

Jacek Kudła

ORCID 0000-0002-4077-3900

jkjacekudla@gmail.com

Alfred Staszak

Uniwersytet Zielonogórski

ORCID 0000-0003-1318-6513

astaszak@uz.zgora.pl

Rola biegłego przy stosowaniu czynności operacyjno-rozpoznawczych służb specjalnych RP w systemie informatycznym

Słowa kluczowe: służby specjalne, kontrola operacyjna, biegły, dostęp do informacji niejawnych, techniki kontroli operacyjnej

Streszczenie. Artykuł podnosi kontrowersyjną kwestię prawnej możliwości dopuszczenia biegłego do udziału w procesie opiniowania wniosków o zastosowanie kontroli operacyjnej na etapie wyrażania zgody na wystąpienie do sądu z wnioskiem przez uprawnione podmioty bądź już na etapie samego procedowania wniosku przez sąd. Autorzy stawiają hipotezę, że w sprawach skomplikowanych prokurator sprawujący nadzór nad czynnościami operacyjno-rozpoznawczymi czy sąd mogą zasięgnąć opinii biegłego posiadającego wiadomości specjalne, ale tylko wówczas, gdy biegły ten posiada certyfikat upoważniający go do dostępu do informacji niejawnych. Artykuł podnosi również kwestię warunków prawnej dopuszczalności stosowania najnowocześniejszych technik inwigilacyjnych oraz stosowania technik specjalnych do przeszukiwania wielkich baz danych.

The role of an expert in the application of operational and reconnaissance activities of the Polish special services in the IT system

Keywords: intelligence services, operational surveillance, expert, access to classified information, operational control techniques

Summary. The article raises the controversial issue of the legal possibility of allowing an expert to participate in the process of assessing applications for operational surveillance—either at the stage of granting consent for submitting an application to the court by authorized entities, or already during the court's examination of such an application. The authors hypothesize that in complex cases, the prosecutor supervising operational and reconnaissance activities or the court may seek the opinion of an expert with specialized knowledge, but only if that expert holds a certificate authorizing access to classified information. The article also addresses the legal conditions under which the use of the most advanced surveillance techniques and special techniques for searching large databases may be permissible.

1. Ogólna charakterystyka możliwości kontroli służb specjalnych w RP

Mimo że obecnie istnieje wiele organów i instytucji państwowych, które *ex lege* mogą sprawować niezależną kontrolę służb specjalnych w RP, to ich możliwości kontrolne są w tym zakresie odpowiednio ustawowo ograniczone. Szczególnie uwidacznia się to w sferze wykonywania przez służby specjalne czynności operacyjno-rozpoznawczych oraz w przypadkach wątpliwości dotyczących sfery pracy operacyjnej. Dlatego w tych przestrzeniach wszelkich interpretacji prawnych winny dokonywać osoby do tego szczególnie przygotowane, posiadające w omawianej dziedzinie wiadomości specjalne, które jednocześnie będą kierowały się podstawową przesłanką wykonywanych przez te służby zadań – stanowi to bezwzględne zapewnienie bezpieczeństwa państwa polskiego (zarówno wewnętrznego, jak i zewnętrznego)¹.

Należy podkreślić, że służby specjalne, realizując czynności operacyjno-rozpoznawcze, wykonują również inne działania i czynności, do których należy zaliczyć: czynności wywiadowcze i kontrwywiadowcze, informacyjne, analityczne, analityczno-informacyjne, operacyjno-wykrywcze². Zgodnie z art. 11 zd. pierwsze ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (dalej: ustawa o ABW i AW)³ służbami specjalnymi są: ABW, AW, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego (dalej: ustawa o SKW i SWW⁴) i Centralne Biuro Antykorupcyjne (dalej: ustawa o CBA⁵)⁶.

Odpowiednio w zakresie swoich kompetencji nadzór (kontrolę) nad służbami specjalnymi w Polsce sprawują następujące organy: Prezydent RP, Prokurator Generalny, Prezes Rady Ministrów, Minister koordynator służb specjalnych, Minister Obrony Narodowej, Szefowie ABW, AW, SKW, SWW i CBA, Sejm (komisje sejmowe, w tym Komisja ds. Służb Specjalnych)⁷, Najwyższa Izba Kontroli, sądy –

¹ M. Gabriel-Węglowski, *Architektura bezpieczeństwa*, „Rzeczpospolita” z 2.02.2022 r., <https://www.rp.pl/sady-i-prokuratura/art35632141-michal-gabriel-weglowski-architektura-bezpieczenstwa> [dostęp: 26.10.2024].

² J. Kudła, *System czynności operacyjno-rozpoznawczych, analityczno-informacyjnych oraz wywiadowczych i kontrwywiadowczych służb specjalnych*, LEX/el. 2016, nr 470060883 [dostęp: 24.01.2022].

³ Ustawa z dnia 24 maja 2002 r., t.j. Dz.U. z 2024 r. poz. 812.

⁴ Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, t.j. Dz.U. z 2024 r. poz. 1405.

⁵ Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, t.j. Dz.U. z 2024 r. poz. 184.

⁶ S. Zalewski, *Kontrola służb specjalnych w Polsce*, Warszawa 2021, s. 28. CBA pozostało służbą specjalną do 1.04.2025 r.

⁷ M. Bożek, *Sejmowa kontrola działalności służb specjalnych i jej ograniczenia wynikające z ustaw kompetencyjnych. Zarys problemu na tle uwarunkowań normatywnych*, „Studia Iuridica Lublinensia” 2013, nr 20, s. 47-70.

w tym Trybunał Konstytucyjny, Naczelny Sąd Administracyjny i odpowiednio pozostałe sądy i prokuratury⁸, Rzecznik Praw Obywatelskich⁹.

Oprócz Szefa danej służby żaden organ bez jego zgody nie ma dostępu do technik stosowanych podczas czynności operacyjno-rozpoznawczych, w tym do tych z zakresu techniki operacyjnej i techniki specjalnej. Szef danej służby specjalnej może w zakresie swojego działania zezwalać funkcjonariuszom i pracownikom „swojej” służby oraz byłym funkcjonariuszom i pracownikom po ustaniu stosunku służbowego lub stosunku pracy, a także osobom udzielającym im pomocy w wykonywaniu czynności operacyjno-rozpoznawczych – na udzielenie informacji niejawniej określonej osobie lub instytucji.

Ustawowe sformułowanie: „mogą zezwalać” nie oznacza, że „muszą zezwalać”¹⁰ i dlatego ocena materiałów i udzielenie określonych informacji z zakresu działania służb specjalnych zależy wyłącznie od jej Szefa. Wyjątki zostały określone w przepisach ustawy danej służby i dotyczą żądania prokuratora albo sądu zgłoszonego w celu ścigania karnego za czyn zabroniony, stanowiący zbrodnię lub występki, którego skutkiem jest np. śmierć człowieka, uszczerbek na zdrowiu lub szkoda w mieniu albo żądanie skierował Rzecznik Interesu Publicznego w celu przeprowadzenia postępowania lustracyjnego. Zakazu udostępniania informacji nie stosuje się również w przypadku żądania prokuratora lub sądu uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych (zob. art. 39 ust. 4, 5 i 6 ustawy o ABW i AW, art. 43 ust. 4, 5 i 6 ustawy o SKW i SWW, art. 28 ust. 3 i 4 ustawy o CBA)¹¹. Informacje te oczywiście nie są ujawniane opinii publicznej. Trudno założyć, że Szef danej służby specjalnej wyrazi zgodę na udzielenie organowi kontrolującemu informacji, która dotyczy taktyki i technik wykonywania czynności operacyjno-rozpoznawczych przez daną służbę specjalną. *A contrario* nie może to oznaczać, że służby nie mogą być w żaden sposób kontrolowane i mogą nie przestrzegać przepisów prawa. Wielokrotnie autorzy podkreślali w literaturze,

⁸ M. Bożek, *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych służących zwalczaniu przestępstw (zarys problemu na tle uwarunkowań normatywnych)*, [w:] E.W. Pływaczewski, W. Filipkowski, Z. Rau, *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy prawno-kryminologiczne*, Warszawa 2015, s. 322-350.

⁹ S. Zalewski, *op. cit.*, s. 78 do strony 150 (zob. opisane szczegółowo kompetencje kontrolne organów).

¹⁰ M. Bożek, *Status prawnoustrojowy Szefa Agencji Bezpieczeństwa Wewnętrznego. Zarys problemu na tle rozwiązań konstytucyjnych i ustawowych*, „Przegląd Sejmowy” 2014, nr 3, s. 77-106: „Szef ABW ma prawo odmówić udzielenia informacji niejawnych (w tym odmówić udostępnienia dokumentów), nawet jeśli z takim żądaniem zwraca się do niego konstytucyjny organ państwa. Użycie w art. 39 ustawy (z 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu) zwrotu «może zezwalać» oznacza, że na szefie ABW nie ciążył taki obowiązek”.

¹¹ J. Kudła, *Zezwolenie oraz udzielenie informacji w trybie art. 20b i 20ba ustawy o Policji*, LEX/el. 2017, numer 470099425 [dostęp: 8.06.2022].

że pod pojęciem klauzuli „ściśle tajne” nie może kryć się zezwolenie na nielegalne działanie służb¹². Zatem dzisiaj konieczne staje się wskazanie na podstawie istniejących przepisów prawa, czy faktycznie możliwa jest skuteczna kontrola służb specjalnych w Polsce¹³, a w szczególności, czy jest ona możliwa i efektywna w konkretnej sprawie na etapie postępowania sądowego.

W kontekście postawionego pytania wydaje się, że warto rozważyć konieczność włączenia pomocnika procesowego sądu i prokuratora, tj. biegłego na etapie wykorzystania materiałów uzyskanych z kontroli operacyjnej w celu dokonania ich prawidłowej oceny, oczywiście po stwierdzeniu zaistnienia okoliczności uzasadniających powołanie takiego biegłego. Naturalnie wyłącznie w tym zakresie, w którym organ procesowy nie jest w stanie samodzielnie dokonać prawidłowej oceny pracy operacyjnej z uwagi na tak zwaną „kuchnię operacyjną”. Jednak formalne wyniki tej kontroli musiałyby pozostać wyłącznie w obszarze dokumentacji niejawnej, w której biegły, wydając opinię¹⁴, mógłby informować organ procesowy w sposób zapewniający dalszą konspirację pracy operacyjnej, czy w jego ocenie doszło do jakichkolwiek uchybień na którymkolwiek etapie jego zdobywania i gromadzenia.

Należy nadto stwierdzić, że zachodzi potrzeba unormowania problematyki czynności operacyjno-rozpoznawczych w sposób szczególny, odmienny od dotychczasowego, w nowej ustawie o pracy operacyjnej¹⁵, gdyż potrzeba zmiany uregulowań w zakresie nadzoru nad pracą operacyjną w społecznej dyskusji nie ulega już żadnej wątpliwości. Zanim zmiana postulowanych przepisów jednak nastąpi, pozostaje umiejętne stosowanie obecnie obowiązujących przepisów w celu skutecznej i rzeczywistej kontroli służb specjalnych, z uwagi na ujawniane nadużycia, które miały miejsce w ostatnich latach, np. związane z użyciem oprogramowania potocznie nazywanego Pegasus¹⁶.

¹² Por. K. Falandys, P. Łabuz, H. Fedewicz, *Nieunikniona reforma służb specjalnych Rzeczypospolitej Polskiej – propozycje de lege ferenda*, „Współczesne Problemy Zarządzania” 2020, nr 1, s. 50 (podsumowanie).

¹³ Na istnienie takiego nadzoru wskazali: A. Tomaszuk, D. Piekarski, P. Opitek, *Nadzór prokuratora nad realizacją kontroli operacyjnej – część I*, „Prokuratura i Prawo” 2021, nr 12, s. 132-152; *część II*, „Prokuratura i Prawo” 2022, nr 1, s. 62-84.

¹⁴ Opinia taka miałaby klauzulę ochrony przewidzianą dla dokumentów niejawnych o klauzuli tożsamej z klauzulą sprawy operacyjnej.

¹⁵ Obecnie trwają prace nad opracowaniem projektu ustawy Kodeks pracy operacyjnej, zob. <https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf> [dostęp: 16.10.2025].

¹⁶ Zob. np. https://pl.wikipedia.org/wiki/Afera_Pegasus czy Raport końcowy z prac Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych – <https://www.senat.gov.pl/aktualnoscilista/art,15764,komisja-nadzwyczajna-ds-inwigilacji-przyjela-raport-ze-swoich-prac.html> [dostęp: 26.09.2024].

Prowadzenie skutecznej kontroli służb specjalnych zawsze związane jest z dostępem do chronionych tajemnicą państwową technik i działań tych służb. Dlatego też nie może ona prowadzić do ujawnienia taktyki i technik stosowanych przez służby specjalne. Nieprzestrzeganie tej zasady uczyni służby nieskutecznymi i co do zasady spowoduje, że nie będą one realizować swoich zadań. Praca operacyjna zawsze będzie niejawną, stąd sposób jej kontrolowania może odbywać się wyłącznie przez wyznaczone osoby, cieszące się zaufaniem zarówno służb, jak i organu procesowego. Biegły sądowy lub osoba powołana przez organ procesowy *ad hoc* kontrolująca ten zakres pracy operacyjnej musi z tych względów, pomimo jedno-razowego wydania zarządzenia przez organ procesowy o dostępie do wskazanych niejawnych materiałów operacyjnych, uzyskać poświadczenie bezpieczeństwa wydane po przeprowadzeniu postępowania sprawdzającego. Z tego też względu nie mogą w postępowaniu uczestniczyć organizacje i stowarzyszenia społeczne, gdyż te nie podlegają procedurze uzyskania dostępu do informacji niejawnych. Warto w tym miejscu wskazać, że prokurator prowadzący konkretne postępowanie przygotowawcze lub sędzia rozpoznający daną sprawę z procedury poprzedzającej uzyskanie dostępu do informacji niejawnych są z mocy prawa zwolnieni.

2. Kontrola służb specjalnych RP na podstawie obowiązujących przepisów prawa

Jak wskazują Aleksander Tomaszuk, Dariusz Piekarski, Paweł Opitek, określone kompetencje do kontroli służb specjalnych RP, tak w zakresie stosowanej kontroli operacyjnej, jak i w czasie wykonywania czynności operacyjno-rozpoznawczych, posiada Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy¹⁷. Kontrola ta ma jednak charakter ograniczony i sprowadza się wyłącznie do oceny przedstawionego materiału operacyjnego przez daną służbę. Najczęściej jest to sam wniosek o zastosowanie kontroli operacyjnej wraz z uzasadnieniem. Naturalnie Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy może podejmować dalsze kroki kontrolne, jednak w praktyce kontrola ta ogranicza się w większości przypadków do przedstawionych przez służby materiałów. Nie wolno zapominać także o stanowisku zajęтым przez Sąd Apelacyjny w Białymstoku, który ustalił, że składane dokumenty w sprawach wnioskowania o kontrolę operacyjną mają charakter blankietowy w takim sensie, że sąd, przychylając się w całości do wniosku, ustosunkuje się do niego w sposób blankietowy, bez konieczności formalistycznego powtarzania wszystkich szczegółowych stwierdzeń zawartych wyczerpująco we wniosku stanowiącego zgodnie z przepisami „awers” postanowienia sądowego.

¹⁷ A. Tomaszuk, D. Piekarski, P. Opitek, *op. cit.*, s. 139. Zob. także art. 13 § 3a pkt 1 ustawy z dnia 28 stycznia 2016 r. Prawo o Prokuraturze, t.j. Dz.U. z 2024 r. poz. 390.

Dopiero gdy sąd nie przychyli się w całości lub w części do wniosku o zastosowanie kontroli operacyjnej, zachodzi konieczność sporządzenia uzasadnienia takiej decyzji, gdzie podane zostaną szczegółowe powody takiego rozstrzygnięcia¹⁸.

Innym ważnym zagadnieniem jest problem konieczności przedstawienia Pierwszemu Zastępcy Prokuratora Generalnego Prokuratorowi Krajowemu we wniosku o zastosowanie kontroli operacyjnej wykorzystywanego środka techniki operacyjnej.

Jednoznacznie należy stwierdzić, że uprawniony prokurator na etapie zapoznania się z materiałami, na podstawie których dana służba wnioskuje o kontrolę operacyjną, nie zapoznaje się ze sprawą operacyjną. Jest to co do zasady prawidłowe postępowanie, ponieważ prokurator nie jest organem, który na etapie wnioskowania powinien zapoznawać się z jej szczegółami, ale tylko z tą częścią, która uzasadnia ten wniosek, w zakresie technik operacyjnych (obserwacji, maskowania, techniki specjalnej) zastosowanej w konkretnej sprawie.

Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy nie prowadzi i nie wykonuje czynności operacyjno-rozpoznawczych, stąd nie ma i nie powinien mieć również dostępu do technicznych aspektów stosowanych podczas tych czynności. Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy podczas oceny materiałów może natomiast dodatkowo omawiać wniosek z przedstawicielem danej służby. Ponadto może on sporządzić notatkę lub w inny sposób udokumentować taką rozmowę, a materiał z niej włączyć do swojejteczki kontrolnej. To na służbach specjalnych RP bowiem spoczywa obowiązek zgromadzenia rzetelnego materiału operacyjnego podczas stosowania metod i form pracy operacyjnej, a następnie, jeśli zostaną spełnione przesłanki ustawowe, przedstawienie wniosku o zastosowanie kontroli operacyjnej.

Obecnie obowiązują procedury pozwalające na zarządzenie kontroli operacyjnej przez daną służbę, w której Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy sprawuje funkcję kontrolną w procesie wnioskowania i dalej wyrażenia zgody przez Sąd Okręgowy w Warszawie. W przypadku Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu zgodnie z art. 27 ust. 1 ustawy ABW i AW (analogicznie art. 17 ust. 1 ustawy o CBA) to sąd na pisemny wniosek Szefa ABW (lub odpowiednio CBA złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego) może, w drodze postanowienia, zarządzić kontrolę operacyjną – gdy inne środki okazały się bezskuteczne albo będą nieprzydatne – przy wykonywaniu czynności operacyjno-rozpoznawczych w celu rozpoznawania, zapobiegania i wykrywania przestępstw, o których mowa we właściwym katalogu – oraz w celu uzyskania i utrwalenia dowodów tych przestępstw,

¹⁸ Wyrok SA w Białymstoku z 16.01.2014 r., II AKa 260/13, LEX nr 1422328.

ujawnienia mienia zagrożonego przeпадkiem, w związku z tymi przestępstwami i ścigania ich sprawców. W przypadku Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego, w celu realizacji zadań określonych w art. 5 ust. 1 pkt 1, 5, 7 i 8 oraz ust. 2 ustawy o SKW i SWW, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne – na podstawie art. 31 tej ustawy – sąd na pisemny wniosek Szefa SKW złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego może, w drodze postanowienia, zarządzić kontrolę operacyjną. Przy czym zasady dokumentowania czynności wynikają z wprost przepisów wykonawczych do ustaw regulujących funkcjonowanie danej służby.

Podobny obowiązek spoczywa na Pierwszym Zastępcy Prokuratora Generalnego Prokuratorze Krajowym, gdy ustawowa metoda pracy operacyjnej służb specjalnych RP w postaci kontroli operacyjnej stosowana jest w trybie niecierpiącym zwłoki. Kontrola prokuratora nad czynnościami operacyjno-rozpoznawczymi została unormowana w Rozporządzeniu Ministra Sprawiedliwości z dnia 13 lutego 2017 r. w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi (dalej: r.s.r.c.p.)¹⁹.

Istotę kontroli badania podstaw faktycznych czynności operacyjno-rozpoznawczych, o których mowa w rozporządzeniu w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi, stanowi ustalenie przez prokuratora, czy odpowiednio przyszła zgoda sądowa i prokuratorska na przeprowadzenie danej czynności zostanie wydana na podstawie rzetelnych ustaleń stanowiących wynik stosowanych wcześniej metod pracy operacyjnej, zatem uzyskanych wiarygodnych informacji podczas wykonywanych czynności operacyjno-rozpoznawczych. Przy czym badania podstaw faktycznych (kontroli) oraz legalności i prawidłowości tych czynności należy dokonać dwuetapowo. Po pierwsze, przed zajęciem przez właściwego prokuratora stanowiska w przedmiocie wniosku, informacji lub zawiadomienia (§ 2, § 3 ust. 2 r.s.r.c.p.), po drugie, w czasie trwania czynności (§ 2, § 7, § 9 ust. 1, § 12 ust. 1 r.s.r.c.p.). Wgląd w materiały uzyskiwane w trakcie kontroli może mieć miejsce wyłącznie podczas trwania czynności (w ich toku).

Na marginesie można dodać, że podstawy faktyczne przeprowadzenia określonych czynności operacyjno-rozpoznawczych mogą zostać zbadane również w ograniczonym zakresie *ex post*. Taka kontrola będzie miała miejsce w sytuacji, gdy na pisemne polecenie Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego upoważniony przez niego prokurator lub zespół prokuratorów

¹⁹ Rozporządzenie Ministra Sprawiedliwości z dnia 13 lutego 2017 r. w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi, t.j. Dz.U. z 2024 r. poz. 1578.

dokona oceny sposobu realizowania przez właściwych prokuratorów okręgowych ich kompetencji w zakresie kontroli nad czynnościami operacyjno-rozpoznawczymi prowadzonymi przez terenowe jednostki policji, Straży Granicznej i Żandarmerii Wojskowej. Badając podstawy faktyczne, ostatecznie właściwy prokurator powinien odpowiednio ustalić, czy informacje znajdujące się w przedłożonych materiałach z czynności operacyjno-rozpoznawczych są wiarygodne, a wniosek zasługiwał na uwzględnienie (§ 3 ust. 1 pkt 1 r.s.r.c.p.).

Przedstawiając rozwiązania prawne w odniesieniu do obecnie obowiązującego stanu prawnego, należy zaproponować *de lege ferenda*, aby w uzasadnionych przypadkach na danym etapie czynności Pierwszy Zastępca Prokuratora Generalnego Prokurator Krajowy mógł skorzystać z pomocy biegłego sądowego. W sprawach trudnych, skomplikowanych miałby wówczas możliwość zasięgnięcia opinii, wydając zarządzenie o dostępie biegłego sądowego do ściśle określonych materiałów niejawnych, z którymi biegły miałby się zapoznać. Nie chodzi tu w żadnym razie o przeniesienie odpowiedzialności z organu procesowego na biegłego sądowego w zakresie wyrażania zgody na czynność kontroli operacyjnej, ponieważ *ex lege* o tym decydują organy procesowe. Natomiast zadaniem biegłego sądowego byłaby ocena na podstawie posiadanych wiadomości specjalnych określonych materiałów i czynności operacyjno-rozpoznawczych służb specjalnych pozwalających na prawidłowe podjęcie różnych decyzji o tak znamiennej skutkach dla bezpieczeństwa obywateli. Naturalnie zatem nie chodzi o powoływanie biegłego sądowego do każdej zastosowanej wcześniej przez służby specjalne kontroli operacyjnej, ale jedynie o przypadki, które takiej wiedzy wymagają i wiążą się z prawidłowym zrozumieniem między innymi tzw. kuchni operacyjnej i innych trudnych zagadnień z zakresu pracy operacyjnej, które dla organu *ex officio* nie są znane i, niestety, nigdy nie będą prawidłowo zrozumiane bez udzielenia określonej pomocy²⁰. W tym przypadku pomocy organu niezależnego, niezależnego także od służb – czyli biegłego sądowego. Naturalnie konieczne jest wyznaczenie krótkiego terminu zapoznania się z materiałami przez biegłego i wydania opinii, w zależności od etapu jego powołania (odpowiednio zarządzenia kontroli operacyjnej na dalszych etapach czynności operacyjno-rozpoznawczych, dalej aż do zakończenia postępowania karnego, jeżeli jest prowadzone w danej sprawie). Odrębnego postępowania wymagałyby przypadki niecierpiące zwłoki. Są to jednak tzw. szczegóły techniczne, które z biegłym sądowym można na bieżąco ustalić. Biegły doskonale mógłby się również wypowiedzieć co do zakresu oraz zasadności objęcia figuranta kontrolą operacyjną, w tym jej najnowszymi środkami technicznymi.

²⁰ Zob. Rola i zadania Wydziału Nadzoru nad Czynnościami Operacyjno-Rozpoznawczymi funkcjonującego w Biurze Prezydyjnym Prokuratury Krajowej, [w:] A. Tomaszuk, D. Piekarski, P. Opitek, *op. cit.*, s. 143.

3. Biegły sądowy i jego merytoryczna pomoc organowi procesowemu w zakresie czynności operacyjno-rozpoznawczych

Biegły sądowy w zakresie czynności operacyjno-rozpoznawczych powoływany jest do większości spraw związanych z szeroko rozumianym przekroczeniem uprawnień przez funkcjonariuszy publicznych lub niedopełnieniem przez nich obowiązków służbowych. Dotyczy to najczęściej prowadzonych przez nich czynności w ramach spraw operacyjnych. Sprawy te dotyczą określonych uchybień, które w ocenie organu procesowego popełnili funkcjonariusze publiczni. Są to sprawy, w których mają już oni przedstawione zarzuty (*ad personam*), jak też postępowania prowadzone (*in rem*). W każdej sprawie, w której wydaje się opinię, biegły sądowy powinien dokonać oceny i znaleźć rozwiązania złożonej i trudnej sytuacji operacyjnej, również uwzględniając między innymi tzw. kuchnię operacyjną, co w konsekwencji pozwala na wydanie opinii rzetelnej, niezależnej, sumiennej i bezstronnej. Biegły sądowy specjalizujący się w zakresie taktyki kryminalistycznej i czynności operacyjno-rozpoznawczych powinien posiadać doświadczenie w realizacji tych czynności, na różnych szczeblach jednostek organizacyjnych je wykonujących (w tym także podczas operacji specjalnych). Konieczne jest też, aby posiadał dużą wiedzę z zakresu ustawodawstwa służb specjalnych i odpowiednio służb policyjnych.

W większości spraw, w których wydaje opinie biegły, materiały dostarcza organ procesowy (prokurator lub sąd, ewentualnie policja lub inne służby śledcze). Materiały te są zawsze szczegółowo określone w postanowieniu, o którym mowa w art. 194 k.p.k. I tak też jest w praktyce, gdyż w postanowieniu prokurator szczegółowo (np. w formie tabeli) określa materiał dowodowy z akt sprawy (np. numery stron, załączniki w postaci teczki operacyjnej ze zdjętą klauzulą tajności – czyli akta jawne lub wskazuje na konkretne materiały niejawne²¹), które odpowiednio przekazuje biegłemu, zadaje pytania i uzasadnia swoje postanowienie. Jest to bardzo ważna czynność procesowa wskazująca na obszar z zakresu czynności operacyjno-rozpoznawczych, który najbardziej go interesuje i z którym ma problemy w interpretacji merytorycznej, gdyż wymagają wiadomości specjalnych.

Udostępnienie materiałów biegłemu zostało unormowane przez ustawodawcę w art. 198 § 1 – 3 k.p.k.²² Zgodnie z tym przepisem, jeżeli jest to niezbędne do wydania opinii, to sąd lub prokurator udostępnia biegłemu poszczególne dokumenty z akt sprawy lub uwierzytelnione kopie tych dokumentów. Dokumenty mogą być

²¹ W przypadku materiałów niejawnych wdrażana jest odrębna procedura na podstawie zarządzenia właściwego prokuratora, o której mowa w § 10 Rozporządzenia Ministra Sprawiedliwości z dnia 9 września 2017 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji, Dz.U. z 2017 r. poz. 1733.

²² J. Skorupka, *KPK. Komentarz*, Warszawa 2021, s. 494-497.

również udostępnione w postaci elektronicznej. Z kolei biegłemu powołanemu z tego względu, że wydana przez innego biegłego opinia jest niepełna lub niejasna albo gdy zachodzi sprzeczność w niej samej lub między różnymi innymi opiniami w tej samej sprawie, przed wydaniem opinii nie udostępnia się tej innej opinii. Inną opinię można udostępnić biegłemu w niezbędnym zakresie, tylko w wyjątkowym, szczególnie uzasadnionym wypadku, gdy przedmiot opinii powołanego biegłego bezpośrednio dotyczy treści tej innej opinii. W wypadku udostępnienia biegłemu dokumentów z akt sprawy, również w postaci elektronicznej lub uwierzytelnionych kopii tych dokumentów, sporządza się w formie notatki urzędowej wykaz dokumentów, których oryginały, postać elektroniczna lub uwierzytelnione kopie zostały przed wydaniem opinii udostępnione biegłemu. Notatka powinna być podpisana przez osobę sporządzającą z podaniem imienia, nazwiska i stanowiska służbowego oraz załączona do akt sprawy.

W przypadku materiałów niejawnych opinia zostaje wydana przez biegłego sądowego po wcześniejszym zarządzeniu organu procesowego o dopuszczeniu do zapoznania się biegłego sądowego z aktami, teczkami niejawnymi²³. Jak w każdej dziedzinie, tak i w tej występuje wiele problemów związanych z wydaniem opinii. Wydając opinie z zakresu czynności operacyjno-rozpoznawczych, podstawowe wyzwanie dla biegłego stanowi merytoryczne, właściwe, rzetelne i trafne wykorzystanie posiadanych przez siebie wiadomości specjalnych dla celów określonych przez organ procesowy w sporządzonej opinii. Organowi procesowemu należy wszechstronnie uzasadnić za pomocą spostrzeżeń w opinii zajęte stanowisko. Jeżeli funkcjonariusz danej służby twierdzi, że dokumentacja z określonej czynności znajduje się w danej tece operacyjnej – to sąd i biegły ten fakt mają obowiązek sprawdzić.

W wielu sprawach nawet doświadczony prokurator czy sędzia nie są w stanie samodzielnie dokonać właściwej oceny materiałów operacyjnych bez posiadania wiadomości specjalnych. W praktyce jednak organ procesowy bardzo często nie powołuje biegłego sądowego, tylko konsultuje dane stanowisko z funkcjonariuszem np. z Centralnego Biura Śledczego Policji czy Biura Spraw Wewnętrznych Policji i na tej podstawie podejmuje decyzję procesową. Zatem należy podkreślić, że takie konsultacje często okazują się nietrafne i powinny skutkować powołaniem biegłego sądowego na dalszym etapie postępowania karnego przed sądem pierwszej lub drugiej instancji.

²³ Zob. wyjątek, o którym mowa w § 6 ust. 1 pkt 1 zd. pierwsze – Rozporządzenie Ministra Sprawiedliwości z dnia 9 września 2017 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji, Dz.U. z 2017 r. poz. 1733.

3.1. Dostęp biegłego sądowego do informacji niejawnych

Co do zasady, każdy biegły sądowy powołany przez organ procesowy (przez sąd lub prokuratora) może mieć dostęp do informacji niejawnych znajdujących się w aktach oznaczonych klauzulą tajności. Jednak aby taki dostęp uzyskał, organ procesowy musi wydać zarządzenie zgodnie z § 10 Rozporządzenia Ministra Sprawiedliwości z dnia 9 września 2017 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji. Przepis ten stanowi, że udostępnienie dokumentów, akt lub przedmiotów oznaczonych klauzulą tajności biegłemu, tłumaczowi lub specjaliście następuje na podstawie zarządzenia prezesa sądu, a w postępowaniu przygotowawczym – na podstawie zarządzenia prokuratora, tylko w zakresie niezbędnym do wykonania czynności procesowej. Przepisy § 6, 8 i 9 przedmiotowego rozporządzenia stosuje się odpowiednio – oznacza to m.in., że biegły sądowy na mocy tegoż zarządzenia może uzyskać dostęp aż do materiałów niejawnych oznaczonych klauzulą „ściśle tajne”, z wyjątkiem dokumentów, akt lub przedmiotów, o których mowa w art. 184 § 1 i art. 156 § 5a k.p.k.

Udostępnienie akt, dokumentów lub przedmiotów oznaczonych klauzulą tajności następuje w obecności wyznaczonego pracownika kancelarii tajnej lub sekretariatu w zależności od klauzuli tajności. W praktyce na tym tle powstaje wiele problemów.

Pracownicy kancelarii tajnych są zwyczajowo przygotowani do dostępu do informacji niejawnych tylko na podstawie poświadczenia bezpieczeństwa, w trybie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych²⁴. Nie każdy biegły sądowy takie poświadczenie bezpieczeństwa posiada, głównie ze względu na koszty jego wydania i konieczności założenia i prowadzenia działalności gospodarczej, w przypadku gdy biegły jest na emeryturze i nie jest zatrudniony w jednostce, która jest uprawniona chociażby do uproszczonego przeprowadzenia postępowania sprawdzającego do klauzuli „poufne”. Zatem problem polega nie na zarządzeniu organu procesowego o dostępie do informacji niejawnych, tylko niechęci w udostępnianiu w tym trybie akt biegłemu sądowemu przez pracowników kancelarii tajnej. Kierownicy kancelarii tajnej, zatem profesjonalści w dziedzinie ochrony informacji niejawnych, twierdzą, że tryb ten nakłada na nich wiele dodatkowych obowiązków (np. stała obecność pracownika kancelarii podczas zapoznawania się biegłego z materiałem z czynności operacyjno-rozpoznawczych).

²⁴ T.j. Dz.U. z 2024 r. poz. 632.

3.2. Cel opinii – opinia jawna i jej część niejawna

Główny cel opiniowania wynika odpowiednio z art. 193 § 1 k.p.k., zatem jeżeli stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych, zasięga się opinii biegłego albo biegłych. Biegły, wykonując postanowienie organu procesowego, realizuje wszystkie cele, w tym postanowieniu określone. Zatem biegły powinien, jeżeli to możliwe, całkowicie rozwiązać problem organu procesowego, odpowiedzieć na jego pytania. Konstruując wnioski, biegły wykorzystuje wszystkie spostrzeżenia zawarte w opinii, które powstały na podstawie posiadanych przez biegłego sądowego wiadomości specjalnych. Należy pamiętać, że zgodnie z regułą (maksymą) *iura novit curia* – odpowiednio za niedopuszczalne uznaje się przeprowadzenie dowodu z opinii biegłego, w celu ustalenia obowiązującego stanu prawnego oraz zasad zastosowania i wykładni obowiązujących przepisów prawa²⁵. Jednak zasada ta nie dotyczy przepisów z zakresu czynności operacyjno-rozpoznawczych (w tym niejawnych instrukcyjnych), ponieważ są one przede wszystkim niejasne i generalnie nieznane organom procesowym. Reguła ta dotyczy często również przepisów prawa międzynarodowego. Dlatego biegły w zakresie czynności operacyjno-rozpoznawczych opiniuje również, w celu ustalenia wykładni niejasnych dla organu procesowego, niejawnych przepisów instrukcyjnych oraz innych z nimi związanych, których rzetelne zrozumienie wymaga wiadomości specjalnych.

Biegły sądowy korzysta z posiadanych wiadomości specjalnych dotyczących metod i form czynności operacyjno-rozpoznawczych, opartych na przepisach prawa oraz wiedzy kryminalistycznej, w tym nauk pokrewnych. Opinia biegłego powinna posiadać wysoką jakość merytoryczną, co jest nieosiągalne w przypadku powołania osoby niekompetentnej i nieposiadającej właściwych kwalifikacji w danej dziedzinie. Organ procesowy w naszej ocenie powinien najpierw poznać merytoryczne kwalifikacje biegłego (jego wiedzę i doświadczenie), a dopiero potem go powołać. Niestety, nawet wtedy, gdy jest on już ustanowiony biegłym sądowym. Zgodnie z art. 194 k.p.k. – przedmiot i zakres ekspertyzy określa się w postanowieniu. W przypadku wydania przez biegłego sądowego opinii niejawnej obowiązują te same rygory procesowe z jednoczesnym uwzględnieniem norm prawnych, o których mowa w ustawie o ochronie informacji niejawnych²⁶. W tej samej sprawie może na przykład być sporządzona opinia jawna na podstawie jawnych materiałów procesowych, zawartych w aktach postępowania karnego, i odrębnie opinia niejawna, która dotyczy wyłączonych z części jawnej – niejawnych materiałów tego postępowania.

²⁵ Por. wyrok SA w Białymstoku z 18.06.2014 r., I ACa 160/14, LEX nr 1506648.

²⁶ Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz.U. z 2019 r. poz. 742.

3.3. Ograniczenia biegłego sądowego w dostępie do materiałów z czynności operacyjno-rozpoznawczych służb specjalnych

Zabronione jest ujawnianie danych o osobie udzielającej pomocy funkcjonariuszom ABW i AW, CBA, czy SKW i SWW w zakresie czynności operacyjno-rozpoznawczych, a zakres dostępu prokuratora lub sądu do informacji z zakresu czynności operacyjno-rozpoznawczych unormowany został szczegółowo określony w przepisach.

Zgodnie z tym przepisami został unormowany obszar ujawnienia organowi procesowemu przez Szefa danej służby określonych informacji. Jednak ustawodawca zabrania ujawniania danych dotyczących osobowego źródła informacji i innych informacji objętych normami prawnymi przepisów służb specjalnych. Wyjątek stanowią skrajne przypadki. I tak na przykład Szefowie Agencji, na podstawie art. 39 ust. 4 i 5 ustawy o ABW i AW, mogą udzielić informacji, w przypadku żądania prokuratora albo sądu, zgłoszonego w celu ścigania karnego za czyn zabroniony, stanowiący zbrodnię lub występki, którego skutkiem jest śmierć, lub przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych. Jak też w przypadku żądania prokuratora lub sądu uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. Z kolei Szefowie SKW i SWW mogą udzielić informacji na podstawie art. 43 ust. 4 i 5 ustawy o SKW i SWW, w przypadku żądania prokuratora albo sądu, zgłoszonego w celu ścigania karnego za czyn zabroniony, stanowiący zbrodnię lub występki, którego skutkiem jest śmierć, albo w celu przeprowadzenia postępowania lustracyjnego lub realizacji zadań z nim związanych, lub przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych. Jak też w przypadku żądania prokuratora lub sądu uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. W przypadku odmowy zwolnienia, o którym mowa wyżej, przez Szefa danej służby specjalnej, można stosować odpowiednio: art. 39 ust. 6 ustawy o ABW i AW; art. 43 ust. 6 ustawy o SKW i SWW lub art. 28 ust. 5 ustawy o CBA. Zależy to od okoliczności sprawy i decyzji organu procesowego, w tym przypadku Pierwszego Prezesa Sądu Najwyższego, który również powinien zasięgnąć w takich wyjątkowych przypadkach opinii biegłego z zakresu czynności operacyjno-rozpoznawczych.

3.4. Odpowiedzialność biegłego sądowego

Ocenić materiał operacyjny nieobiektywnie jest łatwiej niż rzetelnie rozwiązać faktyczny i merytoryczny problem operacyjny. Biegły, dokonując oceny, bierze pod uwagę obiektywne okoliczności przemawiające na korzyść funkcjonariusza

publicznego i na jego niekorzyść. Wnioski opinii należy właściwie uargumentować przy kategoriycznym zachowaniu bezstronności. Nie są w stanie tego uczynić osoby bez prawidłowego przygotowania do sprawowania funkcji biegłego sądowego. Jeszcze raz należy zatem podkreślić, że błędem organu procesowego jest, gdy do opiniowania zostaną powołane osoby, które nie znają kompleksowo zakresu wszystkich czynności operacyjno-rozpoznawczych i odpowiednio zasad procedury karnej, albowiem będzie rodziło ich odpowiedzialność, w najłagodniejszym przypadku dyscyplinarną.

W tym miejscu z dużym uproszeniem, gdyż wykraczałoby to poza ramy niniejszego opracowania, można wskazać, że sankcją dla nierzetelnego biegłego jest skreślenie z listy biegłych czy odpowiedzialność eksperta wobec uczestników postępowania (postępowanie wobec biegłych o odszkodowanie). Odnosząc się zaś krótko do zasad odpowiedzialności biegłych, w przypadku prawa cywilnego należy wyróżnić należytą staranność, o której mowa w art. 355 § 1 i 2 k.c., jako podstawę oceny efektów ich pracy wyrażoną w przedkładanej opinii²⁷.

Natomiast w przypadku odpowiedzialności karnej stosuje się wobec biegłego art. 233 § 4 k.k.²⁸ Biegły może też odpowiadać z art. 271 § 1 k.k.²⁹ i nie ponosi odpowiedzialności za rozstrzygnięcia organu procesowego – jedynie za uczciwość, staranność i sumienność wykonania zleconych mu zadań.

4. Uprawnienia służb specjalnych do stosowania najnowszych środków technicznych podczas kontroli operacyjnej

Na wstępie należy stwierdzić, że rozwój nowych technologii pozwala na jednoczesne skuteczne stosowanie najnowszych środków technicznych (w tym w postaci oprogramowania) przez wszystkie służby. Katalog środków technicznych kontroli operacyjnej stosowanej przez służby specjalne (art. 27 ust. 6 ustawy o ABW i AW i art. 31 ust. 4 ustawy o SKW i SWW), jak też kontroli i utrwalania rozmów, o których mowa z kolei w art. 241 k.p.k., pozostają katalogami otwartymi pozwalającymi nadążyć racjonalnemu ustawodawcy z rewolucją technologiczną. Należy przypomnieć, że kilka lat temu w doktrynie toczył się spór o wykorzystanie nowego na tamten czas środka technicznego. Kwestia dotyczyła podsłuchu poczt

²⁷ Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego, t.j. Dz.U. z 2021 r. poz. 1805 ze zm.

²⁸ Przepis ten stanowi: „Kto jako biegły, rzeczoznawca lub tłumacz, przedstawia fałszywą opinię, ekspertyzę lub tłumaczenie mające służyć za dowód w postępowaniu określonym w § 1, podlega karze pozbawienia wolności od roku do lat 10”.

²⁹ Funkcjonariusz publiczny lub inna osoba uprawniona do wystawienia dokumentu, która poświadcza w nim nieprawdę co do okoliczności mającej znaczenie prawne, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

elektronicznej. Ostatecznie w wyniku przeprowadzonych analiz prawnych przyjęto stanowisko, że katalog środków technicznych, o którym mowa w art. 241 k.p.k., pozostaje katalogiem otwartym³⁰.

Kontrola operacyjna wszystkich służb specjalnych prowadzona jest niejawnie i polega 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 w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych.

Dla celów wykładni systemowej przepisów prawa dotyczących zakresu stosowanych środków technicznych w kontroli operacyjnej należy przypomnieć, że:

- art. 27 ust. 6 pkt 1 ustawy o ABW i AW i art. 31 ust. 4 pkt 1 ustawy o SKW i SWW pozwala na uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych (wszelkich najnowszych środków technicznych, również najnowszych programów), w tym za pomocą sieci telekomunikacyjnych, do której należy zaliczyć: wszelką korespondencję w postaci prowadzonych rozmów (nie tylko telefonicznych), zatem treści tych rozmów. Mogą to być np. rozmowy prowadzone za pomocą smartfonów, w tym telefonów internetowych (VOIP), komunikatorów internetowych; innego rodzaju rozmów, do których stosuje się lub są prowadzone przy użyciu środków technicznych zgodnie z najnowszym rozwojem technologicznym w dziedzinie informatyki, teleinformatyki i telekomunikacji; rozmowy prowadzone z wykorzystaniem łączności radiowej, czyli rozmowy rejestrowane przy użyciu środków technicznych czy też rozmowy utrwalone przy zastosowaniu oprogramowania pozwalającego przełamać zabezpieczenia techniczne urządzeń końcowych (programy szpiegujące);
- art. 27 ust. 6 pkt 2 ustawy o ABW i AW i art. 31 ust. 4 pkt 2 ustawy o SKW i SWW pozwala na uzyskiwanie i utrwalanie obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne, tj. rejestrację i podgląd przy wykorzystaniu urządzeń do utrwalania obrazu i dźwięku

³⁰ Zob. T. Grzegorzczak, [w:] *Kodeks postępowania karnego. Komentarz*, wyd. 3, Kraków 2003, art. 241: „[...] obejmuje treści rozmów innych niż telefoniczne, a więc wszelkie rozmowy, bez względu na to, jak i gdzie są prowadzone...”. Zob. też A. Choromańska, *E-podśłuch zagadnienia wybrane*, [w:] *Czynności dochodzeniowo-sledcze i działania operacyjne policji a rola sądu w postępowaniu przygotowawczym: materiały pokonferencyjne*, red. S. Lelental, J. Kudrelek, I. Nowicka, Szczepiński 2008, s. 278-291.

- po pierwsze w pomieszczeniach np. przy użyciu kamery, rejestratora, nadajnika i odbiornika. Po drugie w pojazdach i innych środkach transportu, np. GPS i GPRS z funkcjami dodatkowymi do utrwalania obrazu i dźwięku. Do miejsc innych niż miejsca publiczne należy zaliczyć np. gabinet lekarski;
- art. 27 ust. 6 pkt 3 ustawy o ABW i AW i art. 31 ust. 4 pkt 3 ustawy o SKW i SWW pozwala na uzyskiwanie i utrwalanie treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej – istotą tego rodzaju środków technicznych jest to, że służą one w przedmiotowym zakresie tylko do uzyskiwania i utrwalania treści korespondencji, zatem treści korespondencji pisemnej, elektronicznej – nie rozmowy. Będzie to m.in.: przesyłka listowa, przesyłka kurierska w części dot. przesyłki listowej będącej przesyłką rejestrowaną. Dotyczy to także poczty elektronicznej. W wyniku wykładni systemowej (art. 27 ust. 6 pkt 3 ustawy o ABW i AW i art. 31 ust. 4 pkt 3 ustawy o SKW i SWW) należy stwierdzić, że racjonalny ustawodawca pocztę elektroniczną zalicza do środków komunikacji elektronicznej (zatem wyróżnia ją jako środek techniczny, co pozwala na zaliczenie poczty elektronicznej do grupy środków technicznych, w kontroli operacyjnej zob. usługa Cloud Computing w Big data³¹). Do grupy tej należy zaliczyć m.in. treść korespondencji pisemnej przekazywanej za pomocą komunikatorów internetowych i innych (m.in. telefonia, telefonia internetowa – korespondencja pisemna);
 - art. 27 ust. 6 pkt 4 ustawy o ABW i AW i art. 31 ust. 4 pkt 4 ustawy o SKW i SWW pozwala na uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych, tj. informatyczny nośnik danych rozumiany jako materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej (art. 3 pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, będzie to np. pamięć USB, interfejs USB, karta SD, inne urządzenia elektroniczne wraz z wbudowaną pamięcią); system teleinformatyczny – to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy Prawo komunikacji elektronicznej i Europejskiego Kodeksu Łączności Elektronicznej³² (informacjami przeka-

³¹ J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo” 2017, nr 7 i 8, s. 31-56.

³² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona). Tekst mający znaczenie dla EOG; Dz.U. UE L. z 2018 r. Nr 321, str. 36 z późn. zm.

zywany mi za pomocą sieci telekomunikacyjnych będą rozmowy telefoniczne, wiadomości SMS, MMS, a także inne informacje przekazywane drogą radiową i internetową, w tym poczta elektroniczna, treści zamieszczane na forach internetowych i czatach). Istotne jest wyjaśnienie pojęcia telekomunikacyjnego urządzenia końcowego – jest to urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończenia sieci, np. modem, terminal, konwerter, urządzenia końcowe ISDN, PSTN; urządzenia transmisji danych, np. X21, X 25, Ethernet, token ring, tokenbus, TCP/IP, frame relay. Na przykład w usłudze Cloud Computing urządzeniem końcowym będzie telefon komórkowy, tablet lub inne dostępne urządzenie. Są to m.in. wszelkie dopuszczone prawem środki. Jest to rodzaj kontroli operacyjnej umożliwiający na przykład przeszukanie komputera w czasie rzeczywistym³³. Dalej w zakresie przedmiotowego rodzaju kontroli operacyjnej mieszczą się m.in. zapisy z urządzeń końcowych rejestrujących transakcje płatnicze (dane) czy np. dane uzyskane w wyniku łączności modemu z telefonem i wiele innych, których nie sposób wymienić;

- art. 27 ust. 6 pkt 4 ustawy o ABW i AW i art. 31 ust. 4 pkt 4 ustawy o SKW i SWW pozwala na uzyskiwanie dostępu i dokonywania kontroli zawartości przesyłek typu: paczka pocztowa, przesyłka kurierska w części dot. paczki pocztowej, przesyłka z korespondencją; za kwalifikacją przesyłki z korespondencją do przedmiotowego zakresu przemawia fakt jej określenia przez racjonalnego ustawodawcę – jako przesyłki pocztowej niebędącej drukiem, zawierającą informację utrwaloną na dowolnym nośniku, w tym utrwaloną pismem wypukłym. Będą to zatem wszystkie przesyłki w rozumieniu prawa pocztowego, które będą podlegały kontroli operacyjnej wyłącznie w zakresie uzyskania do nich dostępu i kontroli ich zawartości – bez możliwości uzyskiwania i utrwalania treści korespondencji, wyłącznie na podstawie tego przepisu (konieczność stosowania odpowiednio pozostałych przepisów prawa, o których mowa w art. 27 ust. 6 ustawy o ABW i AW, art. 31 ust. 4 ustawy o SKW i SWW).

W zakresie kontroli operacyjnej mieszczą się zatem najnowsze środki techniczne, które jak pozostałe mogą zostać zastosowane przez uprawnione polskie służby po spełnieniu warunków dopuszczalności (w tym zasady subsydiarności³⁴), o których mowa odpowiednio w ustawie danej służby.

Oprogramowanie szpiegujące i inne podobnie lub jeszcze efektywniej działające programy mogą zostać zastosowane również na podstawie art. 9 ust. 1 i 4 ustawy

³³ J. Kudła, A. Staszak, *Kontrola operacyjna w systemie informatycznym*, „Studia Iuridica Lublensia” 2021, nr 2, s. 263-284.

³⁴ Zob. możliwość oceny materiałów operacyjnych m.in. na podstawie zasady subsydiarności: J. Kudła, P. Kosmaty, *Ankieta oceny ryzyka z czynności operacyjno-rozpoznawczych*, [w:] *Inspiracje i wspomnienia dedykowane pamięci Jerzego Koniecznego*, red. J. Widacki, Kraków 2021, s. 93-117.

o działaniach antyterrorystycznych³⁵ oraz odpowiednio na podstawie przepisów zezwalających na zastosowanie kontroli operacyjnej urządzenia końcowego. Przy czym, jeśli podczas stosowania danego oprogramowania, w trakcie kontroli operacyjnej, odrębnie stosowano maskowanie czynności (technikę specjalną), to informacje o szczegółach technicznych i taktycznych tych działań nie mogą zostać ujawnione nawet organowi procesowemu.

Najnowsze oprogramowanie szpiegujące służące do inwigilacji szeroko rozumianych urządzeń końcowych zaliczane jest do współczesnych środków technicznych w kontroli operacyjnej³⁶. Działa na zasadzie przełamania zabezpieczeń, na przykład w urządzeniach końcowych bez pomocy operatora (dostawcy usług cyfrowych czy operatora usług kluczowych).

Programy te wykorzystują tzw. Trojany, tj. funkcje, które wykonują nie dające się ustalić przez użytkownika końcowego działania, czy na przykład luki w oprogramowaniu tzw. Zero-Day Exploit³⁷.

Użycie odpowiednio przez określoną służbę oprogramowania szpiegującego³⁸ i innych, w ramach kontroli operacyjnej, należy uznać za czynność mieszczącą się w granicach uprawnień działania danej służby, pod warunkiem spełnienia dopuszczalności stosowania kontroli operacyjnej. Jak słusznie wskazuje Patrycja Kozłowska-Kalisz, art. 267 § 3 k.k. „nie obejmuje – co oczywiste – sytuacji uzyskania informacji na podstawie przepisów prawa pozwalających na stosowanie urządzeń podsłuchowych i innych urządzeń pozyskiwania informacji (por. np. art. 237 i 241 k.p.k., art. 19 ustawy z 6.04.1990 r. o Policji; art. 27 ustawy z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu)”³⁹.

Do zbieżnych poglądów zezwalających na stosowanie najnowszego oprogramowania w ramach kontroli operacyjnej przez uprawnione służby należy zaliczyć poglądy Arkadiusza Lacha czy Włodzimierza Wróbla.

³⁵ T.j. Dz.U. z 2025 r. poz. 194.

³⁶ Por. J. Kudła, *Ukierunkowane zatrzymywanie danych o ruchu i lokalizacji przez uprawnione służby. Omówienie wyroku TS z dnia 5 kwietnia 2022 r., C-140/20 (Commissioner of the Garda Síochána e.a.)*, LEX/el. 2022, nr 151411241 [dostęp: 8.06.2022]. J. Kudła, *Dostęp służb do danych telekomunikacyjnych. Omówienie wyroku TS z dnia 2 marca 2021 r., C-746/18 (Prokuratur)*, LEX/el. 2021, numer 151379507 [dostęp: 8.06.2022] oraz J. Kudła, *Używanie dostarczanych przez firmy telekomunikacyjne danych osobowych i danych o lokalizacji przez służby państw członkowskich UE. Glosa do wyroku TS z dnia 6 października 2020 r., C-623/17*, LEX/el. 2020, numer 386259811 [dostęp: 8.06.2022].

³⁷ F. Radoniewicz, *Hacking w kodeksie karnym – wybrane zagadnienia techniczne i karne*, [w:] *Przestępczość teleinformatyczna 2020*, red. J. Kosiński, G. Krasnodębski, Gdynia 2021, s. 183.

³⁸ M. Hapunik, *Czynności operacyjno-rozpoznawcze a nowe technologie*, [w:] *Prawo karne i kryminologia wobec kryzysów XXI wieku*, red. D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, E.W. Pływaczewski, Warszawa 2022, s. 118.

³⁹ P. Kozłowska-Kalisz, [w:] *Kodeks karny, komentarz*, red. M. Mozgawa, wyd. 9, Warszawa 2019, s. 878.

Arkadiusz Lach uważa, że: „[...] nie wyczerpuje znamion czynów zabronionych z art. 267 § 1-3 k.k. osoba upoważniona do uzyskiwania informacji dla niej nieprzeznaczonej na podstawie przepisów Kodeksu postępowania karnego oraz ustaw policyjnych regulujących podsłuch procesowy i kontrolę operacyjną. W przypadku osób prywatnych, które nie posiadają takowego upoważnienia, dopuszczenie przez organ procesowy dowodu uzyskanego w sposób wyczerpujący znamiona ww. czynów zabronionych nie pozbawia tych czynów bezprawności (zob. postanowienie SN z 27.04.2016 r., II KK 265/15⁴⁰). Warto tu wskazać, że zgodnie z aktualnym brzmieniem art. 168a k.p.k. uzyskanie dowodu w drodze czynu zabronionego nie powoduje z tego tylko powodu jego niedopuszczalności”⁴¹. Podobnie W. Wróbel zauważa, że „nie popełnia przestępstwa z art. 267 § 3 ten, kto posługuje się urządzeniem podsłuchowym w celu uzyskania informacji, do której jest uprawniony”⁴².

Wykorzystanie uzyskanych materiałów powstałych w wyniku stosowania środka technicznego, w postaci oprogramowania szpiegującego i innych programów, następuje w trybie przepisów o kontroli operacyjnej. Natomiast dostęp podejrzanego do materiałów, w których wykorzystywano dane oprogramowanie, każdorazowo powinien być uzgadniany z Szefem danej służby. To ostatecznie on – w porozumieniu z organem procesowym – wraz z biegłym sądowym powinni po wcześniejszych ustaleniach decydować, z jaką konieczną częścią materiałów podejrzanego może się zapoznać. Jeszcze raz należy kategorycznie podkreślić, że podejrzanego nie należy zapoznawać z tą częścią materiałów zastosowanej kontroli operacyjnej, która dotyczy technik oraz wykorzystywanych metod i narzędzi służących do pozyskiwania danych⁴³.

5. Oznaczenie środka technicznego na wniosku o zastosowanie kontroli operacyjnej

Na podkreślenie zasługuje wyróżnienie w literaturze przedmiotu rodzaju kontroli operacyjnej z uwzględnieniem symboli, które powinny się znaleźć na wniosku, o którym mowa w ustawach służb specjalnych, gdzie przykładowo:

- KK oznacza kontrolowanie korespondencji pisemnej,
- KZP kontrolowanie zawartości przesyłek,
- PT kontrolowanie korespondencji w systemie telefonii przewodowej,
- PTK podsłuch telefonii komórkowej,

⁴⁰ „Gdańskie Studia Prawnicze – Przegląd Orzecznictwa” 2017, nr 1, poz. 109, LEX nr 2365149.

⁴¹ A. Lach, [w:] *Kodeks karny. Komentarz*, red. V. Konarska-Wrzeszek, wyd. 3, Warszawa 2020, art. 267, LEX nr 587715945/630822 [dostęp: 6.06.2022].

⁴² *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017, s. 643.

⁴³ M. Bożek, *Status prawnoustrojowy Szefa Agencji Bezpieczeństwa Wewnętrznego...*, s. 77–106.

- PTFax kontrolę korespondencji telefaksowej,
- KKI kontrolę prowadzoną w sieci internetowej,
- PP podsłuchu w pomieszczeniu,
- PDF podglądu przy wykorzystaniu urządzeń do rejestracji obrazu i dźwięku,
- KPO kontrolowanie przemieszczania obiektu przy wykorzystywaniu środków technicznych,
- KUK kontrolowanie urządzenia końcowego⁴⁴.

Stosowany rodzaj kontroli operacyjnej, w tym środka technicznego – ze względu na gwarancje systemowe podnoszone przez Trybunał Konstytucyjny, Sąd Najwyższy, Prokuratora Generalnego, Rzecznika Praw Obywatelskich – powinien być systemowo wyróżniony we wniosku, o którym mowa wyżej⁴⁵. Przedstawione symbole w związku z nowym merytorycznym podziałem rodzajowym kontroli operacyjnej zostały rozszerzone i przyporządkowane indywidualnie do jednostkowego rodzaju kontroli operacyjnej. Dany symbol powinien znaleźć się we wniosku o zastosowanie kontroli operacyjnej składanego do sądu okręgowego przez uprawnioną służbę. Symbol ten w żaden sposób nie dekonspiruje taktyki działania służb, natomiast pozwala na wyodrębnienie i oznaczenie kategorii środka stosowanego podczas kontroli operacyjnej, zgodnie z art. 27 ust. 6 ustawy o ABW i AW i art. 31 ust. 4 ustawy o SKW i SWW.

Warto jeszcze zauważyć, że w obecnym systemie prawa zdefiniowane zostały przez ustawodawcę inne pojęcia mające ogromne znaczenie dla stosowania środków technicznych, w ramach kontroli operacyjnej oraz ich zabezpieczania i w konsekwencji pozwalające na praworządne gromadzenie dowodów cyfrowych. Zaliczyć do nich można m.in. definicję interfejsu rozumianego jako układ elektryczny, elektroniczny lub optyczny, z oprogramowaniem lub bez oprogramowania, umożliwiający łączenie, współpracę i wymianę sygnałów o określonej postaci pomiędzy urządzeniami połączonymi za jego pośrednictwem zgodnie z odpowiednią specyfikacją techniczną⁴⁶. Określone rodzaje interfejsów zdefiniowano w Rozporządzeniu Ministra Infrastruktury⁴⁷, co ma istotne znaczenie dla oznaczenia środka technicz-

⁴⁴ A. Biernaczyk, *Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a, 19b ustawy z dnia 6 kwietnia 1990 r. o Policji*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 116.

⁴⁵ Zob. pkt 4 sentencji wyroku Trybunału Konstytucyjnego z 30.07.2014 r., sygn. akt K 23/11, Dz.U. z 2014 r., poz. 1055.

⁴⁶ Art. 2 pkt 10 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, t.j. Dz.U. z 2021 r. poz. 576 z późn. zm.

⁴⁷ Rozporządzenie 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, Dz.U. Nr 226, poz. 1828.

nego wymienionego we wniosku o zastosowanie kontroli operacyjnej, a ponadto pozwala prokuratorowi i sędziemu precyzyjnie wyróżnić *ex lege* rodzaj użytego środka. Chodzi bowiem o kategoryczne rozróżnienie środków, które są dopuszczalne do zastosowania w ramach: art. 27 ust. 1 ustawy o ABW i AW i art. 31 ust. 1 ustawy o SKW i SWW od tych, które z kolei spełniają warunki dopuszczalności stosowania na podstawie: art. 28 ust. 1 ustawy o ABW i AW i art. 32 ust. 1 ustawy o SKW i SWW. Dla ustalenia legalności procedur zgodnie ze stanowiskiem zajęтым przez Pierwszego Zastępcę Prokuratora Generalnego Prokuratora Krajowego, Trybunał Konstytucyjny, Rzecznika Praw Obywatelskich, trzeba wyraźnie rozróżnić środki techniczne (zarówno od strony technicznej i dalej na tej podstawie formalno-prawnej), które mogą być zastosowane odpowiednio w ramach ww. regulacji⁴⁸. Współcześnie należy zaznaczyć, że rozwój techniki w dziedzinie teleinformatyki jest tak gwałtowny, że faktycznie niektóre z tych środków mogą być wykorzystywane wyłącznie w zakresie kontroli operacyjnej. Wiadomo bowiem, jakie są ograniczenia podmiotowe i przedmiotowe związane ze stosowaniem w praktyce tych unormowań prawnych, chociażby ze względu na konieczność kontroli sądowej kontroli operacyjnej czynności wymienionej, w: art. 27 ust. 1 ustawy o ABW i AW i art. 31 ust. 1 ustawy o SKW i SWW, a w przypadku art. 28 ust. 1 ustawy o ABW i AW i art. 32 ust. 1 ustawy o SKW i SWW w zw. art. 28a ustawy o ABW i AW, art. 32a ustawy o SKW i SWW następcej kontroli sądowej (*a priori*), jak też kontroli prokuratorskiej w momencie przekazania materiałów Pierwszemu Zastępcy Prokuratora Generalnego Prokuratorowi Krajowemu na podstawie art. 28 ust. 6 ustawy o ABW i AW, art. 32 ust. 8 ustawy o SKW i SWW.

Podsumowując – nie może tutaj być żadnej mowy o ograniczaniu i odbieraniu skutecznych narzędzi służbom specjalnym, które są wykorzystane do zwalczania szeroko rozumianej przestępczości mieszczącej się w zakresach przedmiotowo-podmiotowych ustaw tychże służb. Chodzi bowiem o to, że jeśli na przykład ABW i AW, SKW i SWW dopuszcza stosowanie odpowiednio: art. 28 ust. 1 ustawy o ABW i AW i art. 32 ust. 1 ustawy o SKW i SWW, w tym określonego środka technicznego, który dzisiaj ma o wiele większe możliwości techniczne niż w przeszłości, to powinien on wyłączyć lub w sposób trwały uniemożliwić włączanie określonych funkcji w ramach danego środka technicznego (interfejsu, oprogramowania czy w końcu oprogramowania szpiegującego), które mogą zostać potencjalnie wykorzystane *expressis verbis* tylko w zakresie kontroli operacyjnej. Mamy tu na myśli całość wyżej wymienionych interfejsów, o ile tylko stosowane do tej kontroli urządzenia i oprogramowania uzyskały, po pierwsze, stosowną

⁴⁸ Por. odpowiednio do działalności służb specjalnych gromadzenie danych teleinformatycznych, o których mowa w: J. Kudła, *Systemowa analiza zakresu kontroli operacyjnej i art. 20c ustawy o Policji na tle praktyki organów ścigania*, „Prokurator” 2009, nr 2, s. 22-45.

akredytację, po drugie gwarantują odpowiedni poziom ochrony uzyskiwanych danych, a po trzecie także uniemożliwiają ingerencję w samą treść pozyskiwanych danych. Takie zachowanie powinno w pełni zabezpieczyć proces legalnego gromadzenia przez służby specjalne przyszłego materiału dowodowego i zapewnić oczekiwaną proporcję w stosowaniu obu ustawowych metod pracy operacyjnej⁴⁹.

6. Środki techniczne kontroli operacyjnej w wielkich zbiorach danych

Współcześnie zakres stosowania kontroli operacyjnej co do środków znacznie się rozszerzył. Nowe technologie spowodowały, że obecna kontrola operacyjna stała się jeszcze szersza i wszechstronna w stosunku do osób, wobec których jest prowadzona. Jak wynika z analizy najnowszych aktów prawnych dotyczących bezpośrednio lub pośrednio stosowania kontroli operacyjnej – jej obszar sięga *ex officio* już nie jednej osoby, ale wielu osób⁵⁰. Dzieje się to niezależnie od organów, które stosują kontrolę operacyjną oraz nią zarządzają. Bowiem środki techniczne używane za pomocą nowych technologii pozwalają na rozszerzenie granic przedmiotowych, ale przede wszystkim podmiotowych kontroli operacyjnej. Analiza najnowszych środków technicznych pozwala do nich zaliczyć te określone w Europejskim kodeksie łączności elektronicznej⁵¹, czyli: nowe formy zarządzania siecią (sieci emulowane programowo lub sieci programowalne), technologię protokołu internetowego IP, usługę łączności głosowej (jej dwukierunkowość), szeroko rozumiany internet rzeczy IoT, telefonię internetową (VoIP), usługi przekazywania wiadomości i obsługę poczty elektronicznej przez Internet, usługę łączności interpersonalnej oraz usługi polegające wyłącznie lub głównie na przekazywaniu sygnałów, widmo radiowe, usługi polegające całkowicie lub częściowo na przekazywaniu sygnałów, takie jak usługi transmisyjne stosowane na potrzeby świadczenia usług łączności maszyna–maszyna oraz na potrzeby nadawania, usługę dostępu do internetu (IoT), femtokomórki, pikokomórki, metrokomórki lub mikrokomórki i inne.

Technologia sieciowa 5G i 6G jest uznawana przez Komisję Europejską za jeden z najważniejszych czynników sprzyjających rozwojowi obecnych usług cyfrowych⁵². Technologia ta oraz na przykład szybka ewolucja rynku TLD (domena

⁴⁹ Por. M. Chrabkowski, *Zgodność z prawem instalacji urządzeń podsłuchowych w mieszkaniu*, „Palestra” 2013, nr 3-4, s. 109.

⁵⁰ J. Kudła, A. Staszak, *Kontrola operacyjna w systemie informatycznym...*, s. 263-284.

⁵¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona). Tekst mający znaczenie dla EOG, Dz.U. UE L z 2018 r. Nr 321, str. 36 z późn. zm.

⁵² Por. odpowiednio: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej

najwyższego poziomu – ang. Top-Level Domain, TLD) i dynamiczny charakter otoczenia cyfrowego pozwalają na większe możliwości stosowania kontroli operacyjnej. Współczesne sieci łączności elektronicznej obejmują wykorzystanie widma radiowego za pomocą łączy bezprzewodowych. W środowisku łączności bezprzewodowej 5G sieci te powstają w szczególności poza budynkami i na drogach. Wymagania dotyczące możliwości sieci łączności elektronicznej stale rosną, co stawia kontrolę operacyjną w nowym (współczesnym) wymiarze, za którym powinny nadążać zmiany przepisów prawa.

Na podstawie obecnego stanu prawnego zatem, który *de lege lata* powinien ulec zmianie ze względu na rozwój nowych technologii i z tym związanych nowych możliwości środków technicznych, należy dodatkowo wyeksponować istniejący nowy podział środków stosowanych podczas kontroli operacyjnej, co do których należy odpowiednio stosować normy prawne przepisów służb specjalnych, o których wyżej mowa. Stąd dane teleinformatyczne – wymagające zgody sądu na stosowanie kontroli operacyjnej – to wszystkie dane w tzw. usłudze przetwarzania w chmurze obliczeniowej, w Big data (w tym pocście elektronicznej) i innych formach przekazu pozwalające na odczytanie treści rozmów, odtworzenie obrazu i dźwięku, zatem te, o których mowa odpowiednio w: art. 43 ustawy Prawo komunikacji elektronicznej (treść komunikatu elektronicznego)⁵³, z wyłączeniem z kolei danych, które nie znajdują się w ruchu i zostały zabezpieczone bez konieczności wykorzystania przekazu usługi przetwarzania w chmurze obliczeniowej w Big data.

Istnieje obecnie jeszcze nowszy rodzaj danych wynikający z Europejskiego kodeksu łączności elektronicznej – z zakresu usługi przekazu – czyli sieci łączności elektronicznej, które umożliwiają dwukierunkową łączność między (oddalonymi od siebie) użytkownikami końcowymi przy użyciu różnych środków komunikacji (np. tekstu, znaków lub mowy) przez zapewnienie konwersji między tymi środkami komunikacji, co do zasady przez człowieka. Komunikacja tekstowa w czasie rzeczywistym jest definiowana zgodnie z unijnym prawem harmonizującym wymogi dostępności produktów i usług, a odnosi się ona do formy komunikacji tekstowej między dwoma punktami lub w postaci konferencji wielopunktowej, w której tekst wprowadzany jest w taki sposób, że komunikacja jest odbierana

inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji). Tekst mający znaczenie dla EOG, Dz.U. UE L z 2024 r. poz. 1689.

⁵³ Zob. J. Kudła, *Zakres kontroli operacyjnej*, LEX/el. 2023 numer 469951183 (wykładnia prawa zawarta w przypisie 1 przedmiotowego komentarza). Zaprezentowana po raz pierwszy przez J. Kudłę na XVIII Seminarium Kryminalistycznym w Zbąszyniu pt. „Nauki sądowe. Między postępowaniem teorii a realiami praktyki” zorganizowanym przez Prokuraturę Okręgową w Zielonej Górze w dniach 25-27 września 2024 r., <https://www.gov.pl/web/po-zielona-gora/xviii-ogolnopolskie-seminarium-kryminalistyczne-zielona-gora-zbaszyn-25--27-wrzesien-2024> [dostęp: 15.12.2024].

przez użytkownika jako ciągła, widoczna litera po literze. Jednak do współczesnych środków technicznych należy zaliczyć najnowsze programy ogólnie dostępne na rynku technologicznym.

Te wszystkie wyżej wymienione argumenty uzasadniają potrzebę przyszłego zupełnie nowego unormowania zakresu kontroli operacyjnej. Katalog najnowszych środków technicznych dopuszczalnych do stosowania podczas kontroli operacyjnej na dziś jest katalogiem otwartym dostosowanym do systematycznego rozwoju najnowszych technologii. Mianowicie pozwala on odpowiednio służbom wraz z rozwojem najnowszych technologii na stosowanie najnowszych rozwiązań technicznych, w celu zwalczania przestępczości, o której mowa z kolei w katalogu przestępstw danej ustawy. Jednak pozostałe przepisy służb specjalnych związane z jego stosowaniem wymagają pilnych zmian.

Starając się rozwiązać kontrowersyjny przypadek praktyczny, skłaniamy się ku pogładowi, aby na wniosku inicjującym procedurę zastosowania podsłuchu procesowego bądź operacyjnego określić systemowo rodzaj środka kontroli operacyjnej (środek techniczny). Tak jak to uczynił racjonalny ustawodawca w art. 27 ust. 6 ustawy o ABW i AW i art. 31 ust. 4 ustawy o SKW i SWW, który ma być stosowany podczas czynności.

Naturalnie powinien on być oznaczony np. symbolem w postaci kodu cyfrowo-literowego, takiego jak podsłuch poczty elektronicznej, kontrola korespondencji internetowej itd., ponieważ w ten sposób z jednej strony dojdzie do zapewnienia pełnej gwarancyjności obu podsłuchów, a z drugiej nie doprowadzi do dekonspiracji stosowanych metod przez służby specjalne. Problem zachowania ochrony stosowanych metod techniki i taktyki operacyjnej jest konieczny dla przyszłej skuteczności działania tychże służb. Natomiast notoryjnym pozostaje fakt, że nawet w przypadku kontroli operacyjnej (oraz *ex officio* kontroli i utrwalania rozmów) osoba, wobec której ją stosowano, a w przypadku podsłuchu operacyjnego zgromadzono dowody, zapoznaje się w konsekwencji z materiałami postępowania, w tym z treścią wniosków i zarządzeń co w określonym przypadku stosowania prawa stanowi przesłankę gwarancyjną⁵⁴. Zachowując zasadę proporcjonalności, wydaje się, że należy pozostać przy koncepcji podmiotowego (co do osób) i przedmiotowego (co do przestępstw katalogowych) poszerzania zakresu obu podsłuchów z ukierunkowaniem, gdy podsłuch jest stosowany na przedmiot, aby zmierzać do jak najszybszego ustalenia osoby i dokumentować te fakty na bieżąco, w zgromadzonych materiałach. Takie postępowanie staje się niezbędne dla zabezpieczenia potrzeb praktyki, w oderwaniu od której nie może się odbywać poprawne proce-

⁵⁴ Zob. M. Wąsek-Wiaderek, *Konwencyjna zasada kontrydiktoryjności i bezpośredniości i jej wpływ na model polskiego procesu karnego*, [w:] *System prawa karnego procesowego. Zagadnienia ogólne*, red. P. Hofmański, Warszawa 2013, s. 136.

dowanie nad wymienionymi zagadnieniami prawnymi⁵⁵. Wszystkie te przesłanki przemawiają również za subsydnaryjnym stosowaniem podsłuchów⁵⁶.

Służby specjalne, przewidując różne rozwiązania, jakie stosują dzisiaj w stosunku do osób podsłuchiowanych, powinny zadbać o wyraźne wyeksponowanie na wniosku o podsłuch możliwych do zastosowania środków, które np. przy użyciu odpowiednich oznaczeń i określeń technicznych pozwolą spełnić wszelkie wymogi gwarancyjne w przedmiotowym zakresie, a jednocześnie nie narażą służb na ujawnienie metod swojego działania.

Literatura

- Biernaczyk A., *Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a, 19b ustawy z dnia 6 kwietnia 1990 r. o Policji*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009.
- Bożek M., *Sejmowa kontrola działalności służb specjalnych i jej ograniczenia wynikające z ustaw kompetencyjnych. Zarys problemu na tle uwarunkowań normatywnych*, „*Studia Iuridica Lublinensia*” 2013, nr 20.
- Bożek M., *Status prawnoustrojowy Szefa Agencji Bezpieczeństwa Wewnętrznego. Zarys problemu na tle rozwiązań konstytucyjnych i ustawowych*, „*Przegląd Sejmowy*” 2014.
- Choromańska A., *E-podsłuch zagadnienia wybrane*, [w:] *Czynności dochodzeniowo-sledcze i działania operacyjne policji a rola sądu w postępowaniu przygotowawczym: materiały pokonferencyjne*, red. S. Lelental, J. Kudrelek, I. Nowicka, Szczepa 2008.
- Chrabkowski M., *Zgodność z prawem instalacji urządzeń podsłuchowych w mieszkaniu*, „*Palestra*” 2013, nr 3-4.
- Eichstaedt K., [w:] *Kodeks postępowania karnego. Komentarz*, red. D. Świecki, wyd. 1, Warszawa 2013.
- Falandys K., Łabuz P., Fedewicz H., *Nieunikniona reforma służb specjalnych Rzeczypospolitej Polskiej – propozycje de lege ferenda*, „*Współczesne Problemy Zarządzania*” 2020, nr 1.
- Gabriel-Węglowski M., *Architektura bezpieczeństwa*, „*Rzeczpospolita*” z 2.02.2022, <https://www.rp.pl/sady-i-prokuratura/art35632141-michal-gabriel-weglowski-architektura-bezpieczenstwa> [dostęp: 26.10.2024].
- Grzegorzczak T., [w:] *Kodeks postępowania karnego. Komentarz*, wyd. 3, Kraków 2003.
- Hapunik M., *Czynności operacyjno-rozpoznawcze a nowe technologie*, [w:] *Prawo karne i kryminologia wobec kryzysów XXI wieku*, red. D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, W.E. Pływaczewski, Warszawa 2022.
- Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017.
- Kozłowska-Kalisz P., [w:] *Kodeks karny. Komentarz*, red. M. Mozgawa, wyd. 9, Warszawa 2019.
- Kudła J., *Dostęp służb do danych telekomunikacyjnych. Omówienie wyroku TS z dnia 2 marca 2021 r., C-746/18 (Prokuratur)*, LEX/el. 2021, nr 151379507.
- Kudła J., *System czynności operacyjno-rozpoznawczych, analityczno-informacyjnych oraz wywiadowczych i kontrwywiadowczych służb specjalnych*, LEX/el. 2016, nr 470060883.
- Kudła J., *Systemowa analiza zakresu kontroli operacyjnej i art. 20c ustawy o Policji na tle praktyki organów ścigania*, „*Prokurator*” 2009, nr 2.

⁵⁵ Por. K. Eichstaedt, [w:] *Kodeks postępowania karnego. Komentarz*, red. D. Świecki, wyd. 1, Warszawa 2013.

⁵⁶ A. Tomaszuk, D. Piekarski, P. Opitek, *Nadzór prokuratora nad realizacją kontroli operacyjnej – część II*, „*Prokuratura i Prawo*” 2022, nr 1, s. 63-79 (dane statystyczne ze stosowanej kontroli operacyjnej za rok 2021).

- Kudła J., *Ukierunkowane zatrzymywanie danych o ruchu i lokalizacji przez uprawnione służby. Omówienie wyroku TS z dnia 5 kwietnia 2022 r., C-140/20* (Commissioner of the Garda Síochána e.a), LEX/el. 2022, nr 151411241.
- Kudła J., *Używanie dostarczanych przez firmy telekomunikacyjne danych osobowych i danych o lokalizacji przez służby państw członkowskich UE. Glosa do wyroku TS z dnia 6 października 2020 r., C-623/17*, LEX/el. 2020, nr 386259811.
- Kudła J., *Zakres kontroli operacyjnej*, LEX/el. 2023, nr 469951183.
- Kudła J., *Zezwolenie oraz udzielenie informacji w trybie art. 20b i 20ba ustawy o Policji*, LEX/el. 2017, nr 470099425.
- Kudła J., Kosmaty P., *Ankieta oceny ryzyka z czynności operacyjno-rozpoznawczych*, [w:] *Inspiracje i wspomnienia dedykowane pamięci Jerzego Koniecznego*, red. J. Widacki, Kraków 2021.
- Kudła J., Staszak A., *Kontrola operacyjna w systemie informatycznym*, „Studia Iuridica Lublinensia” 2021, nr 2.
- Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo” 2017, nr 7 i 8.
- Lach A., [w:] *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, wyd. 3, Warszawa 2020, art. 267, LEX nr 587715945/630822.
- Radoniewicz F., *Hacking w kodeksie karnym – wybrane zagadnienia techniczne i karne*, [w:] *Przestępczość teleinformatyczna 2020*, red. J. Kosiński, G. Krasnodębski, Gdynia 2021.
- Rozporządzenia Ministra Sprawiedliwości z dnia 9 września 2017 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji, Dz.U. z 2017 r. poz. 1733.
- Skorupka J., *KPK. Komentarz*, Warszawa 2021.
- Tomaszuk A., Piekarski D., Opitek P., *Nadzór prokuratora nad realizacją kontroli operacyjnej*, część I, „Prokuratura i Prawo” 2021, nr 12; część II, „Prokuratura i Prawo” 2022, nr 1.
- Wąsek-Wiaderek M., *Konwencyjna zasada kontrydiktoryjności i bezpośredniości i jej wpływ na model polskiego procesu karnego*, [w:] *System prawa karnego procesowego. Zagadnienia ogólne*, red. P. Hofmański, Warszawa 2013.
- Wyrok Trybunału Konstytucyjnego z 30.07.2014 r., sygn. akt K 23/11, Dz.U. z 2014 r. poz. 1055.
- Wyrok SA w Białymstoku z 16.01.2014 r., II AKa 260/13, LEX nr 1422328.
- Zalewski S., *Kontrola służb specjalnych w Polsce*, Warszawa 2021.