Paragraf 5 / 2024
https://doi.org/10.18778/2956-3747.5.02

Kamil Florczak*

Kontrola operacyjna Agencji Bezpieczeństwa Wewnętrznego

Streszczenie

Celem artykułu jest omówienie kontroli operacyjnej na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Środek ten, potocznie zwany inwigilacją, jest jedną z najdotkliwszych ingerencji w konstytucyjnie zagwarantowaną wolność komunikowania się. Głównym uzasadnieniem dla podejmowania tak daleko idących środków jest bezpieczeństwo państwa czy wykrywanie i zapobieganie przestępstwom. Autor objaśnia instytucję kontroli operacyjnej na gruncie wspomnianej ustawy. Jednak należy zaznaczyć, iż przepisy regulujące inwigilację w innych ustawach są w gruncie rzeczy takie same. Artykuł przedstawia formy kontroli operacyjnej, jej podstawy i cel także w kontekście orzecznictwa polskiego oraz Europejskiego Trybunału Praw Człowieka.

Słowa kluczowe: kontrola operacyjna, Agencja Bezpieczeństwa Wewnętrznego, Konstytucja, wolność komunikowania się, inwigilacja

Operational control of the Internal Security Agency

Abstract

The aim of the article is to discuss operational control on the example of the Act on the Internal Security Agency and the Intelligence Agency. This measure, colloquially known as surveillance, is one of the most severe intrusions into the constitutionally guaranteed freedom of communication. The main justification for taking such far-reaching measures is the security of the state or the detection and prevention of crimes. The author explains the institution of operational control based on the mentioned act. However, it should be noted that the regulations governing surveillance in other acts are essentially the same. The article presents forms of operational control, its basis and purpose also in the context of Polish case law and the European Court of Human Rights.

Keywords: operational control, The Internal Security Agency, Constitution, freedom of communication, surveillance

* Mgr, absolwent Wydziału Prawa i Administracji Uniwersytetu Łódzkiego, e-mail: k.florczak2000@o2.pl, https://orcid.org/0009-0006-5404-3438

1. Wprowadzenie

Konstytucja Rzeczypospolitej Polskiej w art. 49 stanowi, że „zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić tylko na podstawie ustawy i w sposób w niej określony”[1]. Ograniczenie wskazanej wolności może być dokonywane w różny sposób[2]. Jednym z nich jest kontrola operacyjna, potocznie zwana „inwigilacją”. Może ona zostać dokonywana przez wiele służb, w tym przez służby specjalne.

Celem artykułu jest przedstawienie instytucji kontroli operacyjnej jako ingerencji w konstytucyjnie zagwarantowaną wolność komunikowania się przez pryzmat nie tylko unormowań ustawowych, ale biorąc również pod uwagę orzecznictwo sądów polskich i Europejskiego Trybunału Praw Człowieka czy poglądy przedstawiane w literaturze przedmiotu. Zmiany dokonywane przez ostatnie lata spowodowały, że dzisiejsze unormowania zezwalają na znacznie silniejszą ingerencję w prawa człowieka niż miało to miejsce wcześniej. W ramach poczynionych badań można zadać pytanie, czy obecne uregulowania dotyczące kontroli operacyjnej odpowiadają standardowi konstytucyjnemu, zwłaszcza w zakresie prawa do prywatności i wolności komunikowania się. Oparcie rozważań o przepisy normujące organizacje i kompetencje Agencji Bezpieczeństwa Wewnętrznego jest uzasadnione tym, iż podstawowym zadaniem tej formacji jest ochrona bezpieczeństwa państwa. Natomiast ograniczenia wolności komunikowania się w polskim porządku prawnym następują głównie z uwagi na przesłankę bezpieczeństwa państwa określoną w art. 31 ust. 3 Konstytucji RP.

2. Rola Agencji Bezpieczeństwa Wewnętrznego w systemie służb specjalnych

Agencja Bezpieczeństwa Wewnętrznego jest cywilną formacją kontrwywiadowczą[3]. Celem tej służby specjalnej, zgodnie z art. 1 ustawy z dnia 24 maja 2002 r. o ABW i AW[4], jest ochrona bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. W literaturze wskazuje się, że obszary działania ABW to sfera zbierania informacji, walki z przestępczością oraz kontroli, która ma charakter profilaktyczno-ochronny[5]. Zadania służby zostały wskazane w art. 5 ustawy o ABW i AW. Do najważniejszych zadań ABW można zaliczyć m.in.: rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny; rozpoznawanie, zapobieganie i wykrywanie przestępstw (m.in.: szpiegostwa czy terroryzmu, obrotu towarami lub technologiami o znaczeniu strategicznym) czy realizowanie zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych.

1 Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U., nr 78, poz. 483 ze zm.).

2 Jako przykład można wskazać kontrolę korespondencji w czasie stanu wojennego lub wyjątkowego albo liczne ograniczenia wolności komunikowania się skazanego na karę pozbawienia wolności określone w Ustawie z 6.06.1997 r. Kodeks karny wykonawczy (t.j. Dz.U. z 2024 r., poz. 706).

3 Nie poruszam tutaj szerzej podziału służb specjalnych dokonywanych w literaturze. Zazwyczaj takie formacje rozróżnia się na cywilne (ABW, AW i CBA) oraz wojskowe (SKW i SWW). Innym kryterium podziału jest charakter prowadzenia działań. Wówczas można wyróżnić służby wywiadowcze (AW i SWW) oraz kontrwywiadowcze (ABW i SKW); problemem jest tu zakwalifikowanie CBA do jakiejkolwiek grupy, gdyż służba ta wyspecjalizowana jest *de facto* w jednej kategorii spraw. Za m.in.: S. Chomoncik, *Ustawa o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego. Komentarz*, Warszawa 2021, s. 9.

4 Ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2024 r., poz. 812), dalej: ustawa o ABW i AW.

5 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Komentarz*, Warszawa 2017, s. 19.

Podkreśla się, że ABW wśród pozostałych służb pełni rolę wiodącą, jeśli chodzi o bezpieczeństwo państwa[6]. Zresztą taki był zamysł pierwszej reformy cywilnych służb specjalnych w 2002 r.[7] Jak wskazywano wówczas w uzasadnieniu do ustawy: „podstawowym elementem obecnej reformy jest oddzielenie struktur wywiadu od struktur odpowiedzialnych za wewnętrzne bezpieczeństwo państwa, skoncentrowanie zadań wywiadowczych i kontrwywiadowczych w dwóch odrębnych, wyspecjalizowanych centralnych organach administracji rządowej".

Z wyżej przedstawionych zadań można wysnuć co najmniej dwa wnioski. Po pierwsze, ABW jest formacją, której przedmiotem działania jest nie tylko kontrwywiad czy ochrona bezpieczeństwa państwa, ale również, co jest niekiedy krytykowane[8], zwalczanie określonych w ustawie przestępstw. Drugą konkluzją jest to, iż celem ABW jest ochrona bezpieczeństwa państwa, a co za tym idzie – jego obywateli. Potwierdza to również ETPC[9], który w swoim orzecznictwie podkreśla, iż główną intencją stosowania środków, którymi dysponuje ta formacja, jest ochrona bezpieczeństwa i porządku publicznego oraz zapobieganie przestępstwom[10]. Zatem zachodzi domniemanie, że każda ingerencja w prawa i wolności człowieka, w tym w wolność komunikowania się, jest nakierunkowana na zabezpieczenie najważniejszych interesów Polski i jej mieszkańców. Stąd można wywodzić uzasadnienie dla działań, które ingerują w wolność określoną w art. 49 Konstytucji RP. Przy czym muszą mieścić się one w określonych standardach nie tylko dla demokratycznego państwa prawnego, ale też dla poszanowania praw człowieka.

3. Pojęcie i procedura zastosowania kontroli operacyjnej

Kontrolę operacyjną można zdefiniować jako czynność operacyjno-rozpoznawczą[11]. Prawo nie tłumaczy natomiast, czym miały być owe czynności, choć do uregulowania tego było bardzo blisko w 2008 r. Sejm VI kadencji rozpatrywał wówczas projekt ustawy o czynnościach operacyjno-rozpoznawczych, który wprowadzał definicję legalną tych działań jako „zespół przedsięwzięć, jawnych i niejawnych prowadzonych wyłącznie w celu: rozpoznania, zapobiegania i wykrywania przestępstw; odnajdywania osób ukrywających się przed organami ścigania lub wymiarem sprawiedliwości oraz osób zaginionych, jeżeli zachodzi uzasadnione podejrzenie, że ich zaginięcie jest wynikiem przestępstwa, a także odnajdywania rzeczy utraconych w wyniku przestępstwa lub mających związek z przestępstwem; ustalenia tożsamości osób i zwłok w przypadku uzasadnionego podejrzenia przestępczego działania"[12]. W literaturze przedmiotu podejmuje się próby definiowania czynności operacyjno-rozpoznawczych. Dla przykładu można wskazać propozycję Z. Raua, który ujmuje je jako pozaprocesowe czynności polegające na uzyskiwaniu, gromadzeniu, zbieraniu, sprawdzaniu, analizowaniu, przetwarzaniu, przekazywaniu oraz wykorzystywaniu informacji o osobach, miejscach, przedmiotach, zdarzeniach lub zagrożeniach będących przedmiotem prawnie uzasadnionego zainteresowania służby państwowej, a także inne niejawne działania i przedsięwzięcia służące realizacji ustawowych zadań tej służby[13]. Natomiast uchwała

6 M. Hałasiński, *Miejsce i zadania Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa wewnętrznego państwa*, „Studia Administracyjne" 2012, nr 4, s. 303.

7 Jako drugą reformę można wskazać zniesienie Wojskowych Służb Informacyjnych i powołanie na ich miejsce Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego.

8 A. Nyzio, *Wokół zespolenia służb specjalnych*, „Komentarz ZBN" 2020, nr 2, s. 4.

9 Europejski Trybunał Praw Człowieka.

10 Zob. wyrok ETPC z 12.01.2016 r., *Szabó i Vissy v. Węgry*, skarga nr 37138/14, LEX nr 1956289.

11 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 99.

12 Art. 2 ust. 1 projektu ustawy o czynnościach operacyjno-rozpoznawczych, nr druku 353 (Sejm VI kadencji).

13 Z. Rau, *Czynności operacyjno-rozpoznawcze w polskim systemie prawa – działania w kierunku uniwersalnej ustawy*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowane i terroryzmu*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 734.

Sejmu ws. powołania komisji śledczej ws. Pegasusa[14] wskazuje czynności operacyjno-rozpoznawcze jako „kontrolę operacyjną, w tym kontrolę i utrwalanie treści rozmów telefonicznych, kontrolę korespondencji, a także wszelkie inne czynności polegające na kontroli lub utrwalaniu przy użyciu środków technicznych treści rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną lub za pomocą komunikatorów internetowych"[15]. Moim zdaniem ta definicja nie jest odpowiednia, gdyż obejmuje jedynie przykładowe postacie czynności operacyjno-rozpoznawczych oraz jest sformułowana zbyt wąsko.

Celem kontroli operacyjnej jest rozpoznawanie, zapobieganie i wykrywanie przestępstw takich jak szpiegostwo, mających charakter terrorystycznych, czy fałszowanie pieniędzy oraz w celu uzyskania i utrwalenia dowodów i ścigania sprawców. Istotne jest również podkreślenie, że kontrola operacyjna może zostać zastosowana tylko, gdy inne środki podjęte przez funkcjonariuszy okażą się bezskuteczne albo są nieprzydatne. Zatem podjęcie decyzji o rozpoczęciu kontroli operacyjnej powinno być dla sądu decydującego o tym ostatecznością[16]. ETPC podkreśla, że uprawnienia do inwigilacji obywateli są dopuszczalne tylko w takim zakresie, w jakim jest to bezwzględnie konieczne dla ochrony instytucji demokratycznych[17]. Władze publiczne dysponują dość szerokim marginesem oceny przy wyborze środków służących osiągnięciu uprawnionego celu ochrony bezpieczeństwa narodowego. Niemniej jednak, biorąc pod uwagę ryzyko, że system tajnej inwigilacji mający na celu ochronę bezpieczeństwa narodowego może osłabić lub nawet zniszczyć demokrację pod pozorem jej obrony, Państwo musi udowadniać każdorazowo, że istnieją odpowiednie i skuteczne gwarancje przeciwko ewentualnym nadużyciom[18]. Kontrowersyjne z punktu widzenia praw człowieka, w szczególności wobec coraz bardziej rozwijającej się technologii, są sposoby pozyskiwania danych przez służby specjalne, które w pewnej mierze pozostają tajne. Zrozumiałe jest jednak, że co do zasady służby jakiegokolwiek państwa nie będą upubliczniały informacji o stosowanych oprogramowaniach, które będą służyć prowadzeniu kontroli operacyjnej. Wskazuje się, że mogą one stosować wszelkie środki techniczne, które umożliwią uzyskanie informacji[19]. Jedyna wiedza o stosowaniu takich systemów może pochodzić z oficjalnych komunikatów służb lub z doniesień medialnych. Przykładem może być oprogramowanie Pegasus.

Istota inwigilacji została wskazana w art. 27 ust 6 ustawy o ABW i AW. Przepis wskazuje, że kontrola operacyjna jest prowadzona zawsze w sposób niejawny i wyraża się w następujących formach: uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; uzyskiwanie i utrwalanie obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; uzyskiwanie i utrwalanie treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych oraz uzyskiwanie dostępu i kontroli zawartości przesyłek. Samo brzmienie przepisu jasno wskazuje, że kontrola operacyjna jest czynnością

14 Komisja Śledcza do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r.

15 Uchwała z 17.01.2024 r. w sprawie powołania Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r. (M.P. z 2023 r., poz. 70).

16 K. Brylak-Hudyma, *Konstytucyjne prawa i wolności w obliczu nowych systemów inwigilacji*, „Prawo Mediów Elektronicznych" 2020, nr 2, s. 17.

17 Wyrok ETPC z 6.09.1978 r., *Klass i inni v. Niemcy*, skarga nr 5029/71, pkt 42, LEX nr 80801.

18 Decyzja ETPC z 29.06.2006 r., *Weber i Saravia v. Niemcy*, skarga nr 54934/00, pkt 106, LEX nr 282129.

19 M. Tomkiewicz, *Kontrola procesowa i operacyjna a ochrona praw podmiotowych osoby inwigilowanej w Polsce*, „Profilaktyka Społeczna i Resocjalizacja" 2015, nr 25, s. 16.

ingerującą w wolność komunikowania się, tym bardziej, że przyjmuje się bardzo szerokie rozumienie komunikowania z uwagi na ciągły i dynamiczny rozwój technologiczny[20].

Aby mogło dojść do zastosowania kontroli operacyjnej prowadzonej przez ABW, Szef tej służby musi złożyć pisemny wniosek do Sądu. Przy czym pismo musi zawierać także zgodę Prokuratora Generalnego. Sąd, podejmując decyzję, musi brać pod uwagę nie tylko uzasadnienie wskazane we wniosku, ale też wcześniej wspomnianą przesłankę materialną, czyli bezskuteczność innych środków albo ich nieprzydatność (art. 27 ust. 1 ustawy o ABW i AW). Zresztą wniosek powinien wykazywać, że na podstawie dokonanych ustaleń faktycznych oraz charakteru sprawy inne działania nie będą pożyteczne[21] (art. 27 ust. 1a ustawy o ABW i AW). Poza tym uzasadnienie winno przedstawić informacje o toczącym się postępowaniu wobec osoby podejrzanej lub oskarżonego (art. 27 ust. 5 ustawy o ABW i AW). Powyższe jest niezwykle doniosłe z uwagi na możność precyzyjnego zapoznania się z potrzebą zastosowania inwigilacji przez sąd[22]. Co więcej, tak sformułowany przepis pozwala na podjęcie czynności wobec osób, co do których nie toczy się postępowanie karne lub nie przedstawiono jeszcze zarzutów (osoba podejrzana[23]). Na marginesie należy dodać, że obligatoryjne elementy wniosku zawiera art. 27 ust. 7 ustawy o ABW i AW. Wniosek o zastosowanie kontroli operacyjnej nie powinien zatem sprowadzać się do ogólnej potrzeby zastosowania takich środków i stwierdzenie, że dotychczasowe działania okazały się niewystarczające lub nieskuteczne. Wskazuje na to w swoim orzecznictwie ETPC, który w sprawie Dragojević przeciwko Chorwacji stwierdził, że weryfikacja sądowa musi uwzględniać także faktyczne podstawy podejrzewania osoby o planowanie lub popełnienie określonych poważnych czynów zabronionych[24].

Kontrola operacyjna może zostać zarządzona jedynie w przypadkach wskazanych w art. 27 ust. 1 pkt 1–3 ustawy o ABW i AW, to jest w celu rozpoznawania, zapobiegania i wykrywania przestępstw – jest to wymóg celowości tych czynności operacyjno-rozpoznawczych[25]. ABW może zastosować kontrolę operacyjną w stosunku do czynów zabronionych, takich jak m.in. szpiegostwo, terroryzm, korupcja osób pełniących funkcje publiczne, produkcja i obrót technologiami lub towarami o znaczeniu strategicznym dla bezpieczeństwa państwa, nielegalny obrót bronią, pranie brudnych pieniędzy czy ich fałszowanie. W związku z tym należy wskazać niezwykle ważny wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r.[26], w którym stwierdzono, że kontrola operacyjna nie może zostać zastosowana wobec wszystkich przestępstw, których ściganie jest głównym zadaniem ABW. Zgodnie z tym orzeczeniem kontrola operacyjna nie może zostać zastosowana w celu rozpoznawania, zapobiegania i wykrywania przestępstw godzących w podstawy ekonomiczne państwa. Takie działanie jest niezgodne z zasadą demokratycznego państwa prawnego (art. 2 Konstytucji), prawem do prywatności (art. 47 Konstytucji), wolnością komunikowania się (art. 49 Konstytucji) w związku z klauzulą limitacyjną (art. 31 ust. 3 Konstytucji). Trybunał uznał, że takie sformułowanie jest zbyt ogólne oraz uniemożliwia identyfikację typów przestępstw określonych przez ustawę karną. Ponadto stwierdził, że „faktyczne granice niejawnej ingerencji w wolności oraz prawa człowieka nie są wyznaczone w sposób dostatecznie określony przez ustawodawcę, a determinują je organy stosujące prawo. Taki stan rzeczy nie jest do pogodzenia z konstytucyjną zasadą określoności prawa (art. 2 Konstytucji) i zasadą ustawowej formy ograniczeń wolności i praw konstytucyjnych (art. 31 ust. 3 Konstytucji)".

20 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 107.

21 Tamże, s. 101.

22 Tamże, s. 103.

23 S. Waltoś, P. Hofmański, *Proces karny. Zarys systemu*, Warszawa 2020, s. 200.

24 Wyrok ETPC z 15.01.2015 r., *Dragojević v. Chorwacja*, skarga nr 68955/11, LEX nr 1583477.

25 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 101.

26 Wyrok TK z 30.07.2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80.

Podstawowym terminem prowadzenia kontroli operacyjnej jest okres nie dłuższy niż 3 miesiące. Jeżeli nie ustały wyżej wskazane przyczyny zarządzenia inwigilacji, sąd może wydać postanowienie o jednorazowym przedłużeniu czynności na czas nie dłuższy niż kolejne 3 miesiące. Przy czym decyzja musi być poprzedzona wnioskiem Szefa ABW, którego elementem jest zgoda Prokuratora Generalnego (art. 27 ust. 8 ustawy o ABW i AW). Tylko w uzasadnionych przypadkach, które ustawa tłumaczy poprzez pojawienie się nowych okoliczności, istotnych dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów na popełnienie przestępstwa, można przedłużyć kontrolę operacyjną. Aspekty formalne są takie same jak przy pierwszym przedłużeniu, przy czym każde kolejne okresy nie mogą trwać dłużej niż 12 miesięcy (art. 27 ust. 9 ustawy o ABW i AW). Oczywistym jest także fakt, który potwierdza art. 27 ust. 10, iż każdy wniosek o przedłużenie inwigilacji powinien wykazywać potrzebę stosowania tego środka. Kontrowersyjnym jest jednak przyznanie jakiejkolwiek służbie specjalnej w demokratycznym państwie prawnym możliwości stosowania inwigilacji przez bardzo długi okres. Ustawa nie wskazuje górnego limitu, co może wpływać negatywnie na ochronę podstawowych praw i wolności.

Kontrola operacyjna kończy się niezwłocznie po ustaniu przyczyn jej zarządzenia, najpóźniej z upływem okresu, na który została wprowadzona (art. 27 ust. 13 ustawy o ABW i AW). Następnie, Szef ABW informuje Prokuratora Generalnego o wynikach kontroli, które mogą w sobie zawierać informacje zarówno o przebiegu, jak i zebranych materiałach (art. 27 ust. 14 ustawy o ABW i AW). Materiały są przekazywane Prokuraturze, jeśli mają znaczenie dla toczącego się już postępowania, albo dają podstawę do wszczęcia postępowania karnego, czyli gdy zachodzi uzasadnione podejrzenie popełnienia przestępstwa (art. 27 ust. 15 ustawy o ABW i AW oraz art. 303 Kodeksu postępowania karnego[27]).

Nadzór sądowy nad wydawaniem decyzji co do przeprowadzenia kontroli operacyjnej jest podstawą takich czynności operacyjno-rozpoznawczych, które bezpośrednio ingerują w konstytucyjnie zagwarantowane prawa i wolności. Celem badania przez sąd jest niezależna ocena wniosku[28]. Sąd jako organ niezależny opiera się na Konstytucji i ustawach, a wobec tego, badając zasadność wniosku, musi rozważyć dwie wartości, które w tym przypadku będą stać w opozycji: bezpieczeństwo państwa i wolność komunikowania się. Przy czym szczególny wzgląd powinien mieć na prawa jednostki, chroniąc ją przed nieuprawnionymi decyzjami o inwigilacji. Słusznie zwraca uwagę ETPC, że z uwagi na to, że osoba podsłuchiwana nie jest informowana o zastosowaniu wobec niej takich środków, procedury kontrolne muszą zapewniać odpowiednie gwarancje dla jednostki[29]. Ponadto, tak daleko idąca ingerencja w prywatność człowieka, która może być przedmiotem wielu nadużyć zagrażających demokratycznemu społeczeństwu, każe powierzyć kontrolę niezależnemu sądowi. Chociaż Trybunał w sprawie Klass i inni przeciwko Niemcom uznał, że czuwaniem nad zasadnością inwigilacji może zajmować się inny organ niż sąd, dysponujący odpowiednią dozą niezależności[30]. W niezwykle ważnej sprawie Zakharov przeciwko Rosji wskazano na zakres kontroli przejawiający się w tym, że sądy „muszą być w stanie zweryfikować istnienie uzasadnianego podejrzenia przeciwko danej osobie, w szczególności, czy są faktycznie wskazania do podejrzewania osoby o planowanie, popełnianie lub popełnienie czynu zabronionego lub innych czynów (np. czynów zagrażających bezpieczeństwu narodowemu), które dają podstawę do zastosowania środków tajnego nadzoru. Należy również potwierdzić, czy wnioskowane przechwytywanie spełnia wymogi „konieczności w demokratycznym społeczeństwie", o której mowa w art. 8 ust. 2 Konwencji, w tym także, czy jest ono proporcjonalne w stosunku do zakładanego celu, a więc należy zbadać, czy możliwe byłoby jego osiągnięcie poprzez mniej restrykcyjne środki"[31].

27 Ustawa z 6.06.1997 r. Kodeks postępowania karnego (t.j. Dz.U. z 2024 r., poz. 37 ze zm.), dalej: KPK.

28 M. Rojszczak, *Kontrola sądów krajowych nad stosowaniem środków inwigilacji elektronicznej na tle orzecznictwa ETPC*, „Państwo i Prawo" 2022, nr 4, s. 105.

29 *Klass i inni v. Niemcy*, pkt 55.

30 Tamże, pkt 56.

31 Wyrok ETPC z 4.12.2015 r., *Zakharov v. Rosja*, skarga nr 47143/06, pkt 260, LEX nr 1929190.

Analizując orzecznictwo ETPC, M. Rojszczak wysnuł kilka wniosków dotyczących skutecznej kontroli sądowej. Po pierwsze, preferowaną procedurą weryfikacji jest kontrola *ex ante*, czyli przed podjęciem kontroli operacyjnej. Po drugie, jeśli sytuacja wskazuje, że sąd sprawdza zasadność inwigilacji *ex post*, to procedura weryfikacyjna powinna być usystematyzowana. Po trzecie, akceptowanie zdecydowanej większości wniosków o zarządzenie kontroli operacyjnej może dać podstawy do sądzenia, iż ocena jest nieprawidłowa lub niewystarczająca[32]. W Polsce sądem właściwym, który wydaje decyzję w formie postanowienia, jest Sąd Okręgowy w Warszawie (art. 27 ust. 2 ustawy o ABW i AW). Sprawę rozpoznaje on jednoosobowo, a w posiedzeniu może brać udział tylko prokurator i przedstawiciel Szefa ABW (art. 27 ust. 11 ustawy o ABW i AW).

Dosyć kontrowersyjnym rozwiązaniem posługuje się ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[33], która zezwala na prowadzenie kontroli operacyjnej w stosunku do cudzoziemców bez kontroli sądowej. Zgodnie z art. 9 ust. 1 Szef ABW może zarządzić na maksymalny termin 3 miesięcy wobec osoby niebędącej obywatelem polskim *de facto* kontrolę operacyjną w celu rozpoznawania, zapobiegania, zwalczania i wykrywania przestępstw o charakterze terrorystycznym lub szpiegostwa. Przesłanką materialną jest tu obawa co do możliwości prowadzenia przez cudzoziemca działalności terrorystycznej lub szpiegowania[34]. W literaturze wskazuje się, że oprócz braku nadzoru sądu nad stosowaniem czynności inwigilacyjnych dość sporna jest możliwość zastosowania kontroli operacyjnej z uwagi na obawę możliwości prowadzenia działalności terrorystycznej przez cudzoziemca. Taka klauzula generalna powinna być interpretowana obiektywnie, mając na względzie przede wszystkim prawa człowieka zagwarantowane w Konstytucji RP. Zatem obawa nie może mieć charakteru ogólnie wynikającego choćby z wyznania czy przynależności etnicznej[35]. Kolejnym daleko idącym uprawnieniem ABW jest możność rozpoznawania przestępstw. Oznacza to, że formacja może prowadzić działania rozpoznawcze w celu infiltracji danej grupy osób[36]. Kontrola sądowa obowiązuje dopiero przy przedłużeniu inwigilacji, czyli najpóźniej po 3 miesiącach (art. 9 ust. 5 ustawy w zw. z art. 27 ustawy o ABW i AW). Do tego momentu jedyny nadzór sprawuje Prokurator Generalny, co nie daje podstawy sądzić, że kontrola spełnia wymóg bezstronności i niezależności, z uwagi na bezpośrednie połączenie tejże funkcji z Ministrem Sprawiedliwości, czyli funkcją *stricte* polityczną.

Kontrola operacyjna może zostać również zarządzona w trybie nagłym bez uprzedniej zgody sądu. Zgodnie z art. 27 ust. 3 ustawy o ABW i AW „w przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Szef ABW może zarządzić, po uzyskaniu pisemnej zgody Prokuratora Generalnego, kontrolę operacyjną, zwracając się jednocześnie do sądu […], z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, Szef ABW wstrzymuje kontrolę operacyjną oraz poleca protokolarne, komisyjne zniszczenie materiałów zgromadzonych podczas jej stosowania". W literaturze przedmiotu wskazuje się, że sama treść przepisu tłumaczy, czym jest przypadek niecierpiący zwłoki. Byłaby to sytuacja, w której istnieje zagrożenie utraty informacji lub zatarcie albo zniszczenie dowodów przestępstwa[37]. Zgodnie z art. 27 ust. 10 ustawy o ABW i AW

32 M. Rojszczak, *Kontrola sądów*..., s. 105 i n.

33 Ustawa z 10.06.2016 r. o działaniach antyterrorystycznych (t.j. Dz.U. z 2024 r., poz. 92).

34 Ustawa wskazuje na „niejawne prowadzenie czynności polegających na: uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; uzyskiwaniu dostępu i kontroli zawartości przesyłek".

35 M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*, Warszawa 2018, s. 76.

36 Tamże, s. 77.

37 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 104.

wniosek o zatwierdzenie prowadzonej już kontroli operacyjnej musi zawierać nie tylko uzasadnienie, ale też materiały, które udało się uzyskać w ciągu tych 5 dni. Samą ideę takiej inwigilacji należy ocenić raczej pozytywnie. Niejednokrotnie służby muszą działać szybko, stąd prawo zezwala na kontrolę operacyjną w przypadkach nagłych. Dodatkowo istnieje tu sądowa weryfikacja zasadności podjęcia tych czynności *ex post*. Jednak nie powinna być to domyślna procedura kontroli czynności. Należy również zaznaczyć, że tzw. „pięciodniówki" mogą być wykorzystane w sposób absolutnie sprzeczny z zasadą demokratycznego państwa prawnego, zatem kontrola nad tą instytucją powinna być szersza i uwzględniająca zagrożenia natury politycznej.

4. Formy kontroli operacyjnej

Wcześniej wspomniana istota kontroli operacyjnej wyraża jej przedmiotowy zakres. Należy także zaznaczyć, co oczywiste, że zawsze inwigilacja będzie prowadzona w sposób niejawny. Pierwszym przejawem czy formą kontroli operacyjnej jest uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych, inaczej zwane „podsłuchem telefonicznym". O tym, że kontrola rozmów telefonicznych jest ingerencją w szeroko rozumiane prawo do prywatności, a także w jej aspekt, czyli wolność komunikowania się, orzekał już ETPC[38]. Kontrolowane komunikowanie się może być prowadzone w jakikolwiek sposób, natomiast ustawodawca wymienił tu przykładowo sieci telekomunikacyjne, które zostały zdefiniowane w art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[39] i oznaczają one m.in. systemy transmisyjne, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów lub fal radiowych[40]. Zgodnie z art. 27 ust. 12 ustawy o ABW i AW obowiązkiem przedsiębiorcy telekomunikacyjnego jest zapewnienie warunków technicznych i organizacyjnych umożliwiających inwigilację. Kontrola operacyjna prowadzona w taki sposób jest *de facto* identyczna jak przy podsłuchu procesowym[41], na podstawie art. 237 KPK. Ze względu na to można spojrzeć na techniczne aspekty podsłuchu, które reguluje właściwe Rozporządzenie Ministra Sprawiedliwości[42]. Stwarzając warunki, o których mowa wyżej, przedsiębiorca telekomunikacyjny przygotowuje sieć do przeprowadzenia kontroli, organizując specjalny system działający 24 godziny na dobę. Zapewnia on przechwytywanie, odbiór i utrwalanie przekazów informacji oraz ich przechowywanie w taki sposób, aby nie uległy one zniszczeniu (§ 2 ust. 1 i 2 pkt 2 rozporządzenia). Pracownicy przedsiębiorcy telekomunikacyjnego muszą posiadać odpowiednie poświadczenia bezpieczeństwa, a sam ich dostęp do kontroli powinien być ograniczony do minimum (§ 3 rozporządzenia). Zgodnie z § 5 ust. 1 rozporządzenia zbierane są m.in. dane identyfikujące abonentów i użytkowników uczestniczących w połączeniu, lokalizacja czy czas prowadzenia rozmowy ze wskazaniem długości trwania i daty. Wszelkie informacje dotyczące środków technicznych, czyli przykładowo oprogramowań, które są używane w celu kontroli operacyjnej, są niejawne[43]. Natomiast najczęściej o stosowanych systemach opinia publiczna dowiaduje się z mediów. Przykładem jest oprogramowanie Pegasus. Należy

38 Zob. wyrok ETPC z 15.01.2015 r., *Dragojević v. Chorwacja*, skarga nr 68955/11.

39 Ustawa z 16.07.2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2024 r., poz. 34 ze zm.), dalej: Prawo telekomunikacyjne.

40 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 105.

41 M. Bożek, *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych*, „Rocznik Administracji Publicznej" 2015, nr 1, s. 32.

42 Rozporządzenie Ministra Sprawiedliwości z 24.06.2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobu dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów (Dz.U., nr 110, poz. 1052). Kwestie techniczne są bardzo podobne do sposobu pozyskiwania informacji, które opisali B. Opaliński, M. Rogalski oraz P. Szustakiewicz w Komentarzu do ustawy o ABW i AW.

43 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 111.

także zaznaczyć, że ABW jest jedyną uprawnioną służbą do tzw. certyfikacji systemów używanych do inwigilacji, czyli do oceny bezpieczeństwa.

Drugim przejawem kontroli operacyjnej jest uzyskiwanie i utrwalanie obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne. Zatem tutaj funkcjonariusze ABW będą mogli *de facto* mieć dostęp do monitoringu obejmującego zarówno miejsca publiczne, jak i niepubliczne. Te pierwsze można rozumieć jako lokalizację dostępną dla nieograniczonej liczby osób[44].

Zgodnie z art. 27 ust. 6 pkt 3 ustawy o ABW i AW kontrola operacyjna może polegać także na uzyskiwaniu i utrwalaniu korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej. Takie działania służb będą bezpośrednio ingerować w wolność komunikowania się określoną w art. 49 Konstytucji RP. Jednak należy zauważyć, iż ustawa używa określenia węższego od pojęcia „komunikowania się", to jest „korespondencji". Różnicę między tymi wyrażeniami zauważa orzecznictwo m.in. Sądu Najwyższego. W wyroku z dnia 24 września 2010 r. stwierdził on, że „wolność komunikowania się jest jedną z konsekwencji szeroko rozumianej wolności obywatelskiej i osobistej, obejmującej wszystkie formy porozumiewania się między ludźmi, natomiast tajemnica korespondencji jest pojęciem znacznie węższym, związanym przede wszystkim z prawem każdego człowieka do poszanowania jego życia prywatnego, jego prawa do zachowania w tajemnicy treści przekazu kierowanego do innych osób lub instytucji"[45]. Ustawa stanowi także wprost o możliwości uzyskiwania i utrwalania treści korespondencji, więc jej forma jest w zasadzie bez znaczenia.

Czwartym przejawem kontroli operacyjnej jest uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych oraz systemach informatycznych i teleinformatycznych. Większość tych technicznych pojęć jest definiowanych w innych ustawach[46]. Informatyczne nośniki danych posiadają swoją definicję legalną w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne[47]. Są to materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej. Można zatem przykładowo wskazać, że takim urządzeniem jest pamięć zewnętrzna czy pendrive. Telekomunikacyjnym urządzeniem końcowym, zgodnie z Prawem telekomunikacyjnym, jest urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci. Natomiast ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[48] wprowadza definicję systemu teleinformatycznego jako zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu Prawa telekomunikacyjnego. Wskazuje się, że powyższy system należy odróżniać od systemu informatycznego, który nie posiada swojej definicji legalnej oraz nie obejmuje swoim zakresem urządzeń przekazujących dane[49].

Ostatnim przejawem kontroli operacyjnej na gruncie ustawy o ABW i AW jest uzyskiwanie dostępu i kontrola zawartości przesyłek. Przesyłkę można rozumieć według definicji legalnej przesyłki listowej zawartej w Prawie pocztowym[50], to jest jako „przesyłkę pocztową z korespondencją lub druk". Poza tym ustawa definiuje przesyłkę pocztową jako „rzecz opatrzoną oznaczeniem adresata i adresem, przedłożoną do przyjęcia lub przyjętą przez operatora pocztowego w celu przemieszczenia i doręczenia

44 Tamże, s. 105.

45 Wyrok SN z 24.09.2010 r., IV CSK 87/10, Lex nr 622216.

46 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 108.

47 Ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r., poz. 307).

48 Ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344).

49 B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji*..., s. 108.

50 Ustawa z dnia 23.11.2012 r. Prawo pocztowe (t.j. Dz.U. z 2023 r., poz. 1640 ze zm.).

adresatowi". Nadto wyjaśnione jest pojęcie „przesyłki z korespondencją" jako przesyłki pocztowej niebędącej drukiem, zawierającej informację utrwaloną na dowolnym nośniku, w tym utrwaloną pismem wypukłym. Kontrola takich przesyłek będzie miała na celu zdobycie istotnych informacji lub samych poszlak. Dodatkowo służby mogą sprawdzać, czy w przesyłce znajdują się elementy niezgodne z prawem.

5. Podsumowanie

Rzecznik Praw Obywatelskich wielokrotnie zwracał uwagę na problemy wynikające z przedstawionych unormowań. W 2017 r. wskazywał, że świeżo uchwalona ustawa o działaniach antyterrorystycznych przyznała bardzo szerokie uprawnienia służbom specjalnym w zakresie ingerencji w prawo do prywatności, w tym w wolność komunikowania się[51]. Ponadto RPO zwracał uwagę na znowelizowane przepisy Kodeksu postępowania karnego, wprowadzające art. 168a[52], który *de facto* umożliwia uwzględnianie dowodów w postępowaniu, nawet jeśli zostały pozyskane za pomocą czynu zabronionego[53]. W wielu sprawach Rzecznik kierował wnioski do Trybunału Konstytucyjnego w celu zbadania zgodności wprowadzanych przepisów z Konstytucją RP. Jednakże z uwagi na to, że rozpatrywać pisma miał skład, w którym zasiadałyby osoby powołane do TK niezgodnie z Konstytucją[54], RPO każdorazowo wycofywał wnioski, ze względu na możliwość wprowadzenia niepewności prawnej[55].

Agencja Bezpieczeństwa Wewnętrznego jako jedna z najważniejszych służb mundurowych, a śmiało stwierdzę, że jako najważniejsza służba specjalna w Polsce dysponuje istotnymi uprawnieniami godzącymi w prawo do prywatności, a w szczególności jego aspekt, czyli wolność komunikowania się. Bezpieczeństwo państwa i ochrona podstawowych praw i wolności zawsze będą stały ze sobą w niekończącym się konflikcie. Istotne jest, aby w demokratycznym państwie prawnym zarówno służby, jak i nadzorujące je organy administracji rządowej potrafiły wyważyć te wartości. Z jednej strony służby dysponujące tak daleko idącymi uprawnieniami powinny przede wszystkim chronić bezpieczeństwo państwa. Z drugiej jednak dbać o to, aby każda ingerencja była proporcjonalna do stanowionych w Konstytucji praw człowieka. Służby, jak to zostało już kilkukrotnie wspomniane, powinny dbać o różne aspekty bezpieczeństwa państwa, czyli jego obywateli. Nigdy w interesie aktualnie rządzących. Obecne uregulowania i praktyki prowadzą do refleksji, iż kontrola operacyjna w aktualnym kształcie może być wykorzystywana przez różne służby specjalne ponad jej normatywny cel. Nieograniczony termin prowadzenia inwigilacji, jak i skąpość wniosków przesyłanych do sądu mogą stanowić w tej materii adekwatny przykład. *De lege ferenda* należałoby ustalić maksymalny termin prowadzenia działań czy rozwinąć uregulowania dotyczące elementów wniosku, tak aby sąd mógł sprawować rzeczywisty nadzór nad kontrolą operacyjną.

51 Informacja o stanie przestrzegania wolności i praw człowieka i obywatela w 2017 r. oraz o działalności Rzecznika Praw Obywatelskich, Biuletyn Rzecznika Praw Obywatelskich 2018, nr 1, s. 222–223.

52 Przepis znoszący tzw. zasadę nieuznawania owoców zatrutego drzewa. Wprowadzony art. 168a k.p.k. brzmi: „Dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego, chyba że dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności".

53 Informacja o stanie przestrzegania wolności i praw człowieka i obywatela w 2017 r...., s. 225.

54 Tzw. sędziowie-dublerzy.

55 Informacja o działalności Rzecznika Praw Obywatelskich oraz o stanie przestrzegania wolności i praw człowieka i obywatela w roku 2018, s. 174.

Bibliografia

Bożek M., *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych*, „Rocznik Administracji Publicznej" 2015, nr 1, s. 18–47.

Brylak-Hudyma K., *Konstytucyjne prawa i wolności w obliczu nowych systemów inwigilacji*, „Prawo Mediów Elektronicznych" 2020, nr 2, s. 12–19.

Chomoncik S., *Ustawa o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego. Komentarz*, Warszawa 2021.

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz*, Warszawa 2018.

Hałasiński M., *Miejsce i zadania Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa wewnętrznego państwa*, „Studia Administracyjne" 2012, nr 4, s. 303–314.

Nyzio A., *Wokół zespolenia służb specjalnych*, „Komentarz ZBN" 2020, nr 2.

Opaliński B., Rogalski M., Szustakiewicz P., *Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Komentarz*, Warszawa 2017.

Rau Z., *Czynności operacyjno-rozpoznawcze w polskim systemie prawa – działania w kierunku uniwersalnej ustawy*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowane i terroryzmu*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 712–745.

Rojszczak M., *Kontrola sądów krajowych nad stosowaniem środków inwigilacji elektronicznej na tle orzecznictwa ETPC*, „Państwo i Prawo" 2022, nr 4, s. 100–119.

Tomkiewicz M., *Kontrola procesowa i operacyjna a ochrona praw podmiotowych osoby inwigilowanej w Polsce*, „Profilaktyka Społeczna i Resocjalizacja" 2015, nr 25, s. 7–26.

Waltoś S., Hofmański P., *Proces karny. Zarys systemu*, Warszawa 2020.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U., nr 78, poz. 483 ze zm.).

Ustawa z 6.06.1997 r. Kodeks karny wykonawczy (t.j. Dz.U. z 2024 r., poz. 706).

Ustawa z 6.06.1997 r. Kodeks postępowania karnego (t.j. Dz.U. z 2024 r., poz. 37 ze zm.).

Ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2024 r., poz. 812).

Ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344).

Ustawa z 16.07.2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2024 r., poz. 34 ze zm.).

Ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r., poz. 307).

Ustawa z 23.11.2012 r. Prawo pocztowe (t.j. Dz.U. z 2023 r., poz. 1640 ze zm.).

Ustawa z 10.06.2016 r. o działaniach antyterrorystycznych (t.j. Dz.U. z 2024 r., poz. 92).

Rozporządzenie Ministra Sprawiedliwości z 24.06.2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobu dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów (Dz.U., nr 110, poz. 1052).

Uchwała z 17.01.2024 r. w sprawie powołania Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r. (M.P. z 2023 r., poz. 70).