Arkadiusz Ćwik

Zakres dopuszczalnego korzystania z baz danych i rejestrów[1]

1. Analiza kryminalna

Analiza kryminalna jest częścią szerszego pojęcia, tzw. wywiadu kryminalnego, procesu polegającego na ustawicznym pozyskiwaniu, gromadzeniu, dokonywaniu ocen i analiz informacji w celu dalszego ukierunkowania działań uprawnionych służb[2]. Omawianą metodę stosuje się szczególnie w sprawach wielowątkowych, o dużym zasięgu terytorialnym oraz w których sposób popełnienia przestępstwa wskazuje na wysoką specjalizację działalności przestępczej lub rozwojowy charakter sprawy (§ 2 *Zarządzenia nr 1012 Komendanta Głównego Policji z dnia 23 września 2004 r. w sprawie stosowania przez Policję analizy kryminalnej* [3] – dalej: StosAnalKr).

Innymi słowy analizę kryminalną należy rozumieć jako metodę pracy służb polegającą na konsekwentnym i zorganizowanym wyszukiwaniu związków między danymi dotyczącymi przestępstwa z innymi możliwymi do wyróżnienia informacjami, które będą stanowiły podstawę do przygotowania wniosków wspomagających procesy decyzyjne[4]. Przyjmuje się, że analiza kryminalna jest najważniejszą fazą cyklu wywiadu kryminalnego – występuje w nim zawsze, niekiedy nawet wielokrotnie. Pozwala na odczytanie właściwego znaczenia informacji, ich usystematyzowanie oraz poznanie związków między nimi[5]. A zatem analiza informacji poprzedza optymalne dobranie działań wywiadu kryminalnego.

Analiza przygotowywana na potrzeby konkretnej sprawy to próba chronologicznej rekonstrukcji przebiegu (potencjalnie) przestępnego działania w celu zalecenia dalszego kierunku pracy oraz stwierdzenia nieścisłości w informacjach pochodzących z różnych źródeł. Analizą porównawczą określa się wyszukiwanie (według ustalonego wzorca oraz na podstawie wybranych kryteriów) i kojarzenie informacji o podobnych zdarzeniach w celu ustalenia, które z nich mogły być popełnione lub zorganizowane przez te same osoby. Można więc przyjąć, że ten rodzaj analizy dotyczy przestępstw seryjnych[6]. Tym samym zazwyczaj wiąże się z wszczętym postępowaniem karnym.

Analiza grup przestępczych jest rozumiana jako uporządkowanie dostępnych informacji o znanej (lub przypuszczalnie istniejącej) grupie przestępczej, w celu

[1] Fragment pracy magisterskiej pt. *Znaczenie czynności operacyjno-rozpoznawczych dla rozstrzygnięcia o przedmiocie procesu karnego w polskim porządku prawnym*, która zajęła III miejsce w konkursie Szefa ABW na najlepszą pracę magisterską/licencjacką z dziedziny bezpieczeństwa wewnętrznego (edycja – 2013/2014), (rozdział 4). Redakcja dokonała niezbędnych poprawek oraz zmian numeracji przypisów (przyp. red.).

[2] H. Tusiński, M. Bronicki, *Wywiad kryminalny jako kierunek zwiększenia efektywności Policji w zdobywaniu, gromadzeniu i wykorzystywaniu informacji*, w: E.W. Pływaczewski, *Przestępczość zorganizowana*, *świadek koronny*, *terroryzm w ujęciu praktycznym*, Kraków 2005, s. 665.

[3] Dz.Urz. KGP nr 20, poz. 124, z późn. zm.

[4] S. Czarnecki, *Analiza kryminalna – narzędzie pracy Policji*, „Prokurator" 2007, nr 1, s. 22.

[5] H. Tusiński, M. Bronicki, *Wywiad kryminalny jako kierunek...*, s. 669.

[6] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka czyli rzecz o metodach śledczych*, Warszawa 2011, s. 63.

określenia jej struktury, zakresu działalności, zaplecza logistycznego, źródeł finansowania oraz roli każdego z jej członków lub instytucji z nią związanych[7]. Analiza odbywa się najczęściej na podstawie wykazów połączeń oraz informacji o przepływie środków finansowych pomiędzy osobami nią objętymi oraz na podstawie informacji o przemieszczaniu się tych osób. Pozwala też wyznaczyć dalsze kierunki czynności, które, umiejętnie podjęte, mogą całkowicie zdezintegrować daną grupę lub zmienić jej działania, a tym samym doprowadzić do pełnej realizacji funkcji profilaktycznej czynności operacyjno-rozpoznawczych[8].

Jako swoistą formę analizy operacyjnej można rozumieć analizę profilu szczególnego. Jest to próba określenia, na podstawie opisu przestępstwa, cech charakterologicznych i fizycznych osoby, która je popełniła. Od wcześniej wskazanych form analizy kryminalnej różni się podmiotem wykonawczym, którym w tym przypadku jest nie analityk kryminalny, lecz psycholog policyjny. Wydaje się zatem, że ten rodzaj analizy może być utożsamiany z tzw. profilowaniem kryminalnym[9].

Osoba wykonująca analizę posługuje się w tym celu najczęściej specjalistycznym oprogramowaniem[10]. Regułą jest, że analiza sama w sobie nie wnosi do sprawy nowych informacji, lecz porządkuje dotychczas zgromadzone. Efekty omawianego procesu są najczęściej przedstawiane w postaci diagramów analitycznych lub w innych formach wizualizacji danych (§ 9 pkt 3 StosAnalKr). Może to być na przykład wykaz połączeń telefonicznych przedstawiony wraz z wyselekcjonowanymi wydarzeniami zaznaczonymi na osi czasu[11] bądź graf sieci powiązań wynikających z interakcji pomiędzy analizowanymi podmiotami (tzw. aktorami)[12]. Warto podkreślić, że, zdaniem sędziów, korzystanie z wyników otrzymanych z zastosowania omawianego narzędzia może znacznie wspomóc i przyspieszyć postępowanie[13].

2. Dane osobowe

Przepis art. 20 ust. 2a *Ustawy z dnia 6 kwietnia 1990 roku o Policji*[14] (dalej: UPol) przyznaje tej służbie uprawnienie do uzyskiwania, gromadzenia, sprawdzania i przetwarzania danych osobowych o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osobach o nieustalonej tożsamości lub usiłujących ukryć swoją tożsamość, oraz o osobach poszukiwanych, także bez ich wiedzy i zgody.

Przytoczona regulacja różni się od analogicznych uprawnień przewidzianych w pozostałych ustawach policyjnych przede wszystkim umieszczeniem w jej ramach zamkniętego katalogu danych osobowych, do których funkcjonariusze mogą mieć do-

[7] S. Czarnecki, *Analiza kryminalna*..., s. 27.

[8] Por. A. Zygmunt, J. Koźlak, *Zastosowanie podejścia sieci społecznych do wspomagania prowadzenia analizy kryminalnej dotyczącej danych billingowych*, w: *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, *nowoczesne technologie i praca operacyjna*, Z. Rau, L. Paprzycki (red.), Warszawa 2009, s. 675.

[9] Zob. J. Konieczny, M. Szostak, *Profilowanie kryminalne*, Warszawa 2011.

[10] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka, czyli rzecz o*..., s. 75.

[11] S. Czarnecki, *Analiza kryminalna*..., s. 33.

[12] A. Zygmunt, J. Koźlak, *Zastosowanie podejścia sieci społecznych*..., s. 672.

[13] Z. Rau, *Kierunki działań uczestników Polskiej Platformy Bezpieczeństwa Wewnętrznego w zakresie podniesienia efektywności pracy operacyjnej*, „Prokurator" 2006, nr 4, s. 18.

[14] Tekst jednolity: Dz.U. z 2015 r. poz. 355.

stęp. Są nimi dane wrażliwe (poza kodującą częścią DNA), odciski linii papilarnych, zdjęcia, szkice i opisy wizerunku, cechy i znaki szczególne oraz pseudonimy, informacje o miejscu zamieszkania lub pobytu, wykształceniu, zawodzie, miejscu i stanowisku pracy oraz sytuacji materialnej i stanie majątkowym, dokumentach i przedmiotach, którymi sprawca się posługuje, sposobie działania sprawcy, jego środowisku i kontaktach oraz sposobie zachowania się sprawcy wobec osób pokrzywdzonych. Pozostałe ustawy zasadniczo zezwalają na zbieranie, w granicach właściwości danej służby, wszelkich danych osobowych, w tym – o ile jest to uzasadnione charakterem realizowanych zadań – także danych wrażliwych (tak np. art. 34 ust. 1 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[15] – dalej: ustawa o ABW oraz AW).

Takie zróżnicowanie jest wynikiem uchylenia części przepisów w następstwie orzeczeń Trybunału Konstytucyjnego. Upraszczając, można powiedzieć, że organ ten stoi na stanowisku, że w odniesieniu do czynności operacyjno-rozpoznawczych niedopuszczalne jest posłużenie się przez prawodawcę otwartym katalogiem danych, do których pozyskiwania, gromadzenia i przetwarzana uprawniona jest dana służba[16]. Wydaje się jednak, że obecny kształt przepisów uprawniających do zbierania danych o osobie z ustawy o Policji, najbardziej precyzyjnych spośród wszystkich przepisów ustaw policyjnych w tym zakresie, wciąż nie odpowiada wymaganiom konstytucyjnym. W sprawie K 32/04 Trybunał podzielił bowiem stanowisko Rzecznika Praw Obywatelskich, zgodnie z którym przepisy powinny wiązać możliwość gromadzenia danych z charakterem popełnionego czynu. Tylko takie ujęcie czyniłoby zadość przesłance niezbędności wymaganej do ich gromadzenia (art. 51 ust. 2 Konstytucji RP). Posługując się przykładem Rzecznika, można wskazać, że dotyczy to m.in. pobrania odcisków palców osoby, której zarzucane jest popełnienie przestępstwa dokonywanego z użyciem druku. Należy zatem stwierdzić, że dyspozycji przepisu art. 51 ust. 2 Konstytucji RP nie można sprowadzić wyłącznie do obowiązku tworzenia zamkniętych, ustawowych katalogów rodzaju informacji, które mogą okazać się niezbędne w demokratycznym państwie prawa[17].

Omawiane uprawnienie dotyczy zarówno informacji uzyskanych dzięki własnym czynnościom Policji, jak i danych zgromadzonych przez inne organy władzy publicznej (szczególnie w Krajowym Rejestrze Karnym oraz rejestrze numerów PESEL) oraz w zbiorach, w których przetwarza się informacje uzyskane w wyniku wykonywania przez uprawnione organy czynności operacyjno-rozpoznawczych (art. 20 ust. 15 UPol). W drugiej z tych sytuacji, co do zasady, informacje są udostępniane na pisemny wniosek (art. 20 ust. 5 UPol), chociaż ustawodawca przewidział również możliwość ich udostępniania za pomocą urządzeń telekomunikacyjnych (art. 20 ust. 16 UPol). W przypadku konieczności podjęcia niezwłocznego działania, a zwłaszcza podczas pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego, wydaje się, że policjant mógłby jednak zwrócić się ustnie o udzielenie mu tego typu informacji[18]. Nie jest to jednak ja-

[15] Tekst jednolity: Dz.U. z 2010 r. Nr 29, poz. 154, z późn. zm.

[16] Zob. Wyrok TK z dnia 12 grudnia 2005 r., K 32/04, OTK Seria A 2005, nr 11, poz. 132; wyrok TK z dnia 20 czerwca 2005 r., K 4/04, OTK 2005, nr 11A, poz. 132; wyrok TK z dnia 23 czerwca 2009 r., K 54/07, OTK 2009, nr 6a, poz. 86.

[17] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 295.

[18] Por. W. Kotowski, *Komentarz do ustawy o Policji*, Lex 2012, art. 20, nb. 2.

sne, gdyż w przepisie art. 28 ust. 2 pkt 2 ustawy o ABW oraz AW ustawodawca wprost przewidział ustną formę żądania udostępnienia danych.

Dane osobowe usuwa się, jeżeli, po pierwsze, organ Policji powziął wiarygodną informację o tym, że czynu stanowiącego podstawę wprowadzenia informacji do zbioru nie popełniono, albo brakuje danych dostatecznie uzasadniających podejrzenie jego popełnienia. Po drugie również wtedy, gdy zdarzenie lub okoliczność, w związku z którymi wprowadzono informacje do zbioru, nie ma znamion czynu zabronionego. Po trzecie w sytuacji, w gdy osoba, której dane dotyczą, została uniewinniona prawomocnym wyrokiem sądu (art. 17b UPol). Ponadto dane osobowe zebrane w celu wykrycia przestępstwa przechowuje się przez okres niezbędny do realizacji ustawowych zadań Policji (art. 20 ust. 17 UPol). Przeciwnie, należy chyba przyjąć, że dane pozyskane w celach identyfikacyjnych albo służące zapobieżeniu popełnienia przestępstwa mogą być przechowywane bezterminowo. Takie rozwiązanie, zwłaszcza w odniesieniu do drugiej z wymienionych grup informacji, zdaje się niweczyć pozostałe ograniczenia czasowe zawarte w ustawie[19]. Mimo to warto zaznaczyć, że fakt dysponowania danymi osobowymi przez Policję z naruszeniem powyższych reguł (a zatem bezprawnie) czyni zasadnym roszczenie o ochronę dóbr osobistych[20].

Przepisy tylko częściowo wymieniają źródła, z których mogą być pozyskiwane informacje. Podstawowym z nich jest Krajowe Centrum Informacji Kryminalnej (KCIK) powołane *Ustawą z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych*[21] (dalej: ustawa o KCIK). Wskazana ustawa określa zasady gromadzenia, przetwarzania i przekazywania informacji kryminalnych oraz podmioty właściwe w tych sprawach. Zdefiniowano w niej pojęcie „informacji kryminalnej", stanowiące pojęcie nadrzędne w stosunku do terminu „dane osobowe" (zob. art. 13 ust. 2 w zw. z art. 4 pkt 1 ustawy o KCIK), zakres gromadzonej informacji kryminalnej, podmioty zobowiązane do jej przekazywania oraz uprawnione do jej otrzymywania.

Z perspektywy pracy operacyjnej istotne znaczenie ma także System Informacji Operacyjnych, czyli zestaw zbiorów danych prowadzony na potrzeby analizy kryminalnej. W rejestrze tym gromadzi się i przetwarza dane uzyskane przez policjantów podczas wykonywania czynności służbowych, przydatne do zapobiegania, rozpoznawania, ujawniania i wykrywania przestępstw, ustalania metod ich popełniania oraz wykrywania i zatrzymywania sprawców (§ 4 pkt 1 *Decyzji nr 126 Komendanta Głównego Policji z dnia 5 kwietnia 2013 r. w sprawie prowadzenia w Policji zestawu zbiorów danych „System Informacji Operacyjnych*"[22]).

Do innych rejestrów będących źródłem informacji, w tym danych osobowych, można przykładowo zaliczyć Krajowy Rejestr Sądowy, Centralną Ewidencję i Informację o Działalności Gospodarczej, księgi wieczyste czy rejestry prowadzone na podstawie *Ustawy z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej*[23], ewidencję gruntów i budynków, rejestry z biur informacji gospodarczej[24].

Jednak ani w art. 20 UPol, ani w innych przepisach ustaw policyjnych nie wskazano metod pozyskiwania, gromadzenia, sprawdzania i przetwarzania danych osobowych.

---

[19] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*..., s. 299.

[20] Wyrok SN z dnia 4 czerwca 2003 r., I CKN 480/01, Lex 137619.

[21] Tekst jednolity: Dz.U. z 2010 r. Nr 29, poz. 153, z późn. zm.

[22] Dz.Urz. KGP z 2013 r. poz. 29.

[23] Tekst jednolity: Dz.U. z 2013 r. poz. 1410.

[24] Zob. D. Koczorkiewicz, *Uprawnienie Policji do uzyskiwania informacji*, „Prokurator" 2008, nr 2–3, s. 27 i nast.

Dlatego wydaje się, że regulacje te są podstawą do sięgania nie tylko po ustawowo stypizowane metody pracy operacyjnej, takie jak np. konrola operacyjna, przesyłka niejawnie nadzorowana czy zakup kontrolowany, lecz także po metody nienazwane[25], np. wywiad lub obserwację prowadzoną bez użycia środków technicznych pozwalających na niejawnie uzyskiwanie informacji i dowodów oraz ich utrwalanie.

3. Dane telekomunikacyjne

Dostęp do danych telekomunikacyjnych (billingów) jest możliwy dzięki tzw. retencji danych telekomunikacyjnych. Jest nią gromadzenie i archiwizowanie przez usługodawców danych o ruchu w sieciach telekomunikacyjnych w celu zapobiegania, wykrywania i ścigania przestępstw[26]. Przepis art. 180a ust. 1 *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*[27] (dalej: PrTel) nakłada na operatorów publicznej sieci telekomunikacyjnej obowiązek m.in. zatrzymywania i przechowywania danych wytwarzanych w sieci telekomunikacyjnej lub przetwarzanych w ramach ich własnej działalności oraz udostępnienia tych danych na żądanie uprawnionych służb.

Zakres podmiotowy obowiązku retencyjnego nie jest jednak precyzyjny. Problemy interpretacyjne pojawiają się zwłaszcza w kontekście użycia przez prawodawcę określenia „publiczna". Chodzi o to, jakiej kwalifikacji dokonać w przypadku udostępnienia sieci bezprzewodowej w szpitalu czy hotelu, jeżeli w holu hotelowym czy sali przyjęć z usługi mogą korzystać oprócz klientów lub pacjentów także inne osoby, np. odwiedzający[28]. Inny problem interpretacyjny dotyczy sytuacji, w której podmiot będący przedsiębiorcą udostępnia na przykład w swojej kawiarni sieć bezprzewodową. W celu zakwalifikowania go do grona przedsiębiorców telekomunikacyjnych konieczne jest uznanie – oprócz publicznego charakteru możliwości takiego dostępu – także tego, że czyni to w celu zarobkowym, a zatem np. aby pozyskać klientów[29]. Zdaniem M. Siwickiego natomiast osoby fizyczne nie będą objęte obowiązkiem retencyjnym ze względu na to, że nie mogą zostać uznane za przedsiębiorców telekomunikacyjnych. W przypadku udostępnienia Internetu za pośrednictwem sieci bezprzewodowej mogą jednak zostać uznane za usługodawców świadczących usługi drogą elektroniczną w rozumieniu art. 2 pkt 6 *Ustawy z 18 lipca 2001 r. o świadczeniu usług drogą elektroniczną*[30].

Przechodząc na grunt bardziej szczegółowych rozważań, należy stwierdzić, że wskazany obowiązek dotyczy informacji koniecznych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego (w tym inicjującego połączenie oraz tego, do którego jest ono kierowane), daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia a także lokalizacji telekomunikacyjnego urządze-

[25] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*..., s. 290.

[26] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 259–260.

[27] Tekst jednolity: Dz.U. z 2014 r. poz. 243.

[28] M. Siwicki, *Retencja danych transmisyjnych na podstawie art. 180a Prawa telekomunikacyjnego*, „Prokuratura i Prawo" 2011, nr 9, s. 121.

[29] Tamże, s. 122. Jak pokazują przykłady spraw, w których przedsiębiorcy (np. fryzjerzy) podczas prowadzenia swojej głównej działalności udostępniają klientom w rzeczywistości inne usługi (np. polegające na możliwości słuchania radia podczas korzystania z usługi podstawowej), ustalenie tego, czy usługa dodatkowa jest w ogóle skierowana do klientów oraz czy ma charakter zarobkowy, nie jest łatwe. Por. wyrok ETS z dnia 15 marca 2012 r. sygn. C-135/10 (ETS – Trybunał Sprawiedliwości Unii Europejskiej, w poprzednim stanie prawnym zwany potocznie: Europejskim Trybunałem Sprawiedliwości – przyp. red.).

[30] Tekst jednolity: Dz.U. z 2013 r. poz. 1422.

nia końcowego (art. 180c ust. 1 PrTel). W rozporządzeniu wykonawczym uszczegółowiono, z jakich danych składają się powyższe informacje w odniesieniu do stacjonarnej publicznej sieci telekomunikacyjnej (§ 3 *Rozporządzenia Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania*[31] – dalej: RBillingi), ruchomej publicznej sieci telekomunikacyjnej (§ 4 RBillingi), usługi dostępu do Internetu, usługi poczty elektronicznej i usługi telefonii internetowej (§ 6 i 7 RBillingi). Na dane te składają się m.in.: przydzielony numer użytkownika końcowego (w sieciach stacjonarnych i niestacjonarnych), identyfikator anteny stacji BTS wykorzystywany w czasie inicjowania połączenia, data i godzina połączenia oraz daty i godziny zalogowania i wylogowania z usługi poczty elektronicznej lub telefonii internetowej, data i godzina połączenia i rozłączenia z Internetem oraz imię i nazwisko albo nazwa i adres użytkownika końcowego (abonenta – w przypadku stacjonarnej publicznej sieci telekomunikacyjnej). Należy zatem stwierdzić, że danymi telekomunikacyjnymi są dane osobowe. Wskazuje się, że mogą nimi być zawierający nazwisko i imię adres poczty elektronicznej, stały lub przypisywany na dłuższy okres adres IP, login, hasło czy PIN[32].

Przepis art. 180d PrTel, w celu sprecyzowania zakresu danych telekomunikacyjnych, odsyła do art. 159 ust. 1 pkt 1 i 3–5, art. 161 oraz art. 179 ust. 9 omawianej ustawy. Oznacza to, że w skład danych billingowych mogą wchodzić takie dane dotyczące użytkownika, jak numer PESEL, NIP, numer konta bankowego lub karty płatniczej, data i miejsce urodzenia, imiona rodziców, adres korespondencyjny i adres zameldowania, numer karty kredytowej i inne.

Na tym jednak nie koniec, gdyż uprawnione służby mają także dostęp do danych transmisyjnych (danych przetwarzanych w celach przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne), w tym danych lokalizacyjnych (czyli wszelkich danych przetwarzanych w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujących położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych), danych o lokalizacji, czyli danych wykraczających poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku, których gromadzenie jest możliwe tylko za wyraźną zgodą użytkownika w celu świadczenia usług o wartości wzbogaconej, Usługami tymi są np. usługi kryptograficzne, usługi z zakresu bankowości elektronicznej czy usługi anonimowego remailingu[33]. Retencja dotyczy także danych o próbach uzyskania połączenia między zakończeniami sieci, w tym o próbach nieudanych (czyli nieodebranych lub przerwanych).

Bez wątpienia dane billingowe pozwalają dogłębnie poznać zwyczaje, zainteresowania i upodobania osób, których dotyczą[34]. Samo pojęcie billingu rozumiane jako wykaz połączeń telefonicznych[35] może być wysoce mylące. W tym miejscu wypada nadmienić, że w zakresie pojęcia „tajemnica komunikowania się" znajduje się wymiana informacji pomiędzy określonymi podmiotami[36]. Nie bez racji jest twierdzenie, że

[31] Dz.U. z 2009 r. Nr 226, poz. 1828.

[32] M. Siwicki, *Retencja danych transmisyjnych…*, s. 117.

[33] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…*, s. 268.

[34] A. Adamski, *Obywatel bezpieczny, ale przeźroczysty*, „Rzeczpospolita" z 18 VIII 2000 r

[35] A. Staszak, *Prawne podstawy dopuszczalności żądania bilingów*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 4, s. 75.

[36] Treść tajemnicy komunikowania się została szeroko omówiona w rozdziale 2 pracy magisterskiej.

dostęp do danych telekomunikacyjnych ingeruje w prawo do prywatności w podobnym stopniu, jak uzyskiwany za pomocą kontroli operacyjnej dostęp do przekazywanych treści[37]. Niemniej jednak wydaje się, że zbytnim uproszczeniem jest stwierdzenie, że dane telekomunikacyjne nie zawierają żadnych treści przekazywanych komunikatów.

Zgodnie z jedną z typologii dane wytwarzane w czasie aktywności użytkownika w związku z korzystaniem z Internetu można podzielić na: dane zawierające treść (*content data*), dane o ruchu (*traffic data*) oraz dane o dostępie (*access data*). W skład danych o ruchu wchodzą adresy odwiedzanych stron internetowych (*Unique Resource Locator* – URL) oraz nagłówki wiadomości poczty elektronicznej. Nie można jednak uznać tych informacji za generowane automatycznie, a zatem za stricte techniczne. Ich wytworzenie nastąpiło wskutek świadomej działalności użytkownika, w związku z czym w literaturze zaliczane są do pierwszej ze wskazanych grup (*content data*)[38].

Dostęp do danych telekomunikacyjnych, w przeciwieństwie do informacji pozyskiwanych np. za pomocą kontroli operacyjnej, nie został jednak ograniczony przedmiotowo w żaden inny sposób poza tym wynikającym z zakresu działalności danej służby[39]. W literaturze wyrażono pogląd, że dostęp do omawianych danych jest możliwy także w postępowaniu o wykroczenie[40]. *De lege lata*[41] dane telekomunikacyjne można pozyskiwać w stosunku do osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej oraz każdej osoby fizycznej, w tym np. objętej immunitetem czy zobowiązanej do zachowania w tajemnicy informacji ustawowo chronionej. Ponadto ustawy milczą na temat warunku subsydiarności.

Tryb pozyskiwania danych telekomunikacyjnych jest realizowany nie tylko z pominięciem kontroli ze strony niezawisłego i niezależnego organu sądowego, lecz także jakiejkolwiek kontroli zewnętrznej[42]. We wszystkich ustawach policyjnych dostęp do danych może przybrać jedną z trzech form.W pierwszej z nich jest wymagane złożenie pisemnego wniosku odpowiedniego zwierzchnika uprawnionej służby albo jej komórki organizacyjnej[43], albo osób pisemnie upoważnionych do jego złożenia przez rzeczonego zwierzchnika. Drugi tryb przewiduje możliwość wystosowania ustnego[44] żądania udostępnienia omawianych danych przez funkcjonariusza danej służby posiadającego pisemne

[37] K.T. Boratyńska, *Uzyskiwanie i wykorzystywanie bilingu telefonicznego w świetle przepisów o ochronie tajemnicy telekomunikacyjnej*, „Prokurator" 2002, nr 3, s. 78.

[38] A. Adamski, *Problem retencji danych o ruchu na tle przepisów ustawy – Prawo telekomunikacyjne*, niepublikowane materiały konferencyjne (http://www.secure.edu.pl/historia/2004/docs/adamski.pdf), s. 8.

[39] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*…, s. 267.

[40] Miałoby temu służyć postanowienie sądu o zwolnieniu operatora z obowiązku zachowania tajemnicy telekomunikacyjnej na podstawie art. 180 § 1 kpk w zw. z art. 226 kpk w zw. z art. 44 § 5 Kodeksu postępowania w sprawach o wykroczenia (Dz.U. z 2013 r. Nr 395 z późn. zm.). P. Domagała, D. Dróżdż, *Dowodowe wykorzystanie wykazu połączeń telekomunikacyjnych w postępowaniu w sprawach o wykroczenia,* „Iustitia" 2011, nr 2, s. 86. Odmiennego zdania są J. Misztal-Konecka, J. Konecki, *Billing jako dowód w postępowaniu w sprawach o wykroczenia*, „Prokuratura i Prawo" 2010, nr 7, s. 78–87.

[41] Na gruncie obowiązujących przepisów (przyp. red.).

[42] Inaczej niż np. w Holandii, w której dane telekomunikacyjne są udostępniane na wniosek prokuratora i za zgodą sędziego śledczego, i to tylko w stosunku do podejrzanych o popełnienie przestępstw, K.T. Boratyńska, *Uzyskiwanie i wykorzystywanie bilingu*…, s. 77.

[43] To jest Komendanta Głównego Policji, komendanta wojewódzkiego Policji, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Centalnego Biura Antykorupcyjnego, Szefa Służby Kontrwywiadu Wojskowego, Komendanta Głównego Straży Granicznej, komendanta oddziału Straży Granicznej, Komendanta Głównego Żandarmerii Wojskowej, komendanta oddziału Żandarmerii Wojskowej lub Generalnego Inspektora Kontroli Skarbowej, a od 9 października 2014 r. również Komendanta Centralnego Biura Śledczego Policji.

[44] W przypadku organów kontroli skarbowej musi to być jednak wniosek pisemny, zob. art. 36b ust. 2 pkt 2 *Ustawy z dnia 28 września 1991 r. o kontroli skarbowej* (Dz.U. z 2015 r. poz. 553).

upoważnienie przełożonego lub upoważnienie wystawione przez osobę wyznaczoną przez przełożonego. Trzecia możliwość pozwala na dostęp do danych bilingowych za pośrednictwem sieci telekomunikacyjnej, z dochowaniem warunków przewidzianych w drugim z wariantów[45].

Pozyskiwanie danych telekomunikacyjnych nie zostało ograniczone żadnym terminem. W związku z tym niektórzy autorzy wyrażają pogląd, że *de lege lata* możliwe jest nie tylko złożenie wniosku o udostępnienie już istniejących, konkretnych danych, lecz także wezwanie ich dysponenta do ustawicznego przekazywania wytwarzanych informacji dotyczących określonego podmiotu[46]. Poglądy te, przy braku dowodów na rzeczywistą potrzebę istnienia takiej konstrukcji w działaniach służb, należy ocenić jako niedopuszczalną wykładnię rozszerzającą instytucji ingerującej w podstawowe prawa i wolności obywatelskie. Jako argument za odrzuceniem interpretacji zakładającej niedopuszczalność bieżącego pozyskiwania danych telekomunikacyjnych Dobrosława Szumiło-Kulczycka podnosi tezę o braku wzrostu faktycznego poziomu ochrony, przy jednoczesnym powstaniu „pewnych komplikacji w praktyce". Wydaje się, że zwiększenie wygody organów ścigania z powodu braku konieczności złożenia kolejnego wniosku o udostępnienie nowo powstałych danych, nie może być kwestią przesądzającą o intencji ustawodawcy.

Za to bezdyskusyjnie należy przyjąć, że na gruncie obowiązujących przepisów nie ma przeszkód, aby jednorazowy wniosek dotyczył maksymalnego okresu, w jakim dane muszą być gromadzone, czyli 12 miesięcy liczonych od dnia połączenia lub nieudanej próby połączenia (art. 180a ust. 1 pkt 1 PrTel). W tym miejscu należy wytknąć ustawodawcy brak zróżnicowania tego przedziału czasowego w zależności od różnych typów danych telekomunikacyjnych[47].

Analiza przepisów umożliwiających dostęp do danych telekomunikacyjnych dokonana przez Prokuratora Generalnego zaowocowała złożeniem wniosku o stwierdzenie ich niekonstytucyjności[48]. Z treści wniosku wynika, że Prokurator Generalny zarzuca kwestionowanym przepisom nieproporcjonalność oraz zbyt dużą dowolność, jaką ustawodawca pozostawił służbom w stosowaniu omawianego instrumentu.

Sytuację decyzyjną Trybunału Konstytucyjnego do pewnego stopnia upraszczało stwierdzenie nieważności dyrektywy 2006/24 w sprawie zatrzymywania danych[49] (tzw. dyrektywy retencyjnej), wprowadzającej ramy, w których państwa członkowskie

---

[45] Ponadto sieć telekomunikacyjna, za której pośrednictwem dane są udostępniane, musi zapewniać możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane oraz posiadać zabezpieczenia techniczne i organizacyjne uniemożliwiające dostęp osoby nieuprawnionej (art. 20c ust. 5 UPol).

[46] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze…*, s. 268; A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2004, s. 94. Odmiennie A. Lach, który stoi na stanowisku, że gromadzenie i udostępnianie danych w czasie rzeczywistym jest niedopuszczalne, zob. A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 124.

[47] Na przykład w Wielkiej Brytanii dane dotyczące abonenta i dane o połączeniach telefonicznych są objęte obowiązkiem retencyjnym przez 12 miesięcy, dane dotyczące SMS, e-mail, logi związane z połączeniami internetowymi – 6 miesięcy, dotyczące ruchu serwerów proxy dane są zaś przechowywane tylko przez 4 dni, zob. *Retention of Communications Data under. Part 11: Anti-Terrorism*, *Crime & Security Act 2001. Voluntary Code of Practice* [online], Home Office, http://www.opsi.gov.uk/si/si2003/draft/5b.pdf.

[48] Zob. wniosek PG z 21 czerwca 2012 r. dołączony do postępowania w sprawie K 23/11.

[49] *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* (Dz.Urz. UE L 105 z 13 kwietnia 2006 r., s. 54).

Unii Europejskiej były zobligowane do implementacji przepisów zapewniających retencję danych telekomunikacyjnych. Trybunał Sprawiedliwości Unii Europejskiej w wyroku *Digital Rights Ireland*[50] stanął na stanowisku, że cele wskazanego aktu można było osiągnąć środkami, które w mniejszym stopniu ingerują w prawa chronione Kartą Praw Podstawowych Unii Europejskiej, tj. prawa do poszanowanie życia prywatnego i rodzinnego (art. 7 Karty Praw Podstawowych Unii Europejskiej[51] – dalej: KPP) oraz prawa do ochrony danych osobowych (art. 8 KPP). Doszło zatem do naruszenia zasady proporcjonalności (art. 52 ust. 1 KPP). Przepisy polskiego prawa telekomunikacyjnego są wynikiem wdrożenia postanowień powyższej dyrektywy.

Stwierdzenie nieważności unijnej dyrektywy w wyroku prejudycjalnym przez Trybunał Sprawiedliwości Unii Europejskiej, jak zauważa Maciej Taborowski, jest sytuacją stosunkowo niespotykaną i nie w pełni uregulowaną[52]. Formalnie dyrektywa nadal obowiązuje, nie może jednak wywoływać żadnych skutków prawnych, a właściwe organy Unii Europejskiej są zobligowane do usunięcia stanu sprzecznego z prawem. Stwierdzenie nieważności dyrektywy wywołuje ten skutek, że kwestia retencji danych nie może być uznana za regulowaną prawem Unii Europejskiej. Co za tym idzie Trybunał Konstytucyjny był uprawniony do stosowania krajowych standardów ochrony praw podstawowych (art. 53 KPP). M. Taborowski zauważa, że gdyby standardy te okazały się niższe, niż przewiduje to Karta Praw Podstawowych, to kierując się pierwszeństwem, jednolitością i skutecznością prawa unijnego, Trybunał Konstytucyjny mógłby sięgnąć do poziomu minimalnego standardu ochrony określonego przez Trybunał Sprawiedliwości Unii Europejskiej w wyroku *Digital Rights Ireland.* Nie było to jednak konieczne, gdyż Trybunał Konstytucyjny stwierdzając niekonstytucyjność omawianych przepisów zauważył, że pustka legislacyjna w zakresie istnienia niezależnych mechanizmów kontrolnych udostępniania danych telekomunikacyjnych stanowi naruszenie norm ustawy zasadniczej[53].

4. Dane bankowe, ubezpieczeniowe i pocztowe

Uprawnienie do operacyjnego[54] pozyskiwania danych bankowych i ubezpieczeniowych posiada Policja (art. 20 UPol), Centralne Biuro Antykorupcyjne (art. 23 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*[55]) i Straż Graniczna (art. 10c *Ustawy z dnia 12 października 1990 r. o Straży Granicznej*[56]). Przepisy przyznające omawianą kompetencję dwóm ostatnim z wymienionych służb wskazują adresatów żądania, którymi oprócz banków i zakładów ubezpieczeń mogą być spółdzielcze kasy

[50] Wyrok TSUE z dnia 8 kwietnia 2014 r., *Digital Rights Ireland Ltd* v. *Minister for Communications*, *Marine and Natural Resources* i inni oraz *Kärntner Landesregierung* i inni, C-293/12.

[51] Dz.Urz. UE C 303 z 14 grudnia 2007 r., z późn. zm., s. 1.

[52] M. Taborowski, *Skutki wyroku Trybunału Sprawiedliwości Unii Europejskiej stwierdzającego nieważność dyrektywy – uwagi na tle wyroku Digital Rights Ireland*, Lex 195342.

[53] Wyrok TK z 30 lipca 2014 r. K 23/11, OTK Seria A 2014 nr 7, poz. 80. Ze względu na brak jakichkolwiek zewnętrznych mechanizmów kontrolnych TK stwierdził niekonstytucyjność przepisów umożliwiających służbom dostęp do danych telekomunikacyjnych.

[54] Pozyskiwać dane bankowe i ubezpieczeniowe mogą także, w związku z wszczętym postępowaniem przygotowawczym, organy kontroli skarbowej (art. 33 ust. 1 ustawy o kontroli skarbowej), a także, w związku z toczącym się postępowaniem o przestępstwo, Służba Celna (art. 75 ust. 1 ustawy o Służbie Celnej – patrz przyp. 64). Ponieważ w przypadku tych służb wszczęcie procesu warunkuje istnienie omawianego uprawnienia, wydaje się, że czynności te nie mogą być zakwalifikowane jako działania operacyjne.

[55] Tekst jednolity: Dz.U. z 2014 r. poz. 1411, z późn. zm.

[56] Tekst jednolity: Dz.U. z 2014 r. poz. 1402, z późn.zm.

oszczędnościowo-kredytowe, podmioty wykonujące działalność na podstawie *Ustawy z dnia 26 października 2000 r. o giełdach towarowych*[57], podmioty wykonujące działalność ubezpieczeniową, fundusze inwestycyjne, podmioty wykonujące działalność w zakresie obrotu papierami wartościowymi i innymi instrumentami finansowymi na podstawie *Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi*[58]. W ustawie o Policji natomiast oprócz banków i zakładów ubezpieczeniowych brakuje innych podmiotów zobowiązanych do udzielenia informacji stanowiących tajemnicę bankową lub ubezpieczeniową.

Tajemnica bankowa jest gwarancją prawa do prywatności[59]. Instytucja ta nie jest więc przywilejem banku, ten bowiem przyjmuje wyłącznie rolę strażnika chronionych informacji. Dookreślenie zakresu chronionych informacji znajduje się w art. 104 ust. 1 *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe*[60] (dalej: PrBank). Zgodnie z tym przepisem bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, podczas zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje. Przyjmuje się, że posłużenie się przez ustawodawcę zwrotem „wszystkie informacje" oznacza, że przedmiotowy zakres tajemnicy bankowej został oparty na zasadzie maksymalizacji[61]. W celu sprecyzowania tego, co stanowi czynność bankową, należy sięgnąć do art. 5 PrBank, w którym znajduje się ich katalog. W pierwszym ustępie tego artykułu wymieniono czynności bankowe sensu stricto, tj. takie, które ze względu na swój charakter mogą być wykonywane, co do zasady, wyłącznie przez banki (m.in. prowadzenie rachunków bankowych, udzielanie kredytów, emitowanie bankowych papierów wartościowych). W drugiej kategorii (art. 5 ust. 2 PrBank) znalazły się czynności, które są uznawane za czynności bankowe, jeżeli są wykonywane przez bank (w tym udzielanie pożyczek pieniężnych, wykonywanie operacji czekowych czy wekslowych, wydawanie kart płatniczych). Warto odnotować, że informacje przetwarzane przez banki w ramach omawianej instytucji w pewnym zakresie przypadków będą stanowić dane osobowe. Jednak ze względu na to, że prawo bankowe przewiduje ochronę idącą dalej, niż ustawa o ochronie danych osobowych, przepisy tej ostatniej nie będą mieć zastosowania (art. 5 *Ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych*[62]).

Ustawa Prawo bankowe samodzielnie reguluje wyjątki od obowiązku nieujawniania informacji stanowiących tajemnicę bankową. W związku z tym nie jest możliwe np. zwolnienie świadka od obowiązku dochowania tajemnicy bankowej na podstawie przepisów kodeksu postępowania karnego[63], w sytuacji gdy oznaczałoby to naruszenie postanowień ustawy Prawo bankowe[64]. Należy także zauważyć, że dopełnieniem omawianych przepisów kompetencyjnych są postanowienia art. 105 ust. 1 pkt 2 lit. l PrBank

[57] Tekst jednolity: Dz.U. z 2014 r. poz. 197.

[58] Tekst jednolity: Dz.U. z 2014 r. poz. 94, z późn. zm.

[59] A. Jurkowska, *Tajemnica bankowa jako środek ochrony prawa prywatności*, „Gdańskie Studia Prawnicze" 2005, t. 13, s. 221–224.

[60] Tekst jednolity: Dz.U. z 2015 r. poz. 128.

[61] T. Dukiet-Nagórska, *O ujawnianiu tajemnicy bankowej raz jeszcze*, „Prawo Bankowe" 2004, nr 3, s. 62; uchwała SN z dnia 23 maja 2005 r., I KZP 4/06, OSNKW 2006 nr 6 poz. 54.

[62] Tekst jednolity: Dz.U. z 2014 r. poz. 1182, z późn. zm.

[63] Dz.U. z 1997 r. Nr 89, poz. 555, z późn. zm.

[64] T. Dukiet-Nagórska, *O ujawnianiu tajemnicy bankowej*..., s. 59–65.

(w stosunku do regulacji z UPol), art. 105 ust. 1 pkt 2 lit. p PrBank (w stosunku do regulacji z ustawy o CBA) oraz art. 105 ust. 1 pkt 2 lit. t PrBank (w stosunku do regulacji z *Ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej*[65] – dalej: ustawa o SC). Inną konsekwencją takiego stanu rzeczy jest to, że wyjątki pozwalające na ujawnienie tajemnicy bankowej należy interpretować ściśle[66].

Pozyskiwanie informacji stanowiących tajemnicę bankową lub danych ubezpieczeniowych w drodze czynności operacyjno-rozpoznawczych jest możliwe tylko w celu skutecznego zapobieżenia (sic!) przestępstwom, ich wykryciu, ustaleniu sprawców i pozyskaniu dowodów. Zarządzenie omawianego środka jest możliwe tylko w stosunku do przestępstw, co do których możliwe jest prowadzenie kontroli operacyjnej (a w przypadku CBA – przestępstw mieszczących się we właściwości tej służby). Ponadto wskazane na wstępie regulacje wymagają także dochowania zasady subsydiarności.

Zarządzenie pobrania danych bankowych i ubezpieczeniowych następuje na mocy postanowienia właściwego sądu okręgowego, wydanego na wniosek jednego z legitymowanych do jego złożenia podmiotów[67]. Wniosek powinien zawierać elementy pisma procesowego, a ponadto: numer sprawy i jej kryptonim (jeżeli został ustalony), opis przestępstwa z podaniem (w miarę możliwości) jego kwalifikacji prawnej, okoliczności uzasadniające potrzebę udostępnienia informacji i danych, wskazanie podmiotu, którego informacje i dane dotyczą, wskazanie podmiotu zobowiązanego do udostępnienia informacji i danych oraz rodzaj i zakres informacji i danych (art. 20 ust. 6 UPol).

Nie jest jasne, czy pozyskiwanie danych, które dopiero powstaną w związku z przyszłą aktywnością, np. o bieżących obrotach na danym rachunku, mieści się w dopuszczalnym zakresie informacji, o jakie może wnioskować organ. Taki „monitoring" danych bankowych i ubezpieczeniowych, jak uważa D. Szumiło-Kulczycka, w pewnych sytuacjach może istotnie przyczynić się do realizacji funkcji prewencyjnej omawianego środka. Autorka ta zauważa wszakże nieprecyzyjność obowiązujących norm w tym zakresie[68]. Wydaje się jednak, że w związku z brakiem maksymalnych ram czasowych, w których bieżące pozyskiwanie danych mogłoby zostać zarządzone, interpretacja przepisu dopuszczająca taką możliwość chyba jednak nie przechodzi testu proporcjonalności. Dlatego należy się przyłączyć do postulatów cytowanej autorki dotyczących konieczności uzupełnienia ustawowej regulacji i dodatkowo podnieść potrzebę wprowadzenia granic temporalnych pozyskiwania danych bankowych i ubezpieczeniowych. Wydaje się, że mogłyby one być analogiczne do tych, które funkcjonują na gruncie kontroli operacyjnej prowadzonej przez Agencję Bezpieczeństwa Wewnętrznego, czyli maksymalny okres stosowania wynosiłby trzy miesiące, z możliwością jednorazowego przedłużenia o kolejne trzy miesiące (art. 27 ust. 6 ustawy o ABW oraz AW).

Na aprobatę zasługują regulacje wprowadzające obowiązek poinformowania podmiotów objętych omawianym środkiem o jego zastosowaniu. Przepisy te nie są jednak w pełni zharmonizowane. Termin, w którym obowiązek informacyjny powinien zostać zrealizowany, wynosi 90 dni od momentu przekazania danych bankowych lub ubezpieczeniowych, gdy organem wnioskującym była Policja (art. 20 ust. 10 UPol), 120

[65] Dz.U. z 2013 r. Nr 1404, z późn. zm.

[66] R. Szałowski, *Prawna ochrona tajemnicy bankowej*, „Przegląd Ustawodawstwa Gospodarczego" 1999, nr 7–8, s. 2.

[67] Czyli Komendanta Głównego Policji, komendanta wojewódzkiego Policji, Szefa CBA, Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej, a od 9 października 2014 r. również Komendanta Centralnego Biura Śledczego Policji.

[68] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*..., s. 285.

dni, w przypadku gdy udostępnienia informacji żądało Centralne Biuro Antykorupcyjne lub Straż Graniczna (art. 29 ust. 9 ustawy o CBA i art. 10c ust. 9 ustawy o Straży Granicznej). Sąd zarządzający udostępnienie danych ma możliwość odroczenia obowiązku powiadomienia o ich pozyskaniu na czas oznaczony, gdy zostanie uprawdopodobnione, że poinformowanie o zastosowanym środku może zaszkodzić wynikom podjętych czynności operacyjno-rozpoznawczych (art. 20 ust. 11 UPol). Wszczęcie postępowania przygotowawczego w powyższych okresach powoduje natomiast, że informacja o zastosowanym środku musi zostać przekazana podmiotom nim objętym najpóźniej przed zamknięciem postępowania przygotowawczego albo niezwłocznie po jego umorzeniu (art. 20 ust. 12 UPol).

Problem interpretacyjny, jaki może pojawić się w związku z obowiązkiem informacyjnym, dotyczy sytuacji, kiedy kontem bankowym, z którego pozyskiwane są dane, oprócz jego właściciela na podstawie upoważnienia dysponują także inne osoby. Wydaje się, że w takich przypadkach należałoby sporządzić wnioski o udostępnienie danych[69] dla wszystkich osób.

Jeśli chodzi o dane pocztowe, to na ich zakres składają się informacje dotyczące podmiotów korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia usług pocztowych lub korzystania z tych usług, nie obejmują one natomiast treści przekazów[70]. Dane te są objęte tajemnicą pocztową (art. 41 PrPoczt), a normy prawne umożliwiające zapoznanie się z nimi zostały oparte na podobnych zasadach, co regulacje uprawniające do pozyskiwania danych bankowych. Szerszy jest natomiast krąg podmiotów uprawnionych do korzystania z danych pocztowych, gdyż są nimi: Policja, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, organy kontroli skarbowej oraz Służba Celna.

Tryb wnioskowania o dane pocztowe jest analogiczny do trybu pozyskiwania danych telekomunikacyjnych, z pominięciem jednak możliwości dostępu za pośrednictwem systemu teleinformatycznego. Dopuszczalne cele pozyskiwania danych pocztowych zostały natomiast ograniczone do zapobiegania lub wykrywania przestępstw oraz ich sprawców (art. 20d ust. 1 UPol).

[69] J. Kudła, A. Staszak, *Praktyczne aspekty tajemnicy bankowej. Przetwarzanie i wykorzystywanie informacji zgromadzonych na etapie czynności operacyjno-rozpoznawczych*, „Policja" 2010, nr 1, s. 29.

[70] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*..., s. 278.