PRZECIWDZIAŁANIE TERRORYZMOWI A PRAWO DO PRYWATNOŚCI W PRZEPISACH WSPÓLNOTOWYCH UNII EUROPEJSKIEJ

Hanna Rutkiewicz[1]

Streszczenie. Rozwijające się przez stulecia koncepcje wolności i godności człowieka wpłynęły na ujmowanie pojęcia prywatności, a także kształt jej formalnoprawnej ochrony. W opracowaniu podjęto analizę wpływu przepisów wspólnotowych służących przeciwdziałaniu terroryzmowi, funkcjonujących w Unii Europejskiej, na sferę prywatną jednostki, skupiając się przede wszystkim na problematyce ochrony danych osobowych. W tym kontekście jednym z zadań, zarówno prawodawstwa, jak i polityki wspólnotowej, stało się obecnie złagodzenie antynomii dostrzegalnej pomiędzy potrzebami w zakresie zapewnienia bezpieczeństwa i ochrony społeczeństwa przed terroryzmem z jednej strony a zabezpieczeniem jednostki i społeczności przed coraz częstszymi naruszeniami prywatności związanymi z wykonywaniem regulacji antyterrorystycznych z drugiej strony.

W Rezolucji z dnia 14 grudnia 2011 r. w sprawie unijnej polityki przeciwdziałania terroryzmowi Parlament Europejski zaapelował do państw członkowskich o przedstawienie raportów dotyczących efektywności działań oraz środków służących przeciwdziałaniu terroryzmowi, podkreślając, iż znaczącym elementem polityki antyterrorystycznej stała się inwigilacja obywateli i zastosowanie metod: śledzenia i wyszukiwania, masowego gromadzenia danych osobowych, technologii wykrywania i identyfikacji, eksploracji danych i tworzenia profili, oceny ryzyka czy analizy behawioralnej. W dokumencie wskazano na wątpliwą skuteczność tego typu narzędzi, przy niewielkiej efektywności wymiany informacji przez uprawnione podmioty. Wymienione środki, według opinii Parlamentu, powodują przesunięcie ciężaru dowodu na obywatela. W rezolucji zawarto również opinię, że nie powinna mieć miejsca sytuacja, w której działania antyterrorystyczne naruszają prawa zawarte w Karcie Praw Podstawowych Unii Europejskiej. W tym niezwykle istotne jest, że wymienione metody mają wpływ na sferę wolności obywatelskich[2].

W dokumencie wyrażono również ubolewanie z powodu utraty okazji na wyjaśnienie, w jaki sposób niektóre instrumenty UE w zakresie przeciwdziałania terroryzmowi, m.in.: zatrzymywanie danych, dane dotyczące przelotu pasażera (dane PNR) i tzw. porozumienie Swift, wpisują się w unijną strategię przeciwdziałania terroryzmowi. Jak okaże się dwa lata po uchwaleniu omawianej rezolucji – w roku 2013, kontrowersyjna jeszcze przed podpisaniem umowa między Unią Europejską

---

[1] Magister stosunków międzynarodowych Wydziału Prawa i Administracji Uniwersytetu Kardynała Wyszyńskiego w Warszawie.

[2] Rezolucja Parlamentu Europejskiego z dnia 14 grudnia 2011 r. w sprawie unijnej polityki przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania (2010/2311(INI); www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-20110577+0+DOC+XML+V0//PL.

a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu danych z komunikatów finansowych w celu śledzenia środków finansowych należących do terrorystów (TFTP – Terrorist Finance Tracking Program)[3] – dotycząca dostępu do baz Swift (Society for Worldwide Interbank Financial Telecommunication – Stowarzyszenie na rzecz Światowej Międzybankowej Telekomunikacji Finansowej), stanie się tym razem jedną z podstaw afery związanej z podejrzeniami o niezgodne z prawem wykorzystywanie przez Amerykańską Agencję Bezpieczeństwa Narodowego (National Security Agency – NSA) bankowych danych obywateli Unii Europejskiej[4].

W związku z zaistniałą sytuacją rodzą się pytania o to, w jaki sposób Unia Europejska chroni dane osobowe swoich obywateli; czy, a jeśli tak, to w jaki sposób przepisy służące przeciwdziałaniu terroryzmowi naruszają ich prawo do prywatności? Czy regulacje antyterrorystyczne, w tym umowa TFTP, są instrumentami skutecznie zapewniającym bezpieczeństwo, czy raczej furtką do szerokiej inwigilacji i naruszeń sfery prywatnej?

Artykuł 2 Traktatu o Unii Europejskiej stanowi: „Unia opiera się na wartościach poszanowania godności osoby ludzkiej, wolności, demokracji, równości, państwa prawnego, jak również poszanowania praw człowieka, w tym praw osób należących do mniejszości. Wartości te są wspólne Państwom Członkowskim w społeczeństwie opartym na pluralizmie, niedyskryminacji, tolerancji, sprawiedliwości, solidarności oraz na równości kobiet i mężczyzn”[5]. Z kolei art. 7 Karty Praw Podstawowych Unii Europejskiej brzmi: „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się”[6]. W art. 1 tegoż dokumentu stwierdza się: „Godność człowieka jest nienaruszalna. Musi być szanowana i chroniona”. W kwestii praw i wolności obywatelskich, w tym prawa do prywatności, Unia Europejska korzysta przede wszystkim z dorobku Europejskiej Konwencji Praw Człowieka, ale także z konstytucyjnych tradycji państw członkowskich[7].

Koncepcje prywatności kształtujące się na przestrzeni wieków wpłynęły na zakres i sposób ujęcia prawa do ochrony tej sfery życia, pośród innych praw oraz wolności człowieka i obywatela, tak we współczesnych ustawodawstwach państwowych, jak i w prawie międzynarodowym. Pojęcie prywatności łączy się z ideą godności i wolności jednostki, co ma także odzwierciedlenie w przytoczonych wyżej przepisach. Jak zauważa A. Sakowicz, to właśnie niezbywalna i przyrodzona każdemu człowiekowi

[3] Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów programu śledzenia środków finansowych należących do terrorystów; Dz.U. L 195/5 z 2010 r.

[4] *Afera NSA: dane bankowe pod nadzorem służb*?, http://www.europarl.europa.eu/news/pl/news-room/content/20130923STO20630/html/Afera-NSA-dane-bankowe-pod-nadzorem-s%C5%82u%C5%BCb

[5] Traktat o Unii Europejskiej, Dz.U. C 83 z 30.3.2010.

[6] Dz.Urz. UE 2012 C 326.

[7] J. Hołda, *Prawa człowieka. Zarys wykładu*, Warszawa 2008, s. 73.

godność ludzka jest źródłem dobra, jakim jest prywatność. Jest ona wartością pierwotną, transcendentną, zawsze towarzyszącą człowiekowi. Nie może być naruszona przez inną osobę ani prawodawcę. Żadne działania nie są w stanie pozbawić osoby ludzkiej godności[8]. Jest to cecha pierwotna w stosunku do państwa, nie jest przez nie nadawana, a zadanie władz publicznych to zapewnienie ochrony, poszanowanie jej i innych osobistych praw jednostki, takich jak: niezależność, prywatność – praw o charakterze wolnościowym[9].

Uznanie podmiotowości osób względem państwa wpłynęło na postrzeganie prywatności jako prawa do dysponowania sobą, w tym wolności od zewnętrznej ingerencji. Ujmowanie wolności jednostki jako stanu pierwotnego i naturalnego sięga starożytności, jednak dopiero w XVII wieku powszechna stawała się koncepcja o nieodzowności pogodzenia prawa naturalnego z prawem stanowionym[10].

Na rozwój koncepcji prywatności wpłynęły poglądy przedstawicieli szkoły prawa natury – Hugona Grocjusza, Thomasa Hobbesa, Johna Locke'a, którzy twierdzili, że człowiek rodzi się jako istota wolna, zdolna do samodzielnego kierowania swoimi czynami[11]. Beniamin Constant, francuski polityk i filozof żyjący na przełomie XVIII i XIX w., był z kolei prekursorem ujmowania prywatności jako prawa do: odosobnienia, zacisza domowego, intymności[12]. Wolność, jak wskazywał, nie jest pochodną „natury ludzkiej", lecz wynika z indywidualności każdej jednostki[13]. Podobnie tę kwestię postrzegał John Stuart Mill, który w traktacie *O wolności* pisał: „(...) Każdy jest odpowiedzialny przed społeczeństwem jedynie za tę część swego postępowania, która dotyczy innych. W tej części, która dotyczy wyłącznie jego samego, jest absolutnie niezależny; ma suwerenną władzę nad sobą, swoim ciałem i umysłem. To więc jest właściwą dziedziną ludzkiej wolności (...)"[14]. Jego zdaniem wolność zawiera w sobie: prawo do układania życia zgodnie z własnymi przekonaniami, zrzeszenia się jednostek w danym interesie, który nie przynosi szkody innym[15]. Ponadto Mill, mając świadomość istnienia konfliktu pomiędzy interesem zbiorowym i indywidualnym, przyznawał, że istnieją okoliczności, w których państwo może naruszać prywatność obywateli, m.in. w celu zachowania sprawiedliwości czy bezpieczeństwa społecznego[16].

Istotny wkład w dzieje myśli dotyczącej wolności jednostki, w tym prawa do prywatności, wnieśli również: dziewiętnastowieczny filozof Herbert Spencer czy

---

[8] *Prawnokarne gwarancje prywatności*, Kraków 2006, s. 20, 22.

[9] A. Mendis, *Prawo do prywatności a interes publiczny*, Kraków 2006, s. 51.

[10] J. Braciak, op. cit., s. 15.

[11] A. Sakowicz, op. cit., s. 23.

[12] J. Braciak, op. cit., s. 16-17.

[13] W. Szyszkowski, *Beniamin Constant. Doktryna polityczno-prawna*, Warszawa-Poznań, Toruń 1984, s. 154, za: J. Braciak, op. cit., s. 17.

[14] L. Dubel i inni, *Historia doktryn politycznych i prawnych. Materiały źródłowe*, Lublin 2003, s. 343.

[15] Ibidem, s. 343.

[16] I. Berlin, John Stuart Mill, *O wolności*, Warszawa 1999, s. 260, za: Braciak, op. cit., s. 19.

dwudziestowieczni myśliciele – Isaiah Berlin i John Rawls. I tak, podobnie jak poprzednicy, Spencer uważał, że granicą wolności jednostki jest wolność innej osoby. Według niego, wartość ta powinna być mierzona względnie małą liczbą narzuconych jednostce ograniczeń[17]. Isaiah Berlin z kolei podzielił wolność na: pozytywną, określaną jako prawo człowieka „do czegoś", i negatywną, czyli wolność „od czegoś". Jego zdaniem powinien istnieć taki obszar życia, który nie podlega jakiejkolwiek ingerencji. Problemem jest rozdzielenie sfery prywatnej od tej, nad którą istnieje władza publiczna[18]. John Rawls rozważał pojęcie wolności w kontekście ograniczeń prawnych i konstytucyjnych. Jak zauważał, podstawowe wolności tworzą system, który należy oceniać jako całość, a ich definiowanie ma służyć ich państwowej ochronie. Sformułował następującą zasadę: „Każda osoba ma mieć równe prawo do jak najszerszego systemu równych podstawowych wolności możliwego do pogodzenia z podobnym systemem wolności dla innych"[19].

Jak wskazuje się w literaturze przedmiotu, impuls do rozwinięcia formalnoprawnej ochrony prywatności powstał w 1890 r. w Stanach Zjednoczonych po opublikowaniu artykułu *The Right to Privacy*, którego autorami byli prawnicy bostońskiej kancelarii – S.D. Warren i L.D. Brandeis[20]. Praca powstała w związku z pojawieniem się informacji na temat ślubu córki S.D. Warrena w prasie brukowej. Oparto ją o decyzje angielskich i amerykańskich sądów w sprawach o m.in.: pogwałcenie tajemnicy, naruszenie własności czy umowy dorozumianej. Prawnicy wskazali, że omówione wyroki łączy jedna podstawa, jaką jest prawo do prywatności[21]. Ich zdaniem państwo powinno chronić tę wartość ze względu na jej samoistny charakter (*per se*)[22]. Obok wolności i własności zawiera się ona w *corpus iuris* przyrodzonych i indywidualnych praw jednostki[23]. Artykuł został zaliczony do najbardziej wpływowych i najczęściej cytowanych publikacji prawniczych[24], wpłynął na orzeczenia sądów, tworzenie aktów prawnych czy poglądów zawieranych w literaturze fachowej. Mimo że pojawiało się wiele głosów krytycznych dotyczących pracy Warrena i Brandiesa, już niedługo po publikacji jej w „Harvard Law Review", do dziś jest ona kluczowa dla badaczy prawa do prywatności.

Jako konkluzja obrad Nordyckiej Konferencji Prawników z 1967 r. powstała definicja prywatności ujmująca prawo do niej jako fundamentalne dobro każdej osoby. Chroni ono jednostkę przed innymi osobami, społeczeństwem i władzą.

[17] *Historia doktryn politycznych i prawnych. Materiały źródłowe*, op. cit, s. 350.
[18] A. Sakowicz, op. cit., s. 31.
[19] J. Rawls, *Teoria sprawiedliwości*, PWN, Warszawa 2009, s. 107.
[20] S.D. Warren, L.D Brandeis, *The Right to privacy*, „Harvard Law Review" 1890, vol. IV, s. 198.
[21] J. Braciak, op. cit., 30-31.
[22] W. Sokolewicz, *Prawo do prywatności*, (w:) *Prawa człowieka w Stanach Zjednoczonych*, red. L. Pastusiak, Książka i Wiedza, Warszawa 1985, s. 252.
[23] A. Sakowicz, op. cit., s. 63.
[24] Ibidem, s. 57.

Istnieje konieczność zapewnienia każdemu prawnej ochrony przed ingerencją w życie domowe, rodzinnie i prywatne, moralną lub intelektualną wolność przed niekorzystną interpretacją czynów lub słów, przed działalnością związaną z kontrolowaniem, szpiegowaniem, łamaniem tajemnicy zawodowej. Za naruszenie prywatności uznano: naruszenie miejsca zamieszkania, rozpowszechnianie nieprawdziwych oświadczeń na temat danej osoby, kontrolowanie jej za pomocą aparatury podsłuchowej lub przy wykorzystaniu innego sprzętu elektronicznego, jak również nękanie przez dziennikarzy[25].

W literaturze prywatność najczęściej ujmowana jest przez wyodrębnienie sfer życia osobistego lub elementów wymagających ochrony przed zewnętrzną ingerencją.

S. Scoglio wyróżnił następujące jej elementy: 1) prywatność fizyczną (materialną) – związaną z naruszeniami w postaci rewizji czy konfiskaty mienia, 2) prywatność decyzyjną, 3) prywatność informacyjną, służącą kontrolowaniu dostępu do osobistych informacji, 4) prywatność powiązaną z przeżyciami wewnętrznymi jednostki, kształtującą jej osobowość[26]. Zdaniem W.L. Prossera, prawo do prywatności chroni przed czterema rodzajami naruszeń, mianowicie przed: 1) ingerencją w sferę odosobnienia, a także samotności i spraw prywatnych, 2) publicznym ujawnieniem kłopotliwych faktów z życia prywatnego, 3) ujawnieniem faktów stawiających daną osobę w fałszywym świetle, 4) przywłaszczeniem sobie czyjegoś wizerunku lub nazwiska[27]. Z kolei E.J. Bloustein zaznaczył problem związany z różnicą między naruszeniem prywatności a naruszeniem dobrego imienia lub czci. Jego zdaniem w pierwszym przypadku chodzi o dobro nienaruszalnej osobowości, w drugim zaś o reputację danej osoby[28]. Po analizie francuskiego orzecznictwa i decyzji Państwowej Komisji ds. Informatyki i Wolności, inny badacz tematu – J. Robert – stwierdził, że elementami tworzącymi prywatność są: anonimowość – dotycząca m.in. danych o zdrowiu, stanie majątku, uwieczniania, rozpowszechniania wizerunku i głosu, ochronę informacji osobowych; poszanowanie zachowań jednostki – co związane jest z: zajmowanym przez nią terytorium, wizerunkiem kreowanym wobec innych osób, autentyczną osobowością, gdzie naruszeniem jest np. brak zgody na zmianę wpisu dotyczącego płci w aktach stanu cywilnego po dokonaniu medycznej zmiany; poszanowanie relacji międzyludzkich dotyczących: tajemnicy komunikowania się, szacunku dla stosunków panujących w rodzinie, poszanowania uczuć jednostki[29].

---

[25] J. Braciak, op. cit., s. 39-40.

[26] S. Scoglio, *Transforming Privacy: A Transpersonal Philosophy of Rights*, Praeger 1998; za: J.D. Sieńczyło-Chlabicz, *Naruszenie prywatności osób publicznych przez prasę*, Kraków 2006, s. 78.

[27] A. Mendis, op. cit., s. 60.

[28] Ibidem, s. 61.

[29] J. Robert, *Droits de l'homme et libertés fondamentales*, Montchrestien 1994**,** s. 369; za: A. Mendis, op. cit., s. 63.

W Europie elementy ochrony prywatnej sfery życia jednostki, choć nieujmowane jeszcze jako prawo do prywatności, pojawiały się już w XIV w., m.in. w ogłoszonym przez angielskiego króla Edwarda III w 1361 r. *Akcie o sędziach pokoju*. Przewidziano w nim karę aresztu za podsłuchiwanie lub podglądanie. We Francji zaś, w roku 1384, wydano wyrok za naruszenie nietykalności mieszkania (sprawa *I. de S. et ux. v. W de S.*)[30]. W sprawie Semayne v. Gresham z 1604 r. ława królewska wysunęła tezę, że dom dla każdej osoby jest twierdzą[31]. Toczący się w porządku *common law* proces Pope v. Curl z 1741 r. dotyczył z kolei publikacji przez księgarza listów od znanych literatów. W orzeczeniu stwierdzono, że słowa są własnością ich autora, a rozpowszechnianie korespondencji bez jego zgody jest naruszeniem prawa[32]. Z kolei w 1776 r. w Szwecji został przyjęty *Access to Public Records Act*, głoszący, że informacje powinny być wykorzystywane w sposób uzasadniony. W roku 1858 natomiast zakazano we Francji publikowania treści z życia osobistego obywateli[33].

W Unii Europejskiej kompetencje w sądowych sprawach, dotyczących praw człowieka, posiada Trybunał Sprawiedliwości Unii Europejskiej z siedzibą w Luksemburgu. Działania Trybunału dotyczą dokonywania wykładni prawa UE w celu zapewnienia jego stosowania w taki sam sposób we wszystkich państwach unijnych, jak również rozstrzygania sporów między rządami Unii a jej instytucjami. Ponadto rozpatruje sprawy wnoszone przez osoby fizyczne, przedsiębiorstwa i organizacje, które uważają, że ich prawa zostały naruszone przez instytucje UE[34]. W ramach działalności organu orzekano także w sporach dotyczących prawa do prywatności. Uznano m.in., że niedopuszczalne jest naruszenie poufności korespondencji pomiędzy prawnikiem a klientem, z zastrzeżeniem, że informacje wymieniane między nimi dotyczą prawa do obrony (*AM & S Europe Ltd. V. Commision of European Communities* – 155/79, ECR 1982, s. 1575). Trybunał połączył także ochronę danych osobowych z prywatnością, podkreślając istotność poszanowania życia prywatnego przez sektor telekomunikacyjny (*Commision of European Communities v. Grand Duchy of Luxembourg* oraz *Commision of European Communities v. French Republic*)[35].

Normy dotyczące przetwarzania danych osobowych na terenie Unii Europejskiej zawarte są w: *Konwencji Rady Europy (108) o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych*, w *Rozporządzeniu (WE) nr 45/2001 Parlamentu Europejskiego i Rady o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych*, czy w *Decyzji ramowej Rady 2008/977/WSiSW*

[30] J. Braciak, op. cit., s. 32, 35.
[31] A. Sakowicz, op. cit., s. 55, 81.
[32] J. Braciak, op. cit., s. 32.
[33] A. Sakowicz, op.cit., s. 55.
[34] http://europa.eu/about-eu/institutions-bodies/court-justice/index_pl.htm
[35] J. Braciak, op. cit., s. 104-105.

z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, a przede wszystkim w *Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych*.

Postanowienia dyrektywy 95/46/WE mają służyć pogodzeniu dwóch tendencji. Pierwsza z nich dotyczy ochrony podstawowych praw i wolności osób fizycznych, prawa do prywatności w procesie przetwarzania danych osobowych. Druga wyraża się w jednakowym i swobodnym we wszystkich państwach członkowskich, w tym pomiędzy nimi, obiegiem tych danych.

W dokumencie stwierdza się: „Zasady ochrony praw i wolności jednostek, szczególnie prawa do prywatności, które zawarte są w niniejszej dyrektywie, utrwalają i umacniają zasady wyrażone w Konwencji Rady Europy z dnia 28 stycznia 1981 r. w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych”[36].

Artykuł 7 brzmi: „dane osobowe mogą być przetwarzane tylko wówczas gdy osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę”. Przepis ten przewiduje także przypadki, kiedy pomimo braku zgody podmiotu zainteresowanego, informacje o nim mogą być przetwarzane. Dotyczy to sytuacji, w których:
„b) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy; lub
c) przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega; lub
d) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą; lub
e) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane; lub
f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1”[37].

Dyrektywa wprowadza zakaz przetwarzania specjalnych kategorii danych, tzn. dotyczących: pochodzenia rasowego lub etnicznego, opinii politycznych, przekonań religijnych, filozoficznych, przynależności do związków zawodowych czy

[36] Dz.U. L 281 z 23.11.1995.
[37] Ibidem.

przetwarzania danych dotyczących zdrowia i życia seksualnego. Liczba wyjątków od zakazu powoduje jednak, że w pewnym sensie traci on na znaczeniu[38].

Dokument planuje się zastąpić *Rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych*, co wynika z przyjęcia przez Komisję z początkiem roku 2012 r. pakietu zmian regulacji UE w zakresie ochrony danych. Akt ten obowiązywać ma bezpośrednio w krajach członkowskich i nie będzie potrzeby wydawania innych regulacji prawnych wdrażających zawarte przepisy do porządku krajowego. Dzięki temu zaistniałaby możliwość pełnej harmonizacji prawa materialnego na terenie Unii Europejskiej w powyższym zakresie[39].

Zwana również retencyjną, *Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności* oraz zmieniająca dyrektywę 2002/58/WE[40] powstała po zamachach w Madrycie w 2004 r. i Londynie w 2005. Wprowadzono ją w celu ułatwienia działań przy zwalczaniu przestępczości, w szczególności terroryzmu.

Regulacje zawarte w dokumencie stosuje się do danych o ruchu i lokalizacji, które dotyczą osób fizycznych, prawnych oraz do powiązanych z nimi danych niezbędnych do identyfikacji abonenta lub zarejestrowanego użytkownika, z wyłączeniem treści komunikatów elektronicznych, w tym informacji uzyskiwanych przy użyciu sieci łączności elektronicznej (art. 1 ust. 2).

Zgodnie z dyrektywą państwa członkowskie zapewniają zatrzymywanie takich informacji jak:

- dane niezbędne do ustalenia źródła połączenia, w tym: numer nadawcy połączenia, nazwisko i adres abonenta lub zarejestrowanego użytkownika, przyznany identyfikator użytkownika, nazwisko i adres abonenta lub zarejestrowanego użytkownika, do którego w momencie połączenia należał adres IP;
- dane niezbędne do ustalenia odbiorcy połączenia, w tym: wybierany numer odbiorcy połączenia telefonicznego i internetowego, a w przypadku dodatkowych usług, takich jak przekierowanie lub przełączanie połączeń, numery, na które połączenie jest przekierowane, nazwisko, adres abonenta;
- dane niezbędne do określenia narzędzia komunikacji lub tego, co może służyć za narzędzie komunikacji;
- dane niezbędne do określenia daty, godziny i czasu trwania połączenia;

[38] J. Braciak, op. cit., s. 107.
[39] http://www.giodo.gov.pl/1520143/.
[40] Dz.U. L 105 z 13.4.2006.

- dane niezbędne do określenia rodzaju połączenia;
- dane niezbędne do identyfikacji lokalizacji urządzenia komunikacji ruchomej, w tym pozwalające ustalić położenie geograficzne telefonów komórkowych.

Państwa członkowskie mają gwarantować, że wymienione kategorie danych są zatrzymywane na czas nie krótszy niż 6 miesięcy oraz nie dłużej niż dwa lata od daty połączenia. Wszystkie dane z wyjątkiem tych, które zostały udostępnione, a także zachowane, powinny zostać zniszczone pod koniec okresu zatrzymania. Istnieją jednak wyjątki od tego przepisu. Przedłużenie zatrzymania danych o wyznaczony okres może nastąpić w szczególnych przypadkach. Państwo musi wówczas niezwłocznie powiadomić Komisję i pozostałe państwa członkowskie oraz wskazać przyczyny przyjęcia takich środków.

Obecnie Trybunał Sprawiedliwości UE ocenia, czy dyrektywa retencyjna, na podstawie której powstały w krajach członkowskich ogromne bazy danych telekomunikacyjnych, ingeruje w sposób proporcjonalny w prawa podstawowe. Orzeczenie w tej sprawie znane będzie w 2014 r. Postępowanie toczy się w związku z pytaniami o tę kwestię sądów z Irlandii i Austrii, które uznały, że wynikająca z dyrektywy ingerencja w prywatność jest nieproporcjonalna[41].

Grupa Robocza Art. 29[42], składająca się z krajowych organów ochrony danych osobowych w Unii Europejskiej, opublikowała raport dotyczący wdrożenia Dyrektywy 2006/24/WE. Stwierdzono w nim, że implementacja dokumentu w większości państw członkowskich odbyła się z naruszeniem prawa.

Ustalono m.in., że:

- dochodziło do zatrzymywania i przekazywania służbom przez usługodawców danych o ruchu, niezgodnie z postanowieniami dyrektywy;
- postanowienia aktu nie są przestrzegane;
- brakuje rzetelnej oceny dotyczącej spełnienia założonych w dyrektywie celów (ułatwień walki z przestępczością, w szczególności z terroryzmem);
- czas zatrzymywania danych różni się i wynosi w różnych krajach od sześciu miesięcy do dwóch lat;
- wstrzymuje się więcej danych, niż pozwala na to dyrektywa, niektóre państwa pozwalają na zatrzymywanie danych na temat treści komunikacji elektronicznej;
- dane geolokalizacyjne wstrzymuje się w szerszym zakresie, niż pozwala na to dyrektywa[43].

[41] http://panoptykon.org/blog/11072013

[42] www.ec.europa.eu/justice/data-protection/article-29/index_en.htm

[43] www.panoptykon.org/content/wdro-enie-dyrektywy-retencyjnej-w-ue-narusza-prawo-raport-grupy-roboczej-art-29.

Na terenie Polski w związku z wprowadzeniem Dyrektywy 2006/24/WE funkcjonują przepisy pozwalające służbom w niemal dowolny sposób pobierać billingi[44]. Jak wskazuje podpisany 12 czerwca 2013 r. raport Najwyższej Izby Kontroli: *Informacja o wynikach kontroli uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy prawo telekomunikacyjne*[45], pozyskiwanie danych telekomunikacyjnych jest istotną ingerencją w sferę praw i wolności obywatelskich. W raporcie czytamy: „(...) Dzisiejsza technologia pozwala w stopniu niespotykanym nigdy wcześniej gromadzić olbrzymią ilość danych o każdym obywatelu – nie tylko, z kim, kiedy i jak często się kontaktował, czy gdzie w danym momencie przebywał, ale również np. o numerze posiadanego przez niego rachunku bankowego czy karty płatniczej. Połączenie tych danych z informacjami dostępnymi w innych źródłach (bazy administracji państwowej, portale społecznościowe itp.) oraz wykorzystanie zaawansowanych narzędzi informatycznych do ich analizy (np. w celu tworzenia profili zachowań) powoduje, że sfera naszej prywatność uległa znaczącemu ograniczeniu (…)". Co warte jednak zaznaczenia, w dokumencie stwierdza się, że zbierane dane zawierają istotne ślady i dowody, które są wykorzystywane do zapobiegania przestępstwom, do ich ścigania, a także zagwarantowania wymiaru sprawiedliwości w sprawach karnych. Zgodnie ze sprawozdaniem służb wykorzystanie przedmiotowych informacji doprowadziło do skazania za przestępstwa w sprawach, w których bez zatrzymywania danych nie byłoby możliwości ich rozwikłania. Wskazano również, że środek ten doprowadził do oczyszczenia z zarzutów szeregu niewinnych osób, bez konieczności stosowania instrumentów bardziej ingerujących w prywatność – podsłuchów (kontroli i utrwalania rozmów) czy też przeszukań w miejscu zamieszkania. Raport NIK zawiera również informacje o błędach popełnianych przez operatorów. Kontrolerzy NIK spotkali się z sytuacjami, w których udostępniano służbom więcej danych niż wnioskowano. Zdarzało się, że operatorzy w odpowiedzi na pytania o połączenia wychodzące przekazywali informacje o wszystkich połączeniach. Wykryto również, że systemy teleinformatyczne łączące operatorów ze służbami nie zawsze pozwalają na identyfikację osoby żądającej danych. Ponadto służby nie zawsze poddają się prawnemu ograniczeniu, które nie pozwala pytać im o dane starsze niż 12 miesięcy (do stycznia tego roku pochodzące z ostatnich dwóch lat)[46]. W opinii NIK w Polsce nie funkcjonuje niezależny organ weryfikujący zasadność pozyskiwania i wykorzystania

[44] Zgodnie z raportem NIK, do służb w szczególności uprawnionych do pobierania danych retencyjnych zalicza się: Policję, Straż Graniczną, Żandarmerię Wojskową, Agencję Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Służbę Kontrwywiadu Wojskowego, Służbę Celną.

[45] http://www.nik.gov.pl/plik/id,5421,vp,7038.pdf

[46] http://panoptykon.org/wiadomosc/po-kontroli-billingowej-nik-najwyzszy-czas-na-zmiany.

billingów. Nie istnieje również system, który zbierałby informacje, w jakim zakresie pozyskuje się te dane. Wpływa to w konsekwencji na rzetelność wiedzy na ten temat[47].

Dotycząca form współpracy transgranicznej, w szczególności zwalczania terroryzmu, przestępczości międzynarodowej i nielegalnej imigracji, Konwencja z Prüm została podpisana 27 maja 2005 r.[48] przez siedem państw – Belgię, Niemcy, Francję, Luksemburg, Holandię, Austrię i Hiszpanię. Finlandia, Rumunia, Włochy, Portugalia, Słowenia, Szwecja, Bułgaria, Grecja i Polska[49] oficjalnie zadeklarowały chęć przystąpienia do konwencji. Do systemu uregulowań prawnych Unii Europejskiej na mocy Decyzji 2008/615/WSiSW przeniesiono podstawowe elementy konwencji z dnia 27 maja 2005 r.[50]

Decyzja zawiera przepisy dotyczące:

- zautomatyzowanego dostępu do profili DNA, danych daktyloskopijnych i niektórych krajowych rejestracyjnych danych pojazdów,
- wymogów dostarczania danych w związku z istotnymi wydarzeniami,
- warunków dostarczania informacji mających na celu zapobieganie przestępstwom terrorystycznym,
- warunków i trybu intensyfikowania transgranicznej współpracy policji[51].

Zgodnie z decyzją, na państwa UE nakłada się obowiązek stworzenia krajowych zbiorów analiz DNA służących wykrywaniu przestępstw. Dane obejmujące niekodującą część DNA – referencyjne, a także oznaczenie referencyjne, które nie dają możliwości identyfikacji osoby, mogą być udostępniane innym państwom UE w celu zautomatyzowanego przeszukania. Porównywanie profili DNA odbywa się za pośrednictwem krajowych punktów kontaktowych i dotyczy indywidualnych przypadków. Informacje o profilu DNA muszą być przygotowane zgodnie ze wspólną normą ochrony danych, tak by państwo członkowskie występujące z wnioskiem otrzymało odpowiedź wskazującą głównie HIT (trafienie) lub NO-HIT (brak trafienia), a także numer identyfikacyjny w przypadku trafienia. Jeśli stwierdzona zostanie zgodność, instytucja przeszukująca otrzymuje dane referencyjne. W przypadku braku zgodności zapytane państwo członkowskie może zostać zobowiązane do ustalenia profilu DNA wskazanej osoby. Ponadto państwa członkowskie zobowiązane są do zapewnienia dostępu do danych referencyjnych z krajowych zautomatyzowanych systemów identyfikacji daktyloskopijnej (AFIS). Potwierdzenie zgodności danych

[47] http://www.nik.gov.pl/aktualnosci/nik-o-billingach.html

[48] *Dokument roboczy w sprawie decyzji Rady dotyczącej intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną*, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, 10.04.2007; www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824pl.pdf

[49] T. Aleksandrowicz, *Terroryzm międzynarodowy*, op. cit., s. 135.

[50] www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0616:PL:NOT

[51] www.europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_pl.htm

odbywa się poprzez krajowy punkt kontaktowy zapytującego państwa członkowskiego. Krajowe punkty kontaktowe mają również możliwość dostępu do pewnych danych rejestracyjnych pojazdów, poprzez zautomatyzowane przeszukanie on-line.

W celu zapobiegania przestępstwom terrorystycznym, jednak tylko w indywidualnych przypadkach, jak również gdy okoliczności dają podstawy do przypuszczania, że popełnione zostaną przestępstwa, państwa członkowskie mogą wymieniać się następującymi informacjami dotyczącymi wskazanych osób: data, miejsce urodzenia, nazwisko i imiona, wykaz okoliczności dotyczących możliwości popełnienia przestępstwa.

Państwa członkowskie mogą również wprowadzić wspólne patrole i podejmować wspólne operacje w celach ochrony porządku, bezpieczeństwa i prewencji kryminalnej na terytorium danego państwa UE. Wyznaczeni funkcjonariusze i pracownicy z wysyłającego państwa biorą udział w działaniach państwa przyjmującego, a odpowiedzialność za ich działania ponoszą właściwe władze państwa przyjmującego.

Początek współpracy europejskiej służącej zwalczaniu terroryzmu w ramach Wspólnoty Europejskiej związany jest z powołaniem w 1975 r. w Rzymie, podczas spotkania ministrów spraw wewnętrznych państw członkowskich, tzw. grupy TREVI (Terrorisme – Radicalisme – Extremisme – Violence – International). Jej celem miało być koordynowanie działań w zakresie zapobiegania i zwalczania terroryzmu. Grupa funkcjonowała do wejścia w życie Traktatu z Maastricht, czyli do dnia 1 listopada 1993 r.[52] Pozostałe wspólne działania w omawianej sferze mieściły się w tzw. Systemie Informacji Schengen, a następnie obejmowały włączenie dorobku Schengen do I i III Filara Wspólnej Polityki Bezpieczeństwa[53]. 3 grudnia 1998 r. Rada przyjęła Plan działań Rady i Komisji w sprawie sposobu jak najskuteczniejszego wdrożenia postanowień Traktatu z Amsterdamu w dziedzinie przestrzeni wolności, bezpieczeństwa i sprawiedliwości[54].

Przed dniem 11 września 2001 r. Unia Europejska podejmowała także działania w omawianej sferze, uchwalając w szczególności:

- Decyzję Rady z dnia 3 grudnia 1988 r. w przedmiocie objęcia działalnością Europolu przestępstw przeciwko życiu, zdrowiu, wolności osobistej, mieniu, popełnionych lub takich, których popełnienie jest prawdopodobne podczas działań terrorystycznych;
- Wspólne Działanie Rady (96/610/WSiSW) z dnia 15 października 1996 r. w przedmiocie tworzenia i utrzymywania spisu na temat szczególnych uprawnień antyterrorystycznych, umiejętności i wiedzy specjalistycznej ułatwiających współpracę antyterrorystyczną pomiędzy państwami członkowskimi Unii Europejskiej;

[52] T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008, s. 80.
[53] Ibidem.
[54] Ibidem.

- Wspólne Działanie Rady (98/428/WSiSW) z dnia 29 czerwca 1998 r. w przedmiocie utworzenia Europejskiej Sieci Sądowej, określające zadania Sieci w zakresie przestępstw terrorystycznych;
- Zalecenie Rady z dnia 9 grudnia 1999 r. w przedmiocie współpracy w zwalczaniu finansowania grup terrorystycznych[55].

Po 11 września 2001 r. zwalczanie terroryzmu zaliczono do priorytetowych zadań Unii Europejskiej, tworząc nowe rozwiązania, które odwołują się zarówno do dorobku ONZ, jak i Rady Europy, a także uzupełniano i modyfikowano regulacje już istniejące[56].

W ten sposób 28 grudnia 2001 r. z mocy Rozporządzenia Rady (WE) nr 2580/2001 w sprawie szczególnych środków restrykcyjnych stosowanych przeciwko niektórym osobom i podmiotom, mających na celu zwalczanie terroryzmu, Rada formułuje listę osób i podmiotów związanych z działalnością terrorystyczną, co daje podstawę do zamrożenia środków finansowych (funduszy) pozostających w ich dyspozycji. Również 28 grudnia 2001 r. przyjęte zostało Wspólne Stanowisko Rady (2201/930/WPZiB), zawierające wezwanie państw członkowskich Unii Europejskiej do jak najszybszego przystąpienia do konwencji sektorowych[57].

Z kolei Decyzja Rady (2003/48/WSiSW) z dnia 19 grudnia 2002 r. w sprawie wprowadzenia w życie szczególnych środków w odniesieniu do współpracy policyjnej i sądowej w celu zwalczania terroryzmu zalicza zwalczanie terroryzmu do zadań Europolu, Eurojustu i wspólnych zespołów śledczych[58].

Szczególną uwagę należy zwrócić na Decyzję Ramową Rady w sprawie zwalczania terroryzmu (2002/475/WSiSW) z dnia 13 czerwca 2002 r., formułującą odrębną, uniwersalną definicję przestępstwa o charakterze terrorystycznym i zalecającą wprowadzenie we wszystkich państwach członkowskich zbliżonej definicji[59].

W myśl powołanej Decyzji Ramowej przestępstwa o charakterze terrorystycznym stanowią następujące czyny: ataki na życie, które mogą spowodować śmierć; ataki na integralność cielesną osoby; porwania lub branie zakładników; spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, włącznie ze zniszczeniem systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, mienia publicznego lub mienia prywatnego, mogące zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze; zajęcie statku lub innego środka transportu publicznego lub towarowego; wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie broni, materiałów wybuchowych lub jądrowych, broni

[55] Ibidem.
[56] Ibidem, s. 82.
[57] Ibidem.
[58] *Terroryzm międzynarodowy*, op. cit., s. 82.
[59] Dz.U. L 164, 22 czerwca 2002 r., s. 003-007.

biologicznej lub chemicznej, jak również badania i rozwój broni biologicznej i chemicznej; uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, których rezultatem jest zagrożenie życia ludzkiego; zakłócenie lub przerwy w dostawach wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, których rezultatem jest zagrożenie życia ludzkiego; grożenie popełnieniem wyżej wymienionych czynów, pod warunkiem że (obie nw. przesłanki muszą być spełnione łącznie): czyny te, ze względu na swój charakter i kontekst, mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej; zostały one popełnione w celu: poważnego zastraszenia ludności lub bezprawnego zmuszenia rządu albo organizacji międzynarodowej do działania lub zaniechania, lub poważnej destabilizacji, lub zniszczenia podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych państwa lub organizacji międzynarodowej[60].

W myśl powołanej Decyzji Ramowej przestępstwo związane z terroryzmem to:

- kradzież kwalifikowana lub wymuszenie w zamiarze popełnienia czynu określonego w art. l ust. 1 Decyzji,
- fałszowanie dokumentów urzędowych w zamiarze popełnienia takiego czynu oraz w związku z udziałem w działaniach grupy terrorystycznej[61].

Za grupę terrorystyczną powołana Decyzja uznaje grupę zorganizowaną, składającą się z co najmniej z trzech osób, ustanowioną na przestrzeni czasu i działającą w uzgodniony sposób, w celu popełnienia przestępstw terrorystycznych, przy czym grupa taka nie jest tworzona przypadkowo w celu natychmiastowego popełnienia przestępstwa, lecz charakteryzuje się formalnym określeniem ról członków grupy, ciągłością członkostwa lub rozwiniętą strukturą[62].

Decyzją Ramową Rady (2008/919/WSiSW) z dnia 18 listopada 2008 r.[63] znowelizowano powołaną Decyzję, rozszerzając katalog przestępstw związanych z terroryzmem o: publiczne nawoływanie do popełnienia przestępstw terrorystycznych, rekrutację na potrzeby terroryzmu, szkolenie terrorystyczne[64].

Także dnia 13 czerwca 2002 r. Rada przyjęła Decyzję Ramową w sprawie Europejskiego Nakazu Aresztowania i procedury przekazywania osób między państwami członkowskimi (2002/584/WSiSW)[65], zwaną Europejskim Nakazem Aresztowania, mającą stanowić swoiste uzupełnienie już obowiązujących między państwami członkowskimi traktatów dotyczących ekstradycji, m.in. Europejskiej Konwencji o ekstradycji wraz z protokołami dodatkowymi, Europejskiej Konwencji o zwalczaniu

[60] *Terroryzm międzynarodowy*, op. cit., s. 83.
[61] Ibidem.
[62] Ibidem.
[63] Dz.U. L 330/21.
[64] Szerzej: T. Aleksandrowicz, *Nowelizacja Decyzji Ramowej w sprawie zwalczania terroryzmu*, „Terroryzm" 2009, nr 2.
[65] Dz.U. L 190, 18 lipca 2002, s. 001-0020.

terroryzmu w części dotyczącej ekstradycji. Powołana Decyzja Ramowa ma na celu przede wszystkim uproszczenie procedur ekstradycyjnych poprzez zastąpienie ich przekazaniem, co jest równoznaczne z formalną rezygnacją z procedur ekstradycyjnych na poziomie współpracy między rządami na rzecz sprecyzowanych procedur współpracy bezpośrednio między organami sądowymi[66].

Z dniem 12 sierpnia 2012 r. weszła w życie[67] umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych[68]. Obowiązuje ona na terenie całej Unii Europejskiej i służyć ma skutecznemu zapobieganiu terroryzmowi i poważnej przestępczości międzynarodowej, a także zwalczaniu tych zjawisk.

W umowie określono obowiązki stron w odniesieniu do warunków, na jakich dane PNR (Passenger Name Record) mogą być przekazywane, przetwarzane i wykorzystywane oraz chronione. Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Department of Homeland Security – DHS) ma obowiązek przekazywania danych i informacji analitycznych uzyskanych z tych danych do organów ścigania i organów sądowych UE (art. 4).

DHS musi zapewnić wprowadzenie w życie odpowiednich środków technicznych i rozwiązań organizacyjnych służących ochronie danych osobowych i informacji osobowych zawartych w danych PNR przed przypadkowymi, niezgodnymi z prawem czy nieuprawnionymi: zniszczeniem, ujawnieniem, utratą, zmianami, dostępem, przetwarzaniem lub wykorzystywaniem (art. 5). W przypadku gdy dojdzie do naruszenia prywatności, DHS powiadamia w stosownych przypadkach osoby fizyczne, których to dotyczy, w celu ograniczenia ryzyka szkód związanych z nieupoważnionym ujawnieniem danych osobowych i informacji osobowych oraz by wprowadzić techniczne środki zaradcze. Ponadto dane PNR przechowywane są w aktywnej bazie danych przez okres nieprzekraczający pięciu lat. Po upływie pierwszych sześciu miesięcy dane PNR mają być anonimizowane oraz maskowane. Dostęp do tej aktywnej bazy danych posiada ograniczona liczba specjalnie upoważnionych funkcjonariuszy.

Po upływie okresu przechowywania w bazie aktywnej dane PNR mają być przenoszone do bazy archiwalnej na nie więcej niż dziesięć lat. Archiwalna baza danych musi być dodatkowo kontrolowana, a liczba pracowników upoważnionych do korzystania z niej ograniczona. Istnieje możliwość ponownego przywrócenia elementów umożliwiających identyfikację w bazie archiwalnej, w związku z działaniami organów ścigania. W tym przypadku danym PNR mogą być ponownie przywracane

[66] *Terroryzm międzynarodowy*, op. cit., s. 83-84.

[67] www.lex-pol.pl/2012/08/umowa-miedzynarodowa-w-sprawie-przelotu-miedzy-unia-europejska-a-usa-weszla-w-zycie/

[68] DZ.U. L 215/5; www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:215:0005:0014:PL:PDF.

elementy umożliwiające identyfikację osoby, ale jedynie na okres nieprzekraczający pięciu lat (art. 8 ust. 3).

Dane PNR mogą być wykorzystywane i przetwarzane w indywidualnych przypadkach, gdy jest to niezbędne z uwagi na poważne zagrożenie, a także w celu ochrony żywotnych interesów jakiejkolwiek osoby fizycznej lub jeżeli wynika to z nakazu sądu. DHS może wykorzystywać i przetwarzać dane PNR w celu identyfikacji osób, które po przyjeździe do Stanów Zjednoczonych lub przed opuszczeniem tego państwa zostałyby poddane dokładniejszemu przesłuchaniu lub sprawdzeniu, albo takich, co do których może zachodzić konieczność dalszego sprawdzenia (art. 5 ust. 3).

W związku z umową przewoźnicy są zobowiązani do przekazywania DHS danych PNR drogą elektroniczną, najpierw na 96 godzin przed planowym odlotem, a także w czasie rzeczywistym albo w drodze ustalonej liczby rutynowych zaplanowanych transferów, zgodnie z wymogami DHS (art. 14 ust. 3).

Zgodnie z umowami lub uzgodnieniami w zakresie działania organów ścigania i udostępniania informacji, zawartymi między Stanami Zjednoczonymi a którymkolwiek z państw członkowskich UE, Europolem, Eurojustem, DHS przekazuje właściwym organom państw UE oraz Europolowi i Eurojustowi właściwe informacje analityczne uzyskane z danych PNR. Dotyczy to spraw będących przedmiotem wyjaśniania, dochodzenia lub śledztwa, w celu zapobiegania przestępstwom terrorystycznym i powiązanym przestępstwom lub przestępczości międzynarodowej, a także w celu ich wykrywania, prowadzenia dochodzeń lub śledztw, lub ścigania w Unii Europejskiej (art. 18 ust. 1).

Biorąc pod uwagę uprawnienia Departamentu Bezpieczeństwa Wewnętrznego i jego współpracę z innymi agendami USA w zakresie stosowania systemów i aplikacji wykorzystujących dane biometryczne[69], a także przetwarzanie i wykorzystanie przez DHS danych PNR, należy stwierdzić, że instytucja ta jest w posiadaniu następujących

[69] DHS jest odpowiedzialny za następujące federalne systemy wykorzystujące technologie biometryczne:
1. US-VISIT – partnerem DHS w realizacji tego programu jest Departament Stanu. US-VISIT służy kompleksowej kontroli granicznej i ma zastosowanie do niemal wszystkich podróżnych odwiedzających USA. Pobieranie danych biometrycznych polega na wykonywaniu cyfrowej fotografii twarzy i skanowaniu odcisków obu palców wskazujących. Procedury dokonuje się często, jeszcze przed przyjazdem do Stanów Zjednoczonych, w ramach procesu wizowego w kraju macierzystym podróżnego. Ma to na celu sprawdzenie danych biometrycznych w bazach zawierających dane osób podejrzewanych o działalność terrorystyczną i przestępców, pozwala też na wykorzystanie ich do powtórnej autentyfikacji;
2. Visa Waiver Program (VWP) – w ramach tego programu określono wymagania dla paszportów biometrycznych osób, które nie podlegają obowiązkowi wizowemu w Stanach Zjednoczonych. Paszporty osób korzystających z programu VWP wydane po 26 października 2006 r. powinny zawierać zintegrowany układ scalony. Umożliwia on rejestrację, a także odczyt wskazanych informacji biometrycznych i danych podróżnego. Osoby pochodzące z krajów, które nie podlegają obowiązkowi wizowemu i legitymujące się paszportami niespełniającymi tych wymagań, nie są objęte programem VWP. W praktyce podlegają obowiązkowi uzyskania wizy;

informacji dotyczących podróżujących do USA obywateli Unii Europejskiej: biometryczne zdjęcie twarzy, odciski palców, obraz tęczówki oka, numer rezerwacji PNR, data rezerwacji/wystawienia biletu, data(-y) planowanej podróży, imię (imiona) i nazwisko (-a), dostępne informacje dotyczące programów dla stałych klientów i dodatkowych korzyści (na przykład darmowe bilety, zamiana biletu z klasy ekonomicznej na wyższą itd.), inne nazwiska podane w danych PNR, w tym liczba podróżnych wynikająca z danych PNR, wszystkie dostępne informacje kontaktowe (w tym źródło informacji), wszystkie dostępne informacje o płatnościach/fakturowaniu (nie obejmuje to innych szczegółów transakcji dotyczących karty kredytowej lub konta

3. Nexus – program eksperymentalnie wdrażany na lotnisku w Vancouver, dotyczący podróżnych z Kanady, którzy często odwiedzają USA. Polega on na korzystaniu z zautomatyzowanych kiosków, gdzie osoby dokonują weryfikacji swojej tożsamości biometrycznej m.in. z użyciem obrazu tęczówki oka.

Inne programy realizowane przez agendy rządu federalnego USA, związane z kwestią danych biometrycznych, służące celom ochrony granic lub związane z działaniami organów ścigania i sił zbrojnych Stanów Zjednoczonych, to:

- Programy badawcze Narodowego Instytutu Standaryzacji i Technologii (NIST – agendy Departamentu Handlu) – dotyczące aspektów weryfikacji tożsamości i identyfikacji osób za pomocą zdjęć twarzy, odcisków palców i obrazu tęczówki oka. NIST zajmuje się opracowaniem standardów technicznych stosowanych przez inne federalne agendy. Po rekomendacji są one wdrażane w różnego rodzaju systemach informacji kryminalnej, zawierających dane biometryczne;
- Programy Departamentu Obrony (United States Department of Defense) – przede wszystkim Automated Biometrics Identification System – ABIS, stanowiący bazę danych wraz z narzędziami programowymi i aplikacjami dostępowymi. Są one stosowane w celu przechowywania, wieloaspektowego wyszukiwania, a także kojarzenia różnego rodzaju danych biometrycznych osób, które znalazły się w kręgu zainteresowania organów stojących na straży bezpieczeństwa narodowego USA. Z kolei Centrum Fuzji Biometrycznych – Biometrics Fusion Center (BFC) jest wyspecjalizowaną jednostką, w której m.in. testuje się i bada najnowsze komercyjne technologie biometryczne, a następnie wdraża się je na potrzeby jednostek podległych Departamentowi Obrony;
- Programy Departamentu Sprawiedliwości (United States Department of Justice) – program IAFIS (Integrated Automated Fingerprint Identification System), wykorzystywany przez Federalne Biuro Śledcze do zautomatyzowanego porównywania odcisków palców, jak również program NGI (Next Generation Identification – Identyfikacja Nowej Generacji), funkcjonalne rozszerzenie IAFIS. Podstawowym zadaniem NGI jest wspomaganie wykrywania działalności kryminalnej i terrorystycznej poprzez stosowanie zaawansowanych narzędzi identyfikacji biometrycznej i nowoczesnych technik informacji kryminalnej.

Programy Departamentu Stanu (The United States Department of State) – oprócz wskazanego już wcześniej uczestnictwa w programie US-VISIT Departament Stanu odpowiedzialny jest za wdrożenie paszportu biometrycznego, ostatecznie wprowadzonego do produkcji w drugiej połowie 2006 roku. Amerykański paszport biometryczny jest wydawany obywatelom od sierpnia 2006 i spełnia wymagania stawiane w programie WVP paszportom biometrycznym z krajów obcych. Posiada zdjęcie cyfrowe posiadacza dokumentu, a na ostatniej stronie paszportu zakodowane dane; przyt. za: K. Krassowski i I. Sołtyszewski, *Zastosowania biometrii – przegląd kluczowych programów i rozwiązań w zakresie ochrony państwa*, „Problemy Kryminalistyki" 2007, nr 255.

i niepowiązanych z transakcją dotyczącą podróży), trasa podróży dla określonych danych PNR, biuro podróży/agencja turystyczna, informacje o wspólnej obsłudze połączeń, dane o statusie podróży pasażera (w tym potwierdzenia, stan odprawy biletowo-bagażowej), informacje o biletach, w tym numer biletu, bilety w jedną stronę i automatycznie skalkulowana taryfa (cena biletu), wszystkie informacje o bagażu, informacje o miejscu, w tym numer miejsca w samolocie, uwagi ogólne, w tym OSI (informacje o innych usługach, jak loty przesiadkowe), SSI i SSR (informacje lub prośby dotyczące usług specjalnych, np. dzieci bez dorosłego towarzystwa, osoby starsze wymagające opieki, wybór dań, preferencje dotyczące miejsc w samolocie, informacja o stanie zdrowia podróżnych), wszystkie informacje zebrane w systemie danych pasażera przekazywanych przed podróżą (APIS – Zaawansowany System Informacji o Pasażerze), np. nazwisko, obywatelstwo, numer paszportu, data urodzenia, wszystkie dotychczasowe zmiany danych PNR.

Uwzględniając możliwość łączenia i analizy danych biometrycznych z danymi PNR, w tym potencjalne profilowanie tych danych, należy zwrócić uwagę na wyjątkowo szeroki dostęp amerykańskich służb do informacji o obywatelach UE. Istotna dla tej kwestii jest również wspomniana na samym początku umowa podpisana w 2010 r. pomiędzy Unią Europejską i Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych z komunikatów finansowych przez Unię Europejską Stanom Zjednoczonym. Dokument ten przewiduje przekazywanie informacji finansowych dotyczących płatności, celem wykorzystania ich w programie śledzenia środków finansowych należących do terrorystów (TFTP). Komunikaty finansowe dotyczące płatności przechowywane są przez Stowarzyszenie na Rzecz Światowej Międzybankowej Telekomunikacji Finansowej (SWIFT). Co ważne, międzynarodowa grupa ekspertów odpowiedzialna za ocenę realizacji porozumienia SWIFT w 2011 r. doszła do wniosku, że jego funkcjonowanie prowadzi do systemowych naruszeń europejskich standardów ochrony danych osobowych[70]. Umowa TFTP została przyjęta po tzw. „aferze SWIFT", kiedy to opinia publiczna dowiedziała się, że informacje na temat wszystkich operacji przekazywania danych SWIFT były przechowywane w „lustrzanej" bazie danych w USA. Okazało się również, że władze USA nakazały SWIFT przekazanie wnioskowanych danych finansowych. Negocjacje pomiędzy belgijskim organem ochrony danych, Unią Europejską a władzami USA sprawiły, że Stowarzyszenie podjęło decyzję o przeniesieniu „dublowania" informacji o europejskich operacjach do Europy. Miały miejsce także negocjacje między UE i władzami USA, mające służyć znalezieniu prawnego rozwiązania dotyczącego

[70] *PRISM, SWIFT, PNR, SAFE HARBOUR, czyli jak Amerykanie próbują zrozumieć świat*, http://panoptykon.org/biblio/prism-swift-pnr-safe-harbour-czyli-jak-amerykanie-probuja-zrozumiec-swiat.

przekazywania danych osobowych do celów śledzenia środków finansowych należących do terrorystów, po czym umowa TFTP została podpisana[71].

Z kolei we wrześniu 2013 r. po doniesieniach prasowych o włamaniach przez Amerykańską Agencję Bezpieczeństwa Narodowego (NSA) na serwery SWIFT, w trakcie posiedzenia Komisji Praw Obywatelskich Parlamentu Europejskiego (LIBE) poinformowano, że komisarz ds. wewnętrznych Cecilia Malmström zwróciła się do administracji USA o udzielenie wyjaśnień w tej sprawie. Komisarz postanowiła przeprowadzić konsultacje, które zostały przewidziane w porozumieniu dotyczącym programu śledzenia środków finansowych należących do terrorystów. Jej zdaniem, w przypadku wykrycia naruszeń umowy, z pewnością dojdzie do zawieszenia obowiązywania tego dokumentu[72].

Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, a także umowa TFTP to instrumenty ingerujące i naruszające prawo do prywatności obywateli UE. Ponadto dane osobowe cudzoziemców, znajdujące się w bazach na terenie USA, nie są objęte Privacy Act z 1974 r. i nie wchodzą w zakres polityki ochrony prywatności[73]. Jak zaznaczono w raporcie Fundacji Panoptykon[74] „(…) wykorzystywanie danych PNR oznacza automatyczne profilowanie każdego podróżnego jako potencjalnie podejrzanego o terroryzm. Na podstawie ograniczonych danych z systemów rezerwacyjnych wyciągane są kontrowersyjne wnioski, a na czarną listę można trafić przez pomyłkę lub przypadek (np. w Wielkiej Brytanii w wyniku analizy danych PNR na czarnych listach znaleźli się m.in. wegetarianie, osoby wykupujące rezerwacje last minute i pasażerowie podróżujący w jedną stronę) (…)". Z kolei w przypadku umowy TFTP, zobowiązanie do wyrażenia zgody Europolu na otrzymanie przez służby amerykańskie dostępu do danych bankowych osób podejrzanych o terroryzm lub wspieranie terroryzmu w praktyce nie jest respektowane[75].

---

[71] *www.giodo.gov.pl/plik/id_p/2182/j/pl/*

[72] http://www.europarl.europa.eu/news/pl/news-room/content/20130923STO20630/html/Afera-NSA-dane-bankowe-pod-nadzorem-s%C5%82u%C5%BCb

[73] Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, dokument roboczy 2, *Przyszłe porozumienie międzynarodowe między Unią Europejską (UE) a Stanami Zjednoczonymi Ameryki (USA) w sprawie ochrony danych osobowych przekazywanych i przetwarzanych do celów działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych, w tym terroryzmu, w ramach współpracy policyjnej i sądowej w sprawach karnych,* z dn. 10.09.2010; www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dt/830/830120/830120pl.pdf

[74] PRISM, SWIFT, PNR, *Safe Harbour, czyli jak Amerykanie próbują zrozumieć świat*, http://panoptykon.org/biblio/prism-swift-pnr-safe-harbour-czyli-jak-amerykanie-probuja-zrozumiec-swiat

[75] Ibidem.

Przy rozbudowanym systemie przeciwdziałania terroryzmowi, który niewątpliwie służy bezpieczeństwu obywateli, zadaniem Unii Europejskiej jest to, by ingerencja w prywatność, wynikająca z przyjętych regulacji, była jak najmniejsza. Ważne jest, by jak w najmniejszym stopniu przepisy te dotykały osób niebędących terrorystami, co, jak wskazuje zakres i sposoby stosowania środków opisanych w niniejszej pracy, nie zawsze przyświeca ich twórcom i wykonawcom. Przeciwdziałanie terroryzmowi powinno więc w maksymalny sposób godzić prawa, w tym prawo do prywatności, z wprowadzaniem niezbędnych środków prawnych i pozaprawnych.

Choć problematyka niniejszego opracowania koncentruje się na przepisach ingerujących w tzw. prywatność informacyjną, należy zauważyć, że to właśnie dane osobowe są elementem prywatnej sfery życia, niezwykle wrażliwym na naruszenia. Wszelkie czynności związane z ich generowaniem, przetwarzaniem i profilowaniem znajdują się bowiem poza zasięgiem osób, których dotyczą.

LITERATURA:

1. T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008.
2. I. Berlin, *John Stuart Mill. O wolności*, Warszawa 1999.
3. J. Braciak, *Prawo do prywatności*, Wydawnictwo Sejmowe, Warszawa 2004.
4. L. Dubel i inni, *Historia doktryn politycznych i prawnych. Materiały źródłowe*, Lublin 2003.
5. K. Krassowski, I. Sołtyszewski, *Zastosowania biometrii – przegląd kluczowych programów i rozwiązań w zakresie ochrony państwa*, „Problemy Kryminalistyki" 2007, nr 255.
6. A. Mendis, *Prawo do prywatności a interes publiczny*, Kraków 2006.
7. J. Rawls, *Teoria sprawiedliwości*, PWN, Warszawa 2009.
8. A. Sakowicz, *Prawnokarne gwarancje prywatności*, Kraków 2006.
9. S. Scoglio, *Transforming Privacy: A Transpersonal Philosophy of Rights*, Praeger 1998.
10. J.D. Sieńczyło-Chlabicz, *Naruszenie prywatności osób publicznych przez prasę*, Kraków 2006.
11. W. Sokolewicz, *Prawo do prywatności*, (w:) *Prawa człowieka w Stanach Zjednoczonych*, red. L. Pastusiak, Warszawa 1985.
12. W. Szyszkowski, *Beniamin Constant. Doktryna polityczno-prawna*, Warszawa-Poznań, Toruń 1984.
13. D. Warren, L.D. Brandeis, *The Right to privacy*, Harvard Law Review 1890, vol. IV.
14. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-20110577+0+DOC+XML+V0//PL
15. www.europarl.europa.eu/news/pl/news-room/content/20130923STO20630/html/Afera-NSA-dane-bankowe-pod-nadzorem-s%C5%82u%C5%BCb
16. www.europa.eu/about-eu/institutions-bodies/court-justice/index_pl.htm
17. www.giodo.gov.pl/1520143/

18. www.panoptykon.org/blog/11072013
19. www.ec.europa.eu/justice/data-protection/article-29/index_en.htm
20. www.panoptykon.org/content/wdro-enie-dyrektywy-retencyjnej-w-ue-narusza-prawo-raport-grupy-roboczej-art-29
21. www.nik.gov.pl/plik/id,5421,vp,7038.pdf
22. www.panoptykon.org/wiadomosc/po-kontroli-billingowej-nik-najwyzszy-czas-na-zmiany
23. www.nik.gov.pl/aktualnosci/nik-o-billingach.html
24. www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824pl.pdf
25. www.eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0616:PL:NOT
26. www.europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_pl.htm
27. www.lex-pol.pl/2012/08/umowa-miedzynarodowa-w-sprawie-przelotu-miedzy-unia-europejska-a-usa-weszla-w-zycie/
28. www.eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:215:0005:0014:PL:PDF
29. pa.eu/meetdocs/2009_2014/documents/libe/dt/830/830120/830120pl.pdf
30. www.panoptykon.org/biblio/prism-swift-pnr-safe-harbour-czyli-jak-amerykanie-probuja-zrozumiec-swiat
31. www.giodo.gov.pl/plik/id_p/2182/j/pl/
32. www.europarl.euro

COUNTERING TERRORISM AND THE RIGHT TO PRIVACY ACCORDING TO THE EUROPEAN UNION'S LEGISLATION

Abstract. Concepts of freedom and human dignity have evolved over the centuries. They contributed to the recognition of the concept of privacy and its legal and formal model of privacy protection. Study examines the impact of the European Union anti-terrorism legislation on the privacy of individuals. It focuses primarily on the issue of personal data protection. Ensuring the safety and protection of the public against terrorism leads in practice to frequent breaches of privacy. Both the legislation and the EU community policy intended to ensure that the necessary protection against terrorism as little as possible infringe individual rights, including the right to privacy.