PRYWATNOŚĆ W EPOCE WIELKIEGO BRATA: PODSTAWY PROWADZENIA PROGRAMÓW MASOWEJ INWIGILACJI W SYSTEMIE PRAWNYM STANÓW ZJEDNOCZONYCH

MARCIN ROJSZCZAK*

DOI: 10.26399/iusnovum.v13.1.2019.13/m.rojszczak

1. UWAGI WPROWADZAJĄCE[1]

Zagadnienie ochrony prywatności w jej wymiarze prawnym przez ostatnie dziesięciolecia wiązane było głównie z wprowadzaniem obowiązków negatywnych dla państw, prowadzących do respektowania sfery prywatności obywateli przez organy władzy publicznej. W efekcie zarówno w prawodawstwie, jak i literaturze przedmiotu, dyskutując prawne aspekty ochrony prywatności przytacza się podział na zagrożenia wertykalne oraz horyzontalne – traktując każdą z tych płaszczyzn odrębnie. Zagrożenia wertykalne – związane z działalnością państw – przybierają na ogół postać gromadzenia nadmiarowych, nieuzasadnionych informacji o jednostkach, często w następstwie realizacji rozbudowanych programów inwigilacyjnych. Z kolei zagrożenia horyzontalne związane są z naruszeniami w relacjach pomiędzy jednostkami i najczęściej związane są z działalnością przedsiębiorców prowadzących rozbudowane operacje przetwarzania danych.

Dla ukształtowania europejskiej koncepcji ochrony prywatności kluczowe znaczenie miał dorobek prawny organizacji międzynarodowych, zwłaszcza Rady Europy oraz Unii Europejskiej. Otwarcie do podpisu w 1950 roku Europejskiej

* dr, Instytut Nauk Prawno-Administracyjnych Wydziału Prawa i Administracji Uniwersytetu Warszawskiego; e-mail: marcin.rojszczak@gmail.com

[1] Stan prawny oraz odnośniki internetowe aktualne na dzień 14.01.2019 r.

Konwencji Praw Człowieka (EKPC)[2], a zwłaszcza uwzględnienie w katalogu dóbr chronionych sfery prywatności (art. 8) przyczyniło się do podniesienia standardów prawnej ochrony prywatności w kręgu państw-sygnatariuszy traktatu. Bogate orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPC) oraz Trybunału Sprawiedliwości UE (TSUE) przyczyniło się do wzmocnienia i ugruntowania postrzegania prywatności, jako jednego z praw podstawowych. Wraz z ewolucją Wspólnot Europejskich – a zwłaszcza zrozumieniem, że budowa wspólnego rynku wewnętrznego i zacieśnianie więzów gospodarczych nie może następować z pominięciem uznawania i przestrzegania tych samych podstawowych wartości i praw człowieka – wypracowane zostały wspólnotowe przepisy ustawodawcze, prowadzące do wzmocnienia praw i rozszerzenia zobowiązań związanych z ochroną prywatności w cyberprzestrzeni. Po ponad 20 latach od wprowadzenia pierwszych regulacji w tym zakresie (przyjętej w 1995 roku dyrektywy 95/46[3]), instytucje UE uzgodniły i przyjęły nowe ogólne rozporządzenie o ochronie danych (rozporządzenie 2016/679[4]) – pierwszy na świecie ponadnarodowy akt prawny wprowadzający wiążące wymagania w zakresie ochrony prywatności i danych osobowych, nie tylko w relacjach wertykalnych, ale i horyzontalnych[5]. Obecnie europejski model ochrony danych jest uznawany za najbardziej dojrzały na świecie, stanowiący wzór dla działań innych prawodawców[6].

Na tym tle interesująca może być analiza prawnoporównawcza przepisów obowiązujących w UE z prawodawstwem Stanów Zjednoczonych. Prawo do prywatności zostało po raz pierwszy zdefiniowane właśnie na gruncie prawa amerykańskiego i jest związane ze słynną publikacją S. Warrena i L. Brandeisa *Right to privacy* z 1890 roku, w której autorzy postulowali objęcie ochroną prawa do poszanowania odrębności i braku ingerencji w strefę osobistą jednostki („*right to be let alone*")[7].

Także dorobek tamtejszej judykatury jest przywoływany w większości prac omawiających źródła prawnej ochrony prywatności. Jednocześnie jednak konstytucja Stanów Zjednoczonych nie wprowadza wprost gwarancji związanych z prawem

---

[2] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r., Dz.U. z 1993 r. Nr 61, poz. 284.

[3] 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 z 1995 Nr L 281, s. 31.

[4] 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 4.5.2016.

[5] Szersze omówienie przepisów ogólnego rozporządzenia w: M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016; D. Lubasz, E. Bielak-Jomaa (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

[6] P. Schwartz, *The EU-U.S. Privacy Collision: A Turn To Institutions And Procedures*, „Harvard Law Review" 2013, t. 126, s. 1968.

[7] S. Warren, L. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, nr 5, s. 193–220. Artykuł znajduje się na drugim miejscu w zestawieniu najczęściej cytowanych publikacji prawniczych w historii, jest także uznawany za posiadający największy wpływ na naukę prawa. Zob. F. Shapiro, M. Pearse, *The Most-Cited Law Review Articles of All Times*, „Michigan Law Review" 2012, t. 110, s. 1503.

do prywatności, a prawo stanowione w sposób odmienny definiuje prawa jednostek i obowiązki przetwarzających dane. Prawodawca amerykański nie zdecydował się na wprowadzenie jednakowych zasad przetwarzania danych osobowych, obowiązujących zarówno podmioty sektora publicznego jak i prywatnego. Zamiast tego wprowadzane są fragmentaryczne regulacje sektorowe (np. dotyczące operatorów telekomunikacyjnych czy ochrony konsumentów) lub związane z przetwarzaniem określonych grup informacji (np. dane medyczne, informacje finansowe). W USA nie wyznaczono także, znanego z modelu europejskiego, centralnego urzędu odpowiedzialnego za nadzór obszaru ochrony danych osobowych. Odmienne podejście do ochrony prywatności w cyberprzestrzeni powoduje, że w literaturze przedmiotu amerykański model ochrony prywatności jest często przeciwstawiany podejściu wypracowanemu na gruncie nauki europejskiej[8].

Jednocześnie jednak Stany Zjednoczone są jednym z głównych partnerów Unii Europejskiej, także w zakresie usług społeczeństwa informacyjnego. Globalny rynek przetwarzania danych powoduje, że wprowadzenie skutecznych zasad ochrony prywatności nie może być ograniczone do przepisów o zasięgu krajowym czy regionalnym. Stąd też różnice w prawodawstwie pomiędzy UE a USA mają praktyczny wymiar związany z próbą określenia wspólnych zasad gromadzenia, przekazywania i przetwarzania danych osobowych. Problem ten zyskuje na znaczeniu, zwłaszcza biorąc pod uwagę, że znacząca większość najpopularniejszych w Europie serwisów internetowych oraz usług przetwarzania danych jest udostępniana przez przedsiębiorców posiadających siedzibę w Stanach Zjednoczonych i podlegających tamtejszemu prawu.

Dlatego, jak słusznie zauważył J. Cannataci, Specjalny Sprawozdawca ds. Prywatności powołany przez Radę Praw Człowieka ONZ, skuteczna ochrona prywatności w cyberprzestrzeni implikuje stosowanie *„zabezpieczeń bez granic oraz środków ochrony ponad granicami"*[9]. Problem współpracy UE-USA w zakresie wymiany i ochrony danych jest wielopłaszczyznowy – dotyczy zarówno wymiany danych w celach komercyjnych, jak i związanych ze współpracą organów państwowych, na przykład w zakresie wymiarów sprawiedliwości oraz współpracy w sprawach karnych.

Pierwsza z płaszczyzn na kluczowe znaczenie dla sukcesu projektu budowy ponadregionalnej przestrzeni przetwarzania danych, wolnej od ograniczeń i barier blokujących rozwój usług cyfrowych. Brak wypracowania akceptowalnych przez UE i USA zasad ochrony przekazywanych danych może stanowić istotne ograniczenie w dalszym swobodnym rozwoju usług świadczonych w Internecie. O realności takiego scenariusza może świadczyć wydany w 2014 roku wyrok TSUE w sprawie *DRI*[10], w którym stwierdził nieważność decyzji KE stanowiącej podstawę dla

---

[8] P. Schwartz, *The EU-U.S. Privacy Collision…*, *op. cit.*, s. 2008; zob. także spojrzenie na prawodawstwo UE i USA z perspektywy państwa trzeciego – Kanady – w: A. Levin, M. Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, „University of Ottawa Law & Technology Journal" 2005, t. 2, s. 357–395.

[9] Rada Praw Człowieka ONZ, *Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*, 27 lutego 2017, A/HRC/34/60, p. 34.

[10] Wyrok TSUE z dn. 8.04.2014 r. w sprawie Digital Rights Ireland Ltd., sygn.: C-293/12 i C-594/12.

realizacji programu „Bezpieczna przystań". Program ten stanowił podstawę dla realizacji znaczącej części transatlantyckiego transferu danych i podstawę dla szeregu e-usług świadczonych przez amerykańskich przedsiębiorców użytkownikom z obszaru UE. Z konieczności KE oraz Departament Handlu USA uzgodniły nowe zasady wymiany danych, w ocenie Komisji uwzględniające zastrzeżenia Trybunału. Stały się one podstawą do wydania decyzji 2016/1250 KE i zatwierdzenia programu „Tarcza prywatności"[11]. Biorąc pod uwagę argumentację TSUE przedstawioną w sprawie *DRI* oraz rozszerzoną w nowszych orzeczeniach (np. w sprawie *Tele2*, jak również opinii 1/15 dotyczącej umowy USA-Kanada), wydaje się wątpliwe, czy ustanowiony w decyzji 2016/1250 standard ochrony, stosowany przez przedsiębiorców amerykańskich zostanie uznany przez Trybunał za zgodny z prawem UE – w szczególności z normami określonymi w Karcie Praw Podstawowych.

Także współpraca organów władzy publicznej, w szczególności dotycząca wymiaru sprawiedliwości i współpracy w sprawach karnych, jest obszarem ożywionego dyskursu naukowego. Efektem próby wypracowania kompromisu jest zawarta w 2016 roku umowa w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych, zwana w literaturze przedmiotu „*umową parasolową*"[12]. Umowa ta określa zasady gromadzenia, wymiany i przetwarzania danych – jednak sama nie stanowi podstawy do transferu jakichkolwiek danych. Jej celem jest wypracowanie wspólnego standardu, który następnie może być przywoływany jako punkt odniesienia w innych umowach szczegółowych. Współpraca UE i USA w zakresie wymiany danych osobowych jest także przedmiotem umowy z 14 grudnia 2011 r.[13], dotyczącej przekazywania przez europejskie linie lotnicze danych o pasażerach (tzw. danych PNR, *Passenger Name Record*) wykonujących podróże transatlantyckie. Zgodność tej umowy z prawem UE także może zostać wkrótce skutecznie zakwestionowana, zwłaszcza biorąc pod uwagę, że Trybunał wypowiedział się już negatywnie o przepisach projektowanej umowy z Kanadą, która miała zawierać w wielu obszarach analogiczne zapisy i regulacje do umowy zawartej ze Stanami Zjednoczonymi.

W rezultacie uważny obserwator współpracy UE i USA z łatwością może zauważyć poważne trudności, z jakimi strony uzgadniają warunki, na jakich dane z UE mogą podlegać swobodnemu transferowi w celu przetwarzania na terenie USA. Istotną trudność stanowi wypracowanie prawnie wiążących mechanizmów regulujących przekazywanie i przetwarzanie danych w sposób zgodny z prawem

---

[11] Decyzja wykonawcza Komisji (UE) 2016/1250 z 12.07.2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA, Dz. Urz. UE z 2016 Nr L 207, s. 1 (CELEX: 32016D1250).

[12] Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską z dnia 2 czerwca 2016 r. w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych, CELEX: 22016A1210(01), Dz. Urz. UE z 2016 Nr L 336, s. 3.

[13] Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską z dnia 14 grudnia 2011 r. o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, CELEX: 22012A0811 (01), Dz. Urz. UE z 2012 Nr 215, s. 5.

UE, w szczególności pozwalający na dochowanie wysokiego standardu ochrony praw osób, których dane są przetwarzanie.

Zrozumienie przyczyn dla których wypracowanie wspólnych regulacji będzie bardzo trudne – jeżeli nie niemożliwe – wymaga dogłębnego omówienia prawodawstwa obowiązującego w Stanach Zjednoczonych, jak również podstaw ustrojowych oraz kluczowych doktryn, tworzących ramy prawnej ochrony prywatności.

Obszarem dla zrozumienia którego taka analiza może być szczególnie pomocna jest płaszczyzna relacji wertykalnych związanych z ochroną jednostek przed naruszeniami prywatności ze strony władzy publicznej. Przedstawienie i omówienie najważniejszych przepisów regulujących prawną ochronę prywatności może pomóc w zrozumieniu istotnych różnic, których skutkiem jest odmienne podejście do możliwości prowadzenia przez organy władzy publicznej programów inwigilacyjnych w oparciu o hurtowe i nieukierunkowane przechwytywanie danych. W 2014 roku TSUE, badając dopuszczalność transatlantyckiego przekazywania danych i skuteczność ustanowionych prawnych mechanizmów ochrony prywatności, orzekł o nieadekwatności prawodawstwa Stanów Zjednoczonych względem norm ustanowionych w UE. Powstaje zatem pytanie, czy wypracowane w UE standardy faktycznie nie mogą być pogodzone z odmiennym systemem prawnym Stanów Zjednoczonych? Czy Unia Europejska wprowadziła zbyt rygorystyczne przepisy, czy może jednak prawodawstwo Stanów Zjednoczonych niedostatecznie chroni prawa podstawowe? Czy wreszcie jest możliwe wskazanie wspólnej płaszczyzny porozumienia, łączącej oba systemy prawne, a nie podkreślającej występujące różnice?

Celem niniejszego artykułu nie jest omawianie problematyki masowej inwigilacji z perspektywy przepisów europejskich – w szczególności prawa UE czy dorobku orzeczniczego TSUE czy ETPC. Zagadnienie to zostało omówione we wcześniejszych publikacjach autora[14]. Dlatego odwołania do koncepcji wypracowanych na gruncie nauki europejskiej będą wykorzystywane pomocniczo, aby zobrazować najważniejsze różnice, a także przyczyny ich występowania.

2. PROGRAMY MASOWEJ INWIGILACJI W STANACH ZJEDNOCZONYCH

Bez wątpienia znaczący wzrost zainteresowania opinii publicznej możliwościami związanymi z prowadzeniem masowych programów inwigilacyjnych przez służby specjalne Stanów Zjednoczonych związany jest z informacjami ujawnionymi przez E. Snowdena, byłego współpracownika Centralnej Agencji Wywiadowczej oraz Agencji Bezpieczeństwa Narodowego (*National Security Agency*, NSA)[15]. W rze-

[14] Zob. w szczególności: M. Rojszczak, *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" 2017, nr 2, s. 159–188.

[15] Szersze omówienie postaci E. Snowdena oraz zakresu ujawnionych przez niego dokumentów w: G. Greenwald, *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.

czywistości działania NSA, oraz jej poprzedniczki AFSA[16], w zakresie prowadzenia ponadnarodowych programów wywiadu elektronicznego (*signal intelligence*, SIGINT) mają swoje początki w zawartej 5 marca 1946 roku umowie pomiędzy Wielką Brytanią a Stanami Zjednoczonymi[17]. Umowa, do której w późniejszych latach przyłącza się Australia, Kanada i Nowa Zelandia, była kilkukrotnie aneksowana i zmieniana, obowiązuje jednak do dzisiaj. W literaturze przedmiotu, jak również w samych ujawnionych informacjach dotyczących prowadzonej współpracy, program jest określany jako porozumienie „Pięciu Oczu" (ang. *Five Eyes*, FVEY)[18].

Porozumienie *Five Eyes* od początku miało wymiar współpracy wywiadowczej. Pozyskiwanie informacji z wywiadu elektronicznego miało służyć realizacji zadań z zakresu bezpieczeństwa narodowego, w szczególności zwiększeniu potencjału obronnego. Wraz ze wzrostem możliwości technicznych, ewolucji podlegał nie tylko zakres monitorowanych aktywności, ale również zmieniała się skala możliwych programów inwigilacyjnych. Początkowo wywiad elektroniczny ukierunkowany był na gromadzenie informacji z łączności radiowej i telekomunikacyjnej, w latach osiemdziesiątych dwudziestego wieku możliwe było już stworzenie programu prowadzenia globalnego nasłuchu łączności (znanego jako ECHELON)[19], natomiast począwszy od lat 90. XX wieku rozbudowywano możliwości przechwytywania i gromadzenia łączności elektronicznej. Zmianie uległ także krąg osób monitorowanych. Wzrost możliwości technicznych umożliwił gromadzenie i poddawanie dalszej analizie hurtowe ilości danych. Inwigilacja nie musiała być zatem ukierunkowana na konkretny krąg osób, a podejmowane środki nie musiały zakładać istnienia uzasadnionego podejrzenia, że monitorowana aktywność będzie interesująca z uwagi na prowadzone działania wywiadowcze. Można przyjąć, że moment, w którym programy wywiadu elektronicznego pozwoliły na techniczną możliwość monitorowania dowolnej łączności i gromadzenia hurtowych ilości danych stanowi punkt zwrotny dla dalszego rozwoju środków masowej inwigilacji. W rezultacie podejmowane programy przestały służyć *stricte* realizacji działań wywiadowczych – a przez to uzasadnionych interesów państwa – a stały się narzędziem, które z taką samą skutecznością mogą być wykorzystywane do monitorowania i wpływania na zachowanie dużych grup osób, a nawet całych społeczeństw – a zatem stanowić potencjalne zagrożenie dla obszaru ochrony praw podstawowych, w szczególności prawa do poszanowania życia prywatnego.

Dlatego, przed przeprowadzeniem analizy prawnych podstaw prowadzenia programów masowej inwigilacji, należy omówić istniejące możliwości techniczne

---

[16] Agencja Bezpieczeństwa Sił Zbrojnych (*Armed Forces Security Agency)*; dalsze informacje na temat wczesnej historii NSA – zob. Center for Cryptologic History National Security Agency, *The Origins of NSA*, https://goo.gl/KFz2Bj

[17] Odtajniona treść umowy dostępna jest w postaci cyfrowej na stronach NSA: http://cli.re/GrJobx

[18] Odtajniona przez NSA dokumentacja dotycząca partnerstwa FVEY: https://www.nsa.gov/news-features/declassified-documents/ukusa/

[19] Więcej nt. programu ECHELON w: L. Sloan, *ECHELON and The Legal Restraints on Signals Intelligence: A Need for Reevaluation*, „Duke Law Journal" 2001, t. 50, s. 1467–1510; w rzeczywistości systemy tego typu były pierwszymi środkami realizacji programów masowej inwigilacji, w tym przypadku związanej z łącznością telekomunikacyjną.

związane z prowadzonymi obecnie działaniami inwigilacyjnymi, znane opinii publicznej głównie z ujawnionych materiałów wywiadowczych. Wiedza ta z jednej strony zostanie wykorzystana w późniejszych rozważaniach w celu wykazania, w jaki sposób zbyt liberalne prawodawstwo może zostać wykorzystane przez wspólnotę wywiadowczą do rozszerzenia zakresu prowadzonych działań, które w efekcie mogą godzić w podstawowe zasady państwa demokratycznego. Z drugiej strony, skala i kompleksowość realizowanych programów wskazuje na konieczność weryfikacji skuteczności ponadnarodowych systemów ochrony praw człowieka. Stanowi także ważny argument w dyskusji nad potrzebą wypracowania nowych, bardziej skutecznych porozumień międzynarodowych regulujących zakres dopuszczalnej ingerencji państw w aktywność obywateli mającą miejsce w cyberprzestrzeni.

NSA prowadzi kilka odrębnych programów związanych z gromadzeniem danych oraz dysponuje rozbudowanymi możliwościami ich dalszej analizy i przetwarzania. Chociaż poszczególne programy mogą wiązać się z podobnymi możliwościami pozyskiwania dużych zbiorów danych, często ich realizacja prowadzona jest w oparciu o inne przepisy prawne. Także zakres geograficzny programów może być różny, w szczególności może wiązać się z samodzielnym pozyskiwaniem danych poza obszarem własnej jurysdykcji, a także we współpracy ze służbami specjalnymi państw trzecich. Na potrzeby dalszej analizy, przydatny może okazać się podział ze względu na zakres informacyjny gromadzonych danych oraz sposób ich pozyskiwania. W pierwszym przypadku wyróżnić można programy pozwalające na gromadzenie danych towarzyszących łączności elektronicznej, czyli tzw. metadanych[20] (nazwy kodowe MAINWAY oraz MARINA), jak również programy związane z przechwytywaniem także merytorycznej treści przekazu (np. PRISM)[21]. Podział ze względu na sposób gromadzenia danych pozwala wyróżnić działania związane z podsłuchem łączy telekomunikacyjnych (programy grupy UPSTREAM), jak również związane z bezpośrednim dostępem do systemów informatycznych wiodących usługodawców internetowych (PRISM, MUSCULAR). Aby zobrazować możliwości związane z prowadzonymi w Stanach Zjednoczonych programami inwigilacyjnymi, konieczne jest krótkie omówienie najważniejszych z nich.

W ramach PRISM, NSA posiada stały dostęp do centrów przetwarzania danych głównych usługodawców globalnych usług internetowych zlokalizowanych na terytorium Stanów Zjednoczonych. Według danych ujawnionych w 2012 roku, w ramach programu PRISM możliwy był dostęp do danych przechowywanych w serwerowniach Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL oraz Apple[22]. Istotne jest przy tym, że NSA posiadało dostęp bezpośrednio do informacji zgromadzonych przez usługodawców, a więc dane te nie pochodziły z przechwytywania łączności elektronicznej. NSA miało zatem dostęp do pełnej tre-

---

[20] Zob. definicję metadanych w internetowym słowniku Harvard Law School: http://hls.harvard.edu/dept/its/what-is-metadata/

[21] Opis możliwości technicznych związanych z poszczególnymi programami inwigilacyjnymi można odnaleźć w dokumentach NSA ujawnionych przez E. Snowdena, m.in. *Special Source Operation overview*, https://goo.gl/2uQFBQ

[22] The Washington Post, *NSA slides explain the PRISM data-collection program*, http://cli.re/61YMw6

ści informacji gromadzonych przez setki milionów użytkowników – w tym poczty elektronicznej (np. pochodzącej z takich serwisów jak Gmail, Yahoo czy Office 365), repozytoriów plików (Google Drive czy Microsoft OneDrive), ale również usług łączności elektronicznej (jak Skype) czy treści publikowanych na portalach społecznościowych. W ramach PRISM uzyskiwane mogły być dowolne informacje, bez możliwości kontroli ze strony usługodawców, a także żadnej wiedzy ze strony samych użytkowników. Oznacza to także brak powiązania stosowania środków monitorowania komunikacji z wystąpieniem przesłanki związanej z podejrzeniem popełnienia poważnego przestępstwa lub w ogóle związku danej osoby z aktywnościami znajdującymi się w zainteresowaniu służb specjalnych. Co więcej, użytkownik nie ma żadnej możliwości stwierdzenia – nawet następczego – faktu poddania go czynnościom inwigilacyjnym, w efekcie nie posiada realnej możliwości ochrony swoich praw na drodze sądowej.

Oddzielnym zagadnieniem jest ocena, czy wskazani usługodawcy internetowi świadomie przystąpili do programu PRISM. Fakt ten ma o tyle istotne znaczenie, że udostępnienie danych powierzonych przez użytkowników, w tym także danych sensytywnych (np. dotyczących stanu zdrowia, szczegółów życia prywatnego, preferencji politycznych), wbrew uzgodnionym zobowiązaniom kontraktowym (wynikającym z zawartej z usługodawcą umowy) może być podstawą do odpowiedzialności za wyrządzoną szkodę. Należy bowiem rozróżnić prawo właściwe dla miejsca przetwarzania danych (w tym przypadku prawo Stanów Zjednoczonych) od prawa właściwego dla stosunku umownego pomiędzy użytkownikiem a usługodawcą, które to w wielu przypadkach może wskazywać na prawo UE. Bez wątpienia przekazywanie wszystkich powierzonych danych służbom państwowym, bez żadnej kontroli sądowej oraz bez możliwości nadzoru nad prawidłowością (i legalnością) podejmowanych działań nie prowadzi do wzrostu zaufania wobec wskazanych usługodawców. Dlatego też wkrótce po publikacji materiałów przez E. Snowdena, niektórzy z przedsiębiorców wydali oświadczenia, w których zaprzeczali współpracy z NSA, polegającej na udostępnieniu agencji dostępu do danych użytkowników[23].

Program PRISM jest jednym z lepiej poznanych tajnych programów masowej inwigilacji prowadzonych przez NSA, ale nie jedynym. Z perspektywy użytkowników z obszaru UE równie duże znaczenie może mieć grupa programów UPSTREAM, których cechą wspólną jest przechwytywanie łączności elektronicznej, zazwyczaj przesyłanej międzynarodowymi łączami światłowodowymi. Działania tego typu prowadzone są zarówno na terytorium Stanów Zjednoczonych (np. programy FAIRVIEW, STORMVIEW czy OAKSTAR), ale i w państwach trzecich (RAMPART-A) – w ramach współpracy z zagranicznymi służbami specjalnymi, a także operatorami telekomunikacyjnymi. W ramach poszczególnych programów przechwytywany może być różny typ łączności elektronicznej – w szczególności

[23] Zob. np. oświadczenie Google Inc. wydane przez L. Page'a, prezesa zarządu oraz D. Drummonda, wiceprezesa ds. prawnych, w którym zaprzeczają, że jakakolwiek agencja rządowa ma bezpośredni dostęp do danych zgromadzonych na serwerach Google oraz że sama firma uczestniczy w programie PRISM. Źródło: https://googleblog.blogspot.com/2013/06/what.html

metadane, ale również merytoryczna treść przekazu (np. wiadomości e-mail). Z ujawnionych informacji wiadomo, że w ramach RAMPART-A przechwytywana była łączność przekazywana światłowodami Deutsche Telekom na terenie Niemiec (nazwa kodowa EIKANOL)[24], a także Danii. Z kolei pod kryptonimem ORANGE-CRUSH (część programu OAKSTAR) prowadzone było przechwytywanie łączności na terenie Polski – początkowo wyłącznie metadane (od 3 marca 2009), a w późniejszym okresie także pełna treść przekazu (od 25 marca 2009)[25]. Szczegóły współpracy NSA z polskimi służbami specjalnymi nie są znane.

Program RAMPART-A ukierunkowany jest na współpracę z tzw. państwami trzecimi, czyli partnerami nienależącymi do porozumienia FVEY. Z kolei państwa należące do porozumienia prowadzą wspólnie dodatkowe działania związane z przechwytywaniem łączności elektronicznej. Typowym przykładem takiego programu jest TEMPORA oraz MUSCULAR, prowadzone wspólnie przez NSA oraz jej brytyjskiego odpowiednika – GCHQ[26]. W ramach programu MUSCULAR podsłuchiwana jest łączność wymieniana pomiędzy centrami przetwarzania danych firm Google i Yahoo. Z kolei TEMPORA to program podsłuchu łączności przekazywanej za pośrednictwem łączy światłowodowych przebiegających przez terytorium Wielkiej Brytanii.

NSA gromadzi olbrzymie ilości danych, które pozyskuje jednocześnie z wielu źródeł. W efekcie Agencja jest w stanie prowadzić globalne programy inwigilacyjne, ukierunkowane nie na konkretne osoby – ale na społeczności, czy w wariancie skrajnym – całe państwa. Jednym z przykładów tego typu programu inwigilacyjnego jest MYSTIC, który zgodnie z ujawnionymi informacjami pozwala na przechwytywanie całej łączności elektronicznej (rozmów głosowych, poczty e-mail, wiadomości wysyłanych przez komunikatory itp.) pochodzących ze wskazanych państw w celu jej dalszej analizy[27].

W sposób oczywisty powstaje zatem pytanie, czy i w jaki sposób prowadzenie programów takich jak PRISM czy UPSTREAM jest umocowane w amerykańskim prawodawstwie. Czy istniejące i stale rozbudowywane możliwości NSA są należycie nadzorowane, w sposób zgodny z zasadami państwa prawa – a więc z zaangażowaniem odpowiednich i niezależnych organów nadzoru?

Co oczywiste, działania służb specjalnych na całym świecie objęte są w dużej mierze gryfem tajności. Dochowanie tajemnicy nierzadko warunkuje skuteczność podejmowanych działań. Z drugiej strony, brak jakiegokolwiek nadzoru, połączony z możliwością gromadzenia danych o dowolnych osobach, rodzi poważne ryzyko nadużycia władzy. E. Snowden w swoich zeznaniach złożonych przed specjalną komisją Parlamentu Europejskiego i odnosząc się do szerokich uprawnień analityków NSA w dostępie do informacji, stwierdził: „*nie wstając ze swojego fotela, mógłbym*

---

[24] *The German operation Eikonal as part of NSA's RAMPART-A program*, https://goo.gl/4NMLPu

[25] Źródło: https://edwardsnowden.com/2014/06/13/orange-crush/

[26] Centrala Łączności Rządowej (*Government Communications Headquarters*).

[27] The Washington Post, *NSA surveillance program reaches 'into the past' to retrieve, replay phone calls*, https://goo.gl/h1XpNx

czytać prywatne wiadomości każdego z członków tej komisji, jak również dowolnego innego obywatela"[28].

Bez wątpienia kompetencje i działania NSA wykraczają poza dopuszczalne w UE ramy ingerencji władzy publicznej w prawa podstawowe obywateli. Nie ma wątpliwości, że zarówno programy typu PRISM czy MUSCULAR (a więc związane z bezpośrednim dostępem do danych dowolnych użytkowników), jak również UPSTREAM (związane z przechwytywaniem łączności elektronicznej) prowadzą do naruszenia zasady proporcjonalności, która została wskazana zarówno w orzecznictwie ETPC, jak i TSUE jako warunkująca możliwość zastosowania ograniczeń w prawie do prywatności[29].

Próba stworzenia modelu przechwytywania całego ruchu internetowego i poddawania go dalszej, nietransparentnej analizie w oparciu o nieznane algorytmy, musi budzić uzasadniony niepokój w zakresie dotrzymania norm demokratycznego państwa prawnego. Jak trafnie zauważono w rezolucji Parlamentu Europejskiego:

> „programy nadzoru jako kolejny krok w kierunku stworzenia w pełni prewencyjnego państwa, w którym zmianie ulegnie utrwalony w państwach demokratycznych paradygmat prawa karnego, zgodnie z którym jakakolwiek ingerencja w prawa podstawowe podejrzanych wymaga zatwierdzenia przez sędziego lub prokuratora na podstawie racjonalnego podejrzenia i uregulowana prawnie, natomiast promowane będzie połączenie egzekwowania prawa i działań wywiadowczych o zatartych i osłabionych zabezpieczeniach prawnych, często niezgodne z kontrolą i równowagą demokratyczną oraz prawami podstawowymi, szczególnie w kwestii domniemania niewinności"[30].

Tym bardziej interesująca wydaje się analiza prawodawstwa Stanów Zjednoczonych, w oparciu o które programy tego typu są prowadzone.

3. KONSTYTUCYJNE RAMY OCHRONY PRYWATNOŚCI

Jedna z podstawowych różnic pomiędzy amerykańskim a europejskim modelem ochrony prywatności związana jest z brakiem wyróżnienia w Stanach Zjednoczonych prawa do prywatności w katalogu praw podstawowych. W przypadku państw europejskich, konstytucjonalizacja ochrony prywatności jest związana nie tylko z uwzględnieniem jej w normach krajowych, ale wynika również z funkcjonowania tych państw w ponadnarodowych systemach ochrony praw człowieka.

---

[28] Zeznania E. Snowdena z dnia 8 kwietnia 2014 r. przed Komisją Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego, https://goo.gl/ZPksqs, s. 2.

[29] Szerzej: M. Rojszczak, *„Prawne podstawy…"*, *op. cit.*, s. 172–174 (w kontekście orzecznictwa TSUE), s. 181–181 (w kontekście orzecznictwa ETPC).

[30] Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, 2013/2188(INI), sygn.: P7_TA(2014)0230, p. 12.

Konstytucja USA nie wprowadza wprost gwarancji związanych z ochroną prywatności. Podstawę do formułowania tego prawa stanowi Czwarta Poprawka, dotycząca nietykalności osobistej i materialnej oraz zakazująca przeprowadzania nieuzasadnionych rewizji lub zatrzymań[31]. W drodze precedensowych orzeczeń Sądu Najwyższego USA w oparciu o Czwartą Poprawkę wywiedziono istnienie gwarancji konstytucyjnych, związanych z ochroną jednostki przez nieuprawnioną ingerencją w jej sferę prywatności. Warto zauważyć, że chociaż sądy stanowe oraz sądy federalne niższych instancji zajmowały się tym zagadnieniem także wcześniej, to Sąd Najwyższy dopiero w 1965 roku w orzeczeniu wydanym w sprawie *Griswold v. Connecticut* potwierdził, że Czwarta Poprawka obejmuje także prawo jednostki do ochrony swojej prywatności[32].

Zgodnie ze standardem wyznaczonym treścią Czwartej Poprawki, naruszenie sfery prywatności przez organy władzy publicznej może nastąpić po łącznym spełnieniu dwóch przesłanek: (1) istnieniu prawdopodobnej przyczyny (ang. *probable cause*), oraz (2) w oparciu o nakaz sądowy (ang. *warrant*). Ważne jest przy tym, że nakaz sądowy może być wydany wyłącznie w przypadku, gdy organ wnioskujący wskaże okoliczności uprawdopodabniające, że przeprowadzenie żądanych czynności dostarczy określonych rodzajów dowodów potrzebnych z punktu widzenia prowadzonego postępowania. W doktrynie amerykańskiej istnieje kilka modeli oceny przesłanki prawdopodobnej przyczyny, a jak wskazuje A. Kiełtyka termin ten jest bardzo różnie tłumaczony i definiowany w literaturze polskiej[33]. W sposób syntetyczny termin ten można zdefiniować jako wymaganie posiadania uzasadnionego przekonania, że w wyniku przeszukania ujawnione mogą zostać dowody na popełnienie przestępstwa[34]. Zgodnie ze standardem wynikającym z Czwartej Poprawki przeszukanie nie może mieć charakteru prewencyjnego lub nie popartego uzasadnionym oczekiwaniem, że w miejscu jego przeprowadzenia mogą zostać odnalezione określone dowody.

Z uwagi na brak przepisów materialnych – zwłaszcza jasnych norm konstytucyjnych – zakres i treść prawa do prywatności podlegała dalszemu doprecyzowaniu w drodze dalszych orzeczeń Sądu Najwyższego. Proces ten trwał wiele lat i *de facto* do dnia dzisiejszego wiele z aspektów związanych z ochroną prywatności, zwłaszcza w zakresie nowych technik przetwarzania danych, nie jest precyzyjne wyjaśnionych na gruncie judykatury amerykańskiej.

Biorąc pod uwagę badaną problematykę – dotyczącą prawnych podstaw prowadzenia programów masowej inwigilacji – istotne znaczenie znajdują dwie doktryny prawne, wypracowane w dotychczasowym orzecznictwie Sądu Najwyższego.

---

[31] Polskie tłumaczenie Czwartej Poprawki: http://libr.sejm.gov.pl/tek01/txt/konst/usaam4.html

[32] Wyrok Sądu Najwyższego USA z dnia 7 czerwca 1965 r. w sprawie *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[33] A. Kiełtyka, *Podstawa faktyczna zatrzymania i przeszukania według Czwartej Poprawki do Konstytucji Stanów Zjednoczonych Ameryki*, „Prokuratura i Prawo" 2006, nr 2, s. 91–106.

[34] C. Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, „Mississippi Law Journal" 2012, t. 81, s. 2.

Pierwsza z nich dotyczy tzw. testu uzasadnionego oczekiwania prywatności (ang. *reasonable expectation of privacy*)[35], po raz pierwszy zdefiniowanego w sprawie *Katz v. United States*[36]. Test jest przeprowadzany dwuetapowo, w pierwszym kroku konieczna jest ocena, czy analizowane zdarzenie w subiektywnym odbiorze jednostki naruszyło jej sferę prywatności. Dopiero jeżeli odpowiedź na tak sformułowane pytanie jest twierdząca, sąd powinien rozważyć, czy oczekiwanie to było obiektywnie uzasadnione, a więc czy *„społeczeństwo jest gotowe, aby uznać je za uzasadnione"*[37]. Ponieważ obszar subiektywnych odczuć jednostki nie podlega prostej ocenie, w amerykańskiej judykaturze przyjmuje się, że zasadniczym elementem testu jest wyważenie tego, co obiektywnie można uznać za *„uzasadnione"*[38].

Drugą ważną doktryną, pozwalającą na wyznaczenie granic stosowania Czwartej Poprawki jest zasada trzeciej strony (ang. *third party doctrine*). O ile test uzasadnionego oczekiwania prywatności powala na rozszerzenie zakresu ochrony w odniesieniu do okoliczności, które w powszechnym odczuciu związane są z ochroną sfery prywatności, to doktryna trzeciej strony służy do wyłączenia spod ochrony zdarzeń, w których jednostka sama przyczyniła się do ujawnienia informacji. Zgodnie z zasadą trzeciej strony, jeżeli jednostka sama i dobrowolnie przekazała informacje podmiotowi zewnętrznemu, nie może oczekiwać ochrony przed ujawnieniem tych informacji władzy publicznej. Nie ma przy tym znaczenia zakres kontraktowych zobowiązań lub innych uzgodnień pomiędzy stronami dla faktu możliwości pozyskania takich informacji przez organy władzy publicznej bez konieczności przestrzegania trybu wynikającego z Czwartej Poprawki. Przyjmuje się bowiem, że informacje zostały dobrowolnie udostępnione i *de facto* nie należą już do jej sfery prywatności. Przekazanie informacji trzeciej stronie prowadzi więc do braku możliwości uznania, że jednostka posiada uzasadnione oczekiwanie prywatności w związku z treścią przekazanych informacji. Doktryna ta została po raz pierwszy wprowadzona w sprawie *Hoffa v. United States*[39]. Zasada trzeciej strony, zgodnie z wyrokami Sądu Najwyższego, znalazła zastosowanie w odniesieniu do danych bankowych[40] (dostęp do wyciągów bankowych) czy telekomunikacyjnych[41] (dostęp do danych billingowych) – w uogólnieniu wszędzie tam, gdzie dane były dobrowolnie udostępniane i przetwarzane przez podmioty zewnętrzne w związku z prowadzeniem przez nie działalności gospodarczej. W konsekwencji w opisanych

---

[35] Zob. także omówienie sprawy *Katz v. United States* oraz testu uzasadnionego oczekiwania prywatności w: A. Czubik, *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Kraków 2013, s. 155–156.

[36] Wyrok Sądu Najwyższego USA z dnia 18 grudnia 1967 r., sprawa *Katz v. United States*, sygn.: 389 U.S. 347 (1967).

[37] *Ibidem*, s. 361.

[38] O. Kerr, *The Fourth Amendment in cyberspace: can encryption create a resonable expectation of privacy?*, „Connecticut Law Review" 2001, t. 33, s. 507.

[39] Wyrok Sądu Najwyższego USA z dnia 12 grudnia 1966 r., sprawa *Hoffa v. United States*, sygn.: 385 U.S. 293 (1966).

[40] Wyrok Sądu Najwyższego USA z dnia 21 kwietnia 1976 r., sprawa *United States v. Miller*, sygn.: 425 U.S. 435 (1976).

[41] Wyrok Sądu Najwyższego USA z dnia 20 czerwca 1979 r., sprawa *Smith v. Maryland*, sygn.: 442 U.S. 735 (1979).

przypadkach organy ścigania i wymiaru sprawiedliwości mogą uzyskiwać żądane informacje nie w oparciu o nakaz sądowy (ang. *warrant*) – czyli w trybie wynikającym z Czwartej Poprawki, ale na podstawie postanowienia wydanego przez wnioskujący organ (ang. *subpoena*). Warunki zastosowania zasady trzeciej strony zostały syntetycznie przedstawione w wyroku *Couch v. United States*[42], w którym Sąd Najwyższy wskazał na trzy przesłanki, które muszą zostać łącznie spełnione: (1) informacje muszą zostać dobrowolnie przekazane (2) do podmiotu trzeciego, który (3) wykorzystuje je w ramach prowadzonej działalności gospodarczej.

Możliwość zastosowania zasady trzeciej strony do danych przetwarzanych elektronicznie od lat jest przedmiotem licznych niejasności. Problem ten nabrał szczególnego znaczenia w odniesieniu do przedsiębiorców telekomunikacyjnych, którzy dzięki rozwojowi techniki pozyskują szeroką wiedzę na temat aktywności swoich abonentów. Przyjęcie, że zasada trzeciej strony ma zastosowanie do wszystkich metadanych związanych z łącznością elektroniczną generowaną przez użytkownika, prowadziłoby do uznania, że organy władzy publicznej mogą pozyskiwać nie tylko dane bilingowe ale również np. dane o lokalizacji z pominięciem trybu wynikającego z Czwartej Poprawki. Problem ten został rozstrzygnięty dopiero w 2018 roku w precedensowym orzeczeniu Sądu Najwyższego w sprawie *Carpenter v. United States*, w którym sąd wskazał, że zasada trzeciej strony nie znajduje zastosowania do danych o lokalizacji użytkowników[43]. Co ważne, wyrok ten dotyczy wyłącznie geolokalizacji urządzeń abonenckich, nie ogranicza stosowania zasady trzeciej strony w innych przypadkach, w szczególności nie zmienia granic jej stosowania ustalonych we wcześniejszym orzecznictwie[44].

W praktyce amerykańskiego systemu prawnego, rozważając konstytucyjne podstawy ochrony prywatności, konieczne jest odniesienie się także do treści Pierwszej Poprawki, stanowiącej podstawę dla swobody wypowiedzi. Zgodnie z jej treścią, „żadna ustawa Kongresu nie może (…) ograniczać wolności słowa lub prasy". W istocie norma ta stanowi przeszkodę dla wprowadzenia szerszych gwarancji związanych z ochroną prywatności, zwłaszcza we wszystkich obszarach, w których wprowadzone prawo nakładałoby nowe obowiązki związane z regulowaniem publikowanych treści. W europejskim modelu ochrona prywatności jest często wyrażana poprzez autonomię informacyjną jednostki, a więc swobodę w decydowaniu przez nią o zakresie ujawnianych informacji na swój temat oraz kręgu osób, którym dane te są przekazywane. Pierwsza Poprawka stoi na przeszkodzie we wprowadzeniu analogicznego rozwiązania do amerykańskiego systemu prawnego. Wprowadzając zakaz stanowienia przepisów ustawowych, skutkujących ograniczeniem wolności słowa, twórcy konstytucji nie przewidzieli żądnych wyjątków. Oznacza to, że norma ta definiuje swobodę wypowiedzi jako prawo bezwarunkowe, które nie może być

---

[42] Wyrok Sądu Najwyższego USA z dnia 9 stycznia 1973 r., sprawa *Couch v. United States*, sygn.: 409 U.S. 322 (1973).

[43] Wyrok Sądu Najwyższego USA z dnia 24 lipca 2018 r., sprawa *Carpenter v. United States*, sygn.: 585 U.S. (2018).

[44] J. Blanke, *Carpenter v. United States Begs for Action*, „University of Illinois Law Review" 2018, s 260–261, http://cli.re/gzEb5Y

ograniczane nawet w przypadku, gdy prowadzi do naruszenia praw i wolności innych osób.

Czwarta Poprawka co do zasady znajduje zastosowanie w odniesieniu do obywateli i rezydentów Stanów Zjednoczonych[45]. Sąd Najwyższy już w 1972 roku w precedensowym wyroku w sprawie *Keith* przesądził, że przypadki elektronicznego monitorowania łączności krajowej na terenie Stanów Zjednoczonych muszą być realizowane z uwzględnieniem Czwartej Poprawki[46]. Jednak w orzeczeniu wydanym w sprawie *United States v. Verdugo-Urquidez* SN wskazał, że Czwarta Poprawka nie ma zastosowania do czynności przeszukania przeprowadzanych przez agentów federalnych w odniesieniu do własności obcokrajowców znajdującej się poza terytorium Stanów Zjednoczonych. Wyrok ten oznacza, że działania służb specjalnych związane z przechwytywaniem łączności elektronicznej, przeprowadzane poza terytorium Stanów Zjednoczonych, nie muszą być realizowane z poszanowaniem standardów konstytucyjnych wynikających z Czwartej Poprawki. Jednocześnie SN zauważył, że *„zarówno konstytucja jak i prawo stanowione w jej wykonaniu nie mają żadnej mocy za granicą, za wyjątkiem stosowania ich w odniesieniu do naszych własnych obywateli"*[47]. Teza ta wyraża funkcjonujące w amerykańskiej judykaturze przekonanie, że faktycznym celem przyjęcia Czwartej Poprawki nie było ograniczanie władzy publicznej, ale ochrona praw jednostek. W takim rozumieniu funkcja ochronna prawa musi być powiązana z możliwością jego stosowania. Przyjęcie odmiennego podejścia – podkreślającego negatywny obowiązek organów władzy publicznej, mogłaby doprowadzić do wypracowania linii orzeczniczej wskazującej na bezprawność działania organów władzy nie stosujących poza granicami państwa norm prawnych, do stosowania których są zobowiązane na własnym terytorium.

Nawet w odniesieniu do obywateli oraz rezydentów USA, nie każdy przypadek naruszenia sfery prywatności prowadzi do konieczności uwzględnienia ochrony wynikającej z Czwartej Poprawki. Kluczowe znaczenie ma tutaj możliwość zastosowania zasady trzeciej strony, skutkująca wyłączeniem ochrony konstytucyjnej w przypadkach, gdy informacje zostały dobrowolnie przekazane przez osobę innemu podmiotowi. Wyrok *Smith v. Maryland* stał się podstawą do uznania, że metadane związane z usługami telekomunikacyjnymi – zgodnie z zasadą trzeciej strony – nie mogą korzystać z ochrony konstytucyjnej. Chociaż zgodnie z orzeczeniem *Carpenter v. United States* stosowanie tej zasady nie może zostać rozszerzone na dane o lokalizacji użytkownika, to jednak w wielu innych przypadkach organy państwa mają możliwość pozyskania informacji dotyczących łączności elektronicznej z pominięciem kontroli sądowej wynikającej z Czwartej Poprawki. Dlatego praktyczne znaczenie funkcji ochronnej wynikającej z Czwartej Poprawki ogranicza się

---

[45] Ochrona wynikająca z Czwartej Poprawki ma zastosowanie do obywateli – niezależnie od miejsca ich faktycznego pobytu, a także wszystkich osób legalnie przebywających na terytorium Stanów Zjednoczonych (także obcokrajowców). Zob.: E. Corradino, *The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far?*, „Fordham Law Review" 1989, t. 57, s. 618–619.

[46] Wyrok Sądu Najwyższego USA z dnia 19 lipca 1972 r., sprawa *United States v. U.S. District Court*, sygn. 407 U.S. 297 (1972).

[47] E. Corradino, *The Fourth Amendment Overseas…*, *op. cit.*, przyp. 36.

do sytuacji, gdy podmiotem inwigilacji są rezydenci USA a podejmowane czynności obejmują uzyskanie dostępu do merytorycznej treści przekazu (a więc treści komunikacji – rozmów, wiadomości e-mail itp.).

Podsumowując dotychczasowe rozważania, chociaż Czwarta Poprawka wprowadza mechanizmy ochrony przez nieuprawnionymi działaniami organów władzy publicznej, także w zakresie gromadzenia informacji dotyczących sfery życia prywatnego, to praktyczny zakres jej stosowania jest mocno ograniczony zarówno podmiotowo, jak i przedmiotowo.

4. USTAWA O NADZORZE NAD WYWIADEM OBCYM (FISA)[48]

Podstawowym aktem ustawowym, sankcjonującym prowadzenie amerykańskich programów tajnej inwigilacji elektronicznej, w tym także zakładających hurtowe i nieograniczone gromadzenie danych, jest ustawa federalna z 25 października 1978 roku o nadzorze nad wywiadem obcym (*Foreign Intelligence Surveillance Act*, FISA)[49]. Głównym celem uchwalenia przepisów było określenie zasad prowadzenia działań wywiadowczych w odniesieniu do obcokrajowców w sposób, który zapobiegałby możliwości wykorzystania tych samych środków i technik do monitorowania aktywności obywateli USA. Ustawa FISA została przedłożona i przyjęta, jako bezpośrednia konsekwencja wątpliwych pod kątem prawnym działań amerykańskich służb specjalnych, związanych między innymi z inwigilacją opozycji oraz konkurentów politycznych (m.in. Martina Luthera Kinga czy związana z tzw. *aferą Watergate*)[50].

Ustawa była wielokrotnie nowelizowana w sposób znacząco modyfikujący jej pierwotne brzmienie. Jednak dla zrozumienia kształtu wprowadzanych przepisów konieczne jest wyjaśnienie najważniejszych pojęć i konstrukcji prawnych, w oparciu o które została zbudowana. Głównym celem aktu było określenie uprawnień organów ścigania (w tym służb specjalnych) w prowadzeniu działań inwigilacji elektronicznej względem przedstawicieli obcych wywiadów. W tym celu w ustawie zdefiniowano termin „*podmiotu zagranicznego wpływu*" (ang. *foreign powers*), pod którym rozumiano rządy państw trzecich lub ich przedstawicieli, organizacje przez nie kontrolowane (niezależnie od ich formalnego statusu), a także grupy zaangażowane w działania międzynarodowego terroryzmu, jak również związane z proliferacją broni masowej zagłady. Termin ten nie obejmował zatem wyłącznie

---

[48] W literaturze i aktach prawnych funkcjonuje kilka różnych tłumaczeń tytułu amerykańskiej ustawy Foreign Intelligence Surveillance Act: „ustawa o nadzorze zagranicznego wywiadu" (zob. np. rezolucja PE z 14.03.2014, Dz. Urz. UE z 2017 nr C 378, s. 14), „ustawa o nadzorze nad wywiadem obcym" (zob. np. rezolucja PE z 4.07.2013, Dz. Urz. UE z 2016 nr C 75, s. 105), jak również „ustawa o działalności obcych wywiadów" (zob. J. Larecki, *Wielki Leksykon Tajnych Służb Świata*, Warszawa 2017, s. 288). W niniejszym artykule stosowane będzie tłumaczenie „ustawa o nadzorze nad wywiadem obcym", która w ocenie autora najlepiej oddaje znaczenie tytułu oryginalnego.

[49] Ustawa federalna USA z dnia 25 października 1978 r. o nadzorze nad wywiadem obcym (*Foreign Intelligence Surveillance Act*); sygn.: 95-511, publikacja 50 USC § 1801.

[50] J. McAdams, *Foreign Intelligence Surveillance Act (FISA): An Overview*, https://goo.gl/VbfTd8, s. 2.

działalności o charakterze obcego wywiadu. Zakres osób, które mogły zostać poddane technikom inwigilacyjnym został wyznaczony terminem „*agent zagranicznych sił*" (ang. *agent of a foreign power*), przy czym w zastosowanej definicji wyróżniono podział na podmioty niepodlegające prawu USA oraz takie, które podlegają jurysdykcji amerykańskiej. W definicji drugiej ze wskazanych grup (ang. *United States person*) wskazano, że należą do niej obywatele, osoby posiadające prawo stałego pobytu, stowarzyszenia i jednostki nieposiadające osobowości prawnej, w których „*w znaczącej liczbie*" uczestniczą obywatele i rezydenci USA, a także podmioty prawa handlowego, zarejestrowane w Stanach Zjednoczonych. Wprowadzone definicje miały pozwolić na przyjęcie odmiennych zasad prowadzenia czynności inwigilacyjnych wobec podmiotów i osób chronionych przez Czwartą Poprawkę oraz pozostałych osób, wobec których nie istniała konieczność przestrzegania standardów konstytucyjnych.

W rezultacie w ustawie FISA wprowadzono dwa tryby, pozwalające na gromadzenie danych elektronicznych. Pierwszy – realizowany w oparciu o art. 102 – może być wykorzystywany wyłącznie w przypadku inwigilacji elektronicznej realizowanej pomiędzy podmiotami zagranicznego wpływu, przy jednoczesnym spełnieniu przesłanki braku istotnego prawdopodobieństwa (ang. *no substantial likelihood*), że w wyniku realizacji czynności pozyskana zostanie komunikacja osób amerykańskich. Czynności inwigilacyjne mogą być w takim przypadku zatwierdzone przez Prokuratora Generalnego bez potrzeby występowania o wydanie nakazu sądowego. Co warte podkreślenia, zarządzenie czynności inwigilacyjnych nie wiąże się w takim przypadku z koniecznością wykazania istnienia prawdopodobnej przyczyny, a więc przesłanki warunkującej wydanie nakazu sądowego zgodnie z Czwartą Poprawką.

Tryb wynikający z art. 102 może być jednak zastosowany tylko w ograniczonych przypadkach, w szczególności nie może być wykorzystywany do inwigilacji organizacji terrorystycznych, zagranicznych partii politycznych oraz jednostek kierowanych lub kontrolowanych przez obcy rząd (art. 102 w zw. z art. 101 ust. a pkt 4–6 FISA).

Alternatywnie, w każdym przypadku istnieje możliwość przeprowadzenia działań inwigilacji elektronicznej na podstawie nakazu sądowego wydanego przez specjalnie powołany mocą ustawy Sąd ds. Inwigilacji Obcego Wywiadu (*United States Foreign Intelligence Surveillance Court*, FISC). Utworzony na podstawie art. 103 FISA organ sądowy pierwotnie składał się z siedmiu (obecnie – z jedenastu) sędziów, po jednym dla każdego z wówczas funkcjonujących federalnych okręgów apelacyjnych (ang. *federal judicial circuit*), wybranych przez Przewodniczącego Sądu Najwyższego USA. Ponadto wybieranych jest trzech dodatkowych sędziów federalnych, tworzących skład Sądu Odwoławczego ds. Inwigilacji Obcego Wywiadu (*United States Foreign Intelligence Surveillance Court of Review*, FISCR). Sąd Odwoławczy rozpatruje w drugiej instancji wyłącznie skargi na odmowę wydania nakazu zatwierdzającego przeprowadzenie czynności inwigilacyjnych. Łącznie oba organy posiadają wyłączną kompetencję w zatwierdzaniu wniosków składanych w oparciu o ustawę FISA – co w szczególności oznacza, że wydane przez nie decyzje nie mogą być skarżone przed innymi sądami federalnymi, a ich legalność nie może być kwestionowana z wykorzystaniem żadnej innej procedury prawnej. Wyjątek stanowi

możliwość wniesienia kasacji do Sądu Najwyższego od wyroku wydanego przez Sąd Odwoławczy[51], jednak w praktyce jest to uprawnienie przysługujące wyłącznie stronie rządowej – ponieważ jak wcześniej wskazano, do FISCR zaskarżane są tylko postanowienia odmowne wydane przez FISA[52]. Działalność sądów jest przy tym z założenia tajna, przez co należy rozumieć ustawowe zniesienie jawności posiedzeń, składanych wniosków i wydanych nakazów (art. 103 ust. 3 FISA). Co więcej, podmioty do których kierowane są nakazy (np. operatorzy telekomunikacyjni) także z mocy prawa są zobowiązani utrzymać w tajemnicy wszelkie czynności związane z wykonaniem otrzymanego postanowienia, a także sam fakt wydania nakazu[53].

Jak wcześniej wskazano, pierwotna treść aktu była przyjmowana w celu zmniejszenia ryzyka prowadzenia prawnie wątpliwych czynności inwigilacyjnych na terytorium Stanów Zjednoczonych. Celem ustawy było więc zwiększenie praw jednostek, a nie ich ograniczenie. Tajność działań organów sądowych jest zrozumiała, zwłaszcza uwzględniając, że nakazy przez nie wydawane miały dotyczyć wprost obszaru bezpieczeństwa państwa – a w szczególności ochrony przed działalnością obcego wywiadu. Ustawa była przyjmowana w latach 70. XX wieku, dlatego techniki nadzoru elektronicznego w niej omawiane dotyczyły łączności telekomunikacyjnej (podsłuch rozmów głosowych) i – z uwagi na brak wystarczających możliwości technicznych – nie analizowano wówczas ryzyk związanych z możliwością objęcia inwigilacją nieoznaczonej grupy osób.

Pierwotne brzmienie ustawy zostało kilkukrotnie znowelizowane, przy czym prowadzone zmiany mają kluczowe znaczenie z punktu widzenia analizowanej problematyki. Pierwsza z ważnych nowelizacji miała miejsce w 2001 roku i wiązała się z przyjęciem ustawy o zjednoczeniu i wzmocnieniu Ameryki dzięki dostarczeniu właściwych narzędzi potrzebnych do wykrywania i zapobiegania aktom terrorystycznym (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*), w skrócie określanej w literaturze przedmiotu jako *Patriot Act* (PA). Ustawa została przyjęta na skutek wydarzeń z 11 września 2001 roku, jako element działań prawnych prowadzących do wzmocnienia kompetencji organów państwa w walce z organizacjami terrorystycznymi. Rozdział II ustawy wprowadzał wiele zmian do przepisów FISA, skutkujących rozszerzeniem uprawnień organów oraz złagodzeniem wymagań formalnych, związanych z zastosowaniem inwigilacji. Przykładem może być modyfikacja wymagania związanego z celem prowadzonych działań inwigilacyjnych. W pierwotnej treści art. 104 ust. a pkt 7 FISA wymagano, aby jedynym celem działań inwigilacyjnych było pozyskanie informacji na temat działalności obcego wywiadu. W znowelizowanej treści przepisu termin ten zastąpiono zwrotem „*istotny cel*", dzięki czemu nakazy sądowe mogły być wydawane na potrzeby autoryzowania działań wywiadowczych nie wymierzonych wyłącznie w działalność obcych służb specjalnych.

Z punktu widzenia omawianego obszaru badawczego, istotne znaczenie miał art. 215 ustawy nowelizującej, który zmienił treść art. 501 FISA. Zgodnie z nowym

---

[51] Zob. 28 USC § 2106.
[52] Zob. 50 USC § 1881a(h)(6)(B).
[53] Zob. 50 USC § 1861(d).

brzmieniem przepisu, dyrektor Federalnego Biura Śledczego lub jego upoważnieni przedstawiciele mogli skierować do każdego przedsiębiorcy żądanie udostępnienia „istotnych zapisów" (ang. *tangible things*), koniecznych dla trwającego dochodzenia w sprawie międzynarodowego terroryzmu lub działań wywiadowczych. Działania inwigilacyjne mogły także obejmować rezydentów i osoby prawne z obszarów Stanów Zjednoczonych („*United States person*"), jednak pod warunkiem, że jedyną podstawą ich realizacji nie były działania chronione Pierwszą Poprawką. Wymaganie to należało zatem rozumieć w ten sposób, że wyłącznym uzasadnieniem inwigilacji obywateli amerykańskich nie mogły być informacje, które oni sami publikowali, korzystając z przysługującej im swobody wypowiedzi. Wnioski składane na podstawie znowelizowanego art. 501 FISA mogły być rozpatrywane zarówno przez wyznaczony organ sądowy (FISC), jak i przez każdego z sędziów federalnych, niezależnie od okręgu jego jurysdykcji.

W praktyce art. 215 stał się podstawą dla prowadzenia programów inwigilacyjnych, opierających się na hurtowym gromadzeniu metadanych dotyczących łączności elektronicznej. Chociaż upoważnione organy nie uzyskiwały na jego podstawie dostępu do informacji dotyczących treści komunikacji, to możliwość gromadzenia i dalszego przetwarzania dużych zbiorów danych opisujących sposób korzystania z usług łączności danych (połączenia telefoniczne, wiadomości e-mail) pozwala przy wykorzystaniu zaawansowanych algorytmów *Big Data* odkrywać wzorce zachowania oraz identyfikować relacje pomiędzy osobami. W praktyce wszelkie informacje, jakie operatorzy usług telekomunikacyjnych, finansowych czy nawet zdrowotnych przetwarzali w związku ze świadczonymi usługami, mogły został uzyskane w trybie wynikającym z art. 215. Brak jakiegokolwiek ograniczenia co do wskazania zakresu podmiotowego żądanych danych pozwalał na występowanie przez uprawnione organy z wnioskiem o przekazanie wszystkich informacji, będących w posiadaniu zobowiązanego przedsiębiorcy i związanych ze świadczeniem przez niego usługami. Nie bez znaczenia był także fakt, że w redakcji art. 215 nie odwołano się do konieczności spełnienia przesłanki „*prawdopodobnej przyczyny*", zamiast tego wskazując jako wystarczający dużo mniej restrykcyjny warunek, aby żądane informacje pozostawały „*w związku*" z toczącym się dochodzeniem.

Nakazy wydane na podstawie art. 215 bez wątpienia nie pozwalały na przechwytywanie treści rozmów telefonicznych. Rozmowy takie nie były bowiem informacją wytworzoną przez operatorów telekomunikacyjnych, a wskazany przepis *de facto* umożliwiał pozyskanie informacji, będących w posiadaniu przedsiębiorców w związku z prowadzoną przez nich działalnością. Procedura wynikająca z art. 215 łączy się zatem z omówioną wcześniej zasadą trzeciej strony, która skutkuje wyłączeniem informacji dobrowolnie przekazanych przedsiębiorcom z ochrony wynikającej z Czwartej Poprawki. Nie jest jednak jasne, czy i w jakim zakresie na podstawie tego przepisu możliwe było uzyskanie dostępu do wiadomości elektronicznych składowanych przez operatorów usług e-mail. O ile bowiem w przypadku połączeń telefonicznych rejestrowanie łączności nie jest koniecznym elementem świadczenia usługi, to w przypadku wiadomości e-mail ich treść w sposób oczywisty musi być zapisana i przechowana na serwerach pocztowych w celu przekazania odbiorcy. W efekcie – w zależności od interpretacji – możliwe było uznanie, że zawartość

merytoryczna wiadomości elektronicznych może być udostępniona na podstawie art. 215 PA[54].

Przykładem zastosowania trybu wynikającego z art. 215 jest ujawnione w domenie publicznej postanowienie FISC z 25 kwietnia 2013 roku, w którym nakazano podmiotom z grupy kapitałowej Verizon (jeden z głównych operatorów telekomunikacyjnych w Stanach Zjednoczonych)[55] przekazywanie metadanych dotyczących wszystkich połączeń krajowych i połączeń zagranicznych wykonywanych przez wszystkich użytkowników operatora. W nakazie wskazano, że przekazywane dane mają obejmować między innymi numery stacji wywołującej i wywoływanej, identyfikatory IMSI, IMEI, a także czas trwania połączenia. Należy zauważyć, że zakres przekazywanych danych w żaden sposób nie wynikał z konieczności uzyskania tych informacji w związku z prowadzonymi postępowaniami karnymi – żądano przekazania danych dotyczących wszystkich połączeń każdego z abonentów. Jest to zatem przykład ingerencji w prawo do prywatności, która nie spełnia zasady proporcjonalności, w efekcie – nie może być uznana za zgodną z EKPC czy prawem UE. Sąd amerykański (FISC) nie weryfikował zasadności żądanych danych, a jedynie przeprowadził ocenę zgodności wniosku z podstawą prawną – w tym przypadku art. 501 FISA.

Nakaz wydany w przypadku Verizon nie należy do wyjątków. Według informacji medialnych, podobne postanowienia zostały wydane w odniesieniu do dwóch innych wiodących operatorów telekomunikacyjnych[56]. Ponadto z opublikowanych statystyk FISC wynika, że w latach 2004–2013 (a więc przed ujawnieniem przez E. Snowdena informacji o skali programów prowadzonych NSA), FISC akceptował bez modyfikacji 99% złożonych wniosków[57]. Z kolei w roku 2015 wskaźnik ten wyniósł 96% (5 zmodyfikowanych wniosków na 142 złożone)[58].

W rezultacie, art. 215 stał się podstawą dla wprowadzenia systemu rejestrowania danych dotyczących większości (jeżeli nie wszystkich) połączeń telefonicznych wykonywanych pomiędzy abonentami na terenie Stanów Zjednoczonych, jak również łączności zagranicznej. Jest to skala inwigilacji nieznana wcześniej w państwach demokratycznych, w sposób oczywisty prowadząca do zwiększenia ryzyka nadużycia władzy. Służby specjalne zyskały bowiem szczegółowe informacje nie tylko na temat łączności realizowanej przez osoby, które były lub mogły być podejrzewane o popełnienie lub planowanie poważnego przestępstwa, ale również setek milionów obywateli niepodejmujących żadnych działań przestępczych,

---

[54] Pytany o tą kwestię podczas przesłuchania przez komisją Senatu USA, gen. K. Alexander, ówczesny szef NSA, zeznał, że art. 215 stanowi podstawę wyłącznie dla gromadzenia metadanych, a w przypadku potrzeby przechwycenia treści komunikacji konieczne jest wcześniejsze uzyskanie zgody sądu. Szczegóły: *NSA chief drops hint about ISP Web, e-mail surveillance*, https://www.cnet.com/news/nsa-chief-drops-hint-about-isp-web-e-mail-surveillance/

[55] Podkreślenia wymaga także fakt, że Verizon – poza obsługiwanymi przez spółkę MCI Networks połączeniami międzynarodowymi – zarządza także znaczną częścią sieci szkieletowej Internetu na terytorium Stanów Zjednoczonych (tzw. sieć warstwy pierwszej, ang. *tier 1*).

[56] The Wall Street Journal, *U.S. Collects Vast Data Trove*, http://cli.re/LJnAAn

[57] J. Mornin, *NSA Metadata Collection And The Fourth Amendment*, „Berkeley Technology Law Journal" 2014, t. 29, s. 986.

[58] Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Court Orders 1979–2016*, https://epic.org/privacy/surveillance/fisa/stats/default.html

a także adwokatów, dziennikarzy, polityków i innych grup społecznych, których komunikacja nie powinna być monitorowana przez władzę publiczną bez istnienia ku temu ważnej i realnej przesłanki.

Kolejne zmiany związane z możliwością prowadzenia rozbudowanych, masowych programów inwigilacji związane są z przyjętą w 2008 roku ustawą o zmianie ustawy o nadzorze nad wywiadem obcym (*Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, FAA)[59]. Zgodnie z art. 101 FAA zastąpiono wcześniejszą treść rozdziału VII FISA nowymi regulacjami dotyczącymi dodatkowych procedur mających zastosowanie wobec osób przebywających poza terytorium Stanów Zjednoczonych. Zgodnie z wprowadzonym brzmieniem art. 702 FISA, Prokurator Generalny oraz Dyrektor Wywiadu Krajowego (*Director of National Intelligence*, DNI), działając wspólnie, zostali upoważnieni do autoryzowania objęcia działaniami inwigilacyjnymi osób, co do których istniały rozsądne podstawy, że znajdują się poza obszarem Stanów Zjednoczonych. Celem podejmowanych środków miało być pozyskanie informacji na temat działalności obcego wywiadu. Wskazany przepis nie określał konieczności uzyskania zgody sądu, nie wprowadzał także ograniczeń co do zakresu gromadzonych informacji. Natomiast zgodnie z art. 702 ust. 2, wydana zgoda nie mogła w sposób celowy obejmować osób, wobec których:

– było wiadomo, że w czasie gromadzenia danych przebywały na terytorium Stanów Zjednoczonych,
– są obywatelami lub rezydentami Stanów Zjednoczonych, przebywającymi zagranicą,
– celem stosowania inwigilacji było pozyskanie informacji na temat obywateli lub rezydentów Stanów Zjednoczonych, kontaktujących się z nadzorowanymi osobami.

Wszystkie wskazane ograniczenia prowadziły zatem do wyłączenia z możliwości objęcia autoryzacją wydaną na podstawie art. 702 FISA osób fizycznych i prawnych USA, niezależnie od ich lokalizacji oraz wszelkich osób przebywających na terytorium Stanów Zjednoczonych. Jak wcześniej wskazano, w jurysprudencji Sądu Najwyższego przesądzono, że w każdej z opisanych sytuacji zastosowanie znajduje Czwarta Poprawka, a zatem prowadzenie działań inwigilacyjnych musi być poprzedzone uzyskaniem nakazu sądowego wydanego po zweryfikowaniu istnienia prawdopodobnej przyczyny (ang. *probable cause*). Dlatego też w samej treści art. 702 ust. b dodano punkt (5) wskazujący, że działania przeprowadzane na podstawie wydanej zgody „*muszą być przeprowadzone w sposób zgodny z Czwartą Poprawką do Konstytucji USA*".

Tryb wynikający z art. 702 nie zakłada także weryfikacji sądowej wydanych decyzji administracyjnych. Prawodawca przewidział dla organu sądowego funkcję okresowego przeglądu oraz certyfikacji warunków realizacji programów (w szczególności sposobu określania kręgu osób poddanych inwigilacji oraz tzw. procedur minimalizacji)[60]. Sąd nie dokonuje jednak oceny zasadności inwigilacji konkretnych

[59] Ustawa federalna USA z dnia 10 lipca 2008 r. o zmianie ustawy o nadzorze nad wywiadem obcym (*Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*); sygn.: 110–261, publikacja 50 USC § 1801, t. ogłoszony: https://goo.gl/deFnBE

[60] 50 USC § 1881a (d–e)(2).

osób, jego kognicja ogranicza się do weryfikacja zasad (procedur) według których analitycy uprawnionych organów dokonują typowania celów inwigilacji. Oznacza to, że rola organu sądowego ogranicza się do analizy deklaracji uprawnionych organów, bez sprawdzenia, w jaki sposób deklaracje te są stosowane w praktyce.

O ile art. 215 PA był podstawą dla prowadzenia programów masowego gromadzenia metadanych, to przepis art. 702 FISA umożliwił realizację rozbudowanych działań inwigilacyjnych obejmujących także dostęp do merytorycznej treści przekazów (w tym połączeń głosowych, wiadomości e-mail czy treści wymienianych za pośrednictwem komunikatorów internetowych). Chociaż obie podstawy prawne w sposób bezpośredni oddziaływały na sferę prywatności użytkowników usług łączności elektronicznej, to od strony formalnej stanowiły one podstawę realizacji innych programów inwigilacyjnych. Programy oparte na art. 215 PA obejmowały wszystkich użytkowników korzystających z określonych środków łączności. Z kolei programy oparte na art. 702 FISA miały mniej globalny charakter, jednak z uwagi na możliwość dostępu do danych użytkownika – ich wpływ na sferę prywatności był większy. Ponieważ obie grupy programów administrowane są przez tą samą agencję federalną (NSA), należy oczekiwać, że sposób ich realizacji jest silnie skorelowany, dzięki czemu możliwe jest uzyskiwanie bardziej szczegółowych i dokładnych informacji na temat jednostki oraz jej relacji z innymi osobami.

Ostatnia z istotnych nowelizacji FISA jest związana z przyjętą w 2015 roku ustawą o reformie uprawnień rządu federalnego w zakresie dostępu do określonych danych komercyjnych, przeprowadzania inwigilacji elektronicznej, stosowania urządzeń rejestrujących, przechwytujących i śledzących oraz stosowania innych form gromadzenia danych w obszarze wywiadu zagranicznego, przeciwdziałania terroryzmowi, dochodzeń kryminalnych i innych celów (znana w literaturze także jako *Freedom Act, FA*)[61]. W ustawie wprowadzono szereg istotnych zmian, w tym dwie kluczowe – związane z omówionym wcześniej art. 501 FISA (w brzmieniu nadanym art. 215 PA) oraz art. 702 FISA (w brzmieniu nadanym przez art. 101 FAA). W szeregu przepisów szczegółowych ustawy wprowadzono wprost zakaz hurtowego (nieukierunkowanego) gromadzenia danych. W tym celu prawodawca wskazał, że wnioski i nakazy wydane na podstawie art. 501 FISA muszą być uzupełnione informacją o selektorach (wyszukiwanych terminach), stanowiących podstawę do wskazania zakresu informacji, jaki ma być udostępniony. Treść art. 501 została zastąpiona brzmieniem obowiązującym przed wejściem w życie *Patriot Act*, w ten sposób powodując, że legalnie wątpliwa podstawa prawna dla prowadzenia programów masowej inwigilacji przestała obowiązywać. Jednocześnie, zgodnie z art. 301, wprowadzono zakaz dowodowy dotyczący informacji pozyskanych na podstawie art. 702 ust. 1 FISA, ale z naruszeniem ograniczeń wynikających z art. 702 ust. 2 FISA. Informacje tego typu – z pewnymi wyjątkami – nie mogą być wykorzystane w toku spraw rozpatrywanych przez organami sądowymi i administracyjnymi, a także być wykorzystane w żaden inny sposób czy przekazane innej organizacji czy agencji.

[61] Ustawa federalna USA z dnia 2 lipca 2015 r. (*USA Freedom Act of 2015*); sygn.: 114-23, t. ogłoszony: https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf

Zgodnie z treścią art. 403 ust. b FFA, w przypadku braku podjęcia dalszych działań legislacyjnych, uprawnienie wynikające z art. 702 FISA miało wygasnąć w dniu 31 grudnia 2017 roku. Dlatego też z początkiem 2017 roku w Stanach Zjednoczonych rozpoczęła się dyskusja na temat potrzeby i zakresu dalszego przedłużenia czasu obowiązywania przepisu art. 702 FISA. Przedstawiciele władzy wykonawczej, tacy jak Dyrektor Wywiadu Krajowego, rekomendowali przedłużenie obowiązywania przepisów bez zmiany ich zakresu – w szczególności bez przyjmowania uregulowań wzmacniających prawa obywatelskie kosztem swobody prowadzenia programów wywiadowczych[62]. Z drugiej strony, organizacje ochrony praw człowieka podkreślały potrzebę przebudowania regulacji art. 702 w taki sposób, aby ograniczyć możliwość powtórzenia się stwierdzonych w przeszłości przypadków nadużycia uprawnień. Postulowano między innymi uwzględnienie zakazu gromadzenia danych nie dotyczących wprost podmiotów inwigilacji, jak również – na wzór rozwiązań wynikających z Czwartej Poprawki – wprowadzenie testu *„prawdopodobnej przyczyny"* jako przesłanki warunkującej zastosowanie technik inwigilacyjnych[63]. Ostatecznie, zgodnie przyjętym tekstem ustawy wydłużono okres stosowania uprawnień wynikających z art. 702 FISA aż do końca 2023 roku[64]. Jednocześnie poszerzono także zakres komunikacji, która mogła być objęta środkami inwigilacji. Wcześniej obowiązujące przepisy nie stanowiły podstawy dla gromadzenia tzw. danych pośrednich (*„about data"*), a więc danych wymienianych przez osoby trzecie, których treść mogła wskazywać na odniesienie do obiektu inwigilacji. Według organizacji ochrony praw człowieka możliwość gromadzenia danych pośrednich może stanowić sposób na omijanie przez służby specjalne ograniczeń prawnych związanych z rejestrowaniem łączności[65]. W nowej ustawie wprowadzono procedurę pozwalającą na legalizację gromadzenia danych pośrednich.

Wynikające z ustawy FISA dwa tryby prowadzenia rozbudowanych programów inwigilacji elektronicznej – a więc art. 501 (metadane) oraz art. 702 FISA (merytoryczna treść przekazu) – stanowiły podstawę dla różnych programów wywiadowczych realizowanych przez NSA. W szczególności w oparciu o nakazy wydane na podstawie art. 501 prowadzone były programy MAINWAY oraz MARINA, polegające na gromadzeniu metadanych dotyczących całej komunikacji elektronicznej realizowanej na terenie Stanów Zjednoczonych – związanej z połączeniami głosowymi (MAINWAY) oraz łącznością internetową (MARINA). Z kolei na podstawie nakazów wydawanych w trybie wynikających z art. 702 prowadzono programy PRISM oraz UPSTREAM. Z uwagi na różną podstawę prawną, odmienny jest nie

---

62 Reuters, *White House supports renewal of spy law without reforms: official*, https://goo.gl/LfRcbF

63 L. Donohue, *The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law*, https://goo.gl/7h5irH

64 Zob. art. 201(a)(1)(A) ustawy federalnej z dnia 19 stycznia 2018 r. o zmianie ustawy z o nadzorze nad wywiadem zagranicznym w celu usprawnienia gromadzenia danych wywiadowczych oraz gwarancji, odpowiedzialności i nadzoru nad pozyskiwaniem informacji wywiadowczych oraz w celu rozszerzenia tytułu VII tego aktu (*FISA Amendments Reauthorization Act of 2017*); sygn.: 115-118, t. ogłoszony: http://cli.re/LjQp4V

65 *All About „About" Collection*, Electronic Frontier Foundation, http://cli.re/gzWJM5

tylko zakres merytoryczny gromadzonych informacji, ale krąg osób poddanych inwigilacji. W przypadku art. 702 zastosowanie znajdują ograniczenia związane z rezydentami Stanów Zjednoczonych. Z kolei w przypadku art. 501, uwzględniając omówioną wcześniej zasadę trzeciej strony, metadane nie podlegają ochronie konstytucyjnej wynikającej z Czwartej Poprawki. W efekcie mogą być gromadzone i przetwarzane przez organy władzy publicznej także w odniesieniu do komunikacji rezydentów Stanów Zjednoczonych, bez żadnych dodatkowych ograniczeń prawnych.

Wraz z reformą związaną z przyjęciem ustawy *Freedom Act* skutkującą przywróceniem brzmienia art. 501 FISA do treści sprzed 2001 roku, niektóre z programów – jeżeli są nadal prowadzone – wymagają innej podstawy prawnej. W literaturze przedmiotu, nie bez przyczyny, zauważa się, że sposób wprowadzenia tej zmiany, polegający na uchyleniu treści normy i przywróceniu w jej miejsce brzmienia obowiązującego ponad 15 lat temu (przed 2001 rokiem), skutkuje powstaniem niespójności przepisów i w efekcie potencjalną luką prawną, która może być wykorzystana do prowadzenia kolejnych tajnych programów inwigilacji.

Z uwagi na brak transparentności działań NSA, w chwili obecnej nie jest możliwe wskazanie, na ile wprowadzenie *Freedom Act* pozwoliło na osiągnięcie zamierzonego celu – a więc uniemożliwienie nieograniczonego gromadzenia metadanych – i zobligowania, aby służby specjalne uzyskiwały dostęp do potrzebnych danych po weryfikacji, że informacje te są faktycznie potrzebne w toku prowadzonych dochodzeń i nie służą wyłącznie do analityki prewencyjnej.

5. ROZPORZĄDZENIE WYKONAWCZE PREZYDENTA NR 12333 Z 1981 ROKU

Konstytucja Stanów Zjednoczonych określa kompetencje władzy wykonawczej i ustawodawczej w sposób odmienny od stosowanych w państwa europejskich. W szczególności szereg działań, zwłaszcza dotyczących bezpieczeństwa państwa, należy do obszaru prerogatyw prezydenta. Realizacja tych uprawnień szczególnych – przybierająca formę rozporządzeń egzekutywy (znanych pod nazwą „*rozporządzeń wykonawczych*") – nie wymaga dla swojej ważności istnienia dodatkowej delegacji w aktach stanowionych przez Kongres. Ponadto szereg przepisów ustawodawczych nadaje Prezydentowi szczególne uprawnienia i kompetencje, pozwalające na wprowadzanie rozbudowanych przepisów prawnych, w europejskim prawodawstwie zazwyczaj wymagających regulacji w formie ustawowej.

Przykładem aktu tego rodzaju jest Rozporządzenie wykonawcze Prezydenta nr 12333 (*Executive Order 12333*)[66]. Obok ustawy o nadzorze nad wywiadem obcym, stanowi ono drugą istotną podstawę dla prowadzenia programów inwigilacji elek-

[66] Rozporządzenie wykonawcze nr 12333 z dnia 4 grudnia 1981 r. w sprawie działań wywiadowczych Stanów Zjednoczonych (*Executive Order 12333: United States Intelligence Activities*), t. ogłoszona: 46 FR 59941 (http://cdn.loc.gov/service/ll/fedreg/fr046/fr046235/fr046235.pdf), t. jednolity: https://goo.gl/DZTui7

tronicznej. Co do zasady, dokument omawia kompetencje i uprawnienia służb specjalnych w prowadzeniu działań wywiadowczych. Akt ten ma szczególne znaczenie w przypadku programów realizowanych poza terytorium Stanów Zjednoczonych, w takich przypadkach nie obowiązują bowiem ograniczenia wynikające z przepisów ustawy FISA. Rozporządzenie nr 12333 od momentu jego wydania w 1981 roku było trzykrotnie zmieniane[67], przy czym każda z nowelizacji prowadziła do złagodzenia wymagań oraz rozszerzenia kompetencji organów wspólnoty wywiadowczej.

Rozporządzenie określa warunki przeprowadzania działań inwigilacji elektronicznej, także w odniesieniu do rezydentów Stanów Zjednoczonych. Definiuje przy tym mniej restrykcyjne wymagania, niż wynikające zarówno z Czwartej Poprawki, jak i trybów przewidzianych w ustawie FISA. W punkcie 2.3 rozporządzenia wskazano katalog dziewięciu przesłanek pozwalających na gromadzenie tego typu informacji, które łącznie tworzą bardzo szerokie ramy dla legalnego gromadzenia danych. Ponadto, nawet jeżeli żaden z warunków nie zostanie spełniony, wprowadzono także dodatkową podstawę zezwalającą na „*incydentalne*" gromadzenie danych, towarzyszące działaniom podejmowanym na podstawie innych wymienionych przesłanek. Ponieważ prawodawca nie zakreślił żadnych granic ani ograniczeń związanych z „*incydentalnym gromadzeniem danych*", w literaturze przedmiotu wskazuje się, że w oparciu o wymieniony przepis możliwe jest gromadzenie dowolnie dużych zbiorów danych, które znajdują się – w nawet dalekiej relacji – do informacji będących w uzasadnionym zainteresowaniu służb. Według dostępnych informacji, znaczna część działań realizowanych w ramach grupy programów UPSTREAM prowadzona jest w oparciu o podstawę, jaką stanowi punkt 2.3 ust. c rozporządzenia – zezwalający na gromadzenie danych w związku z legalnymi działaniami wywiadowczymi, kontrwywiadowczymi, a także dochodzeniami związanymi z międzynarodowym handlem narkotykami oraz terroryzmem[68].

W przeciwieństwie do FISA, działania prowadzone w oparciu o rozporządzenie nr 12333 nie wymagają zgody sądu, nie podlegają także okresowym przeglądom organów wymiaru sprawiedliwości. W rozporządzeniu nie wprowadzono żadnych ograniczeń dotyczących zakresu pozyskiwanych informacji, w szczególności prowadzących do uniemożliwienia prowadzenia na jego podstawie programów masowej inwigilacji zakładających hurtowe i nieograniczone gromadzenie danych. Z odtajnionego w 2014 roku przez NSA dokumentu wynika, że Agencja prowadzi większość działań w zakresie rozpoznania elektronicznego wyłącznie na podstawie rozporządzenia nr 12333[69].

Biorąc pod uwagę charakter sieci Internet – w której transfer informacji nie jest związany z fizycznymi granicami geograficznymi, programy oparte na rozporządzeniu nr 12333 mogą służyć *de facto* do przechwytywania dowolnych treści. Wiadomość

---

[67] Zmiany zostały wprowadzone na mocy rozporządzenia wykonawczego nr 13284 z dnia 23 stycznia 2003 r., rozporządzenia wykonawczego nr 13355 z dnia 27 sierpnia 2004 r. oraz rozporządzenia wykonawczego nr 13470 z dnia 30 lipca 2008 r.

[68] Ars Technica, *The executive order that led to mass spying, as told by NSA alumni*, https://goo.gl/TJsNvH

[69] NSA, *Legal Fact Sheet: Executive Order 12333*, https://goo.gl/N6D9k1

e-mail, której zarówno nadawca jak i odbiorca znajdują się w tym samym państwie, może być przekazywana łączami telekomunikacyjnymi przebiegającymi przez obszar państw trzecich. Dlatego wprowadzanie niższych standardów w zakresie przechwytywania łączności przekazywanej poza obszarem Stanów Zjednoczonych w rzeczywistości prowadzi do możliwości przechwytywania na tej podstawie dowolnej komunikacji – także dotyczącej własnych obywateli. W mediach opisywane są przypadki wskazujące, że NSA stosuje celowe techniki przekierowania określonego ruchu internetowego do innych jurysdykcji, aby w ten sposób móc przechwycić komunikację z pominięciem ograniczeń wynikających z przepisów krajowych[70]. Przykład ten wskazuje na ograniczoną skuteczność przepisów ustawowych stanowionych w Stanach Zjednoczonych, mających w zamierzeniu prowadzić do poszanowania praw człowieka w cyberprzestrzeni (w szczególności – prawa do prywatności). Obecnie zakres dopuszczalnej ingerencji w prawa podstawowe zależy od procedury technicznej zastosowanej przez organ władzy publicznej. Te same dane, niosące taką samą wartość informacyjną, będące własnością tej samej osoby – mogą być różnie chronione przed ingerencją ze strony państwa, w zależności od miejsca ich składowania. Jest to bez wątpienia rozwiązanie nieznane w europejskim modelu ochrony danych i w sposób oczywisty niezgodne zarówno ze standardami wynikającymi z prawa UE (art. 7 i art. 8 ust. 1 w zw. z art. 52 ust. 1 KPP), jak i konwencji europejskiej (art. 8 ust. 2 EKPC).

O ile w wyniku reformy FISA przeprowadzonej w 2015 roku, znaczna część najbardziej kontrowersyjnych przepisów stanowiących podstawę dla prowadzenia rozbudowanych programów inwigilacyjnych została zmieniona lub uchylona, nowelizacja ta w żadnej sposób nie wpłynęła na programy realizowane w oparciu o rozporządzenie nr 12333. W rezultacie uprawnienia służb specjalnych wynikające z tego rozporządzenia stanowią większe zagrożenie dla prywatności użytkowników Internetu niż regulacje FISA w obecnym kształcie.

6. PODSUMOWANIE

Przedstawione rozważania pozwalają na nakreślenie kilku kluczowych różnic pomiędzy prawodawstwem USA a regulacjami wynikającymi z EKPC oraz obowiązującymi na terenie UE w odniesieniu do możliwości, zakresu i podstaw prawnych prowadzenia masowych programów inwigilacyjnych.

W pierwszej kolejności brak konstytucjonalizacji prawa do prywatności i oparcie jego głównych założeń na prawie precedensów (orzeczenia SN USA) skutkuje fragmentarycznością i częściowo niespójnością przyjętego modelu ochrony. Organy władzy publicznej są zobowiązane do stosowania Czwartej Poprawki, ale tylko w odniesieniu do rezydentów (niezależnie od miejsca ich pobytu) oraz osób przebywających legalnie na obszarze Stanów Zjednoczonych. Obcokrajowcy nie

[70] The New York Times, *NSA Gets More Latitude to Share Intercepted Communications*, https://goo.gl/iKBuba

posiadają żadnych praw wynikających z Czwartej Poprawki, nawet jeżeli ich dane są przechowywane i przetwarzane na terenie Stanów Zjednoczonych. Odmienne traktowanie różnych grup jednostek na poziomie norm konstytucyjnych znajduje dalsze odzwierciedlenie w przepisach ustawowych i wykonawczych.

Jednocześnie w przepisach podkonstytucyjnych dostrzegalna jest erozja warunków koniecznych, uzasadniających podjęcie działań inwigilacyjnych także względem własnych rezydentów. O ile na poziomie Czwartej Poprawki wymagane jest spełnienie przesłanki „*prawdopodobnej przyczyny*" potwierdzone wydaniem nakazu sądowego, to do podjęcia działań – mających taki sam skutek faktyczny (inwigilacja elektroniczna) – z wykorzystaniem trybów szczególnych wynikających z ustawy FISA, wystarczy już, aby „*istotnym*" celem inwigilacji było pozyskanie informacji wywiadowczych, a spełnienie tej przesłanki w niektórych przypadkach nie musi nawet podlegać niezależnej weryfikacji przez sąd. Wprowadzenie odrębnego organu sądowego, dedykowanego do rozpatrywania spraw związanych z inwigilacją elektroniczną, którego sama działalność przez wiele lat pozostawała tajna, wydawane orzeczenia nie mogły być kwestionowane przez innymi sądami federalnymi, a sposób prowadzenia postępowania nie zakładał udziału żadnego przedstawiciela reprezentującego interesy obywateli – w sposób oczywisty zwiększał ryzyko braku przejrzystości działań wymiaru sprawiedliwości. Do dzisiaj postanowienia wydawane przez FISA nie dają żadnej – także następczej – możliwości ochrony praw osobom, których prywatność została naruszona. Już sam fakt wydania przez tajny sąd blankietowego postanowienia zezwalającego na prewencyjną inwigilację kilkuset milionów osób sprawia, że funkcjonujący w Stanach Zjednoczonych model prawodawstwa jest bliższy opisanemu w „*Procesie*" F. Kafki niż znanemu z europejskich państw demokratycznych.

Służby specjalne Stanów Zjednoczonych mogą prowadzić rozbudowane działania inwigilacyjne w oparciu o co najmniej trzy podstawy prawne – art. 501 FISA (dostęp do metadanych usług łączności elektronicznej), art. 702 FISA (dostęp do całej treści przekazu) oraz punkt 2.3 rozporządzenia nr 12333 (działania podejmowane poza terytorium USA). Każdy z tych trybów może być stosowany jako prawna podstawa prowadzenia programów zakładających hurtowe i nieograniczone gromadzenie danych. Tryby wynikające z poszczególnych przepisów mogą być stosowane zamiennie – i skutkować innym stopniem ingerencji w prawa podstawowe. Przechwycenie i przetwarzanie treści tej samej wiadomości e-mail może:

a) wymagać zgody sądu i spełnienia warunków wynikających z Czwartej Poprawki lub
b) wymagać zgody sądu bez badania warunków wynikających z Czwartej Poprawki (art. 702 FISA) lub
c) nie wymagać zgody sądu i być realizowane w oparciu o autoryzację wydaną przez uprawnionego przedstawiciela władzy wykonawczej (rozporządzenie nr 12333)
   – przy czym wybór podstawy formalnej nie zależy od obiektywnych przesłanek merytorycznych (np. wrażliwość informacji czy wartość dowodowa), ale od miejsca i sposobu przechwycenia wiadomości.

W sposób oczywisty jest to model różny od wynikającego z dorobku orzeczniczego ETPC. Z wypracowanej przez Trybunał linii orzeczniczej wynika, że stosowanie technik inwigilacji powinno być ograniczone ze względu na[71]:

– kategorie przestępstw, z którymi może wiązać się autoryzacja zastosowania środków inwigilacyjnych,
– kategorie osób, które mogą być jej poddane,
– ograniczenie czasu stosowania środków,
– procedurę określającą zasady badania, przechowywania i wykorzystywania zgromadzonych danych,
– środki ostrożności zastosowane w przekazywaniu zgromadzonych danych innym podmiotom,
– kryteria, według których zebrane dane powinny zostać usunięte bądź zniszczone.

Prawodawstwo obowiązujące w Stanach Zjednoczonych w sposób wyraźny nie wypełnia większości ze wskazanych warunków minimalnych. Konsekwencją braku przejrzystości i rozliczalności działań nie tylko służb specjalnych, ale i ustanowionych organów sądowych, jest to, co w orzecznictwie ETPC nazywane się brakiem przewidywalności przepisów, skutkującym niewystarczającą ochroną przed arbitralnością podejmowanych decyzji[72].

Odmienne ramy prawne, w jakich mogą być prowadzone masowe działania inwigilacyjne służb specjalnych w UE i USA są skutkiem różnego wyważenia znaczenia poszczególnych praw podstawowych – w szczególności prawa do prywatności oraz prawa do bezpieczeństwa (z którym wprost związany jest obszar bezpieczeństwa publicznego). W istocie zakres dopuszczalnej inwigilacji obywateli przez własne państwo to kwestia nie tylko prawna, ale także socjologiczna i kulturowa, mająca wpływ na kształtowanie społeczeństwa.

Powyższe zastrzeżenia w zakresie prawodawstwa Stanów Zjednoczonych dyskutowane są również przez przedstawicieli tamtejszej nauki prawa. W trwającym dyskursie pojawiają się poglądy zarówno wskazujące na konieczność reformy istniejących przepisów w kierunku wzmocnienia prawa do prywatności na wzór europejski, jak również wskazujące, że obowiązujące normy konstytucyjne wykluczają wprowadzenie odmiennego systemu ochronnego. Nie bez znaczenia jest także, że szanowani przedstawiciele judykatury nie widzą potrzeby zmian systemowych. Przykładem może być R. Posner[73], sędzia federalnego sądu apelacyjnego, którego publikacje należą do najczęściej cytowanych w amerykańskiej nauce prawa[74]. Sędzia Posner uzasadnia, że prawo do prywatności nie może być naruszane przez NSA w wyniku masowego gromadzenia danych, ponieważ w dużej części ich przetwa-

---

[71] Postanowienie ETPC z dnia 29 czerwca 2006 r. w sprawie *Weber i Saravia v. Niemcy*, sygn. 54934/00, § 95.

[72] Wyrok ETPC z dnia 2 sierpnia 1984 r. w sprawie *Malone v. Wielka* Brytania, sygn. 8891/79, § 67.

[73] Szersze omówienie poglądów R. Posnera w: J. Kuisz, *Konstytucja w sytuacjach zagrożenia bezpieczeństwa państwa na tle teorii R.A. Posnera*, PiP 2013, nr 12, s. 46–59.

[74] Według danych na rok 2000, R. Posner był najczęściej cytowanym autorem artykułów prawniczych w Stanach Zjednoczonych. Zob. F. Shapiro, M. Pearse, *The Most-Cited Law Review Articles of All Times*, „Michigan Law Review" 2012, t. 110, s. 1506, przyp. 42.

rzanie odbywa się automatycznie – a komputery nie mając podmiotowości prawnej, nie mogą naruszać prywatności[75]. Jest to argumentacja błędna, pomijająca zupełnie fakt, że istotnym składnikiem ochrony prywatności jest autonomia informacyjna – wyrażająca się poprzez możliwość decydowania przez jednostkę, kto i w jakich warunkach otrzymuje dostęp do informacji traktowanych przez nią jako wrażliwe. Prowadzenie programów masowej inwigilacji prowadzi do wypaczenia tej idei – a w konsekwencji do pozbawienia jednostki swobody decydowania. Przeciwnicy rozszerzenia zakresu ochronnego związanego z prawem do prywatności często wskazują na nieuchronną kolizję takiego rozwiązania z zapisami Pierwszej Poprawki. Jest to ważny argument, tym bardziej, że jakakolwiek propozycja wymagająca dla swej skuteczności nowelizacji norm konstytucyjnych jest w warunkach amerykańskich nierealna. W interesujący sposób problem ten przedstawił E. Volokh, nazywając europejskie standardy prywatności *„prawem do zakazania innym mówienia na twój temat"*[76]. Korzystając z tej parafrazy E. Volokh dowodzi, że realizacja tego prawa sprowadza się do nadania władzy publicznej narzędzi do ograniczenia wolności wypowiedzi innym – co w sposób oczywisty jest nie do pogodzenia z Pierwszą Poprawką. Argumentację tę odrzuca P. Schwartz, wskazując na liczne przypadki innych przepisów, które już obecnie pozwalają władzy wykonawczej wpływać na treść czy kształt informacji pojawiających się w przestrzeni publicznej[77]. Niezależnie od różnych poglądów w tej kwestii, nie ulega wątpliwości, że Pierwsza Poprawka może być rozpatrywana jako ograniczająca zakres prawa do prywatności – ale w relacjach horyzontalnych, a nie wertykalnych. Trudno uznać, aby prowadzone przez organy władzy publicznej programy masowej inwigilacji setek milionów osób korzystały z ochrony związanej ze swobodą wypowiedzi (merytoryczny zakres Pierwszej Poprawki).

Z kolei N. Young zdefiniował cztery najważniejsze postulaty, które powinny być uwzględnione w dalszych dyskusjach nad zakresem potrzebnej reformy przepisów inwigilacyjnych w Stanach Zjednoczonych:

– zakaz prowadzenia tajnych programów inwigilacyjnych, czyli takich, których samo nawet istnienie nie jest znane opinii publicznej,
– brak legalności prowadzenia masowych programów inwigilacyjnych, pozwalających władzy na rejestrowanie całości informacji przesyłanych w Internecie,
– możliwość dochodzenia zadośćuczynienia za doznaną krzywę przez osoby niesłusznie objęte działaniami inwigilacyjnymi,
– odrzucenie w prawodawstwie podziału na techniki inwigilacji i monitorowania aktywności w zależności od pomiotu, który je stosuje – a więc bez rozróżniania na podmioty prywatne i publiczne[78].

---

[75] R. Posner, *Privacy, Surveillance, and Law*, „The University of Chicago Law Review" 2008, t. 75, s. 254.

[76] E. Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, „Stanford Law Review" 2000, t. 52, s. 1050–1051.

[77] P. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, „Stanford Law Review" 2000, t. 52, s. 1559–1572.

[78] N. Richards, *The Dangers of Surveillance*, „Harvard Law Review" 2013, t. 126, s. 1958–1964.

Przedstawione rozważania prowadzą do wniosku, że obecne prawodawstwo Stanów Zjednoczonych w sposób znacząco odmienny od znanego na gruncie rozwiązań europejskich definiuje zakres i możliwości stosowania środków masowej inwigilacji przez organy władzy publicznej. Problem ten już obecnie stanowi trudność w rozwijaniu wspólnego rynku przetwarzania danych pomiędzy UE i USA. Uwzględniając wnioski płynące z orzecznictwa TSUE, należy oczekiwać, że próba ujednolicenia zasad ochrony prywatności na poziomie krajowych rozwiązań prawnych jest zadaniem skomplikowanym – a w przypadku Stanów Zjednoczonych – może być wręcz niemożliwa. Dlatego rozsądną alternatywą, biorąc pod uwagę istniejące różnice i koncepcje budowy nowoczesnych społeczeństw, jest oparcie wzajemnych relacji pomiędzy UE i USA – także w zakresie dopuszczalnych działań związanych ze stosowaniem środków masowej inwigilacji – na prawnie wiążącej umowie międzynarodowej. W ten sposób możliwe byłoby wprowadzenie skutecznych gwarancji związanych z dopuszczalnym zakresem użycia danych użytkowników z UE przekazanych do przetwarzania na terenie USA. Oczekiwanie na ewentualną reformę przepisów amerykańskich wydaje się być pozbawione podstaw. Chociaż w ostatnich latach ustawa FISA była kilkukrotnie nowelizowana, a zakres wynikających z niej uprawnień inwigilacyjnych modyfikowany, to nie podjęto żadnych prac zmierzających do ograniczenia swobody stosowania środków wynikających z rozporządzenia 12333. W efekcie należy uznać, że w dającej się przewidzieć przyszłości prawodawstwo amerykańskie będzie w znacząco odmienny sposób definiowało zakres praw podstawowych, takich jak prawo do prywatności, niż regulacje obowiązujące w UE.

BIBLIOGRAFIA

Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

Corradino E., *The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far?*, „Fordham Law Review" 1989, t. 57, s. 617–635.

Czubik A., *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Kraków 2013.

Greenwald G., *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.

Jaskiernia J., *Ustawodawstwo a sądowa kreacja prawa w Stanach Zjednoczonych Ameryki*, PiP 1994, nr 9, s. 28–38.

Kerr O., *The Fourth Amendment in cyberspace: can encryption create a resonable expectation of privacy?*, „Connecticut Law Review" 2001, t. 33, s. 503–533.

Kiełtyka A., *Podstawa faktyczna zatrzymania i przeszukania według Czwartej Poprawki do Konstytucji Stanów Zjednoczonych Ameryki*, „Prokuratura i Prawo" 2006, nr 2, s. 91–106.

Kowalik-Bańczyk K., *Prawo do prywatności w Internecie – kolizja między amerykańskim i europejskim modelem ochrony*, [w:] J. Jaskiernia (red.), *Amerykański system ochrony praw człowieka*, (red.), Toruń 2015.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016.

Kuisz J., *Konstytucja w sytuacjach zagrożenia bezpieczeństwa państwa na tle teorii R.A. Posnera*, PiP 2013, nr 12, s. 46–59.

Lee C., *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, „Mississippi Law Journal" 2012, t. 81, s. 1–50.
Levin A., Nicholson M., *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, „University of Ottawa Law & Technology Journal" 2005, t. 2, s. 357–395.
Makarzec P., *Amerykańska koncepcja „Prawa do prywatności" jako fundament prawnej ochrony danych osobowych*, [w:] J. Jaskiernia (red.), *Amerykański system ochrony praw człowieka*, Toruń 2015.
Mornin J., *NSA Metadata Collection And The Fourth Amendment*, „Berkeley Technology Law Journal" 2014, t. 29, s. 985–1006.
Motyka K., *Prawo do prywatności i dylematy współczesnej ochrony praw człowieka na przykładzie Stanów Zjednoczonych*, Lublin 2006.
Mucha B., *Data mining a współczesny kształt prawa do prywatności w Stanach Zjednoczonych Ameryki*, [w:] J. Jaskiernia (red.), *Efektywność europejskiego systemu ochrony praw człowieka. Ewolucja i uwarunkowania europejskiego systemu ochrony praw człowieka*, Toruń 2012.
Posner R., *Privacy, Surveillance, and Law*, „The University of Chicago Law Review" 2008, t. 75, s. 245–260.
Richards N., *The Dangers of Surveillance*, „Harvard Law Review" 2013, t. 126, s. 1958–1964.
Rojszczak M., *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" 2017, nr 2, s. 159–188.
Schwartz P., *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, „Stanford Law Review" 2000, t. 52, s. 1559–1572.
Schwartz P., *The EU-U.S. Privacy Collision: A Turn To Institutions And Procedures*, „Harvard Law Review" 2013, t. 126, s. 1966–2009.
Sloan L., *ECHELON and The Legal Restraints on Signals Intelligence: A Need for Reevaluation*, „Duke Law Journal" 2001, t. 50, s. 1467–1510
Volokh E., *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, „Stanford Law Review" 2000, t. 52, s. 1049–1124.
Warren S., Brandeis L., *The Right to Privacy*, „Harvard Law Review" 1890, nr 5, s. 193–220.

PRYWATNOŚĆ W EPOCE WIELKIEGO BRATA: PODSTAWY PROWADZENIA PROGRAMÓW MASOWEJ INWIGILACJI W SYSTEMIE PRAWNYM STANÓW ZJEDNOCZONYCH

Streszczenie

Celem artykułu jest omówienie podstaw prawnych dla prowadzenia rozbudowanych programów inwigilacji elektronicznej przez służby specjalne Stanów Zjednoczonych. Zagadnienie zostało omówione zarówno poprzez analizę prawa stanowionego, jak również aktualnego orzecznictwa sądów federalnych. Przedstawiano i wyjaśniono kluczowe normy konstytucyjne, a także wprowadzone rozwiązania ustawowe (w szczególności ustawę o nadzorze nad wywiadem obcym) oraz rozporządzenia wykonawcze prezydenta (w tym rozporządzenie 13355). Odniesienie rozważań do ram prawnych obowiązujących w państwach UE posłużyło nie tylko do zobrazowania pojawiających się różnic, ale również do poszukiwania przestrzeni dla wypracowania wspólnych standardów prowadzenia działań inwigilacji elektronicznej, czy szerzej – ochrony prywatności w cyberprzestrzeni – w sposób akceptowalny przez obie strony.

Słowa kluczowe: masowa inwigilacja, inwigilacja elektroniczna, wywiad elektroniczny, FISA, FISC, EO 13335

PRIVACY IN THE ERA OF BIG BROTHER: GROUNDS FOR MASS SURVEILLANCE PROGRAMMES IN THE LEGAL SYSTEM OF THE UNITED STATES

Summary

The purpose of the article is to discuss the legal framework for extensive electronic surveillance activities conducted by the United States intelligence services. This problem was discussed both through the analysis of statutory law as well as current federal court case law. Key constitutional provisions as well as federal acts (in particular the Foreign Intelligence Surveillance Act) and presidential executive orders (including EO 13355) were presented and explained. The reference to the legal framework of EU was used not only to illustrate the emerging differences, but also as an attempt to search for space for developing common standards for conducting electronic surveillance activities, or more broadly – for protecting privacy in cyberspace – in a manner that could be accepted by both US and EU.

Keywords: bulk surveillance, electronic surveillance, signal intelligence, FISA, FISC, EO 13335

Cytuj jako:

Rojszczak M., *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych [Privacy in the era of Big Brother: grounds for mass surveillance programmes in the legal system of the United States]*, „Ius Novum" 2019 (Vol. 13) nr 1, s. 235–265. DOI: 10.26399/iusnovum.v13.1.2019.13/m.rojszczak

Cite as:

Rojszczak, M. (2019) '*Privacy in the era of Big Brother: grounds for mass surveillance programmes in the legal system of the United States*'. *Ius Novum* (Vol. 13) 1, 235–265. DOI: 10.26399/iusnovum.v13.1.2019.13/m.rojszczak