Teka Kom. Praw. – OL PAN, t. XI, 2018, nr 2, 443–458

UZYSKIWANIE I WYKORZYSTYWANIE DLA CELÓW BEZPIECZEŃSTWA INFORMACJI O OSOBIE A PRAWA JEDNOSTKI (ZAGADNIENIA WYBRANE)

Adam Taracha

Katedra Kryminalistyki i Prawa Dowodowego
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
Polska
https://orcid.org/0000-0001-8630-2496

Streszczenie. Autor omawia związek między uprawnieniami służb policyjnych do uzyskiwania, gromadzenia i przetwarzania informacji o osobach w ramach czynności operacyjno-rozpoznawczych koniecznych do zapewnienia bezpieczeństwa i porządku publicznego a ochroną praw jednostki. Zgodnie z art. 8 ust. 2 EKPC, dopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa do prywatności w przypadkach przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi m.in. na bezpieczeństwo publiczne oraz zapobieganie przestępstwom. Zakres tej ingerencji powinien ulec poszerzeniu (objąć szerszy obszar) w sytuacji, gdy zagrożenie bezpieczeństwa państwowego, bezpieczeństwa publicznego lub dobrobytu gospodarczego kraju wzrasta w wyniku działań terrorystycznych. Wzrost zagrożenia przestępczością (w tym atakami terrorystycznymi, na skalę nieznaną dotychczas w Europie) nakazuje szczególny umiar w działaniach legislacyjnych ograniczających możliwości służb policyjnych i służb specjalnych w zakresie działań operacyjnych.

Słowa kluczowe: czynności operacyjno-rozpoznawcze, uzyskiwanie, gromadzenie i przetwarzanie informacji o osobie, służby policyjne, służby specjalne, prawo do prywatności, terroryzm

Zagrożenie współczesną przestępczością (w tym zorganizowaną i terroryzmem) z jednej strony i postęp techniczny (szczególnie w obszarze informatyzacji) z drugiej, spowodowało konieczność wprowadzenia nowych instytucji prawnych, które umożliwiłyby organom ścigania skuteczną walkę z przestępczością. Szerokie uprawnienia w zakresie gromadzenia i przetwarzania informacji, które otrzymały służby policyjne i specjalne (w tym także poprzez dostęp do baz danych innych organów i instytucji) mogą budzić obawy, że wprowadzone instytucje zbyt mocno wkraczają w obszar praw człowieka. Z drugiej strony, jest oczywiste, że obecnie trudno byłoby skute-

cznie zwalczać przestępczość bez wykorzystania możliwości, jakie stwarza współczesna technika, z której zdobyczy korzystają także przestępcy.

W związku z uchwaleniem nowelizacji prawa policyjnego w dniu 15 stycznia 2016 r.[1] oraz w czasie prac nad ustawą o zwalczaniu terroryzmu z dnia 10 czerwca 2016 r.[2] pojawiły się głosy, że służby policyjne i służby specjalne otrzymały zbyt szerokie uprawnienia wkraczające w obszar praw człowieka.[3] Nie ulega jednak wątpliwości, że służby odpowiedzialne za bezpieczeństwo państwa muszą mieć dostęp do informacji niezbędnych do wykonywania ich ustawowych zadań. Konflikt między prawami jednostki, w tym prawem do prywatności, a działaniami służb policyjnych zdobywającymi informacje (w tym także w sposób tajny) wydaje się nieunikniony[4]. Trudno jest bowiem pogodzić sprzeczne cele, którymi są efektywne zwalczanie przestępczości (w szczególności terroryzmu i przestępczości zorganizowa-

[1] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, Dz. U. poz.147.

[2] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz. U. poz. 904 z późn. zm.

[3] Zob. m.in. Wniosek Rzecznika Praw Obywatelskich z dnia 18 lutego 2016 r o stwierdzenie niezgodności z Konstytucją Rzeczypospolitej niektórych przepisów ustaw policyjnych (znowelizowanych ustawą z 15 stycznia 2016 r.); Fundacja Panoptykon, *Ustawa antyterrorystyczna wchodzi w życie – co się zmienia* (1.07.2016), w: https://panoptykon.org/wiadomości/ustawa-antyterrorystyczna-wchodzi-w-życie-co-się-zmienia [dostęp:15.03.2018]; *Stanowisko Fundacji Panoptykon w sprawie projektu ustawy o działaniach antyterrorystycznych* (10.05.2016), w: obserwatoriumdemokracji.pl/wp-content/…/Panoptykon_uat_opinia_10.05.2016.pdf [dostęp:15.03.2018]; *Rzecznik Praw Obywatelskich skarży ustawę antyterrorystyczną do Trybunału Konstytucyjnego* (11.07.2016), w: https://www.rpo.gov.pl/pl/content/rzecznik-praw-obywatelskich-skarży-ustawę-antyterrorystyczną-do-trybunału-konstytucyjnego [dostęp:13.03.2018]; *Wniosek Rzecznika Praw obywatelskich o stwierdzenie niezgodności z Konstytucją Rzeczypospolitej niektórych przepisów ustawy z 10 czerwca 2016 r. o działaniach antyterrorystycznych*, w: https://www.rpo.gov.pl/pl/tagi/wniosek-do-tk [dostęp:12.03.2018]; M. Szuniewicz–Stępień, *Działania operacyjno-rozpoznawcze w ustawie antyterrorystycznej a europejski standard ochrony praw człowieka – wybrane zagadnienia*, w: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, red. W. Zubrzycki, K. Jałoszyński, A. Babiński, Wyższa Szkoła Policji w Szczytnie, Szczytno 2016, s. 335–368.

[4] Orzecznictwo Europejskiego Trybunału Praw Człowieka, nie kwestionując prawa państw stron konwencji w zakresie poddawania środkom tajnej kontroli osób objętych jurysdykcją tych państw, stwierdza że nie jest to prawo nieograniczone. Warunkiem stosowania tych środków jest ich ustawowe uregulowanie opatrzone gwarancjami zapobiegającymi nadużyciom, a stosowanie tych środków powinno podlegać dostatecznej kontroli Orzecznictwo Trybunału jest tu niezwykle konsekwentne poczynając już od sprawy z 1978 r. – Klass, seria A, nr 28, EHRR 214; zob. m.in. W. Hermeliński, *Bezpieczeństwo publiczne a prawo jednostki do prywatności*, „Palestra" 1–2 (2013), s. 17–20.

nej) przy użyciu tajnych działań (często z użyciem podstępu) i zapewnienie obywatelom prawa do prywatności. Należy jednak pamiętać, że jednym z podstawowych zadań państwa jest zapewnienie bezpieczeństwa i porządku publicznego oraz ochrona życia, zdrowia i mienia obywateli[5].

Europejska Konwencja Praw Człowieka w przyjętej zasadzie poszanowania prawa i praworządności obliguje państwa strony do ograniczenia działań służb policyjnych i służb specjalnych tylko do sytuacji dozwolonych i dostatecznie uzasadnionych przez prawo krajowe[6].

Największe zaniepokojenie opinii publicznej budziły (i nadal budzą) działania służb policyjnych i specjalnych określane jako kontrola operacyjna[7] i tzw. prowokacja policyjna[8], gdyż stanowią najmocniejszą ingerencję w prawa człowieka. Znacznie mniejsze zainteresowanie towarzyszy uprawnieniom tych służb do uzyskiwania, gromadzenia i przetwarzania informacji (poza uzyskanymi w trybie kontroli operacyjnej), chociaż, jak się wydaje, rola tych uprawnień wraz z postępującym w szybkim tempie rozwojem techniki informatycznej i tworzonych baz danych – będzie stale rosnąć. Właśnie tym zagadnieniom poświęcony będzie dalszy wywód.

W Polsce służby policyjne i służby specjalne mogą korzystać zarówno z informacji, które uzyskały, zgromadziły i przetworzyły w ramach własnych działań, jak też zgromadzonych i przechowywanych w bazach danych przez inne organy, instytucje rządowe i samorządowe oraz przez podmioty

---

[5] Obowiązek zapewnienia obywatelom, przez organy państwa, właściwego poziomu bezpieczeństwa wynika wprost z przepisów Konstytucji RP. Natomiast w doktrynie i orzecznictwie niemieckim obowiązek ten („czynienia niezbędnych przedsięwzięć dla zachowania publicznego spokoju, bezpieczeństwa i porządku oraz dla odpierania zapowiadającego się niebezpieczeństwa grożącego zbiorowości lub pojedynczym jej członkom") wywodzono z osiemnastowiecznego ustawodawstwa (norma zawarta w par.10 II. 17 Landrechtu z 1794 r.). Zob. szerzej: W. Szwarc, *Zarys ewolucji pojęcia „Policji" w Monarchii Pruskiej w XVII i XIX w.*, w: *Wybrane problemy teorii i praktyki państwa i prawa*, red. H. Groszyk, L. Dubel, Wydawnictwo UMCS, Lublin 1986, s. 117–133.

[6] Przepisy tego prawa powinny być dostępne dla wszystkich, jasno określać zasady ich stosowania i być ściśle przestrzegane w praktyce. Zob. m.in. Sprawa Sunday Times, seria A nr 30,2 EHRR 245, 49 orzeczenia; P. Duffy, *Policja a Konwencja o ochronie praw człowieka i podstawowych wolności*, w: *Prawa człowieka a Policja. Problemy teorii i praktyki*, red. A. Rzepliński, Wydawnictwo Centrum Szkolenia Policji w Legionowie, Legionowo 1994, s. 254–255.

[7] Czynność ta przeprowadzana jest niejawnie i obejmuje takie działania, jak kontrola rozmów telefonicznych, kontrola korespondencji (w tym także elektronicznej) i przesyłek oraz tajny podgląd i podsłuch w pomieszczeniach.

[8] Zwana także transakcją pozorną, obejmująca „zakup kontrolowany" i „kontrolowaną łapówkę".

prywatne. Polskie ustawodawstwo reguluje obecnie dość szczegółowo problematykę uzyskiwania, gromadzenia i przetwarzania informacji w tym także w sposób niejawny[9]. Należy jednak zauważyć, że są to regulacje stosunkowo świeżej daty. Zarówno na gruncie ustawy o Ministrze Spraw Wewnętrznych i zakresie działania podległych mu organów z dnia 19 lipca 1983 r.[10], jak też tzw. ustaw policyjnych z 6 kwietnia 1990 r. (ustawa o Policji, Urzędzie Ochrony Państwa i Urzędzie Ministra Spraw Wewnętrznych)[11], były to regulacje bardzo lakoniczne[12].

W literaturze przedmiotu podnoszono konieczność precyzyjnego określenia tych uprawnień[13]. Problem ten próbowano rozwiązać ustawą z dnia 27 lipca 2001 r. o zmianie ustawy o Policji, ustawy o działalności ubezpieczeniowej oraz ustawy – Prawo bankowe, ustawy o samorządzie powiatowym oraz ustawy – Przepisy wprowadzające ustawy reformujące administrację publiczną[14]. W myśl tej noweli, prawo Policji do uzyskiwania, gromadzenia, sprawdzania i przetwarzania informacji uległo znacznemu rozszerzeniu. Art. 20 ust. 1 pozostał niezmieniony. Natomiast znowelizowany art. 20 ust. 2 pozwalał na przetwarzanie danych osobowych – osób podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstw ściganych z oskarżenia publicznego, osób o nieustalonej tożsa-

[9] W tym tworzenia i wykorzystywania zbiorów danych daktyloskopijnych i biologicznych wykorzystywanych w analizie DNA.

[10] Dz. U. Nr 38, poz. 173.

[11] Dz. U. Nr 30, poz.179, 180, 181.

[12] Kwestię gromadzenia i wykorzystywania informacji regulowały art. 20 ust. 1 ustawy o Policji oraz art. 11 ustawy o UOP, które pozwalały na uzyskiwanie informacji (w tym także tajnie i poufnie), gromadzenie ich, sprawdzanie i przetwarzanie – z wyjątkiem sytuacji przewidzianych w art. 19 ustawy o Policji oraz w art. 10 ustawy o UOP (kontrola korespondencji i stosowanie techniki operacyjnej). Przepisy te pozwalały zarówno na prowadzenie takich czynności operacyjnych, jak obserwacja (informacje uzyskiwane tajnie i poufnie) oraz na gromadzenie danych w sposób jawny, w tym także w trakcie czynności procesowych (m.in. pobieranie śladów daktyloskopijnych i biologicznych do badań DNA).

[13] W literaturze przedmiotu wskazywano także, że niektóre z czynności organów ścigania skierowanych na uzyskiwanie informacji wymagają utworzenia odrębnego przepisu (np. regulującego przebieg czynności obserwacji w działaniach operacyjno-rozpoznawczych, czy też administracyjno-porządkowych).

[14] Dz. U. Nr 100, poz. 1084. Nowela wprowadziła przepis art. 15 ust. 1 pkt 5a pozwalający funkcjonariuszom Policji na obserwowanie i rejestrowanie przy użyciu środków technicznych obrazu i zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych podejmowanych na podstawie ustawy – także i dźwięku towarzyszącego tym zdarzeniom.

mości lub usiłujących ukryć swą tożsamość oraz osób poszukiwanych, także bez ich wiedzy i zgody. Dotyczy to także danych podlegających szczególnej ochronie (art. 27 ust. 1 ustawy o ochronie danych osobowych)[15].

Policja może (art. 20 ust. 15) w celu zapobieżenia lub wykrycia przestępstw oraz identyfikacji osób uzyskiwać, gromadzić i przetwarzać informacje, w tym również dane osobowe ze zbiorów prowadzonych na postawie odrębnych przepisów przez organy władzy publicznej, a w szczególności z Krajowego Rejestru Skazanych oraz Powszechnego Elektronicznego Systemu Ewidencji Ludności. Administratorzy danych gromadzonych w tych rejestrach są obowiązani do nieodpłatnego ich udostępnienia. Nowela także znacznie rozszerzyła prawo do korzystania przez Policję (i inne służby) z informacji zgromadzonych przez podmioty prywatne[16].

Problem uzyskiwania, gromadzenia i przetwarzania informacji przez służby policyjne w trybie działań własnych oraz dostęp do zbiorów danych gromadzonych przez inne podmioty doskonale jest widoczny na przykładzie uzyskiwania i gromadzenia przez służby policyjne i specjalne śladów daktyloskopijnych i genetycznych (DNA) pozwalających na identyfikację osób oraz korzystania przez te służby z danych telekomunikacyjnych, którymi dysponują operatorzy[17].

Nie ulega wątpliwości, że realizacja funkcji wykrywczej i dowodowej organów ścigania byłaby niemożliwa bez odpowiednich zbiorów kryminalistycznych (baz danych). Skuteczność działania organów ścigania zależy od wielkości tych baz i możliwości korzystania z ich zawartości. Niewątpliwie wśród licznych zbiorów kryminalistycznych największe znaczenie mają obecnie zbiory daktyloskopijne i zbiory danych DNA. Na rozwój bazy danych w zbiorach daktyloskopijnych wpływ miała komputeryzacja

[15] Z tym, że dane dotyczące kodu genetycznego wyłącznie o niekodujących regionach genomu (art. 20 ust. 2 pkt 1 ustawy o Policji).

[16] Art. 20 ust. 3 umożliwia Policji dostęp do informacji dotyczących umów ubezpieczenia, a w szczególności do przetwarzanych przez zakłady ubezpieczeń danych podmiotów w tym osób, które zawarły umowę ubezpieczenia, a także przetworzonych przez banki informacji stanowiących tajemnicę bankową. Informacje te udostępnia się na podstawie postanowienia wydanego na pisemny wniosek Komendanta Głównego Policji albo komendanta wojewódzkiego Policji przez sąd okręgowy właściwy miejscowo ze względu na siedzibę wnioskującego organu (art. 20 ust. 5). Dostęp ten został ograniczony przedmiotowo, może jedynie zmierzać do zapobieżenia przestępstwom określonym w art. 19 ust. 1 ustawy o Policji lub wykrycia albo ustalenia ich sprawców i uzyskania dowodów.

[17] W obu tych sytuacjach zastrzeżenia do obowiązujących przepisów zgłaszał Rzecznik Praw Obywatelskich oraz wypowiadał się TK.

zbiorów daktyloskopijnych, która pozwoliła na wprowadzenie systemów automatycznej identyfikacji daktyloskopijnej (*AFIS – Automated Fingerprint Idetification System*)[18].

Jednak możliwości wykrywcze organów ścigania uzyskiwane dzięki systemowi *AFIS* w Polsce w ostatnich latach wyraźnie zmalały. Wynika to ze zmian, jakie ustawodawca wprowadził do ustawy o Policji nowelą z dnia 20 września 2006 r. Zmiany te spowodował wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r., w którym Trybunał uznał za niezgodne z Konstytucją przepisy art. 19 ust. 4, art. 19 ust. 18, art. 20 ust. 2 pkt 1 oraz art. 20 ust. 17 ustawy o Policji[19]. Art. 20 ust. 2 ustawy o Policji został uznany za niezgodny z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji RP przez to, że nie precyzuje, w jakich sytuacjach można gromadzić informacje o osobach podejrzanych o popełnienie przestępstwa ściganego z urzędu, i nie określa rodzajów tych informacji w sposób wyczerpujący. W uzasadnieniu Trybunał podniósł także, że art. 20 ust. 2 zezwala na gromadzenie informacji o osobach podejrzanych o popełnienie przestępstwa ściganego z urzędu, niezależnie od faktycznej potrzeby zebrania tych informacji w danym postępowaniu karnym[20].

Nowela wprowadziła art. 20 ust. 2c w brzmieniu „Informacji, o których mowa w art. 20 ust. 2a, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej czy identyfikacyjnej w prowadzonym postępowaniu". W praktyce przyjęto ścisłą wykładnię tego przepisu dopuszczającą możliwość pobrania od osoby podejrzanej odcisków palców (i śladów biologicznych) tylko wtedy, gdy w prowadzonym postępowaniu takie ślady zostały ujawnione i zabezpieczone. Oznacza to, że w sprawach, w których nie ujawniono takich śladów Policja nie może pobierać od osób podejrzanych materiału do badań identyfikacyjnych. Niewątpliwie taka interpretacja tego przepisu nawiązuje wprost do uzasadnienia wyroku Trybunału Konstytucyjnego. Jednak jej przyjęcie w istotny sposób ograniczyło uprawnienie funkcjonariuszy Policji do pobierania, uzyskiwania, gromadzenia, przetwarzania i wykorzystywania, w celach realizacji zadań ustawowych, informacji

[18] Stało się możliwe ustalenie, czy sprawca pozostawiający nawet pojedynczy ślad na miejscu zdarzenia figuruje w kartotece daktyloskopijnej. Oznaczało to oczywiście przełom w możliwościach wykrywczych dzięki zastosowaniu techniki daktyloskopijnej także w praktycznym wymiarze. W Polsce centralny system identyfikacji daktyloskopijnej (*AFIS*) uruchomiono w maju 2000 r.

[19] Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. Dz. U. Nr 250, poz. 2116.

[20] Uzasadnienie, pkt 5.3., s. 24.

o osobach podejrzanych (art. 20 ust. 2), w tym także odcisków palców (art. 20 ust. 2a) i śladów biologicznych do analizy DNA. Oznacza to, że prawdopodobieństwo uzyskania pozytywnego wyniku podjętych poszukiwań w tej bazie staje się coraz mniejsze. Spadek ilości kart wprowadzanych do systemu *AFIS* (po wejściu w życie omówionych wyżej zmianach w ustawie o Policji) jest bardzo duży[21]. Wpływ kart do Centralnej Registratury Daktyloskopijnej łącznie w latach 2008-2016 (247 739) był znacznie mniejszy niż średnia wielkość wpływu w jednym roku w latach 2001-2006 (315 981). Zmiany te jednoznacznie należy łączyć z wprowadzeniem noweli przepisu art. 20 ust. 2a ustawy o Policji, co spowoduje w najbliższych latach istotne zmniejszenie możliwości wykrywania sprawców przestępstw w oparciu o ślady daktyloskopijne[22].

Podobnie wygląda sytuacja, gdy chodzi o tworzenie baz danych śladów biologicznych wykorzystywanych w analizie DNA. Baza ta jest bardzo nieliczna, gdyż zaczęto ją tworzyć w 2007 r., już po wejściu w życie znowelizowanego przepisu art. 20 ustawy o Policji, który w sposób zasadniczy ograniczył jej rozbudowę[23].

Niewątpliwie zmiana przepisu art. 20 ust. 2c ustawy o Policji w istotny sposób ograniczyła możliwości działań wykrywczych Policji – zwiększając

---

[21] Wpływ kart do registratury CRD w latach 1991-2016 wyglądał następująco:

1991 – 17 082	1998 – 66 075	2004 – 297 728	2010 – 18 657	2016 – 32 273
1992 – 14 329	1999 – 40 358	2005 – 276 785	2011 – 20 844	
1993 – 11 501	2000 – 101 868	2006 – 332 226	2012 – 27 242	
1994 – 14 118	2001 – 271 229	2007 – 131 604	2013 – 33 559	
1995 – 16 761	2002 – 377 820	2008 – 21 545	2014 – 41 600	
1997 – 41 390	2003 – 340 099	2009 – 20 336	2015 – 31 683	

[22] W literaturze przedmiotu zwracano uwagę na to, że wprowadzone przez ustawodawcę zmiany spowodowały zmniejszenie liczby daktyloskopowanych osób, co z kolei w ujemny sposób odbiło się na zasobach policyjnych bazy danych *AFIS*. J. Misztal, *Daktyloskopia w Polsce w XX wieku,* „Problemy Kryminalistyki" 262 (2008), s. 68–69; B. Krzemińska, *Kompetencje Wydziału Daktyloskopii CLK KGP we współpracy międzynarodowej*, „Problemy Kryminalistyki" 262 (2008), s. 31; A. Taracha, *Wykorzystanie śladów daktyloskopijnych w realizacji funkcji wykrywczej przez Policję*, w: *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, red. E. Gruza, M. Goc, T. Tomaszewski, Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, Warszawa 2010, s. 341–346.

[23] Wpływ profili do Bazy Danych DNA w Polsce w latach 2008-2016 przedstawiał się następująco: 2008 – osoba 3337, NN ślad – 490; 2009 – osoba 4404, NN ślad – 850; 2010 – osoba 2375, NN ślad – 503; 2011 – osoba 2245, NN ślad – 480; 2012 – osoba 3373, NN ślad – 737; 2013 – osoba 2150, NN ślad – 726; 2014 – osoba 3677, NN ślad – 901; 2015 – osoba 6460, NN ślad – 1030; 2016 – osoba 9637, NN ślad – 1826. W 2016 r. wielkość bazy danych DNA w Polsce (46 579) była mniejsza nawet w porównaniu z takimi państwami, jak Litwa (87 310) czy Łotwa (53 546).

gwarancje praw podejrzanego (najczęściej rzeczywistego sprawcy) ponad rzeczywistą potrzebę. Obecna regulacja prawna przyjęta w art. 20 ust. 2c (i jego wykładnia) wprowadza ograniczenia większe niż przewidziane w art. 74 k.p.k., który zezwala na pobieranie od podejrzanego i osoby podejrzanej śladów biologicznych, takich jak odciski palców (bez żadnych ograniczeń) i wymazu ze śluzówki policzków – pozwalających na analizę DNA (jeżeli jest to nieodzowne i nie zagrażałoby to zdrowiu podejrzanego lub innych osób)[24].

Także dostęp służb policyjnych i służb specjalnych[25] do danych telekomunikacyjnych budził szereg zastrzeżeń głównie ze względu na bardzo dużą liczbę tych ingerencji[26]. W Unii Europejskiej przygotowanie nowych regulacji prawnych mających zapewnić skuteczniejszą walkę ze szczególnie niebezpieczną przestępczością rozpoczęto w końcu lat 90-tych ubiegłego wieku[27]. Wprowadzenie efektywnych środków (w tym tajnych działań organów ścigania) zwalczania tych zjawisk przestępczych wiązało się jednak z koniecznością ograniczenia praw i wolności obywateli. Dopiero w dniu 29 czerwca 2005 r. został opublikowany *Projekt Decyzji Ramowej w sprawie przechowywania danych przetwarzanych i gromadzonych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej lub danych o publicznych sieciach komunikacyjnych w celu śledzenia, wykrywania ścigania przestępstw, w tym przestępstwa terroryzmu*[28]. Parlament Europejski i Rada

[24] Kodeks postępowania karnego zawiera obowiązek poddania się takim badaniom przez podejrzanych i osoby podejrzane niezależnie od rodzaju zabezpieczonych w prowadzonej sprawie śladów.

[25] Polskie prawo pozwala na uzyskiwanie danych telekomunikacyjnych (billingowych) zarówno w drodze czynności procesowych (art. 218 k.p.k.), jak i w drodze czynności operacyjno-rozpoznawczych (art. 20c ustawy o Policji, art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, art. 10b ustawy o Straży Granicznej, art. 30 ustawy o Żandarmerii Wojskowej oraz wojskowych organach porządkowych, art. 36b ustawy o kontroli skarbowej, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, art.18 ustawy o Centralnym Biurze Antykorupcyjnym).

[26] Na przykład w Polsce w latach 2009-2014 liczba wniosków o udostępnienie danych telekomunikacyjnych wzrosła dwukrotnie i przekroczyła liczbę 2 mln zapytań (odpowiednio w roku: 2009 – 1 089 029; 2010 – 1 399 144; 2011 – 1 874 107; 2012 – 1 762 620; 2013 – 1 754 006; 2014 – 2 177 916).

[27] Zob. Zalecenie nr R (96) 8 Komitetu Ministrów Rady Europy dla państw członkowskich dotyczące polityki kryminalnej w okresie przemian, postanowienia Traktatu Amsterdamskiego, postanowienia Rady Europy ze spotkań w Tampere oraz Santa Maria da Feira.

[28] *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic services or data on public communications*

Unii Europejskiej przyjęły w dniu 15 marca 2006 r. Dyrektywę 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającą dyrektywę 2002/58/WE[29]. Podstawowe kwestie dotyczyły określenia obowiązku zatrzymywania danych (art. 3) i okresów zatrzymywania (art. 6), dostępu do danych (art. 4), kategorie danych przeznaczonych do zatrzymania (art. 5), ochronę i bezpieczeństwo danych oraz wymogi dotyczące przechowywania zatrzymanych danych (art. 7 i 8) oraz ustanowienia organu odpowiedzialnego za nadzór nad stosowaniem przepisów dyrektywy (art. 9)[30]. Komisja proponowała przyjęcie okresu przechowywania danych ustalając go na 6 miesięcy – Internet i 12 miesięcy – telefon. Natomiast w Parlamencie Europejskim przeważał pogląd, że okres ten powinien wynosić od 6 do 12 miesięcy zarówno dla Internetu, jak i telefonów, zaś w Radzie (UE) preferowano okres 6 miesięcy dla Internetu i od 6 do 24 miesięcy dla telefonów (według sondażu Komisji)[31]. Ostatecznie Parlament Europejski i Rada (po długiej dyskusji) przyjęły w dniu 15 marca 2006 r. Dyrektywę 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności. W dyrektywie przyjęto termin przechowywania danych nie mniej niż 6 miesięcy i nie dłużej niż 24 miesiące (art. 6 dyrektywy). W uzasadnionych sytuacjach kraj członkowski mógł otrzymać zgodę na przechowywanie danych transmisyjnych przez dłuższy okres (na-

networks for purpose of investigation, detection and prosecution of crime and criminal offences including terrorism, Nr dok. 10609/05 COPEN 102 TELECOM 64.

[29] Dz. U. L 105 z 13.4.2006, s. 54–63.

[30] Najwięcej rozbieżności dotyczyło ustalenie minimalnych i maksymalnych okresów zatrzymania danych. Komisja wolności obywatelskich, sprawiedliwości i spraw wewnętrznych Parlamentu Europejskiego przedstawiła swój raport dotyczący projektu Dyrektywy Ramowej w dniu 28 listopada 2005 r. (sprawozdawcą był Alexander Nuno Alvaro).

[31] Zob. *Report on the proposal for directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic services and amending Directive 2002/58/ec (COM(2005)0438-C6-0293/2005-2005/0182(COD))*. Committee on Civil Liberties, Justice and Home Affairs, s. 32–36. Projekt decyzji (po pierwszym czytaniu) zobowiązywał operatorów telekomunikacyjnych do przechowywania przez okres 12 miesięcy (od daty ich powstania) danych transmisyjnych (*traffic data, location data*) obejmujących dane nadawcy i odbiorcy, czas trwania połączenia oraz miejsca, z którego połączenie było prowadzone (w przypadku korzystania z telefonu komórkowego), a w wypadku poczty elektronicznej adresu nadawcy i odbiorcy, czasu przesyłania i objętości e-maila. Parlament Europejski przyjął projekt dyrektywy w pierwszym czytaniu w dniu 14 grudnia 2005 r.

wet do czterech lat) lub krótszy (ale nie krótszy niż 6 miesięcy). Mimo uchylenia Dyrektywy 2006/24/WE przez wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r., należy zauważyć, że termin 6 miesięcy przez wiele lat uważany był za termin minimalny (nie podlegający skróceniu). Propozycja, aby był to termin maksymalny nie wydaje się trafna, gdyż można wskazać sytuacje, gdy okres ten może okazać się zbyt krótki. Obecnie w Polsce termin przechowywania danych telekomunikacyjnych przez operatorów wynosi 12 miesięcy[32] i jest taki sam, jak w wielu krajach UE.

Zgodnie z dyrektywą, państwa członkowskie zobowiązane są do podjęcia środków w celu zagwarantowania, że zatrzymane dane udostępniane będą jedynie uprawnionym przez prawo właściwym organom krajowym, w szczególnych przypadkach, przy spełnieniu wymogu konieczności oraz proporcjonalności (podlegając odpowiednim przepisom prawa Unii Europejskiej lub międzynarodowego prawa publicznego, w szczególności Europejskiej Konwencji o Ochronie Praw Człowieka zgodnie z interpretacją Europejskiego Trybunału Praw Człowieka)[33].

Ujawnienie skali ingerencji, jeżeli chodzi o dostęp do danych telekomunikacyjnych w Polsce, spowodowało, że zostały podjęte działania zmierzające do ograniczenia liczby wniosków o udostępnienie danych oraz poddania tych działań zwiększonej ochronie. Rzecznik Praw Obywatelskich w dniu 3 sierpnia 2011 r. złożył w Trybunale Konstytucyjnym wniosek o uznanie za niezgodne z Konstytucją RP przepisów ustaw policyjnych pozwalających na dostęp do danych telekomunikacyjnych, określanych także jako tzw. billing[34], oraz przepisów tych ustaw, które nie przewidują znisz-

[32]Został skrócony z 24 miesięcy do 12 miesięcy od dnia 21 stycznia 2013 r.

[33] Kategorie danych przeznaczonych do zatrzymania dyrektywa określa dość precyzyjnie. Należą do nich: dane niezbędne do ustalenia źródła połączenia w telefonii stacjonarnej i komórkowej oraz dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej; dane niezbędne do ustalenia odbiorcy połączenia w telefonii stacjonarnej i komórkowej oraz elektronicznej poczty internetowej i telefonii internetowej; dane niezbędne do określenia daty, godziny i czasu trwania połączenia w telefonii stacjonarnej i komórkowej oraz elektronicznej poczty internetowej i telefonii internetowej; dane niezbędne do określenia rodzaju połączenia; dane niezbędne do określenia narzędzia komunikacji lub tego, co może służyć za narzędzie komunikacji telefonii stacjonarnej, komórkowej oraz w przypadku dostępu do Internetu, elektronicznej poczty internetowej i telefonii internetowej, a także dane niezbędne do identyfikacji lokalizacji urządzenia komunikacji ruchowej. Dane te są także zatrzymywane i przechowywane w przypadku nieudanych prób połączenia (art. 3 ust. 2).

[34] Wniosek dotyczył następujących przepisów: art. 20c ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji; art. 10b ust. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej; art. 36b ust. 1 pkt 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej; art. 30 ust. 1 ustawy

czenia tych spośród pozyskanych danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania[35]. Zdaniem RPO, uprawnienia służb policyjnych w zakresie dostępu do danych telekomunikacyjnych są niezgodne z art. 49 w zw. z art. 31 ust. 3 Konstytucji RP oraz art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Natomiast brak przepisów nakazujących zniszczenie danych, które nie zawierają informacji mających znaczenie dla prowadzonego postępowania jest niezgodny z art. 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji RP[36]. RPO niewątpliwie miał rację wskazując, że brak w niektórych ustawach policyjnych przepisów nakazujących niszczenie danych dotyczących ruchu telekomunikacyjnego (tzw. billingu), gdy są one już nieprzydatne w prowadzonym postępowaniu, jest niezgodny z Konstytucją RP. Przepisy takie znajdują się w części ustaw policyjnych, a w niektórych nie. Różnica ta wynika nie z powodów merytorycznych, które uzasadniałyby takie rozróżnienie między służbami, lecz z tego powodu, że część tych ustaw została już znowelizowana, a część jeszcze nie[37].

W maju 2012 r. w Kancelarii Prezesa Rady Ministrów (Biuro Kolegium do spraw służb specjalnych) przygotowano dokument zatytułowany *Założenia projektu ustawy o zmianie niektórych ustaw, w związku z pozyskiwaniem*

---

z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych; art. 28 ust. 1 pkt 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; art. 18 ust. 1 pkt 1 ustawy z dnia 9 czerwca o Centralnym Biurze Antykorupcyjnym; art. 32 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

[35] Dotyczył następujących przepisów: art. 36b ust. 5 ustawy z dnia 28 września 1991 r. o kontroli skarbowej; art. 28 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; art. 18 ustawy z dnia 9 czerwca o Centralnym Biurze Antykorupcyjnym; art. 32 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

[36] Dz. U. z 1993 r. Nr 61, poz. 284.

[37] Natomiast wniosek Rzecznika Praw Obywatelskich o uznanie za niekonstytucyjne przepisów o dostępie do danych telekomunikacyjnych, które nie zawierają treści pojęciowej (treści korespondencji) wydaje się nietrafny. RPO cały wywód opiera na stwierdzeniu, że tzw. dane telekomunikacyjne także objęte są tajemnicą komunikowania się. Jak się wydaje, jest to zbyt szerokie ujęcie. Komunikowanie się to przekazywanie informacji. Natomiast dane telekomunikacyjne, do których dostęp, w oparciu o przepisy, niezgodne zdaniem RPO z Konstytucją, mają służby policyjne i służby specjalne w Polsce, nie mogą zawierać danych, które ujawniają treść komunikatu (gdyż w oparciu o przepisy o retencji danych nie mogą być zatrzymywane takie informacje). Takie rozwiązanie prawne zakazujące zatrzymywania przez operatora danych zawierających treść przekazu przyjęte jest zarówno w prawie europejskim (art. 5 ust. 2 Dyrektywy 2006/24 WE) oraz w polskim prawie telekomunikacyjnym (art. 180a ust. 6 ustawy – prawo telekomunikacyjne).

i wykorzystywaniem danych telekomunikacyjnych[38]. Najdalej idącą propozycją zmian przedstawioną w *Założeniach* było ograniczenie zakresu pozyskiwania i wykorzystywania danych podlegających retencji. Zgodnie z projektem, pozyskiwanie i wykorzystywanie danych telekomunikacyjnych przez uprawnione służby, prokuraturę i sądy byłoby możliwe jedynie dla potrzeb postępowań w ściganiu przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata oraz o ściganie przestępstw popełnionych przy użyciu środków komunikacji elektronicznej. Ograniczenie to nie obowiązywałoby w postępowaniach dotyczących ścigania przestępstw celnych. Pozyskiwanie i wykorzystywanie danych telekomunikacyjnych przez poszczególne służby byłoby możliwe także w przypadku ścigania tych przestępstw, w odniesieniu do których służby te mogą wnioskować o zastosowanie kontroli operacyjnej. Pozyskany w taki sposób dowód mógłby zostać przeprowadzony przed sądem tylko wówczas, gdy ustalenie określonej okoliczności faktycznej innymi dowodami będzie niemożliwe (zasada subsydiarności).

Z pewnością wprowadzenie obowiązku wykazania, że ustalenie określonych stanów faktycznych przy użyciu innych niż dane retencyjne dowodów nie było możliwe (lub niecelowe) jest tworzeniem gwarancji ponad skalę ingerencji w prawa i wolności obywateli. Zasada subsydiarności powinna być stosowana w wypadku kontroli operacyjnej oraz kontroli korespondencji i utrwalania rozmów, gdyż czynności te bardzo głęboko ingerują w prawo do komunikowania się obywateli. Natomiast wykorzystywanie retencyjnych danych telekomunikacyjnych, zarówno w postępowaniu karnym i cywilnym oraz w ramach czynności operacyjno-rozpoznawczych, stanowi znacznie łagodniejszą formę ingerencji i w proporcji do jej uciążliwości dla obywatela powinny być stosowane odpowiednie zabezpieczenia gwarancyjne. Oprócz tego podstawowego argumentu przemawiającego za niestosowaniem zasady subsydiarności w odniesieniu do wykorzystywania w postępowaniu dowodowym danych retencyjnych, należy podnieść, że zasada ta prowadzi do nieuniknionego wydłużenia procesu karnego w związku z koniecznością wykazania, że inne dowody okazały się nieprzydatne. W ten sposób uszczerbku doznawałaby istotna zasada procesu karnego – zasada szybkości postę-

[38] W założeniach przyjęto wprowadzenie następujących zmian: 1) utworzenie instytucji Pełnomocnika ds. ochrony danych osobowych i telekomunikacyjnych; 2) ograniczenie pozyskiwania i wykorzystywania danych podlegających retencji, 3) zwiększenie nadzoru Prokuratury, 4) wprowadzenie obowiązku niszczenia danych, 5) wprowadzenie obowiązku sprawozdawczego (projekt z dnia 28 maja 2012 r.).

powania. Prokurator musiałby wykazać, że ustalenie konkretnego stanu faktycznego było niemożliwe przy wykorzystaniu innych źródeł dowodowych (musiałby wskazać przy użyciu jakich konkretnie), aby móc wprowadzić do procesu dowód z danych retencyjnych. W niektórych wypadkach, co trafnie podnosił Prokurator Generalny, prowadziłoby to do utraty dowodu (minąłby czas przechowywania danych retencyjnych)[39].

Zgodnie z *Założeniami*, zwiększenie nadzoru Prokuratury polegałoby na zobowiązaniu podmiotów uprawnionych do pozyskiwania i wykorzystywania danych telekomunikacyjnych do przekazywania prokuratorowi, wraz z materiałem dowodowym zawierającym takie dane, informacji o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu. W ramach nadzoru nad zgodnością z prawem pozyskiwania i wykorzystywania danych telekomunikacyjnych – prokurator dokonywałby analizy i oceny, uwzględniając w szczególności faktyczną i prawną podstawę do pozyskiwania i wykorzystywania tych danych (zakres i sposób przeprowadzania tych czynności, okres ich stosowania i terminowość ich zarządzania, przeprowadzanie niszczenia materiałów zbędnych)[40]. Ostatecznie nie nadano *Założeniom* dalszego biegu w procesie legislacyjnym, a jedyne zmiany w tym zakresie wprowadziła ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw[41].

Zgodnie z wyrokiem Trybunału Konstytucyjnego, ustawa z dnia 15 stycznia 2016 r. wprowadziła kontrolę sądową wykorzystywania danych telekomunikacyjnych przez służby policyjne w działaniach operacyjno-rozpoznawczych. Wprowadziła obowiązek przekazywania przez służby policyjne (i służby specjalne) sądowi okręgowemu w okresach półrocznych spra-

[39] Pismo Prokuratora Generalnego do Ministra Spraw Wewnętrznych z 17.08.2012 r., PG VII G 025-255/12, s. 3.

[40] Przeciwko takiemu zwiększaniu obowiązków prokuratora w nadzorze nad pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych zdecydowanie wypowiedział się Prokurator Generalny. Trafnie zauważył, że pozyskiwanie i wykorzystywanie danych telekomunikacyjnych w ramach procesu karnego (jako czynność procesowa) obwarowane jest szeregiem gwarancji procesowych, które bez wątpienia odpowiadają standardom demokratycznego państwa prawa (konieczność powiadomienia osoby o zastosowaniu tego rodzaju czynności, możliwość złożenia zażalenia) i nie wymagają wprowadzania dodatkowych przepisów gwarancyjnych. Także przepisy prawne regulujące pozyskiwanie i wykorzystywanie tych danych w ramach czynności operacyjno-rozpoznawczych, zdaniem Prokuratora Generalnego, stanowią wystarczającą gwarancję praw obywateli.

[41] Dz. U. z 2016 r. poz. 147.

wozdań obejmujących liczbę przypadków pozyskania danych telekomunikacyjnych, pocztowych i internetowych oraz kwalifikację prawną czynów w sprawach, w których wystąpiono o udostępnienie danych. W ramach tej kontroli, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie uprawnionym służbom danych telekomunikacyjnych, pocztowych i internetowych.

Przed nowelizacją dostęp do danych telekomunikacyjnych, pocztowych i internetowych przez służby policyjne i służby specjalne nie podlegał żadnej kontroli przez organ zewnętrzny. Rozwiązanie przyjęte w ustawie z 6 lutego 2016 r. wprowadzające kontrolę *ex post* wykorzystywania przez uprawnione służby danych telekomunikacyjnych, pocztowych i internetowych – uznać należy za trafne[42].

***

Przedstawione przykłady czynności operacyjno-rozpoznawczych wskazują wyraźnie na skomplikowany związek między możliwościami efektywnego ścigania karnego a ochroną praw człowieka. Nowelizacja art. 20 ust. 1 ustawy o Policji zwiększająca (ponad rzeczywistą potrzebę) gwarancje praw podejrzanego i osoby podejrzanej spowodowała, że możliwości jakie daje rozwój nauki w realizacji funkcji ścigania poprzez wykorzystanie śladów biologicznych (daktyloskopii i DNA) zostały znacznie ograniczone[43].

Natomiast nowelizacja przepisów dotyczących korzystania z danych telekomunikacyjnych w ramach czynności operacyjno-rozpoznawczych zwiększyła gwarancje praw jednostki bez uszczerbku dla efektywności działań służb policyjnych i specjalnych. Wspomniane wyżej stanowisko Prokuratora Generalnego, w którym zdecydowanie opowiedział się przeciw poddaniu pozyskiwania i wykorzystywania danych telekomunikacyjnych (w ramach czynności operacyjno-rozpoznawczych) nadzorowi prokuratora uznać należy za trafne. Nie można uzależniać wszystkich decyzji dotyczących czynności

[42] Innego zdania był RPO, który w dniu 18 lutego 2016 r. zaskarżył do TK (sygn. akt K 9/16) m.in. art. 20c ust. 1 ustawy o Policji (i odpowiadające mu przepisy innych ustaw) jako niezgodne z Konstytucją RP, podnosząc zbyt szeroki zakres stosowania tej instytucji (w stosunku do wszystkich przestępstw) oraz brak wymogu subsydiarności. W związku z tym, że RPO w dniu 14 marca 2018 r. cofnął wniosek i wniósł o umorzenie postępowania, zastrzeżenia podniesione przez RPO we wniosku do TK mają w tej chwili charakter historyczny.

[43] Jest to doskonały przykład (niestety negatywny) na ograniczającą funkcję norm prawnych – w sytuacji, gdy osiągnięcia nauk technicznych pozwalają na zwiększenie możliwości wykrywczych organów ścigania.

operacyjno-rozpoznawczych od zgody organów zewnętrznych, gdyż spowodowałoby to faktyczny paraliż organów ścigania. Przyjęta w noweli kontrola *ex post* (wykorzystywania danych telekomunikacyjnych w działaniach operacyjnych) wykonywana przez niezawisły sąd jest rozwiązaniem trafnym – z jednej strony nie utrudnia zbytnio prowadzenia czynności operacyjno-rozpoznawczych, a z drugiej, poddaje tę działalność kontroli organu zewnętrznego – zgodnie z wyrokiem Trybunału Konstytucyjnego.

Poszukując rozwiązań, które zapewniłyby równowagę między zakresem uprawnień organów ścigania w ich działalności (w tym także w czynnościach operacyjno-rozpoznawczych) a ochroną praw człowieka, należy mieć na uwadze stopień zagrożenia przestępczością (w tym w szczególności terroryzmem i przestępczością zorganizowaną). Wzrost zagrożenia przestępczością (w tym atakami terrorystycznymi, na skalę nieznaną dotychczas w Europie) nakazuje szczególny umiar w działaniach legislacyjnych ograniczających możliwości służb policyjnych i służb specjalnych w zakresie działań operacyjnych.

Zgodnie z art. 8 ust. 2 EKPC niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa do prywatności z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób. Kluczowe znaczenie ma tutaj zakres pojęcia „konieczne". Nie ulega wątpliwości, że zakres ten powinien ulec poszerzeniu (objąć szerszy obszar) w sytuacji gdy zagrożenie bezpieczeństwa państwowego, bezpieczeństwa publicznego lub dobrobytu gospodarczego kraju wzrasta w wyniku działań terrorystycznych, z czym mamy do czynienia niewątpliwie w chwili obecnej. Należy postawić pytanie, czy dotychczasowe środki okazały się wystarczające, czy też nie? Jeśli nie, to należy wyposażyć służby odpowiedzialne za bezpieczeństwo państwa i porządek publiczny w dodatkowe uprawnienia[44], a nie wprowadzać przepisy ograniczające możliwości efektywnego działania tych służb.

[44] Tak postąpiono w USA po zamachach w dniu 11 września 2001 r. wprowadzając zmiany ustawowe (w kilkunastu ustawach), zwiększające uprawnienia służb odpowiedzialnych za bezpieczeństwo określane jako *Patriot Act*.

PIŚMIENNICTWO

Duffy, Peter. 1994. „Policja a Konwencja o ochronie praw człowieka i podstawowych wolności." *Prawa człowieka a Policja. Problemy teorii i praktyki*, red. Andrzej Rzepliński, 251–282. Legionowo: Wydawnictwo Centrum Szkolenia Policji w Legionowie.

Hermeliński, Wojciech. 2013. „Bezpieczeństwo publiczne a prawo jednostki do prywatności." *Palestra* 1–2:17–26.

Krzemińska, Beata. 2008. „Kompetencje Wydziału Daktyloskopii CLK KGP we współpracy międzynarodowej." *Problemy Kryminalistyki* 262:29–40.

Misztal, Jan. 2008. „Daktyloskopia w Polsce w XX wieku." *Problemy Kryminalistyki* 262:63–71.

Szuniewicz–Stępień, Marta. 2016. „Działania operacyjno-rozpoznawcze w ustawie antyterrorystycznej a europejski standard ochrony praw człowieka – wybrane zagadnienia." W *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, red. Waldemar Zubrzycki, Kuba Jałoszyński, i Aleksander Babiński, 335–368. Szczytno: Wyższa Szkoła Policji w Szczytnie.

Szwarc, Wojciech. 1986. „Zarys ewolucji pojęcia «Policji» w Monarchii Pruskiej w XVII i XIX w." W *Wybrane problemy teorii i praktyki państwa i prawa*, red. Henryk Groszyk, i Lech Dubel, 117–133. Lublin: Wydawnictwo UMCS.

Taracha, Adam. 2010. „Wykorzystanie śladów daktyloskopijnych w realizacji funkcji wykrywczej przez Policję." W *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, red. Ewa Gruza, Mieczysław Goc, i Tadeusz Tomaszewski, 341–346. Warszawa: Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW.

OBTAINING AND USING INFORMATION ON A PERSON FOR SAFETY PURPOSES AND THE RIGHTS OF THE INDIVIDUAL (SELECTED ISSUES)

Summary. The Author discusses the relationship between the rights of police services to obtain and process information on persons during police investigative operations necessary to the provision of safety and public order and the protection of rights of the individual. According to Art. 8 of the ECHR the interference by a public authority with the exercise of the right to privacy is admissible when it is in accordance with the law and is necessary in a democratic society in the interests of, among others, public safety and for the prevention of crime. The scope of that interference should be broadened (refer to a more extensive sphere) in the case in which the threat to the state's safety, public safety or economic welfare increases due to terrorist actions. The increase in the crime threat (including terrorist attacks on a scale unknown before in Europe) demands special moderation in legislative actions restricting the rights of police services and of special services in the sphere of investigative operations.

Key words: police investigative operations, obtaining, gathering and processing of information on a person, police service, special service, the right to privacy, terrorism