: Enhancing Public Safety in the Interior of the United States, 82 FR 8799, http://cli.re/67wa3x.
10. Greenleaf G. (2015), *The UN Special Rapporteur: Advancing a Global Privacy Treaty?*, Privacy Laws & Business International Report, t. 136, https://ssrn.com/abstract=2672549, s. 4.
11. Jaskiernia J. (1994), *Ustawodawstwo a sądowa kreacja prawa w Stanach Zjednoczonych Ameryki*, „Państwo i Prawo", nr 9, s. 28–38.
12. Johnson E. (2017), *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, "Stanford Law Review", t. 69, s. 867–909.
13. Karta Praw Podstawowych Unii Europejskiej z dn. 30.03.2010 r. (Dz.Urz. UE z 2010 nr C 83, s. 389).
14. Konstytucja Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.).
15. Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dn. 28.01.1981 (Dz.U. 2003 Nr 3, poz. 25).
16. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4.11.1950 r. (Dz.U. 1993 Nr 61, poz. 284).
17. Kowalik-Bańczyk K. (2015), *Prawo do prywatności w Internecie – kolizja między amerykańskich i europejskim modelem ochrony*, [w:] *Amerykański system ochrony praw człowieka*, J. Jaskierni (red.), Toruń.
18. Kuisz J. (2013), *Konstytucja w sytuacjach zagrożenia bezpieczeństwa państwa na tle teorii R.A. Posnera*, „Państwo i Prawo", nr 12, s. 46–59. DOI: https://doi.org/10.5604/08672245.1157063.
19. Laskowski J. (2015), *Problemy ochrony danych wrażliwych we współpracy antyterrorystycznej UE i USA*, [w:] *Amerykański system ochrony praw człowieka*, J. Jaskierni (red.), Toruń.
20. Majer P. (2012), *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 7, s. 11–19.
21. Marshall W. (2008), *Eleven Reasons Why Presidential Power Inevitably Expands and Why It Matters*, "Boston University Law Review", t. 88, s. 505–522.
22. Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku 19.12.1966 r. (Dz.U. 1977 Nr 38, poz. 167).
23. *Most famous social network sites worldwide as of September 2017, ranked by number of active users (in millions)*, Statista, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

24. Motyka K. (2006), *Prawo do prywatności i dylematy współczesnej ochrony praw człowieka*, Lublin, s. 88–94.
25. Motyka K. (2006), *Prawo do prywatności i dylematy współczesnej ochrony praw człowieka*, Lublin.
26. *National Security Strategy of the United States of America*, The White House 2017, http://cli.re/g15MZm.
27. Opinia TSUE z 26.07.2017 r., sygn. 1/15, ECLI:EU:C:2017:592.
28. Powszechna Deklaracja Praw Człowieka z dn. 10.12.1948 r., http://libr.sejm.gov.pl/tek01/txt/onz/1948.html.
29. Pułło A. (1997), *System konstytucyjny Stanów Zjednoczonych*, Wydawnictwo Sejmowe.
30. *Rezolucja na rzecz zapewnienia ochrony danych i prywatności stałego miejsca w międzynarodowym prawie*, 35. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności 2013, https://goo.gl/YnVNgR.
31. Rojszczak M. (2017), *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, „Studia Prawa Publicznego", nr 2, s. 159–189. DOI: https://doi.org/10.14746/spp.2017.2.18.6.
32. Rojszczak M. (2018), *Skuteczność ochrony praw podmiotów danych wynikających z prawa UE w świetle umowy Tarcza Prywatności oraz prawodawstwa federalnego USA*, „Transformacje Prawa Prywatnego", nr 1.
33. Rozporządzenie 2016/679 Parlamentu Europejskiego i Rady (UE) z 27.04.2016 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 4.5.2016).
34. Safjan M., Bosek L. (2016), *Konstytucja RP*, t. 2: *Komentarz do art. 87–243*, Warszawa.
35. Schwartz P. (2013), *The EU–U.S. Privacy Collision: A Turn To Institutions And Procedures*, "Harvard Law Review", t. 126, s. 1966–2009.
36. Skrzydło J. (1995), *Wolność słowa a wymogi bezpieczeństwa narodowego*, „Państwo i Prawo", nr 9, s. 46–60.
37. Stone G. (2007), *National Security v. Civil Liberties*, "California Law Review", t. 95, s. 2203–2212.
38. Szuniewicz M. (2016), *Ochrona bezpieczeństwa państwa jako przesłanka ograniczenia praw i wolności jednostki w świetle Europejskiej Konwencji Praw Człowieka*, Warszawa.
39. *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, Directorate General for Internal Policies Policy 2015, http://www.europarl.europa.eu/studies.
40. Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE z 2016 C Nr 202, s. 47).
41. Traktat o Unii Europejskiej (Dz.Urz. UE z 2016 C Nr 202, s. 13).
42. Ustawa federalna USA z 25.10.1978 r. o nadzorze nad wywiadem obcym (*Foreign Intelligence Surveillance Act*), 92 Stat. 1783, publikacja 50 U.S.C. §1801.
43. Ustawa federalna USA z 31.12.1974 r. o ochronie prywatności (*Privacy Act*), sygn. 88 Stat. 1896, publikacja 5 U.S.C. § 552a.
44. Wyrok ETPC z 12.01.2016 r. w sprawie *Szabo i Vissy v. Węgry*, sygn. 37138/14.
45. Wyrok ETPC z 29.06.2006 r. w sprawie *Weber i Saravia v. Niemcy*, sygn. 54934/00.
46. Wyrok ETPC z 3.04.2007 r. w sprawie *Copland v. Wielka Brytania*, sygn. 62617/00.

47. Wyrok Sądu Najwyższego USA z 28.02.1990 r., sprawa *United States v. Verdugo-Urquidez*, sygn. 494 U.S. 259 (1990).
48. Wyrok Sądu Najwyższego USA z 9.01.1973 w sprawie *Couch v. United States*, sygn. 409 U.S. 322 (1973).
49. Wyrok TK z 11.05.2005 r., sygn. K 18/04.
50. Wyrok TS (TSUE) z 17.12.1970 r. w sprawie *Internationale Handelsgesellschaft*, sygn. 11/70.
51. Wyrok TSUE z 21.12.2016 r. w sprawie *Tele2 Sverige AB*, sygn. C-203/15.
52. Wyrok TSUE z 26.02.2013 r. w sprawie *Melloni*, sygn. C-399/11, p. 59.
53. Wyrok TSUE z 4.12.1974 r. w sprawie *van Duyn*, sygn. 41/74.
54. Wyrok TSUE z 6.10.2015 r. w sprawie *Schrems*, sygn. C-362/14.
55. Wyrok TSUE z 8.04.2016 r. w sprawie Data Rights Ireland, sygn. C-239/12, p. 69.