

Konstytucyjność działań operacyjnych służb ochrony państwaMarta Bendig¹

Organy służb ochrony państwa zostały powołane m.in. do podejmowania działań mających na celu zwalczanie i przeciwdziałanie przestępczości zorganizowanej, która w ostatnich latach rozwija się w zatrważającym tempie. Działania przestępców podejmowane są na szeroką skalę i przyjmują coraz bardziej wyszukane formy. Wynika to przede wszystkim z nieustannego rozwoju technologicznego i przemian społecznych. Sprawcy czynów zabronionych dążą do tego, aby prowadzona przez nich działalność przestępcza nigdy nie ujrzała światła dziennego, a organy ścigania nie uzyskały obciążających ich dowodów. Z tego względu do minimum starają się ograniczyć dostęp osób trzecich do informacji na ich temat. Państwo, aby skutecznie reagować na akty bezprawia – wykrywać, zwalczać oraz zapobiegać przestępczości, korzysta z różnego rodzaju metod i środków technicznych, prowadząc działania operacyjne. Coraz bardziej pożądanym źródłem informacji stają się przedstawiciele zawodów zaufania publicznego (zwłaszcza prawnicy i dziennikarze), którzy znajdują się w posiadaniu poufnych danych na temat jednostki. Spoczywający na nich obowiązek dyskrecji zawodowej jest gwarancją zapewnienia jednostce realizacji przysługujących jej praw i wolności konstytucyjnych. Z tego względu należy zastanowić się, w jaki sposób służby mogą ingerować w poszczególne wartości, oraz w jakim stopniu podejmowane przez nie działania mogą zagrażać prawidłowemu wykonywaniu czynności zawodowych przez podmioty upoważnione do zachowania tajemnicy zawodowej.

1. Metody pozyskiwania danych na temat jednostki

Służby „mundurowe” chcąc przeciwdziałać przestępczości zorganizowanej podejmują czynności operacyjno – rozpoznawcze, które zorientowane są na pozyskiwanie niezbędnych informacji na temat jednostki, weryfikowanie uzyskanych danych oraz ich dalsze wykorzystywanie. Przepisy ustaw szczególnych, które odnoszą się do sposobu organizacji i funkcjonowania określonych służb, przewidują różnego rodzaju metody umożliwiające realizację powierzonych im zadań. Wśród nich bardzo ważną rolę odgrywa kontrola operacyjna. W ramach przyznanych uprawnień organy mogą uzyskiwać i utrzymywać treści rozmów telefonicznych prowadzonych z wykorzystaniem dostępnych urządzeń telekomunikacyjnych, uzyskiwać i utrzymywać obraz bądź dźwięk, kontrolować treść korespondencji, zawartość przesyłek, jak również pozyskiwać dane

¹ Opracowanie odnosi się do wybranych zagadnień, przedstawionych szerzej przez autorkę w ramach pracy dyplomowej pt. „Karnoprawna ochrona tajemnicy zawodowej a uprawnienia służb ochrony państwa w zakresie czynności operacyjnych”, przygotowanej pod kierunkiem dr hab. Andrzeja Adamskiego, prof. UMK.

zawarte w nośnikach informatycznych². Katalog czynności podejmowanych w ramach kontroli operacyjnej jest katalogiem zamkniętym³, a prowadzone działania mają charakter niejawny. Przepisy w żaden sposób nie ograniczają ani rodzaju pozyskiwanych danych, ani też zakresu podejmowanych działań⁴. Uzyskiwane informacje mogą odnosić się zarówno do sfery życia prywatnego jednostki, jak i do podejmowanej przez nią aktywności zawodowej. Należy wyraźnie wskazać, iż ustawodawca nie wskazał dokładnie środków technicznych, które mogą być wykorzystywane przez służby, zatem mają one pod tym względem nieograniczone możliwości. Mogą więc korzystać m.in.: z urządzeń podsłuchowych, mikrofonów kierunkowych, urządzeń rejestrujących obraz i dźwięk za pomocą metadanych lub nawigacji satelitarnej⁵. Bez znaczenia jest forma komunikowania się podmiotów między sobą czy wykorzystywany w tym celu nośnik informacji. Oznacza to, iż organy mają możliwość pozyskiwania treści nie tylko tych przekazywanych osobiście czy pisemnie, ale również w drodze komunikacji telefonicznej czy e – mailowej⁶.

Coraz częściej treść przekazywanych komunikatów przestaje być dla służb satysfakcjonującym źródłem informacji. Z tego też względu w ostatnich latach bardzo mocno wzrosła rola pozyskiwania danych od przedsiębiorców telekomunikacyjnych. Służby, występując o udostępnienie danych abonenckich⁷, mogą wejść w posiadanie nie tylko informacji na temat danych osobowych abonenta, ale również uzyskać różnego rodzaju informacje na temat okoliczności związanych ze zrealizowanym połączeniem lub jego potencjalną próbą (chodzi tu szczególnie o datę połączenia, czas jego trwania, rodzaj połączenia, częstotliwość połączeń, położenie geograficzne urządzenia ruchomego umożliwiającego komunikację na odległość), jak również szczegółowe dane o przeglądanych stronach internetowych, czy informacje niezbędne dla ustalenia: zakończenia sieci, telekomunikacyjnego urządzenia końcowego, jak również użytkownika końcowego – zarówno inicjującego połączenie, jak i tego, do którego jest ono

² Ustawa z dnia 6 kwietnia 1990r. o Policji, Dz. U. 1990, nr 30, poz. 179 ze zm., art. 19 ust. 6 pkt 1) – 5).

³ Zob. przepisy wybranych ustaw m.in.: ustawa z dnia 6 kwietnia 1990r. o Policji, Dz. U. 1990, nr 30, poz. 179 ze zm., art. 19 ust.6; ustawa z dnia 9 czerwca 2006r. o Centralnym Biurze Antykorupcyjnym, Dz. U. 2006, nr 104, poz. 708 ze zm., art. 17 ust. 5; ustawa z dnia 12 października 1990r. o Straży Granicznej, Dz. U. 1990, nr 78, poz. 462 ze zm., art. 9e ust. 7; ustawa z dnia 24 sierpnia 2001r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz. U. 2001, nr 123, poz. 1353 ze zm., art. 31 ust. 5.

⁴ M. Szczepaniec, *Ochrona informacji poufnych w świetle standardów konstytucyjnych*, [w:] A. Adamski, M. Leciak (red.), *Krajowy model regulacji prawnej przetwarzania danych w obszarze monitorowania, wykrywania i zapobiegania przestępstwom (analiza i ocena po wyroku Trybunału Konstytucyjnego z 30 lipca 2014, K/11)*, Warszawa 2015, s. 115 – 116.

⁵ M. Tomkiewicz, *Stosowanie kontroli operacyjnej w toku postępowania karnego*, „Roczniki Nauk Prawnych”, tom XXVI, nr 4, Lublin 2016, s. 122; Wyrok TK z dnia 30 lipca 2014r., sygn. K 23/11, OTK ZU A/2014, nr 7, poz. 80.

⁶ M. Rogalski, *Kontrola korespondencji*, Warszawa 2016, s. 10.

⁷ A. Staszak, *Prawne podstawy dopuszczalności żądania bilingów*, „Przegląd Bezpieczeństwa Wewnętrznego”, nr 4, Warszawa 2011, s. 75; podobnie: postanowienie SN z dnia 25 marca 2010r., sygn. I KZP 37/09, Izba Karna, Baza Orzeczeń Sądu Najwyższego; M. Rogalski, *Udostępnianie danych telekomunikacyjnych sądom i prokuratorom*, „Prawo i Prokuratura”, nr 12, Warszawa 2015, s. 68.

kierowane⁸. Uzyskanie takich danych stanowi obecnie jeden z najprostszych sposobów uzyskania informacji na temat jednostki – służby nie mają obowiązku podawania powodu, dla którego występują o ujawnienie takich danych, a dostawca usług telekomunikacyjnych nie musi analizować, czy dane te są niezbędne dla toczącego się postępowania oraz jaki jest rzeczywisty cel ich pozyskiwania. Wystarczy więc, że funkcjonariusz złoży w tej sprawie odpowiedni wniosek, albo skieruje żądanie ustne, a wówczas przedsiębiorca ma obowiązek przekazać określone informacje, przy czym może udostępniać je również drogą elektroniczną⁹. Należy zauważyć, że tego rodzaju czynności operacyjne nie wymagają zgody organu nadrzędnego na ich realizację. Przepisy przewidują jedynie kontrolę *post factum* sądu okręgowego (w ramach której przyznają sądowi możliwość zapoznania się z materiałami, które uzasadniają podjęcie takich działań), jak też obligują służby do sporządzenia półrocznych sprawozdań z pozyskiwania tego rodzaju danych¹⁰. Regulacja ta wydaje się być jednak niepełna. Sporządzane przez służby sprawozdania ograniczają się wyłącznie do wskazania liczby przypadków sięgania po dane telekomunikacyjne, ich rodzaje oraz kwalifikacje prawną czynów uzasadniających występowanie po nie. Wydaje się, że sprawozdania te powinny zawierać dodatkowe informacje, odnoszące się m.in.: do niektórych okoliczności związanych ze sprawą, częstotliwości korzystania przez służby z takich metod oraz inne dane statystyczne. Część zawartych w sprawozdaniach informacji powinna zostać przekazana do wiadomości publicznej, aby społeczeństwo nie tylko miało świadomość podejmowania takich działań, ale przede wszystkim obraz korzyści, jakie z takiego wynikają, w kontekście zwalczania i zapobiegania przestępczości zorganizowanej. Wątpliwości budzi fakt, iż pozyskiwanie danych podlega jedynie kontroli następczej. Mając na względzie, iż w ten sposób organy silnie ingerują w prywatność jednostki, uzyskując na jej temat bardzo szczegółowe informacje, należałoby wprowadzić bardziej skuteczne gwarancje realizacji jej praw. Po pierwsze, przepisy powinny przewidywać obowiązek uzyskania obligatoryjnej zgody na podjęcie takich czynności, co pozwoliłoby ograniczyć ich podejmowanie jedynie do sytuacji, w których jest to naprawdę niezbędne dla dobra wymiaru sprawiedliwości. Z uwagi na stosowane środki, tego rodzaju kontrola miałaby szczególne znaczenie w przypadku podmiotów wykonujących zawody zaufania publicznego, na których spoczywa obowiązek zachowania tajemnicy zawodowej. Mając na względzie fakt, iż zachowanie poufności we wzajemnych kontaktach jest jednym z podstawowych warunków wykonywania czynności zawodowych, pozwoliłoby to na bardziej skuteczną ochronę praw dysponenta informacji. Na ten moment przepisy nie precyzują sytuacji, które uzasadniałyby gromadzenie takich danych¹¹. Zawierają one bardzo ogólne stwierdzenia, które wskazują, że

⁸ Ustawa z dnia 16 lipca 2004r. Prawo telekomunikacyjne, Dz. U. 2004, nr 171, poz. 1800 ze zm., art. 179 ust. 3 pkt. 1 lit. a), art. 180c; M. Rogalski, *Kontrola korespondencji*, Warszawa 2016, s. 10; Wyrok TK z dnia 30 lipca 2014r., sygn. K 23/11, OTK ZU A/2014, nr 7, poz. 80.

⁹ Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. 1990, nr 30, poz. 179 ze zm., art. 20ca ust. 2.

¹⁰ Ibidem, art. 20ca ust. 1, ust. 2.

¹¹ M. Kiziński, *Retencja danych telekomunikacyjnych*, „Prawo i Prokuratura”, nr 1, Warszawa 2016, s. 152.

służbom przysługuje prawo podejmowania takich działań w celu zapobiegania lub wykrywania przestępczości, bądź w celu ratowania życia lub zdrowia ludzkiego, wsparcia działań poszukiwawczych lub ratowniczych. Dlatego też zakres spraw uzasadniających występowanie przez organy o tego rodzaju dane jest ujęty bardzo szeroko¹², co też może prowadzić do nadmiernego wykorzystania przyznanych im w tym zakresie kompetencji.

2. Wpływ działań operacyjnych na prawa i wolności obywatela

W kontekście podejmowanych rozważań warto byłoby się zastanowić, w jaki sposób podejmowane przez służby czynności mogą wpływać na prawa i wolności jednostki, oraz czy stosowane metody mogą nadmiernie w nie ingerować. Czy działania te, aby na pewno będą realizować zasadę subsydiarności i stanowić swoiste *ultima ratio*? Jak zostało to już wcześniej wskazane, służby w toku wykonywanych przez siebie zadań mogą ingerować w prawo do prywatności jednostki¹³. Ponieważ przepisy nie definiują, czym jest prywatność, należy odnieść się w tej kwestii do orzecznictwa Trybunału Konstytucyjnego, który wskazuje, iż jest to „*autonomia informacyjna jednostki, oznaczająca prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby*”¹⁴. Realizując to prawo, jednostka ma możliwość „*samostanowienia o swym życiu osobistym w aspekcie przedmiotowym, podmiotowym oraz czasowym*”¹⁵, oraz sprawowania pełnej kontroli nad tym, komu ujawnia informacje na swój temat. Ponieważ prawo do prywatności nie ma charakteru bezwzględnego i podlega pewnym ograniczeniom¹⁶, aby zachować podstawowe granice ochrony danego dobra, przepisy muszą określać przesłanki przemawiające za podjęciem określonych działań w tym zakresie, jak również wyraźnie określać granice takiej ingerencji¹⁷. Z tego względu przepisy Konstytucji przewidują, iż obowiązek ujawnienia informacji na temat danej osoby może wynikać jedynie z przepisów ustawy¹⁸. Oznacza to, iż jednostka dalej może swobodnie decydować o przekazaniu przez nią informacji na jej temat, a konieczność ich ujawnienia w oparciu o przepisy ustawy nie może być traktowana w kategorii ograniczenia autonomii jej praw. Konstytucja przewiduje również, iż pozyskiwanie i gromadzenie informacji o jednostce musi następować w sposób zgodny z zasadą demokratycznego państwa prawa. Dlatego też konieczność zachowania przez organy państwa podstawowych standardów, może stanowić silną barierę przed bezpodstawnym żądaniem

¹² M. Rogalski, *Kontrola korespondencji*, Warszawa 2016, s. 226 – 227.

¹³ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r., Dz. U. 1997, nr 78, poz. 483 ze zm., art. 47.

¹⁴ Wyrok TK z dnia 19 lutego 2002r., sygn. U 3/01, Dz.U. Nr 019, poz. 197.

¹⁵ Wyrok TK z dnia 25 lipca 2013r., sygn. K 41/02, OTK ZU 6A/2002, poz. 83.

¹⁶ A. Sakowicz, *Prawnokarne gwarancje prywatności*, Kraków 2006, s. 98.

¹⁷ Wyrok TK z dnia 20 listopada 2002r., sygn. K 41/02, OTK ZU 6A/2002, poz. 83.

¹⁸ Konstytucja RP z dnia 2 kwietnia 1997r. Dz. U. 1997, nr 78, poz. 483 ze zm., art. 51 ust.1.

ujawnienia informacji na potrzeby działania organów ścigania¹⁹. Mimo, iż trudno jest ocenić, jakie informacje powinny być przekazywane organom władzy publicznej, to regulacji tej nie powinno się traktować jedynie w kategorii ograniczenia prawa jednostki do decydowania o tym, jakie dane na temat jej osoby powinny zostać ujawnione²⁰. Przepis ten należy bowiem interpretować w powiązaniu z regulacją wskazaną w art. 31 ust. 3 Konstytucji²¹, która wskazuje, iż prawa i wolności jednostki mogą podlegać pewnym ograniczeniom, jednakże, muszą one wynikać wyłącznie z przepisów ustawy i mogą być ustanawiane tylko wtedy, gdy jest to konieczne dla zapewnienia podstawowych praw ogółu – bezpieczeństwa, porządku publicznego, ochrony zdrowia, środowiska, moralności publicznej oraz praw i wolności innych osób. Ingerencja w prawa jednostki musi być niezbędna dla osiągnięcia określonych celów, jak również musi być w jak najmniejszym stopniu dolegliwa dla danego podmiotu. Dlatego też podjęcie działań przez służby wymaga dokonania oceny, czy udało się zachować konstytucyjną zasadę subsydiarności. Działania te powinny być bowiem podejmowane wyłącznie wtedy, gdy uprzednio stosowane środki okazały się bezskuteczne, oraz jeżeli istnieje ryzyko, że inne środki nie przyniosą oczekiwanych rezultatów²². Ważne, aby wykorzystywane środki były proporcjonalne do realizacji określonego celu. Organy mają obowiązek, aby utrzymać właściwą proporcję pomiędzy wartościami, jakie w tym przypadku podlegają ochronie prawnej – z jednej strony jest to interes prywatny jednostki, z drugiej konieczność zapewnienia bezpieczeństwa państwa i jego obywateli. Rozstrzygnięcie kolizji dóbr, jaka tutaj występuje wymaga rozpatrzenia sytuacji *in concreto*, bowiem nie da się przyznać na stałe pierwszeństwa któremukolwiek z nich. Bezspornym jest jednak, że zapewnienie bezpieczeństwa państwa i porządku publicznego stanowi jedno z podstawowych zadań organów państwa. Dlatego też organy każdorazowo muszą uwzględnić, czy dla jego prawidłowej realizacji konieczna jest ingerencja w prawa jednostki, a jeśli tak, to w jakim stopniu ograniczenie to może mieć miejsce. Powinny wziąć pod uwagę również wynikające z tego korzyści²³.

Powyższe rozważania pozwalają zatem wysnuć wniosek, iż w aspekcie podejmowania działań operacyjnych nie można bezkrytycznie przyjąć, że organom przysługuje kompetencja do ingerowania w prawa jednostki²⁴. W rzeczywistości każdemu podmiotowi przysługuje prawo zachowania całkowitej swobody w korzystaniu z przyznanych mu praw, tyle, że w granicach, jakie wynikają z przepisów konkretnej ustawy. Decydując się na ich ograniczenie, organy władzy państwowej mają obowiązek, aby zapewnić jednostce należyte gwarancje materialne

¹⁹ Wyrok TK z dnia 20 listopada 2002r., sygn. K 41/02, OTK ZU 6A/2002, poz. 83.

²⁰ Wyrok TK z dnia 17 czerwca 2008r., sygn. K 8/04, OTK ZU 5A/2008, poz. 81.

²¹ Ibidem.

²² P. Pochodyła, S. Franc, *Kontrola operacyjna oraz zakres jej stosowania*, „Zeszyty Naukowe WSEI”, tom I, nr I, Lublin 2001, s. 205.

²³ Wyrok TK z dnia 25 lipca 2013r., sygn. K 41/02, OTK ZU 6A/2002, poz. 83.

²⁴ M. Rogalski, *Kontrola korespondencji*, Warszawa 2016, s. 6, za: wyrok TK z dnia 30 lipca 2014r., sygn. K 23/11, OTK ZU A/2014, nr 7, poz. 80.

i proceduralne, które pozwolą skutecznie realizować przyznane jej prawa. Aktualne przepisy przewidują wiele rozwiązań prawnych w tym zakresie, jednak zasadniczym problemem jest się tu pojawia, jest brak możliwości zakwestionowania podejmowanych wobec jednostki działań operacyjnych. Ustawodawca w art. 51 ust. 4 Konstytucji, przewidział możliwość żądania przez jednostkę sprostowania oraz usunięcia informacji, które są nieprawdziwe, niepełne lub zebrane w sposób sprzeczny z ustawą. Aby jednak skutecznie realizować to prawo, podmiot inwigilowany musiałby posiadać wiedzę o podejmowanych wobec niego działaniach. Na ten moment organy nie muszą informować o tym jednostki, jak również nie mają obowiązku udostępnienia jej zgromadzonych w toku czynności materiałów²⁵. Wyjątek dotyczy jedynie sytuacji, w której jednostka zdążyła dowiedzieć się o tym, iż podlegała inwigilacji i zostało wobec niej podjęte postępowanie sądowe²⁶. Brak gwarancji w postaci obligatoryjnego obowiązku informacyjnego (realizowanego chociażby *post factum*) uniemożliwia skorzystanie z ewentualnego środka zaskarżenia. Dlatego też należy stwierdzić, iż na ten moment jednostka nie ma możliwości skutecznego zakwestionowania zasadności bądź legalności²⁷ podjętych wobec niej działań operacyjno – rozpoznawczych, jak również dalszego wykorzystania pozyskanych materiałów w toku postępowania przed sądem.

3. Gwarancja dyskrecji zawodowej w świetle czynności operacyjnych

Prawo do prywatności silnie wiąże się z ochroną tajemnicy zawodowej, należy więc zastanowić się, jak plasuje się sytuacja między prowadzeniem działań operacyjnych, a zapewnieniem prawidłowości wykonywania czynności zawodowych. Obowiązek zachowania dyskrecji i poufności informacji umożliwia ochronę interesów jej dysponenta²⁸. W przypadku tajemnicy obrończej, to właśnie stosunek zaufania, jaki powstaje między pełnomocnikiem, a jego klientem sprawia, że klient staje się bardziej skłonny do współpracy i decyduje się na ujawnienie wszystkich okoliczności faktycznych sprawy. Gdyby obawiał się, że powierzone pełnomocnikowi informacje znajdują się w posiadaniu służb, mógłby przekazywać je bardzo wybiórczo, a niekiedy nawet wprowadzać obrońcę w błąd, co do stanu rzeczywistego. Dlatego też nagminne stosowanie urządzeń podsłuchowych lub innych form pozyskiwania informacji na temat jednostki, w przypadku tajemnicy obrończej może ograniczyć skuteczność działania pełnomocnika, a w oczach społeczeństwa być odebrane, jako stawające wbrew interesom klienta²⁹. Podobnie jest

²⁵ Ustawa z dnia 6 kwietnia 1990r. o Policji, Dz. U. 1990, nr 30, poz. 179 ze zm., art. 19 ust. 16.

²⁶ Postanowienie TK z dnia 25 stycznia 2006r., sygn. S 2/06, OTK ZU 2006/ 1A/13.

²⁷ M. Tomkiewicz, *Kontrola procesowa i operacyjna a ochrona praw podmiotowych osoby inwigilowanej w Polsce*, „Profilaktyka społeczna i resocjalizacja”, nr 25, Warszawa 2015, s. 17.

²⁸ Wyrok TK z dnia 30 lipca 2014r., sygn. K 23/11, OTK ZU A/2014, nr 7, poz 80.

²⁹ M. Rogalski, *Kontrola korespondencji*, Warszawa 2016, s. 11.

w przypadku tajemnicy dziennikarskiej. Uzyskanie przez dziennikarzy informacji od anonimowych informatorów często wiąże się z koniecznością zachowania w tajemnicy ich tożsamości. Ma to na celu nie tylko zapewnienie ochrony dziennikarskich źródeł informacji czy też praw i interesów osób trzecich, ale przede wszystkim zagwarantowanie wolności prasy³⁰. Dlatego też pozyskiwanie bilingów, podsłuchiwanie prowadzonych rozmów czy montowanie urządzeń audiowizualnych w redakcjach może stanowić poważne zagrożenie dla ochrony wzajemnych relacji między tymi podmiotami.

Ustawodawca, który dostrzegł konieczność uregulowania niniejszej kwestii, zdecydował się na wprowadzenie zróżnicowanego mechanizmu ochrony informacji stanowiących tajemnicę zawodową nie tylko w toku prowadzenia postępowania przed sądem, ale również w związku z prowadzeniem działań kontroli operacyjnej. Wprowadził odrębny tryb ochrony w przypadku informacji objętych tajemnicą obrończą i tajemnicą duchownego oraz tych, które obejmują inne rodzaje tajemnic zawodowych. Mając na względzie fakt, iż zgodnie z przepisami procesowymi, nie można wykorzystać w charakterze materiału dowodowego informacji, które stanowią tajemnicę o charakterze bezwzględnie, również w tym przypadku przyjęto rozwiązanie zgodnie z którym materiały te podlegają niezwłocznie komisyjnemu i protokolarnemu zniszczeniu³¹, co pozwala na ich skuteczną eliminację z obrotu prawnego. W sytuacji, gdy istnieje podejrzenie, że uzyskane wiadomości mogą stanowić treść tajemnic określonych w art. 180 § 2 k.p.k.³² tryb ten jest bardziej rozbudowany. W pierwszej kolejności materiały przekazywane są do prokuratury, skąd następnie kierowane są do sądu wraz z wnioskiem o dopuszczenie ich do ich dalszego wykorzystania. To sąd podejmuje decyzje, w której albo zezwala na ich wykorzystanie w toku postępowania (przy czym decyzja ja nie jest tożsama ze zwolnieniem z obowiązku zachowania tajemnicy zawodowej na etapie przesłuchania konkretnej osoby w charakterze świadka), albo też zwraca je organom służb nakazując ich niezwłoczne zniszczenie. Ustawodawca nie przewidział żadnych mechanizmów nadzorujących nad procesem niszczenia tego rodzaju danych, co oznacza, iż to służby mają uprawnienia decyzyjne w zakresie określenia wszelkich procedur w tym zakresie i nie podlegają pod tym względem żadnej kontroli z zewnątrz. Należy zwrócić uwagę na podstawowe problemy, jakie się tutaj pojawiają. Skoro to funkcjonariusz danej służby podejmuje decyzje o tym, czy materiały powinny być przekazane do dalszej analizy pod kątem zapewnienia należytej ochrony tajemnicy zawodowej, to czy jest to właściwa osoba do podejmowania tak poważnych decyzji, które ewidentnie wpływają na dalszy tryb postępowania z uzyskanymi materiałami? Wydaje się, że wszystkie materiały operacyjne powinny trafiać bezpośrednio pod ocenę organów sądowych. Brak precyzyjnego określenia terminu ich niszczenia, jak również wydłużenie toku postępowania

³⁰ I. Zielinko, *Tajemnica dziennikarska w prawie prasowym*, „Prawo i Prokuratura” nr 7 – 8, Warszawa 2009, s. 150.

³¹ Ustawa z dnia 6 kwietnia 1990r. o Policji, Dz. U. 1990, nr 30, poz. 179 ze zm., art. 19 ust. 15f pkt. 1).

³² Ustawa z dnia 6 czerwca 1997r. Kodeks postępowania karnego, Dz. U. 1997, nr 89, poz. 555 ze zm., art. 180 § 2.

w sytuacji, gdy istnieje podejrzenie, że zebrane materiały mogą stanowić m.in.: tajemnicę dziennikarską, adwokacką czy radcowską, może prowadzić do bardzo poważnych skutków dla jednostki. Nieprawidłowe ich zabezpieczenie oraz zbyt długi czas przechowywania niewątpliwie zwiększa ryzyko zapoznania się z ich treścią przez osoby postronne – niezwiązane zupełnie ze sprawą, jak również na kwestie ich wykorzystywania w toku dalszych działań. Coraz częściej można dostrzec, że służby zmierzają do gromadzenia i przechowywania danych przez dłuższy okres czasu nawet wtedy, gdy nie mają one znaczenia dla danego postępowania i nie są związane z osobami podejrzanymi o prowadzenia działalności przestępczej. Wyraźnie należy jednak podkreślić, że działania operacyjne powinny być prowadzone jedynie dla konkretnego postępowania³³, dlatego też wszelkie dążenia ustawodawcy do prewencyjnego przechowywania danych wydają się być bardzo niepokojące i należy poddać je krytycznej ocenie. Jeżeli zgodnie z art. 51 ust. 2 Konstytucji, organy mogą pozyskiwać informacje na temat jednostki jedynie w granicach niezbędnych w demokratycznym państwie prawa, to skoro brakuje określenia celu ich pozyskiwania, to jednocześnie nie ma spełnionej cechy niezbędności działania³⁴. Wątpliwości budzi również fakt, iż w stosunku do przedstawicieli zawodów zaufania publicznego, ustawodawca nie ograniczył stosowanych w toku czynności operacyjnych środków technicznych. Warto byłoby, aby służby podejmując czynności operacyjno – rozpoznawcze w stosunku do podmiotów, na których spoczywa obowiązek zachowania tajemnicy zawodowej stosowały wyłącznie takie środki, które do minimum ograniczą dostęp funkcjonariuszy do treści informacji.

4. Podsumowanie

Podejmowanie działań operacyjnych jest bez wątpienia słuszne, a wręcz niezbędne dla zapewnienia prawidłowego funkcjonowania państwa, szczególnie w związku z zapewnieniem bezpieczeństwa narodowego i porządku publicznego poprzez zwalczanie przestępczości zorganizowanej. Wykorzystywane środki pozwalają na bieżące monitorowanie aktywności życiowej jednostki w przestrzeni publicznej, a co za tym idzie pozwolą na skuteczne weryfikowanie podejrzeń w stosunku do osoby podlegającej kontroli. Dzięki temu organy mogą ukierunkowywać swoje dalsze działania, co też zwiększa skuteczność ich realizacji. Jednakże, jak potwierdziły dotychczasowe rozważania, zbieranie danych na temat jednostki, może stanowić naruszenie naczelných zasad funkcjonowania państwa, odnoszących się do zapewnienia jednostce prawa do prywatności, oraz wolności i ochrony tajemnicy komunikowania się³⁵, co odgrywa szczególną rolę

³³ Wyrok TK z dnia 12 grudnia 2005r., sygn. K 32/04, OTK ZU 11A/2005, poz. 132.

³⁴ M. Tomkiewicz, *Kontrola procesowa i operacyjna a ochrona praw podmiotowych osoby inwigilowanej w Polsce*, Profilaktyka społeczna i resocjalizacja, nr 25, Warszawa 2015, s. 21.

³⁵ M. Rogalski, *Kontrola korespondencji*, Warszawa 2016, s. 229.

w sytuacjach, gdy komunikacja objęta jest ochroną tajemnicy zawodowej. Niewątpliwie problem ten został wreszcie dostrzeżony przez ustawodawcę, niestety jedynie w kontekście prowadzenia czynności kontroli operacyjnej. Zagadnienie to całkowicie pominięto w odniesieniu do pozyskiwania danych telekomunikacyjnych, co bez wątpienia stanowi poważną lukę w przepisach i wymaga uwzględnienia przez krajowego legislatora w przyszłości. Obecna regulacja również budzi poważne wątpliwości – jest niepełna i chaotyczna, pomija wiele istotnych problemów związanych z ochroną tajemnicy zawodowej, szczególnie w kontekście zachowania odpowiednich gwarancji dla jednostki. Należy bowiem pamiętać, że tajemnica zawodowa ma chronić poufność informacji, a nie osobę jej depozytariusza³⁶. Dlatego też stanowi ona jeden z podstawowych obowiązków, jakie spoczywają na nim z tytułu wykonywania określonego zawodu.

Warto byłoby uzupełnić obowiązujące przepisy o regulację, które w pewien sposób będą niejako różnicowały podejmowanie działań operacyjnych wobec przedstawicieli zawodów zaufania publicznego. Na pierwszy rzut oka wydawać by się mogło, iż w ten sposób ustawodawca naruszyłby jedną z fundamentalnych dla polskiego systemu prawnego zasad – zasadę równości wobec prawa. Ze stwierdzeniem tym nie można się jednak zgodzić. Naruszeniem niniejszej zasady byłoby raczej całkowite wyłączenie tej kategorii podmiotów spod podlegania działaniom operacyjnym. Mając zatem na względzie ich szczególną rolę w społeczeństwie, prestiż wykonywanego zawodu, oraz odpowiedzialność, jaka na nich ciąży ustawodawca powinien zapewnić im odpowiednie warunki wykonywania wybranego zawodu. Nadmierna inwigilacja może bowiem doprowadzić od sytuacji, w której druga strona utraci zaufanie niezbędne do wykonywania nałożonych na jednostkę obowiązków zawodowych. Wydaje się, że tylko w ten sposób możliwym jest skuteczne realizowanie przyznanych jednostce praw, a co za tym idzie prawidłowe jej funkcjonowanie w społeczeństwie. Na tle aktualnych problemów, wprowadzenie uprzedniej kontroli sądowej, obligatoryjnego obowiązku informacyjnego i ograniczenie katalogu przestępstw, których popełnienie uzasadnia możliwość podjęcia określonych działań, stanowi niezbędne minimum, jakie należy zagwarantować w kontekście zapewnienia ochrony tajemnicy zawodowej. Ustawodawca powinien jasno i wyraźnie określić przysługujące jednostce gwarancje. Tylko w ten sposób będzie mogła ona zachować pewność, co do tego, że państwo dąży do zachowania należytych standardów realizacji praw wynikających z ustawy zasadniczej.

³⁶ M. Rusinek, *Kontrola operacyjna a ochrona tajemnicy zawodowej w świetle wyroku TK z dnia 30 lipca 2014r.*, [w:] A. Adamski, M. Leciak (red.), *Krajowy model regulacji prawnej przetwarzania danych w obszarze monitorowania, wykrywania i zapobiegania przestępstwom (analiza i ocena po wyroku Trybunału Konstytucyjnego z 30 lipca 2014, K/11)*, Warszawa 2015, s. 124.

Konstytucyjność działań operacyjnych służb ochrony państwa

Marta Bendig

O autorze

Studentka V roku prawa na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu, magistrantka w Katedrze Prawa Karnego, Wiceprezes Studenckiego Koła Naukowego Prawa Karnego.

Zainteresowania naukowe: prawo karne, prawa i wolności jednostki, bezpieczeństwo państwa

Streszczenie

Niniejsze opracowanie stanowi zasygnalizowanie niektórych problemów, jakie wiążą się z prowadzeniem czynności operacyjnych w związku z ochroną tajemnicy zawodowej. W pierwszej kolejności wskazano metody pozyskiwania informacji i wynikające z nich zagrożenia dla jednostki. W dalszej kolejności wskazano, które z wartości konstytucyjnych mogą podlegać ewentualnym ograniczeniom wskutek nazbyt silnej ingerencji ze strony państwa, oraz wskazano, w jakim stopniu uzasadnionym będzie podejmowanie działań kontrolnych w kontekście ewentualnych zagrożeń dla bezpieczeństwa państwa. Meritum pracy koncentruje się na szczegółowej analizie przepisów odnoszących się do ochrony tajemnicy zawodowej z perspektywy prowadzenia przez służby ochrony państwa działań kontroli operacyjnej, wskazaniu problemów prawnych, jakie się z tym wiążą i proponowanych w tym zakresie rozwiązań.

Słowa kluczowe

inwigilacja, kontrola operacyjna, dane telekomunikacyjne, tajemnica zawodowa, prawo do prywatności

Constitutionality of operational activities of state protection services

Marta Bendig

Summary

This study is a signal to some of the problems associated with the conduct of operational activities in connection with the protection of professional secrecy. In the first place, the methods of obtaining information and the resulting threats to the individual were indicated. Subsequently, it was pointed out which of the constitutional values may be subject to possible restrictions as a result of overly strong state interference, and it was indicated to what extent it would be justified to undertake control activities in the context of possible threats to the security of the state. The work merit focuses on a detailed analysis of provisions relating to the protection of professional secrecy from the perspective of operating by the state security services, operational control, indication of legal problems that arise and solutions proposed in this regard.

Key words

surveillance, operational control, data telecommunications, professional secrecy, the right to privacy