UNIWERSYTET WARSZAWSKI
Wydział Prawa i Administracji
Instytut Nauk Prawno-Administracyjnych

mgr Marcin Rojszczak

Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji

Autoreferat rozprawy doktorskiej

Promotor: dr hab. Cezary Banasiński
Recenzenci: prof. dr hab. Czesław Martysz, UŚ
prof. dr hab. Andrzej Wróbel, INP PAN

Warszawa 2018

I. Uzasadnienie wyboru tematu

Pomimo upływu ponad pięćdziesięciu lat od uwzględnienia prywatności w katalogu praw podstawowych nadal nie wypracowano w nauce uniwersalnej i powszechnie akceptowanej treści tego prawa oraz standardów jego ochrony. Zagadnienie to zyskuje na znaczeniu wraz z coraz powszechniejszym wykorzystaniem nowoczesnych środków komunikacji i przetwarzania danych. Fenomen cyberprzestrzeni oraz związany z nią brak terytorialności, pozorna anonimowość i łatwość w dystrybucji informacji skutkują potrzebą ponownej analizy czy obowiązujące normy prawne niejednokrotnie ustanowione kilkadziesiąt lat wcześniej są wystarczające i adekwatne do ochrony prywatności w odniesieniu do nowych zagrożeń technologicznych.

Upowszechnienie Internetu oraz dynamiczny rozwój technik przetwarzania informacji, w tym pojawienie się zupełnie nowych modeli przetwarzania, takich jak chmura obliczeniowa czy analizy *Big Data*, zwiększyło potrzebę wprowadzenia skutecznych mechanizmów ochrony praw w cyberprzestrzeni. Możliwość gromadzenia i przetwarzania dużych zbiorów danych, pozyskanych z wielu rozproszonych baz i ich swobodne, globalne przetwarzanie doprowadziło do powstania rynku brokerów danych – przedsiębiorców, posiadających bazy danych na temat setek milionów osób, w których uwzględniono informacje na temat ich stanu zdrowia, indywidualnych preferencji, sytuacji finansowej czy przynależności do określonych mniejszości. *Profilowanie* – a więc tworzenie na podstawie informacji pozyskiwanych z wielu elektronicznych baz danych opisu jednostki – stało się skuteczną techniką marketingu produktów i usług, ale również badania i przewidywania zachowania ludzi albo całych społeczności, a w wariancie bardziej rozbudowanym – skutecznym narzędziem inwigilacji. W efekcie normy prawne i możliwości techniczne coraz częściej postrzegane są w kategoriach dychotomii, pozostawiając jednocześnie nierozstrzygniętymi formułowane wątpliwości etyczne i moralne.

W polskiej literaturze brakuje kompleksowego opracowania dotyczącego problematyki ochrony prywatności w cyberprzestrzeni. Dominują ujęcia ukierunkowane na przedstawienie prywatności jako elementu prawa międzynarodowego[1] lub systemów ochrony praw człowieka[2]. W ostatnich latach, na skutek większej atencji związanej z negatywnymi

---

[1] A. Czubik, *Prawo do prywatności: Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Instytut Multimedialny 2013.

[2] K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak (red.), *Prawo prywatności jako reguła społeczeństwa informacyjnego*, CH Beck 2017.

zjawiskami mającymi miejsce w cyberprzestrzeni, publikowane są opracowania dotyczące cyberprzestępczości[3] oraz cyberbezpieczeństwa – rozumianego głównie w wymiarze zapewnienia ochrony infrastruktury systemów i sieci przed atakami[4]. Ochrona prywatności w cyberprzestrzeni pozostaje natomiast poza obszarem szerszego zainteresowania doktryny.

II. Przedmiot i cel rozprawy

Przedmiotem badań niniejszej pracy była analiza prawnych środków ochrony prywatności przed zagrożeniami związanymi z rozwojem nowych sposobów przetwarzania danych. Z uwagi na złożoność i wieloaspektowość tego zagadnienia, jego badanie wykracza poza przestrzeń nauki prawa, nie może bowiem pomijać aspektów technicznych związanych z funkcjonowaniem cyberprzestrzeni i zagrożeń w niej występujących. Rozważania dotyczące skuteczności norm prawnych bez odniesienia i omówienia technologii, które normy te mają regulować, są obarczone ryzykiem, że przedstawione wnioski byłyby niepełne i wybiórcze.

Celem rozważań przedstawionych w pracy było ustalenie przyczyn niedopasowania istniejących lub proponowanych przepisów prawnych do regulowanej technologii. Dyskutując tę kwestię, określono także brzegowe warunki, jakie powinny zostać spełnione, aby rozwiązania normatywne posiadały potencjał do skutecznej ochrony prywatności w cyberprzestrzeni.

III. Główna teza pracy

Podstawową tezą pracy było stwierdzenie, że istniejące regulacje prawne – w szczególności prawnomiędzynarodowe - nie zapewniają skutecznej ochrony przed zagrożeniami dla prywatności wynikającymi z nowoczesnych technik przetwarzania danych.

Analiza przestrzeni badawczej wyznaczonej powyższą tezą pozwoliła na identyfikację, weryfikowanych w pracy, kilku powiązanych ze sobą hipotez szczegółowych:

- czy obecne normy prawnomiędzynarodowe – wynikające z systemów ochrony praw człowieka, ustanawiające przepisy ochronne w zakresie prawa do prywatności oraz ochrony danych osobowych – są wystarczające do regulowania zdarzeń oddziałujących na prywatność, a mających miejsce w cyberprzestrzeni?

---

[3] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013.
[4] M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa 2014.

- czy prawo unijne ma potencjał prowadzący do standaryzacji w zakresie ochrony prywatności, a w efekcie do stworzenia bezpiecznej przestrzeni przetwarzania danych, wykraczającej poza granice państw członkowskich UE?
- czy niedoskonałości prawa ponadnarodowego mogą być uzupełnione na płaszczyźnie prawa krajowego; w szerszym ujęciu – jaka jest rola prawodawcy krajowego w badanym obszarze i czy w ogóle krajowe normy ochronne mają praktyczne znaczenie z punktu widzenia sposobu funkcjonowania sieci Internet?
- wreszcie – czy biorąc pod uwagę techniczne aspekty związane z nowymi technikami przetwarzania informacji, klasyczne rozumienie *„prywatności"* jako wolności człowieka od ingerencji (zainteresowania) ze strony świata zewnętrznego jest nadal aktualne? W jaki sposób rozwiązać oczywiste niedopasowanie Internetu bez granic oraz terytorialności, cechującej stanowione normy prawne?

IV. Metody badawcze

Przygotowując dysertację, skorzystano z kilku metod badawczych. Podstawową była metoda formalno-dogmatyczna, związana z analizą krajowych oraz międzynarodowych (w tym unijnych) aktów prawnych odnoszących się do badanej problematyki. Zakres przepisów poddanych analizie objął normy krajowe (konstytucyjne oraz ustawowe), a także regulacje prawnomiędzynarodowe, które funkcjonują w krajowym porządku prawnym – czy to na skutek ratyfikacji określonego traktatu, czy w następstwie ustanowienia norm prawnych przez organizację międzynarodową, której RP jest członkiem.

Metoda formalno-dogmatyczna została uzupełniona metodą prawno-porównawczą oraz historycznoprawną. W efekcie możliwe stało się nie tylko zidentyfikowanie i analiza obowiązujących norm prawnych, ale również ocena ich skuteczności w odniesieniu do nowoczesnych technik przetwarzania informacji. Ponadto podejście takie pozwoliło na przedstawienie ewolucji badanych rozwiązań prawnych nie tylko na płaszczyźnie krajowej, ale również międzynarodowej. W części drugiej pracy szerzej wykorzystano komparastykę prawniczą, do zobrazowania zwłaszcza różnic pomiędzy modelem ochrony prywatności obowiązującym w nauce europejskiej oraz rozwiązaniami stosowanymi w Stanach Zjednoczonych Ameryki.

Istotnym elementem pracy była także analiza orzecznictwa, w tym międzynarodowych organów sądowych i kontrolnych. Z uwagi na znaczenie norm prawnomiędzynarodowych dla

badanej problematyki, szczególną uwagę poświęcono analizie orzecznictwa ETPC oraz TSUE. W pracy wykorzystano też informacje udostępnione przez krajowe organy władzy publicznej na podstawie przepisów ustawy o dostępie do informacji publicznej[5].

V. Konstrukcja pracy

Rozprawę podzielono na osiem rozdziałów, zgrupowanych w dwóch częściach. Część pierwszą poświęcono omówieniu istniejących i planowanych norm prawnych w badanym obszarze, ze szczególnym zwróceniem uwagi na analizę ich adekwatności do różnych form elektronicznego przetwarzania informacji oraz możliwych negatywnych konsekwencji dla sfery prywatności jednostek. Z kolei w części drugiej rozważania formalno-dogmatyczne uzupełniono o analizę skuteczności przepisów w odniesieniu do konkretnych zastosowań technicznych, realizowanych w cyberprzestrzeni. W pierwszym rozdziale wyjaśniono podstawowe pojęcia i terminy – takie jak *prywatność* i związane z nią *prawo do prywatności*, a także *cyberprzestrzeń* oraz wzajemną relację pomiędzy ochroną danych osobowych a ochroną prywatności. Szczególną uwagę zwrócono na wyjaśnienie uniwersalnej roli prywatności jako potrzeby warunkującej prawidłowy rozwój osobowości człowieka.

W rozdziale drugim została zawarta analiza i omówienie konstytucyjnych i międzynarodowych przepisów będących w polskim systemie prawnym źródłem norm ochronnych związanych z prawem do prywatności. Pokazano także ewolucję postrzegania prywatności na gruncie prawodawstwa organizacji międzynarodowych (w szczególności ONZ, RE i UE). Rozważania dotyczące prawa materialnego uzupełniono analizą skuteczności środków ochrony prawnej – w szczególności powołanych organów kontrolnych i sądowych, a także znaczenia wydawanych przez nich rozstrzygnięć dla sytuacji prawnej jednostek na gruncie przepisów krajowych. Przedstawiono również analizę najważniejszych norm konstytucyjnych, mających wpływ na badaną problematykę, wraz z ich porównaniem ze standardami ochrony wynikającymi z traktatów międzynarodowych.

Rozdział trzeci zawiera analizę najważniejszych aktów prawnomiędzynarodowych, w większości o charakterze niewiążącym, wprowadzających wytyczne dotyczące ochrony danych osobowych. Regulacje te mają znaczący wpływ na kształtowanie zarówno prawodawstwa krajowego wielu państw, ale również norm ponadnarodowych – takich jak prawo UE.

---

[5] Ustawa z 6.09.2001 o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764 ze zm.)

W kolejnym, czwartym rozdziale poddano rozważaniom najważniejsze akty prawne oraz obszary regulacji związane z prawem UE. Reforma unijnych przepisów o ochronie danych osobowych to doskonały przyczynek nie tylko do oceny, na ile wprowadzane regulacje mogą stanowić kompleksowe rozwiązanie problemu ochrony prywatności w cyberprzestrzeni, ale również oceny na ile proponowany przez prawodawcę sposób budowania bezpiecznej przestrzeni przetwarzania informacji w relacjach z państwami trzecimi (nienależącymi do UE/EOG) jest realny i możliwy do zastosowania.

W rozdziale piątym omówiono przepisy krajowe oraz rolę krajowego prawodawcy w obszarze ochrony prywatności w cyberprzestrzeni. Uwzględniając funkcjonowanie Polski w kilku systemach praw człowieka (MPPOP[6], EKPC[7], KPP[8]) oraz pamiętając o istotnej roli przepisów stanowionych przez UE w zakresie ochrony prywatności, analizie poddano, czy i w jakim zakresie krajowy prawodawca dysponuje przestrzenią do stanowienia dodatkowych regulacji kształtujących prawne granice prywatności.

W kolejnych trzech rozdziałach omówiono wybrane zagadnienia dotyczące najważniejszych, zdaniem autora, problemów związanych z ochroną prywatności w cyberprzestrzeni. W rozdziale szóstym omówiono przetwarzanie w modelu chmury obliczeniowej, w rozdziale siódmym przeprowadzono analizę dużych zbiorów danych (*Big Data*), a w rozdziale ósmym poddano rozważaniom środki prawne umożliwiające organom władzy publicznej prowadzenie programów nieograniczonej inwigilacji.

Rozprawę kończy podsumowanie, w którym zebrano wnioski cząstkowe, weryfikujące hipotezy badawcze i na ich podstawie określono, czy i w jaki sposób normy prawnomiędzynarodowe powinny tworzyć ramy ochronne i regulacyjne w zakresie prawa do prywatności w cyberprzestrzeni.

VI. Podsumowanie wniosków

Podstawowym ograniczeniem istniejących norm prawnych jest ich terytorialność, skutkująca brakiem możliwości całościowego uregulowania zjawisk mających miejsce w cyberprzestrzeni. Jest to wada immamentnie ograniczająca zarówno skuteczność regulacji krajowych, jak i norm prawnomiędzynarodowych.

---

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

[7] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dn. 4.11.1950 (Dz.U. 1993 Nr 61, poz. 284).

[8] Karta praw podstawowych UE (Dz. Urz. UE z 2016 r. nr C 202, s 389-405).

Funkcjonujące systemy ochrony praw człowieka doprowadziły do ugruntowania mechanizmów ochrony prywatności w prawodawstwie wielu państw. Nie okazały się jednak środkiem wystarczającym, aby zapewnić ochronę tych samych praw w przestrzeni wirtualnej. W wyniku przeprowadzonej analizy zidentyfikowano w pracy dwie najważniejsze przyczyny takiego stanu rzeczy – pierwsza to brak powszechności istniejących norm prawnomiędzynarodowych, druga to ograniczona skuteczność ustanowionych mechanizmów kontrolnych.

Stanowione prawo, którego zasięg oddziaływania wyznaczony jest granicami terytorialnymi, nie może być skuteczne w regulowaniu zjawisk mających miejsce w przestrzeni niefizycznej, jaką jest cyberprzestrzeń. W sposób oczywisty cyberprzestrzeń wykracza swoim zasięgiem poza każdy system ochrony prywatności – niezależnie czy jest wprowadzany przepisami krajowymi (normy konstytucyjne), traktatami regionalnymi (np. EKPC lub KPP) czy ponadregionalnymi (MPPOP). Tylko w przypadku, gdyby wszystkie państwa na świecie przystąpiły do określonego traktatu, normy prawne wprowadzane jego mocą miałyby pełne zastosowanie do wszystkich zdarzeń realizowanych w cyberprzestrzeni – jest to jednak założenie nierealne.

Brak uniwersalności systemów ochrony praw człowieka nie jest jednak jedynym problemem stojącym na przeszkodzie, aby mogły one stanowić skuteczny mechanizm ochrony prywatności w cyberprzestrzeni. Równie ważne ograniczenie wiąże się z ich wyraźnie ochronnym charakterem, pozbawionym w większości przypadków rozwiązań regulacyjnych. Jak wykazano w pracy, przepisy o ochronie danych tym różnią się od ogólnych norm dotyczących ochrony prywatności, że oparte są na reżimie publicznoprawnym – wprowadzają funkcje regulacyjne i kontrolne, mające na celu podniesienie standardów przetwarzania informacji a nie tylko reagowanie na występujące naruszenia. Celem międzynarodowych aktów prawnych dotyczących ochrony prywatności w cyberprzestrzeni powinno być zatem wprowadzenie podobnych zasad przetwarzania informacji na normowanym obszarze. Nie może być to osiągnięte bez uwzględnienia regulacji publicznoprawnych, na przykład dotyczących obowiązku powołania niezależnego nadzoru lub organów współpracy międzynarodowej władnych do definiowania wspólnych standardów. Pominięcie rozwiązań regulacyjnych uniemożliwia osiągnięcie tego samego poziomu ochrony prywatności w różnych państwach. Konsekwencją jest także niewielka przydatność międzynarodowych systemów ochrony praw człowieka w ograniczaniu naruszeń horyzontalnych.

Bazując na wnioskach szczegółowych z przeprowadzonej analizy w odniesieniu do systemów ochrony praw człowieka (rozdział 2), ram prawnej ochrony danych osobowych

(rozdział 3 i 5), ale także uwzględniając wnioski i doświadczenia ze stosowania prawa UE (rozdział 4) zdefiniowano następujące warunki brzegowe, które powinny zostać uwzględnione przy projektowaniu rozwiązań legislacyjnych mających na celu skuteczną ochronę prywatności w cyberprzestrzeni:

1) podstawę formalną powinna stanowić umowa międzynarodowa o charakterze prawnie wiążącym.
2) przedmiotem umowy powinno być ustanowienie organizacji międzynarodowej właściwej do definiowania wymagań i nadzorowania ich przestrzegania w zakresie przetwarzania danych w cyberprzestrzeni.
3) sposobem realizacji tego celu powinno być nadanie organizacji międzynarodowej kompetencji potrzebnych do stanowienia własnych standardów postępowania i norm prawnych w odniesieniu do cyberprzestrzeni, o charakterze regulacyjnym, a nie *stricte* ochronnym.
4) prawo stanowione przez organizację międzynarodową powinno mieć charakter bezpośrednio skuteczny w systemach prawnych państw-stron umowy.
5) w ramach umowy powinien zostać powołany organ posiadający kompetencje opracowywania wytycznych i rekomendacji, którego wzorem może być Grupa Robocza Art. 29 powołana na podstawie dyrektywy 95/46 (element samoregulacji rynku).
6) umowa powinna powoływać lub wskazywać organ sądowy, przy czym poddanie się procedurze rozstrzygania sporów nie powinno zależeć od opcjonalnego uznania przez strony, a wydane wyroki powinny mieć skutek *erga omnes*.

W powyższej propozycji bez trudu można odnaleźć zapożyczenia z istniejących umów międzynarodowych, w szczególności traktatów ustanawiających UE, Konwencji Rady Europy nr 108, jak i EKPC oraz MPPOP.

W pracy odniesiono się do kwestii dwóch problemów, które mogą być wskazywane jako ograniczające skuteczność przedstawionej propozycji – pierwszym jest brak uniwersalności postulowanego traktatu, drugim trudność w ustanowieniu akceptowalnych ponadnarodowo standardów ochrony danych.

Zdaniem autora uniwersalność (powszechność) nie warunkuje skuteczności w zakresie regulacji zdarzeń mających miejsce w przestrzeni wirtualnej. Internet bez granic to idea, jednak idea nieprawdziwa. To utopia - i jak każda utopia - wprowadzając uogólnienia, prowadzi do fałszu. Internet zawsze miał granice, co więcej zawsze istniały w nim mechanizmy regulacyjne.

Nie jest zatem prawdą, że Internet jest zjawiskiem zawieszonym w przestrzeni niezależności, gdzie nic i nikt nie jest w stanie wpłynąć na jego kształt. Już dzisiaj niektóre państwa skutecznie separują swoje fragmenty cyberprzestrzeni od sieci globalnej, tworząc rodzaj *„krajowego internetu"*. Państwa niedemokratyczne, zwłaszcza niektóre państwa arabskie, mają własne mechanizmy nadzoru usług udostępnionych użytkownikom Internetu, co wynika głównie z obawy, że swobodna wymiana treści będzie stanowiła zagrożenie dla przyjętych norm ustrojowych. Internet ma więc granice, tyle że w chwili obecnej są one budowane przez państwa niedemokratyczne, a celem ich wprowadzania jest ograniczanie praw własnych obywateli.

Dlatego w opinii autora budowa społeczeństwa opartego na wiedzy i informacji wymaga odrzucenia koncepcji *„Internetu bez granic"*. Internet bez granic to też Internet bez regulacji, co z kolei prowadzi do nadużyć. Jeżeli Internet ma stanowić ważne, a w niektórych obszarach podstawowe, medium komunikacji, ale także budowy relacji międzyludzkich, a w szerszym kontekście – tworzenia e-społeczeństwa, to konieczne jest wzmocnienie zaufania i wiarygodności z nim związanej. Prawo stanowione w zgodzie z zasadami państwa demokratycznego służy ochronie wartości ustrojowych, w tym poszanowania praw podstawowych. Brak możliwości skutecznej ochrony praw podstawowych takich, jak prawo do prywatności, czyni z koncepcji Internetu bez granic pusty slogan o ograniczonej przydatności w zakresie budowy społeczeństwa informacyjnego. Prawodawstwo krajowe nie ma potencjału potrzebnego, aby problem ten rozwiązać. Realizacja zaproponowanej koncepcji, a więc powołanie nowej organizacji międzynarodowej i przekazanie jej niezbędnych kompetencji regulacyjnych przez państwa-strony traktatu, doprowadziłaby do powstania bezpiecznej przestrzeni przetwarzania w ramach obecnie istniejącej sieci Internet, z którą można by wiązać większe gwarancje w zakresie bezpieczeństwa i wiarygodności prowadzonych procesów przetwarzania. Zatem powszechność nie jest warunkiem skuteczności przedstawionej koncepcji. Ponieważ mechanizmy wprowadzone traktatem miałyby głównie funkcje regulacyjne, przystępujące państwa mogłyby uprościć (zlikwidować) procedury międzynarodowego transferu danych, skoordynować działanie krajowych organów nadzoru, ale przede wszystkim zapewnić możliwość korzystania z tych samych swobód i obowiązków przez rozproszone geograficznie podmioty. Złożone problemy prawne mogłyby zostać rozwiązane w stosunkowo prosty sposób, np. dostawcy świadczący usługi w chmurze mogliby zostać zobowiązani, aby wszystkie centra przetwarzania danych były lokalizowane na terytorium państw uczestniczących w systemie, a transfer dużych zbiorów danych do państw trzecich mógłby zostać objęty odpowiedniemu nadzorowi.

Poważniejszą trudnością zdaje się wypracowanie w gronie państw potencjalnie zainteresowanych udziałem w takim porozumieniu wspólnie akceptowalnych standardów ochrony danych osobowych. Problem ten jest doskonale zauważalny w przypadku prawodawstwa UE i USA. W przypadku Unii ograniczeniem może być redakcja art. 6 ust. 3 TUE, w którym zaliczono EKPC do katalogu zasad ogólnych prawa, jak również nadanie orzeczeniom ETPC dotyczącym ochrony prywatności *de facto* rangi wiążącej w systemie prawa UE. W efekcie przyjęte rozwiązanie traktatowe może stać na przeszkodzie przystąpieniu UE do jakiejkolwiek umowy międzynarodowej, której wykonanie będzie wymagało przekazywania danych osobowych z Unii, jeżeli postanowienia tej umowy nie będą przewidywały nałożenia standardów ochrony wyznaczonych przez EKPC na pozostałe strony traktatu, co wydaje się rozwiązaniem niewykonalnym. Problem ten doprowadził już do stwierdzenia nieważności decyzji KE 2000/520, stanowiącej podstawę prowadzenia programu Bezpieczna przystań (transfer z UE do USA danych osobowych w ramach współpracy gospodarczej), a w lipcu 2017 stał się jedną z przyczyn stwierdzenia przez TSUE[9] braku możliwości zawarcia umowy UE – Kanada w zakresie wymiany danych PNR[10]. Wydaje się zatem, że Unia, wiążąc sposób interpretacji postanowień Karty praw podstawowych od wykładni przepisów EKPC, wprowadziła standardy ochrony skutkujące znacznym utrudnieniem współpracy międzynarodowej w dziedzinie przetwarzania danych osobowych.

Z drugiej strony, w prawodawstwie Stanów Zjednoczonych – największego globalnego dostawcy usług przetwarzania danych – ochrona prywatności nie jest wprost zdefiniowana w przepisach rangi konstytucyjnej. Ochrona danych osobowych jest traktowana wybiórczo i sektorowo, przy czym nie wprowadzono nawet nadzorującego przestrzegania standardów urzędu ombudsmana.

Dlatego wydaje się, że wypracowanie wspólnych ram prawnych postulowanej umowy międzynarodowej może wymagać podjęcia także prac dostosowawczych na poziomie prawa krajowego. Uwaga ta ma szczególne znaczenie w odniesieniu do Stanów Zjednoczonych z uwagi na istniejące w tym państwie ograniczenia natury konstytucyjnej.

Podsumowując najważniejsze wnioski przedstawione w rozprawie, należy też odnieść się do płaszczyzny prawa polskiego. Pomimo silnych gwarancji związanych z ochroną

---

[9] Opinia TSUE 1/15 z 26.07.2017 r. (ECLI:EU: C:2017:592).

[10] *Passenger Name Record* – dane dotyczące pasażera; w art. 2 pkt 1 ustawy z 9.05.2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz.U. z 2018 r. poz. 894), dane PNR zdefiniowano jako: „dane dotyczące przelotu pasażera, w tym dane osobowe, które są przetwarzane w związku z prowadzeniem działalności gospodarczej przez przewoźników lotniczych w celu dokonania rezerwacji lub realizacji lotu w ramach przewozu lotniczego".

prywatności, wynikających zarówno z przepisów konstytucyjnych, jak i ratyfikowanych norm prawnomiędzynarodowych, przedstawiono w pracy liczne uwagi krytyczne związane głównie z wprowadzaniem środków ustawodawczych skutkujących prawnie wątpliwą ingerencją w obszar praw podstawowych. Przykładem mogą być rozważania związane z przyjętymi w 2016 roku ustawami zwiększającymi możliwości prowadzenia inwigilacji elektronicznej przez uprawnione organy[11]. W opinii autora ochrona praw obywateli będzie musiała coraz częściej być opierana na stosowanych bezpośrednio przepisach prawnomiędzynarodowych i/lub na rozstrzygnięciach międzynarodowych organów sądowych. Stąd też, także z perspektywy krajowej, realizacja propozycji wypracowania nowego traktatu zapewniającego ochronę prywatności w cyberprzestrzeni jest wnioskiem, który poprzez pozbawienie krajowej władzy możliwości wydawania arbitralnych decyzji przyczyni się do wzmocnienia mechanizmów ochrony praw podstawowych w cyberprzestrzeni.

Przedstawiona koncepcja może wydawać się trudna w realizacji. Być może nie zostanie ona nigdy zastosowana w praktyce. Projekt *Panoptykonu* J. Benthama znalazł praktyczne zastosowanie dopiero wiele lat po jego sformułowaniu i to w obszarze z gruntu odmiennym od pierwotnie zakładanego (kontrola społeczeństwa w miejsce nadzoru nad więźniami). Niewykluczone zatem, że przedstawiona w pracy propozycja budowy uniwersalnego traktatu mającego za cel wprowadzenie skutecznych środków ochrony praw podstawowych w cyberprzestrzeni zostanie podjęta dopiero w bardziej odległej przyszłości, co nie powinno zmieniać faktu, że jest ona warta dalszych analiz.

[11] Zob. ustawa z 15.01.2016 o zmianie ustawy o Policji oraz innych ustaw (Dz.U. z 2016 r. poz. 147) oraz ustawa z 10.06.2016 o działaniach antyterrorystycznych (Dz.U. z 2016 r. poz. 904 ze zm.).