Paweł Opitek[1]

Kontrola operacyjna urządzenia końcowego

Streszczenie

Artykuł dotyczy jednej z metod prowadzenia podsłuchów w ramach czynności operacyjno-rozpoznawczych, którego przedmiotem jest urządzenie elektroniczne takie, jak np. telefon lub laptop. W artykule scharakteryzowano, jak należy rozumieć metodę kontroli operacyjnej polegającą na „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych". Opisano, co znaczy każdy zwrot użyty we wskazanej definicji, jakie warunki prawne i faktyczne muszą być spełnione, aby realizować taką kontrolę i uzyskać wartościowy materiał dowody. Artykuł pokazuje, czym są „formy", „metody", „środki techniczne" i „narzędzia" w pracy operacyjnej. Podjęto polemikę z poglądami doktryny w zakresie dopuszczalności i warunków realizacji „podsłuchu" urządzenia końcowego argumentując, że jest to dopuszczalna metoda uzyskiwania informacji w działaniach pozaprocesowych. Na końcu podsumowano podjęty temat badawczy.

Słowa kluczowe

Kontrola operacyjna, podsłuch, służby specjalna, przestępczość, dane informatyczne, ślady cyfrowe, dowody, elektroniczny nośnik danych.

1. Wprowadzenie

Czynności operacyjno-rozpoznawcze stanowią „gorący" temat do dyskusji z kilku powodów: mają one charakter „niejawny", a więc są pewną zagadką, która wymaga rozszyfrowania. A ponieważ czynności takie wkraczają w podstawowe prawa i wolności obywatelskie, to wyjaśnienie formułowanych pytań dotyczących charakteru i zakresu pracy operacyjnej jest ważne dla wielu osób. Jednak publiczne udzielenie odpowiedzi o szczegółach na-

[1] Dr Paweł O p i t e k, prokurator Prokuratury Okręgowej w Krakowie delegowany do Prokuratury Krajowej, ekspert Instytutu Kościuszki, członek Polskiego Towarzystwa Kryminalistycznego i Rady Naukowej Stowarzyszenia Ekspertów Blockchain, wykładowca akademicki, związany z Krajową Szkołą Sądownictwa i Prokuratury.

potyka na poważne ograniczenia natury faktycznej i prawnej. Formy i metody realizacji czynności operacyjno-rozpoznawczych, a więc „technikalia" pracy służb muszą pozostać w ukryciu, aby były skuteczne w walce z przestępczością, a funkcjonariusze i osoby udzielające pomocy organom ścigania czuły się bezpieczne. Budzi to pewne niezrozumienie u ludzi, którzy uważają, że działania służb powinny mieć transparentny charakter w nieograniczonym wymiarze. W ostateczności dochodzi do kolizji dwóch stanowisk: twierdzi się, że czynności operacyjno-rozpoznawcze, w tym kontrola operacyjna, to niezbędne narzędzie walki z najpoważniejszymi formami przestępczości. Z drugiej strony w dyskursie społecznym często deprecjonuje się „podsłuchy" jako aktywność opresyjną państwa nadużywaną przez służby. Słusznie zauważa T. Łodziana, że wielką szkodą dla instytucji kontroli operacyjnej i szerzej – wymiaru sprawiedliwości jest demonizowanie takiej kontroli, głównie przez pryzmat domysłów i hipotez wygłaszanych nierzadko przez osoby, które nie legitymują się wykształceniem i doświadczeniem prawniczym, a pomija się empiryczne badania, polegające chociażby na lekturze spraw, gdzie informacje z kontroli operacyjnej stanowiły materiał dowodowy, w oparciu o który został wydany wyrok skazujący[2].

W mediach szczególnie komentowane są działania pozaprocesowe ukierunkowane na urządzenia końcowe, realizowane za pomocą programu „Pegasus". Z dyskursu toczącego się na ten temat wynika, że chodzi o metodę kontroli operacyjnej polegającą na „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych", a więc z telefonu lub laptopa. Jest to jedna z metod realizacji „podsłuchu" opisana w ustawie o Policji i w dziewięciu pozostałych aktach prawnych przyznających kompetencje poszczególnym służbom do realizacji kontroli operacyjnej. W artykule przedmiotowa regulacja omówiona zostanie przede wszystkim na przykładzie ustawy o Policji, chociaż w tym zakresie treść przepisów „branżowych" we wszystkich ustawach kompetencyjnych jest identyczna i poczynione ustalenia odnoszą się także do Centralnego Biura Antykorupcyjnego, Agencji Bezpieczeństwa Wewnętrznego, Krajowej Administracji Skarbowej, Straży Granicznej, czy Służby Więziennej.

2. Wykładnia art. 19 ust. 6 pkt 4 ustawy o Policji

Kontrola urządzenia końcowego, której legalna definicja znajduje się w art. 19 ust. 6 pkt 4 ustawy z dnia 6 kwietnia 1990 r. o Policji[3] (dalej: uPol), to po-

[2] T. Ł o d z i a n a, Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika, Palestra 2022, nr 9, https://palestra.pl, data odczytu: 25 lutego 2023 r.
[3] Dz. U. z 2020 r., poz. 360 ze zm.

toczna nazwa jednej z metod kontroli operacyjnej polegającej na „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych”[4]; przytoczona definicji zawiera następujące elementy:

- znamiona czasownikowe: „uzyskiwanie i utrwalanie”,
- przedmiot realizacji kontroli: „dane”,

dane zawarte są w:

- „informatycznych nośnikach danych”,
- „telekomunikacyjnych urządzeniach końcowych”,
- „systemach informatycznych” i
- „systemach teleinformatycznych”.

W procesie wykładni prawa podstawowe znaczenie ma odtworzenie językowego znaczenia użytych przez ustawodawcę zwrotów i słów. Zgodnie ze Słownikiem Języka Polskiego PWN[5] „uzyskiwanie” oznacza otrzymywanie czegoś, co było przedmiotem starań, a „utrwalanie” polega na zarejestrowaniu jakiejś treści w pamięci komputera w celu jej późniejszego odtworzenia. Kontrola operacyjna to starania podjęte przez Policję lub inną służbę, aby utrwalić dane w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw „katalogowych”.

W mowie polskiej termin „dane”, podobnie, jak „informacje”, należy do trudno definiowalnych z uwagi na jego pierwotny charakter; w języku potocznym nawet używa się ww. zwrotów zamiennie. Odkodowaniem pojęcia „dane” szczególnie zajmują się dwie dziedziny nauki: zarządzanie wiedzą i teoria informacji, ale one także nie wypracowały jednoznacznych, zadowa-

[4] Identycznie sformułowana metoda kontroli operacyjnej znajduje się ponadto w art. 11n ust. 5 pkt 4 ustawy z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (tekst jedn. Dz. U. z 2022 r., poz. 2487, 2600), art. 9e ust. 7 pkt 4 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2020 r., poz. 305 ze zm.), art. 118 ust. 4 pkt 4 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (tekst jedn. Dz. U. z 2022 r., poz. 813, 835, 1079 z późn. zm.), art. 31 ust. 7 pkt 4 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jedn. Dz. U. z 2021 r., poz. 1214, z 2022 r., poz. 655, 1488, 2600), art. 27 ust. 6 pkt 4 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. Dz. U. z 2022 r., poz. 557, 1488, 2185, z 2023 r., poz. 240), art. 17 ust. 6 pkt 4 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz. U. z 2022 r., poz. 1900, z 2023 r., poz. 240), art. 31 ust. 4 pkt 4 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (tekst jedn. Dz. U. z 2023 r., poz. 81), art. 43 pkt 4 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (tekst jedn. Dz. U. z 2023 r., poz. 66, z 2022 r., poz. 2600, z 2023 r., poz. 240) i art. 23p ust. 5 pkt 4 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (tekst jedn. Dz. U. z 2022 r., poz. 2470, z 2023 r., poz. 240).

[5] https://sjp.pwn.pl/, data odczytu: 25 lutego 2023 r.

lających i powszechnie akceptowanych definicji tego słowa[6]. Stąd wniosek, że podejmowane w orzecznictwie i doktrynie prawa karnego próby wytyczenia ścisłej granicy pomiędzy wspomnianymi pojęciami mają praktyczny charakter i dotyczą np. stosowania przepisów penalizujących określone zachowania w okolicznościach konkretnej sprawy.

„Oczyszczając" przedpole do dalszej dyskusji, zacząć należy od wykładni językowej użytego w art. 19 ust. 6 pkt 4 uPol zwrotu „dane". Słownik Języka Polskiego PWN[7] stanowi, że „dane" to fakty, liczby, na których można się oprzeć w wywodach oraz informacje przetwarzane przez komputer. Komentowany przepis dotyczy ostatniego rodzaju danych, o czym świadczy dalsza treść art. 19 ust. 6 pkt 4 uPol: „zawarte w informatycznych nośnikach danych (…)". Chodzi zatem o „dane informatyczne", których definicja znajduje się w Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r.[8], której Rzeczpospolita Polska jest stroną. Oznaczają one dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny (art. 1 lit b Konwencji)[9]. Wynika z tego, że synonimem „danych informatycznych" są „dane komputerowe" będące „nośnikiem (medium) informacji, faktów i koncepcji, które dopiero sprowadzone do postaci danych komputerowych są czytelne dla systemu informatycznego. W tym celu muszą zostać „zakodowane" w języku binarnym – zamienione w ciąg „0" i „1", a następnie mogą zostać zapisane na nośniku (np. płycie CD, DVD lub na dysku twardym) czy przesłane za pośrednictwem sieci jako impulsy energetyczne. W świetle definicji danymi komputerowymi są też programy odpowiadające za wykonywanie funkcji przez system informatyczny"[10]. Wynika z tego, że „dane informatyczne" są zrozumiałe tylko i wyłącznie dla urządzeń komputerowych, a dopiero ich odpowiednie przetworzenie może dostarczyć „informacje".

„Informacje" stanowią to, co powiedziano lub napisano o kimś lub o czymś, zakomunikowanie czegoś, także dane przetwarzane przez komputer – tyle o „informacjach" mówi Słownik Języka Polskiego[11]. Informacje

[6] M. G r a b o w s k i, A. Z a j ą c, Dane, informacja, wiedza – próba definicji, Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie 2009, nr 798, s. 102–103.

[7] Https://sjp.pwn.pl/, data odczytu: 25 lutego 2023 r.

[8] Dz. U. z 2015 r., poz. 728.

[9] Podobnie brzmi definicja „danych komputerowych" zawarta w art. 2 pkt b Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW; „dane komputerowe" oznaczają przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny.

[10] F. R a d o n i e w i c z, Odpowiedzialność karna za przestępstwo hackingu, Prawo w Działaniu 2013, nr 13, s. 123.

[11] Https://sjp.pwn.pl/szukaj/informacje.html, data odczytu: 25 lutego 2023 r.

pochodzą z wyselekcjonowania danych tak, aby były użyteczne dla odbiorcy, niosą ze sobą jakiś sens i mają znaczenie dla człowieka. Informacje są tym, co powstaje w wyniku pewnych działań myślowych (obserwacji, analiz) z sukcesem zastosowanych do danych, by odkryć ich istotę lub znaczenie. Z kolei „dane" reprezentują nieustrukturyzowane, surowe fakty dotyczące zjawisk i obiektów, które dopiero po odpowiednim przekształceniu mogą, ale nie muszą, stać się informacją.

Przechodząc do dalszych elementów opisu metody kontroli operacyjnej zawartej w art. 19 ust. 6 pkt 4 uPol, to definicja legalna „informatycznego nośnika danych" znajduje się w art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[12]; zgodnie z nią chodzi o „materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej". Definicja ta odwołuje się do statycznie pojętego nośnika (materiału lub urządzenia), obejmującego tworzywo magnetyczne, optyczne lub magneto–optyczne służącego do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej. W tym ujęciu materiał to jednolite tworzywo na powierzchni lub wewnątrz którego są przechowywane dane (np. dysk), a urządzenie to rozwiązanie bardziej złożone i zdolne do samodzielnego przetwarzania danych (np. komputer)[13]. W praktyce, omawiana w tym szczególnym zakresie metoda pracy operacyjnej zazwyczaj ukierunkowana będzie na urządzenie elektroniczne odłączone od sieci Internet, gdzie systemy zarządzania danymi są kodowane za pomocą odpowiednich symboli po to, aby można je było rejestrować, przetwarzać oraz przesyłać do świadomości odbiorcy w postaci komunikatu[14]. W takiej sytuacji dane można przechwycić nie zdalnie, ale np. podłączając się do przedmiotu kontroli kablem USB i kopiując artefakty na *pendrive*.

„Dane", stanowiące przedmiot kontroli operacyjnej, mogą być ponadto zawarte w „telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych".

Termin „telekomunikacyjne urządzenie końcowe" został zdefiniowany w art. 2 pkt 43 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[15] jako „urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci". Są to telefony (stacjonarne i komórkowe), tablety, komputery, faksy, drukarki, kryptowalutowy portfel sprzętowy – jednym słowem wszystkie urządzenia, dzięki którym można odczytać

[12] Tekst jedn. Dz. U. z 2023 r., poz. 5.

[13] M. G r a b o w s k i, A. Z a j ą c, Dane, informacja, wiedza – próba definicji, Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie 2009, nr 798, s. 16; B. K w i a t e k, Nośnik dokumentu elektronicznego, (w:) Dokument elektroniczny w ogólnym postępowaniu administracyjnym, WKP 2020, LEX.

[14] Zob. M. G r a b o w s k i, A. Z a j ą c, Dane, informacja, wiedza – próba definicji, Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie 2009, nr 798, s. 16.

[15] Tekst jedn. Dz. U. z 2022 r., poz. 1648, 1933, 2581.

lub przesłać jakąś informację. Urządzenia odbierają i/lub wysyłają dane, które po przetworzeniu przez algorytm mają postać informacji w formie rozmów telefonicznych, krótkich wiadomości typu SMS lub MMS, wiadomości e–mail, wiadomości przesłanych komunikatorami typy Signal lub Whatsapp, danych geolokalizacyjnych GPS itd. Chodzi więc o „komunikat", a więc każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych (art. 2 pkt 17 ustawy Prawo telekomunikacyjne). Wynika z tego, że rozgraniczenie pomiędzy „informatycznym nośnikiem danych", a „telekomunikacyjnym urządzeniem końcowym" sprowadza się do funkcji nawiązywania przez przedmiot komunikacji z urządzeniami zewnętrznym. Waloru takiego nie posiada płyta CD/DVD lub kostka pamięci USB działająca w trybie *off-line*.

Jeśli chodzi o „system informatyczny", to oznacza on każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych (art. 1 lit a Konwencji o cyberprzestępczości). Definicja „systemu informatycznego" znajduje się także w Dyrektywie Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW[16]; zgodnie z nią „system informatyczny" oznacza urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez to urządzenie lub tę grupę urządzeń, w celach ich eksploatacji, użycia, ochrony lub utrzymania (art. 2 pkt a Dyrektywy).

Ostatni zakres przedmiotowy, o którym mowa w art. 19 ust. 6 pkt 4 uPol, to „system teleinformatyczny". Zgodnie z art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[17] chodzi o „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 z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne".

Wynika z tego, że forma pracy operacyjnej opisana w art. 19 ust. 6 pkt 4 uPol dotyczy dwojakiego rodzaju danych informatycznych:

- statycznych (zawartych w informatycznych nośnikach danych i telekomunikacyjnych urządzeniach końcowych) oraz

[16] Https://eur–lex.europa.eu/legal–content/PL/TXT/?uri=CELEX%3A32013L0040, data odczytu: 25 lutego 2023 r.

[17] Tekst jedn. Dz. U. z 2023 r., poz. 57.

– dynamicznych (transmitowanych w systemach informatycznych i teleinformatycznych).

W każdym przypadku cyfrowe artefakty mogą zostać odebrane w formie dźwięku lub obrazu za pomocą specjalnych algorytmów przetwarzania danych.

Podsumowując tę część rozważań, to kontrola operacyjna polegająca na „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych" oznacza gromadzenie i zabezpieczanie informacji przetwarzanych przez komputer i reprezentujących nieustrukturyzowane, surowe fakty dotyczące zjawisk i obiektów, które dopiero po odpowiednim przekształceniu mogą, ale nie muszą, stać się informacją, a następnie utrwalenie takiej informacji[18].

3. Kontrola urządzenia końcowego jako jedna z metod realizacji kontroli operacyjnej

W debacie publicznej pokutuje pogląd, że kontrola operacyjna ukierunkowana na urządzenie końcowe ma wyjątkowo ofensywny charakter, a metoda ta niekiedy określana jest mianem „cyber–broni". Twierdzi się, że umożliwia ona zbieranie wszelkich danych dostępnych za pomocą telefonu lub innego urządzenia objętego kontrolą. Oczywiście, analizowana praca operacyjna wkracza w podstawowe prawa i wolności człowieka związane z jego sferą życia prywatnego, czy tajemnicą komunikowania się, ale nie jest bardziej „ofensywna", aniżeli inne metody realizacji „podsłuchów" zarządzane przez sąd. Nie sposób przecież *in abstracto* stwierdzić, że treść rozmów telefonicznych, czy wiadomości e–mail zawiera mniej wrażliwe treści, aniżeli np. zapis korespondencji tekstowej prowadzonej za pomocą komunikatora internetowego. Wykładnia językowa ustawowego zapisu „uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych" jednoznacznie wskazuje, że chodzi o artefakty zawarte wewnątrz nośnika, urządzenia lub systemu. Nieprawdziwe są twierdzenia, jakoby wdrożenie kontroli operacyjnej na podstawie art. 19 ust. 6 pkt 4 uPol umożliwiło zarządzanie mikrofonem oraz kamerą telefonu i rejestrację zapisu audio–video z otoczenia aparatu, a więc totalną inwigilację osoby. Obraz i dźwięk z otoczenia smartfonu pochodzą bowiem ze świata zewnętrznego, a „podsłuch" urządzenia końcowego dotyczy tylko i wyłącznie tego, co znajduje się w jego środku, tj. danych wytworzonych przez użytkownika końcowego oraz otrzymanych od innego abonenta sieci informatycznej lub teleinformatycznej. Nie chodzi więc o „podsłuchiwanie" sypialnianego pokoju, aktu

[18] P. Opitek, Poważnie kontrolować można nie tylko terrorystów, Rzeczpospolita z dnia 20 stycznia 2022 r.

religijnego spowiedzi w konfesjonale, czy rozmów prowadzonych w prywatnym mieszkaniu, a takie mylące opinie pojawiały się w debacie publicznej.

Zgodnie z art. 19 ust. 6 uPol „kontrola operacyjna prowadzona jest niejawnie i polega na:

1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
5) uzyskiwaniu dostępu i kontroli zawartości przesyłek".

Ustawodawca precyzyjnie nakreślił, zgodnie ze stanowiskiem wielokrotnie artykułowanym przez Trybunał Konstytucyjny, zamknięty katalog metod służących do niejawnego pozyskiwania informacji i dowodów, co ogranicza arbitralność organów państwa, a ponadto umożliwia sprawowanie efektywnej kontroli nad niejawną działalnością operacyjno-rozpoznawczą w zakresie wykorzystywanych metod pozyskiwania informacji o osobach. W wyroku z dnia 30 lipca 2014 r. TK[19] stwierdził bowiem: „Z punktu widzenia zasady określoności prawa istotne jest natomiast sprecyzowanie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach. Raz jeszcze należy podkreślić, że nie chodzi o wskazanie parametrów technicznych, ale rodzajowych nazw poszczególnych środków i informacji możliwych do pozyskania za ich pomocą (np. 'podsłuch rozmów telefonicznych', 'podsłuch i podgląd pomieszczeń i osób', 'podsłuch techniczny środków łączności przewodowej i radiowej', 'nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu', 'nadzór elektroniczny środków łączności przewodowej lub radiowej')"[20]. Treść art. 19 ust. 6 uPol

[19] OTK-A 2014, nr 7, poz. 80.

[20] Uzasadnienie do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11. W stanie prawnym rozpatrywanym przez TK poważne zastrzeżenia budziła metoda kontroli operacyjnej w brzmieniu art. 19 ust. 6 pkt 3 uPol: „stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych". W skardze Rzecznika Praw Obywatelskich do TK podnoszono zarzuty, że katalog środków technicznych, jakie mogą stosować służby policyjne i ochrony państwa, jest nieograniczony. Trybunał uznał jedna, że „z punktu widzenia zasady określoności prawa i ustawowej formy ograniczeń konstytucyjnych wolności i praw nie jest bezwzględnie konieczne stworzenie zamkniętego katalogu środków technicznych kontroli operacyjnej. W niektórych wypadkach może być to wręcz szkodliwe dla sprawności oraz efektywności działań operacyjnych służb, zważywszy, że sposoby przekazywania informacji

oraz pozostałych ustaw regulujących metody pracy operacyjnej, dokładnie odpowiada trybunalskiemu stanowisku.

Stosowanie art. 19 ust. 6 uPol wymaga, oprócz wykładni językowej, uwzględnienia wykładni systemowej i celowościowej, aby właściwie odtworzyć intencje tzw. racjonalnego ustawodawcy. Wykładnia systemowa pozwala na ustalenie sensu przepisu ze względu na obowiązywanie innych przepisów regulujących tą sama instytucję prawną tak, aby interpretowana norma była z nimi zgodna (postulat niesprzeczności systemu prawa). Wykładnia celowościowa zmierza natomiast do ustalenia treści przepisu ze względu na cel, któremu ten przepis służy.

Każdy z punktów artykuły 19 ust. 6 stanowi samodzielną podstawę prawną do zarządzenia opisanej w nim szczególnej, odmiennej od pozostałych, metody realizacji kontroli operacyjnej; *a contrario* nie można zarządzać kontroli, której opis podany we wniosku o zarządzenie kontroli odbiega od literalnego brzmienia wzorca ustawowego albo zachodzi rozbieżność pomiędzy słownym opisem metody kontroli i przywołaną podstawą prawną jej stosowania. Treść art. 19 ust. 6 uPol uwydatnia cel ustawodawcy: sąd zarządzając kontrolę, a wcześniej prokurator wydając zgodę na wystąpienie z wnioskiem do sądu, ma prawo i obowiązek dokładnie poznać zakres przedmiotowy kontroli: jakiego, zindywidualizowanego urządzenia ona dotyczy i do jakich danych oraz informacji wnioskodawca otrzyma dostęp z wykorzystaniem tego urządzenia. Teoretycznie rzecz biorąc, podstawę prawną kontroli operacyjnej polegającej na uzyskiwaniu obrazu i dźwięku za pomocą kamery i głośnika smartfonu stanowiłby art. 19 ust. 6 pkt 2 uPol („uzyskiwanie i utrwalanie obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne"), a nie art. 19 ust. 6 pkt 4 uPol. Pomijając rozważania techniczne, czy taka kontrola jest w ogóle możliwa, a ponadto pożądana z punktu widzenia ryzyka dekonspiracji działań służb (ograniczona wydajność baterii telefonu przy użyciu funkcji kamery, „grzanie się" aparatu podczas nagrywania, a więc możliwość ujawnienia podsłuchu), to mogłaby ona zostać wdrożona tylko w zupełnie wyjątkowych sytuacjach i trwać przez krótki okres czasu (np. kilka minut w momencie wręczania przez figuranta łapówki). Z kolei wyrażając zgodę na rejestrację rozmów telefonicznych i odczyt krótkich wiadomości tekstowych SMS sąd stosuje art. 19 ust. 6 pkt 1 i 3 uPol, a nie kontrolę operacyjną ukierunkowaną na urządzenie końcowe (art. 19 ust. 6 pkt 4 uPol).

są coraz bardziej wyrafinowane. To z kolei mogłoby ograniczać sprawność działania organów państwa odpowiedzialnych za jego bezpieczeństwo i porządek publiczny, prowadząc w konsekwencji do niewywiązywania się państwa z jednego z podstawowych jego zadań, jakim jest ochrona bezpieczeństwa obywateli". Przepis art. 19 ust. r pkt 3 uPol został zmieniony ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 147) i w obecnym kształcie obowiązuje od dnia 7 lutego 2016 r.

Nie ma więc mowy o „totalnej inwigilacji" tzw. figuranta w wyniku zastosowania kontroli operacyjnej urządzenia końcowego. Jednak w toczącej się dyskusji na temat legalności stosowania takiej kontroli większość argumentów opiera się na emocjach, sympatiach politycznych, czy *quasi*-eksperckich wywodach całkowicie oderwanych od analizy obowiązujących przepisów prawa. Jeśli chodzi o rzeczowe, budujące polemikę, głosy, to można wyodrębnić trzy główne zarzuty mające, zdaniem ich autorów, przemawiać przeciwko dopuszczalności stosowania art. 19 ust. 6 pkt 4 uPol. Twierdzą oni, że omawiana metoda pracy operacyjnej:

- aktywnie oddziałuje na system informatyczny telefonu wprowadzając w nim dowolne zmiany,
- umożliwia generowanie fałszywych dowodów na urządzeniu końcowym,
- system jest nieakredytowany i nie zapewnia „bezpieczeństwa teleinformatycznego" i ochrony informacji niejawnych.

Jeśli chodzi o tezę sformułowaną w pkt 3, to obowiązkiem służby stosującej określone rozwiązanie techniczne jest zagwarantowanie, aby odpowiadało ono zasadom bezpieczeństwa w tym spełniało wymogi określone w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[21], a nadzór nad funkcjonowaniem systemu ochrony takich informacji sprawuje Szef ABW. Realizacja obowiązku ochrony ma charakter praktyczny, a nie teoretyczny, i nie sposób ocenić go *in abstracto* na podstawie wykładni i analizy obowiązujących przepisów prawa, a więc problem ten jest poza analizą niniejszego artykułu. Warto dodać tylko, że prokurator wyrażając zgodę na wystąpienie do sądu z wnioskiem o zarządzenie kontroli operacyjnej, a sąd zarządzając kontrolę, ma prawo sądzić, że jej realizacja będzie zgodna z obowiązującymi przepisami prawa w tym z ustawą o ochronie informacji niejawnych.

Twierdzenie *ex cathedra*, że dane uzyskane w trakcie prowadzenia kontroli operacyjnej urządzenia końcowego są zmanipulowane, stanowi samo w sobie manipulację. Jest rzeczą oczywistą, że każde dane cyfrowe, podobnie, jak inne, tradycyjne ślady kryminalistyczne, są teoretycznie podatne na zmiany. Hipotetycznie można zmanipulować nagranie obrazu i dźwięku dokonane w trakcie pozaprocesowej obserwacji, a na etapie procesu karnego dane znajdujące się w pamięci zabezpieczonego telefonu komórkowego, z którego nie sporządza się przecież kopii binarnej. Jednak nie rezygnuje się *a priori* z tych śladów; wręcz przeciwnie: uzyskuje się na ich podstawie dowody bazując na założeniu, że organy ścigania działają na podstawie i w granicach prawa. Przeciwnicy uzyskiwania cyfrowych artefaktów na podstawie art. 19 ust. 6 pkt 4 uPol zapominają, że taką samą postać binarną mają dane rejestrowane w ramach pozostałych form kontroli operacyjnej, tj. „przechwytywania" rozmów telefonicznych, obrazu lub dźwięku z pomiesz-

[21] Tekst jedn. Dz. U. z 2019 r., poz. 742; z 2022 r., poz. 655, 1933.

czenia, a mimo to z góry nie deprecjonują oni wartości dowodowej tak pozyskanych informacji.

Nie znajduje oparcia w obowiązujących przepisach argument, jakoby kontrola operacyjna mogła być realizowana tylko i wyłącznie za pośrednictwem dostarczyciela usług telekomunikacyjnych lub teleinformatycznych, który udostępni Policji lub służbom swoją infrastrukturę. Otóż, art. 19 ust. 12 i 12a uPol stanowi, że przedsiębiorca telekomunikacyjny oraz usługodawca świadczący usługi drogą elektroniczną zapewniają warunki techniczne i organizacyjne umożliwiające prowadzenie przez Policję kontroli operacyjnej stosownie do posiadanej infrastruktury. *Ratio legis* tego przepisu jest takie, że zobowiązuje on firmę telekomunikacyjną do bezpłatnego udostępnienia organom ścigania swojego zaplecza technologicznego, co ułatwi prowadzenie kontroli operacyjnej, szczególnie rejestrację rozmów telefonicznych. Żaden przepis ustaw kompetencyjnych nie obliguje jednak Policji, Centralnego Biura Antykorupcyjnego, czy Agencji Bezpieczeństwa Wewnętrznego do korzystania przez służbę z takiej infrastruktury w ramach realizacji ustawowych zadań; *a contrario*: Policja, CBA i ABW mają prawo wdrożyć kontrolę operacyjną urządzenia końcowego przy wykorzystaniu własnych narzędzi i urządzeń technicznych.

Jeśli chodzi o wartość dowodową informacji uzyskanych na podstawie omawianej metody „podsłuchu", to ostatecznie niezawisły sąd rozstrzyga samodzielnie zagadnienia faktyczne i prawne budując swoje przekonanie o wartości dowodowej zgromadzonego przez oskarżyciela publicznego materiału na podstawie wszystkich przeprowadzonych dowodów, ocenianych swobodnie z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego. Przepis art. 19 ust. 6 pkt 4 uPol ma moc powszechnie obowiązującego prawa i ustawodawca przewidział odpowiednie mechanizmy jego konstytucyjnej kontroli, których ewentualne uruchomienie leży w gestii uprawnionych podmiotów. Abstrakcyjnej normy prawnej nie można jednak „delegalizować" na podstawie „opinii eksperckich", czy wyroku sądu powszechnego. W tym ostatnim przypadku sąd sprzeciwiłby się fundamentalnej zasadzie demokratycznego państwa prawa, tj. trójpodziału władzy; głosi ona, że prawo ustanawia parlament, a niezawisły sąd stosuje je rozpatrując konkretną sprawę. Sąd ma prawo ocenić, czy ekstrakcja danych nie naruszyła porządku prawnego, czy dane w czasie transmisji nie były modyfikowane, w jaki sposób kontrola wpłynęła na administrowanie telefonem przez prawowitego posiadacza aparatu, czy podjęte przez służbę działania mieściły się w ramach przyznanych jej kompetencji itd. Wymaga to analizy całego materiału dowodowego zgromadzonego w sprawie, a więc nie tylko samych informacji uzyskanych w ramach kontroli operacyjnej, ale także pozostałych dowodów wytworzonych w trakcie czynności operacyjno-rozpoznawczych, i przekazanych do procesu, oraz dowodów uzyskanych na etapie postępowania przygotowawczego. Podstawą wy-

korzystania każdego rodzaju informacji pozyskanych w toku kontroli operacyjnej jest w pierwszej kolejności ustalenie legalności tak pozyskanych informacji[22], co odbywa się *in concreto* na sali sądowej, a nie *in abstracto* w studiu telewizyjnym, czy na łamach gazety.

Patrząc ogólnie na ustawy kompetencyjne, to słuszny jest pogląd zawarty w ekspertyzie prawnej sporządzonej przez naukowców z Katedry Prawa Karnego Uniwersytetu Jagiellońskiego, że „użycie systemów teleinformatycznych, których integralną częścią są programy komputerowe, pozwalające utrwalać, bez wiedzy i zgody użytkownika, prowadzone rozmowy telefoniczne oraz pobierać wiadomości SMS/MMS oraz wiadomości z komunikatorów używanych przez osobę poddaną kontroli operacyjnej, w tym wiadomości wysyłane i otrzymywane przed datą rozpoczęcia kontroli operacyjnej, jest zgodne z przepisami polskiego prawa, pod warunkiem wykorzystania do tego celu akredytowanych przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego programów komputerowych zapewniających bezpieczeństwo informacji niejawnych, których funkcjonalności nie umożliwiają ingerencji w treść danych zgromadzonych w urządzeniu ani udostępniania tych danych osobom trzecim, nieuprawnionym do dostępu do informacji niejawnych”[23]. Trudno w realiach XXI w. zakwestionować dopuszczalność stosowania programu komputerowego pozwalającego na podsłuchiwanie rozmów prowadzonych za pomocą komunikatorów typu Signal czy Whatsapp. Co więcej, nie stoi w sprzeczności z obowiązującymi przepisami uzyskiwanie i utrwalanie obrazu i dźwięku, rejestrowanego przez posiadacza telefonu za pomocą funkcjonalności samego urządzenia końcowego. Dozwolone jest zatem pobranie zdjęcia/filmu/nagrania audio, które wykonał sam jego użytkownik[24]. W zakresie uprawnień służb mieści się także monitorowanie tego, co „figurant” sprawy robi na swym telefonie i pobieranie tych danych, które zostały na niego ściągnięte przez użytkownika inwigilowanego systemu informatycznego[25]. W ramach kontroli operacyjnej urządzenia końcowego można pobierać z tego urządzenia dane dostępowe do innych zasobów informacji (hasła, klucze)[26]. Warto rozważyć natomiast, czy urządzenie takie może być wykorzystane, jako „punkt dostępu” do zasobów chmurowych, jeśli sąd zarządził kontrolę na podstawie art. 19 ust. 6 pkt 4 uPol oraz art. art. 19 ust. 6 pkt 3 uPol i wskazał, że w przypadku „uzyskiwania

[22] Zob. postanowienie Sądu Najwyższego Izba Karna z dnia 5 października 2015 r., sygn. V KK 171/15.

[23] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casusu Pegasusa), Krakowski Instytut Prawa Karnego, data publikacji: 15 lutego 2022 r., s. 1.

[24] Tamże, s. 35–36.

[25] Tamże, s. 37.

[26] Tamże, s. 38.

i utrwalania treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej" chodzi o zindywidualizowany zasób danych umieszczonych na platformie ustalonego administratora. Zdaniem autora działania takie są zabronione w stosunku do serwerów zlokalizowanych poza granicami Polski, bo wtedy aktywność Policji naruszyłaby jurysdykcję miejscową obcego państwa. Jeśli wziąć pod uwagę serwery zlokalizowane w kraju, to opisane działanie teoretycznie byłoby możliwe, gdyby nie modyfikowało danych zawartych w telefonie (pasywna aktywność służb), co w praktyce wydaje się trudne do wykonania.

4. „Środki techniczne" realizacji kontroli operacyjnej

Termin „środki techniczne", w aspekcie stosowania przepisów o kontroli operacyjnej, jest różnie rozumiany. Potwierdziły to ustalenia Trybunału Konstytucyjnego zawarte w fundamentalnym rozstrzygnięciu dla kształtowania się przepisów o kontroli operacyjnej w Polsce, tj. wyroku z dnia 30 lipca 2014 r. (sygn. K 23/11)[27]. Trybunał wskazał, że brak jest legalnej definicji „środków technicznych" i różna była praktyka oznaczania ich we wnioskach o zarządzenie kontroli operacyjnej i postanowieniach sądu. „Co do zasady – ustalił Trybunał – sądy nie określają w postanowieniu o zarządzeniu kontroli operacyjnej rodzaju środka technicznego, jaki w danej sprawie ma być zastosowany. Jedynie z odpowiedzi Prezesa Sądu Okręgowego w Poznaniu oraz Prezesa Sądu Okręgowego w Rzeszowie wynika, że określały one rodzaj środka technicznego. Jak wskazał Prezes Sądu Okręgowego w Poznaniu, w sądzie tym określa się rodzaj środka przez wskazanie, że kontrola operacyjna ma polegać na przykład na podsłuchu telefonu komórkowego wraz z sms o wskazanym numerze bądź numerze IMEI, podsłuchu telefonu stacjonarnego o wskazanym numerze, podsłuchu konkretnego pomieszczenia, kontroli korespondencji internetowej wskazanego adresu e–mail"[28]. TK zauważył ponadto, że z przeprowadzonej analizy repertoriów i akt zakończonych spraw sądowych nie wynikało, że istnieje utrwalona linia orzecznicza dotycząca rozumienia wyrażeń zawartych w przepisach regulujących przesłanki zarządzenia kontroli operacyjne. Wyniki analizy akt spraw sądowych nie potwierdziły również tezy, jakoby Sąd Okręgowy w Warszawie określał w postanowieniu rodzaj środka technicznego, który ma być stosowany w konkretnej sprawie. Środek ten wskazywany był generalnie we wnioskach kierowanych do sądu przez szefów poszczególnych służb[29].

[27] OTK-A 2014, nr 7, poz. 80.
[28] Tamże.
[29] Tamże.

Porządkując znaczenie terminologiczne zwrotów stosowanych przy opisie kontroli operacyjnej, doprecyzować zatem należy pojęcia: „metoda" i „forma" pracy operacyjnej oraz „środek techniczny" i „narzędzia" wykorzystywane w kontroli. Uporządkowanie takie ma duże znaczenie dla jasnego oddzielenia od siebie poszczególnych instytucji prawnych. Faktem jest natomiast, że autorzy opracowań naukowych i sądy zamiennie używają słów: „metoda", „forma" i „środek techniczny" dla określenia poszczególnych aspektów pracy operacyjnej.

Czynności operacyjno-rozpoznawcze realizowane są w ramach form pracy operacyjnej przy wykorzystaniu określonych metod i środków. Forma pracy operacyjnej to procedura obejmująca gromadzenie informacji oraz weryfikację działalności noszącej znamiona czynu zabronionego. Formy pracy operacyjnej mogą odnosić się do podmiotu (osoby, środowiska osób, nieznanego sprawcy przestępstwa) lub przedmiotu (obiektu, miejsca, budynku, zjawiska). Do form pracy operacyjnej należy zaliczyć: sprawdzenie, rozpoznanie, rozpracowanie, poszukiwanie[30].

Metody pracy operacyjnej natomiast, to zespół powiązanych ze sobą jawnych i niejawnych przedsięwzięć oraz działań zastosowanych w sposób mający doprowadzić do osiągnięcia wyznaczonego celu lub wykonania określonego zadania. Większość stosowanych w pracy operacyjnej metod jest znana, stosowana i nazwana; chodzi m.in. o współpracę z osobowym źródłem informacji, przedsięwzięcie werbunkowe, kombinację operacyjną, operację specjalną, działania maskujące, kontrolę operacyjną, zakup kontrolowany, kontrolowane wręczenie lub przyjęcie korzyści majątkowej, przesyłkę niejawnie nadzorowaną, obserwację, wywiad operacyjny, zasadzkę i analizę kryminalną[31]. W pracy służb funkcjonują, a komentowane są w piśmiennictwie prawniczym, ogólne zasady prowadzenia tego typu działań chociaż postęp nauk technicznych powoduje, że ciągle tworzone są nowe metody prowadzenia czynności operacyjnych. Metoda zatem, to istota działania prowadząca do osiągnięcia zamierzonego celu, tj. zgromadzenia informacji w sposób określony w pkt 1–5 artykułu 19 ustawy o Policji.

Innym pojęciem, stosowanym zamiennie z terminem „metody", jest „technika". Rozróżnienie pomiędzy nimi polega na tym, że dopiero metoda charakteryzująca się wysokim stopniem uszczegółowienia staje się techniką[32]. Do realizacji jednej z metod prowadzenia kontroli operacyjnej służą środki techniczne, których działanie polega najczęściej na przekazywaniu informacji na odległość; zatem chodzi o smartfon, telefon stacjonarny, laptop, kamerę monito-

[30] Zob. Projekt ustawy z 2008 r. o czynnościach operacyjno-rozpoznawczych, http://orka.sejm.gov.pl/proc6.nsf/projekty/353_p.htm, data odczytu: 25 lutego 2023 r.
[31] Tamże.
[32] Z. M a r t y n i a k, Metody organizacji i zarządzania, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków 1999, s. 23.

ringu wizyjnego, faks, drukarkę czy serwer. Urządzenia takie zawierają dane cyfrowe statuujące informacje, które dostarczają organom ścigania wiedzy (komunikatów) na temat podmiotu objętego kontrolą operacyjną.

W takim znaczeniu termin „środki techniczne" został użyty w § 3 ust. 1 pkt 2 rozporządzenia Ministra Sprawiedliwości z dnia 13 lutego 2017 r. w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi[33], który obliguje prokuratora do analizy i oceny wniosku o zarządzenie kontroli operacyjnej także pod kątem dopuszczalność stosowania środków technicznych. Regulacja ta zakotwiczona jest w art. 57 § 2 ustawy z dnia 28 stycznia 2016 r. Prawo o prokuraturze[34], zgodnie z którym Prokurator Generalny, Prokurator Krajowy lub upoważniony przez nich prokurator sprawuje kontrolę nad czynnościami operacyjno-rozpoznawczymi poprzez wgląd w materiały zgromadzone w toku kontroli operacyjnej w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych. Z kolei art. 36 § 4 Prawa o prokuraturze stanowi ustawową delegację dla Ministra Sprawiedliwości do określenia, w drodze rozporządzenia, sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi określonymi w art. 57 § 2, mając w szczególności na uwadze zapewnienie merytorycznej i efektywnej kontroli podstaw faktycznych wnioskowanych czynności, zapewnienie legalności i prawidłowości inicjowania i przeprowadzania tych czynności oraz konieczność poszanowania podstawowych praw i wolności obywatelskich[35].

Zgodnie z § 3 ust. 1 pkt 2 rozporządzenia: „Przed zajęciem stanowiska w przedmiocie wniosku, informacji lub zawiadomienia dokonuje się ich analizy i oceny, uwzględniając w szczególności dopuszczalność stosowania środków technicznych z uwagi na rodzaj, miejsce i sposób ich wykorzystania". Zakres przedmiotowy tego obowiązku wyznacza § 1 stanowiąc, że rozporządzenie określa sposób realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi w stosunku do Policji i wszystkich służb uprawnionych do stosowania kontroli operacyjnej, o których mowa w przepisach:

1) art. 19, art. 19a oraz art. 19b ustawy z dnia 6 kwietnia 1990 r. o Policji,
2) art. 11n i 11o ustawy z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych,
3) art. 9e, art. 9f oraz art. 9g ustawy z dnia 12 października 1990 r. o Straży Granicznej

[33] Dz. U. z 2017 r., poz. 292.
[34] Tekst jedn. Dz. U. z 2022 r., poz. 1247, 1259, 2582, z 2023 r., poz. 240.
[35] Szczegółową analizę zakresu kontroli zawiera artykuł: A. Tomaszuk, D. Piekarski, P. Opitek, Nadzór prokuratora nad realizacją kontroli operacyjnej, cz. I, Prokuratura i Prawo 2021, nr 12.

4) art. 118, art. 119 oraz art. 120 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej,
5) art. 31, art. 32 oraz art. 33 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych,
6) art. 27, art. 29 oraz art. 30 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
7) art. 17 oraz art. 19 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym,
8) art. 31, art. 33 oraz art. 34 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
9) art. 42–54 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa,
10) art. 23p, art. 23q oraz art. 23r ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej.

Według art. 19 ust. 7 pkt 4 uPol wniosek organu Policji do sądu o zarządzenie kontroli operacyjnej powinien zawierać w szczególności dane osoby lub inne dane, pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego będzie ona stosowana, ze wskazaniem miejsca lub sposobu stosowania kontroli. Miejsce wskazuje się, jeśli czynności dotyczą rejestracji obrazu lub dźwięku poprzez indywidualizację pokoju hotelowego lub pojazdu samochodowego, w którym będzie zamontowany „podsłuch". Jednak w sytuacjach, gdy ludzie komunikują się ze sobą w cyberprzestrzeni (rozmawiają przez telefon lub komunikator), to wskazanie miejsca działania środka jest niemożliwe. Pozostaje zatem oznaczyć sposób stosowania kontroli, co wiąże się z treścią art. 19 ust. 7 pkt 5 uPol: wniosek organu Policji o zarządzenie przez sąd okręgowy kontroli operacyjnej powinien zawierać w szczególności cel, czas i rodzaj prowadzonej kontroli operacyjnej, o której mowa w ust. 6. Co ważne, art. 19 ust. 7 pkt 5 ustawy o Policji odwołuje się do art. 19 ust. 6 tej ustawy z czego wynika, że dla prawodawcy odpowiedź na pytanie o „rodzaj stosowanej kontroli" zawiera się w metodach kontroli opisanych w art. 19 ust. 6 ustawy o Policji. Poniżej przedstawiono przykładowe sytuacje realizacji kontroli operacyjnej z wyszczególnieniem: celu, czasu i rodzaju prowadzonej kontroli (19 ust. 7 pkt 5 uPol) oraz stosowanego w jej trakcie środka technicznego (§ 3 ust. 1 pkt 2 rozporządzenia).

Przykład nr 1

Komendant Główny Policji wnosi o zarządzenie na okres 3 miesięcy kontroli operacyjnej polegającej na uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych oraz uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej w postaci karty SIM o numerze MSISDN xxx współpracującej z aparatem telefonicznym marki xxx (art. 19 ust. 6 pkt 1 i 3 uPol);

- cel kontroli: uzyskiwanie i utrwalanie treści rozmów oraz uzyskiwanie i utrwalanie treści korespondencji,
- czas kontroli: na okres 3 miesięcy,
- rodzaj prowadzonej kontroli: użycie środków technicznych w tym za pomocą sieci telekomunikacyjnych i środków komunikacji elektronicznej,
- stosowany środek techniczny: karta SIM o numerze MSISDN xxx współpracująca z aparatem telefonicznym (telefonem komórkowym) marki xxx.

Środkiem technicznym jest karta SIM o numerze MSISDN xxx współpracująca z aparatem telefonicznym/telefonem komórkowym; takie określenie zawarte we wniosku o zarządzenie kontroli operacyjnej jest wystarczające, gdyż powszechnie wiadomo, że uzyskiwanie i utrwalanie treści rozmów oraz uzyskiwanie i utrwalanie treści korespondencji może odbywać się poprzez dostęp do sieci telekomunikacyjnych, a ustawa nakłada na dostarczycieli usług telekomunikacyjnych, pocztowych i elektronicznych obowiązek zapewnienia na własny koszt warunków technicznych oraz organizacyjnych umożliwiających prowadzenie kontroli operacyjnej (art. 19 ust. 12 i 12a uPol).

Przykład nr 2

Komendant Główny Policji wnosi o zarządzenie na okres 3 miesięcy kontroli operacyjnej, która polega na uzyskiwaniu i utrwalaniu obrazu i dźwięku osób z pomieszczeń innych niż miejsca publiczne, tj. lokalu xxx za pomocą urządzenia rejestrującego obraz i dźwięk (art. 19 ust. 6 pkt 2 uPol);

- cel kontroli: uzyskanie zapisu audio-video,
- czas kontroli: na okres 3 miesięcy,
- rodzaj prowadzonej kontroli: uzyskiwanie i utrwalanie obrazu i dźwięku,
- stosowany środek techniczny: urządzenie rejestrujące obraz i dźwięk zainstalowane w lokalu xxx.

Środkiem technicznym jest urządzenie rejestrujące obraz i dźwięk zainstalowane w lokalu xxx, które umożliwia uzyskiwanie oraz utrwalanie obrazu i dźwięku (powszechnie wiadomo, że kamera rejestruje obraz i dźwięk).

Przykład nr 3

Komendant Główny Policji wnosi o zarządzenie na okres 3 miesięcy kontroli operacyjnej polegającej na uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych, tj. z aparatu telefonicznego o nr IMEI xxx (art. 19 ust. 6 pkt 4 uPol).

- cel kontroli: uzyskiwanie i utrwalanie danych zawartych w telekomunikacyjnym urządzeniu końcowym,
- czas kontroli: na okres 3 miesięcy,

- rodzaj prowadzonej kontroli: uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych,
- stosowany środek techniczny: aparat telefoniczny o nr IMEI xxx.

Środkiem technicznym jest aparat telefoniczny o nr IMEI xxx (powszechnie wiadomo, że telefon, tj. telekomunikacyjne urządzenie końcowe, ma w swojej pamięci zapisane dane/informacje/materiały, a ponieważ telefon pracuje w trybie *on-line* i łączy się z urządzeniami zewnętrznymi, to można połączyć się zdalnie z telefonem, a następnie utrwalić i uzyskać znajdujące się w jego pamięci dane).

5. „Narzędzia" do realizacji kontroli operacyjnej

W poprzednim rozdziale opisano, jak należy rozumieć termin „środek techniczny" w aspekcie prokuratorskiej kontroli wniosków o zarządzenie kontroli operacyjnej znajdującej umocowanie w art. 36 § 4 i art. 57 § 2 ustawy Prawo o prokuraturze i doprecyzowanej w rozporządzeniu Ministra Sprawiedliwości z dnia 13 lutego 2017 r. w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi. Jednak terminowi „środek techniczny" niekiedy przypisuje się jeszcze inne znaczenie np. programu komputerowego, które sprawia, że konkretna metoda pracy operacyjnej jest efektywna. W tym ujęciu „środek techniczny" odpowiada pojęciu „narzędzie".

Jeśli przepisy określające metody działania operacyjnego muszą spełniać cechę dostatecznej określoności, to wymóg ten nie dotyczy parametrów technicznych narzędzi wykorzystywanych do kontroli operacyjnej[36]. Zdaniem W. Kozielewicza szczegółowe wskazywanie w ustawie o jakie środki techniczne („narzędzia") umożliwiające uzyskiwanie i utrwalanie danych chodzi powodowałoby, że w przepisie należałoby wymienić trudną bliżej do określenia liczbę środków technicznych, która służy do prowadzenia kontroli operacyjnej (np. podsłuch elektroniczny, mikrofon kierunkowy, tzw. konie trojańskie i innego rodzaju komputerowe programy szpiegujące, GPS). Inną rzeczą jest to, pisze wymieniony Autor, czy współczesny stan techniki, m.in. różnorodność niezwykle wyrafinowanych urządzeń umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a także jej dynamiczny rozwój pozwalają, nawet teoretycznie, na stworzenie zamkniętego katalogu środków technicznych dopuszczalnej kontroli operacyj-

[36] Por. A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych…, *op. cit*., s. 30–31.

nej, i czy to byłoby rozwiązanie sensowne[37]. Co istotne, W. Kozielewicz już w 2013 r. dopuszczał możliwość stosowania „komputerowych programów szpiegujących" w tym „trojanów", a więc narzędzi typowych do kontroli końcowych urządzeń informatycznych. Komentując obowiązujący w tym czasie art. 19 ust. 6 pkt 3 uPol[38], W. Kozielewicz stwierdził: „dobrze się stało, iż ustawodawca zezwolił na stosowanie wszelkich dostępnych środków technicznych, umożliwiający uzyskiwanie w sposób niejawny dowodów i informacji oraz ich utrwalanie. Jedynie przykładowo wskazał w tym przepisie, że może tu chodzić o takie środki techniczne, które pozwalają na uzyskiwanie i utrwalanie treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych"[39]. Warto dodać, że propozycję definicji kontroli operacyjnej ukierunkowanej na „urządzenie końcowe" przedstawił zespół ds. zmian legislacyjnych wynikających ze wspomnianego wyroku TK z dnia 30 lipca 2014 r., powołany decyzją przewodniczącego Kolegium do spraw Służb Specjalnych (prezesa Rady Ministrów) z dnia 8 października 2014 r.[40]

Pojawiają się błędne zapatrywania prawne na temat możliwości posiadania przez służby narzędzi do przełamywania zabezpieczeń. W jednej z opinii zrównano instytucję pozyskiwania programów komputerowych przez ABW do realizacji oceny bezpieczeństwa systemów teleinformatycznych (art. 32a uABW) z możliwością użycia takich programów w celu realizacji kontroli operacyjnej. Autorzy opinii sformułowali pogląd, że art. 32a uABW stanowi wyłączną podstawę prawną do nabywana i wykorzystywania takich programów przez ABW zapominając, że opisana w nim procedura należy do wyłącznej kompetencji Szefa ABW i dotyczy zupełnie innych działań, aniżeli kontrola

[37] W. Kozielewicz, Środek techniczny umożliwiający uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie – kilka uwag o wykładni art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji, (w:) A. R. Pach, Z. Rau, M. Wągrowski (red.), Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa. Szanse i zagrożenia, Wydawnictwo Wolters Kluwer Polska, Warszawa 2013, s. 945–946.

[38] „Kontrola operacyjna prowadzona jest niejawnie i polega na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych".

[39] W. Kozielewicz, „Środek techniczny umożliwiający uzyskiwanie w sposób niejawny informacji i dowodów…, *op. cit*. s. 945. Podobnie A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek zwrócili uwagę, że zmieniającą się wciąż rzeczywistość technologiczna i rozszerzanie możliwości technicznych ingerowania w prawa i wolności obywatelskie powoduje, że nie sposób sformułować w ustawie środków technicznych służących do realizacji kontroli operacyjnej, a próby takie, wbrew intencji ustawodawcy, rodziłyby ryzyko niekontrolowanego, samoczynnego rozszerzania się zakresu zastosowania norm prawnych, (w:) A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych…, s. 31.

[40] P. Opitek, Poważnie kontrolować można nie tylko terrorystów, Rzeczpospolita z dnia 20 stycznia 2022 r.

operacyjna zarządzana przez sąd. Gdyby pójść tropem Autorów opinii, to przepis szczególny ustawy o ABW powinien wymieniać środek techniczny w postaci przełamania zabezpieczenia pojazdu po to, aby sąd mógł zarządzić rejestrację obrazu i dźwięku w samochodzie (art. 19 ust. 6 pkt 2 uPol). Poza tym art. 269b § 1 k.k. mówi o pozyskiwaniu programów komputerowych „umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym", a przecież zarządzenie przez sąd kontroli, a więc udzielenie służbie zgody na dostęp do danych, nie można nazwać „nieuprawnionym dostępem"[41].

Trybunał Konstytucyjny zauważył natomiast, że narzędzie musi posiadać dwojakiego rodzaju właściwości:

1) po pierwsze, ma mieć charakter techniczny, czyli być w jakiś sposób oparte na nowych technologiach,
2) po drugie – powinno pozwalać nie tylko pozyskiwać informacje, ale równocześnie je utrwalać[42].

Kolejną cechę narzędzi wykorzystywanych do kontroli operacyjnej stanowi ich tajny charakter w rozumieniu ustawy o ochronie informacji niejawnych (dalej: u.o.i.n.). Zakres przedmiotowy i podmiotowy wspomnianej ustawy zawiera się w treści art. 1 u.o.i.n.; określa on zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie opracowywania informacji oraz niezależnie od formy i sposobu ich wyrażania; chodzi m.in. o zasadę klasyfikowania informacji niejawnych oraz organizowania ochrony takich informacji (art. 1 ust. 1 u.o.i.n.).

Skoro definicję materialną pojęcia „informacje niejawne" zawiera art. 1 ust. 1 u.o.i.n., to dla ustalenia jego zakresu nie trzeba odwoływać się do art. 5 u.o.i.n., albowiem poszczególne przepisy tego artykułu nie tworzą dodatkowej definicji terminu „informacje niejawne", lecz stanowią szczegółowe rozwinięcie pojęcia zdefiniowanego w art. 1 ust. 1 u.o.i.n., służące celom odpowiedniego zakwalifikowania w zakresie stopnia ochrony tychże informacji, a nie samej potrzeby ich ochrony[43]. Przesłanki materialne oznaczenia informacji niejawnych poprzez nadawanie im klauzuli tajności zostały określone w art. 5: ust. 1 (klauzula „ściśle tajne"), ust. 2 (klauzula „tajne"), ust. 3 (klauzula „poufne") i ust. 4 (klauzula „zastrzeżone"). Wykładnia językowa użytego w ustawie zwrotu „informacjom niejawnym nadaje się klauzulę (…), jeżeli ich nieuprawnione ujawnienie spowoduje (…)" oznacza, że fakt, czy

[41] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych…, *op. cit*., s. 15–16.

[42] Uzasadnienie do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11.

[43] Uzasadnienie do wyroku Naczelnego Sądu Administracyjnego z dnia 25 kwietnia 2019 r., sygn. I OSK 2344/18, LEX nr 2677192.

informacja ma charakter niejawny nie zależy od tego, czy została opatrzona klauzulą tajności; klauzula taka ma natomiast za zadanie zapewnić określonej informacji wzmożoną ochronę[44]. Co ważne, dla ochrony przewidzianej w przepisach ustawy o ochronie informacji niejawnych istotne jest bowiem to, że istnieje już sama możliwość zagrożenia dóbr, czy też powstania określonej szkody, co dotyczy również czynności operacyjno-rozpoznawczych, które mogą być prowadzone w przyszłości[45].

Jeśli chodzi o zakres podmiotowy ustawy o ochronie informacji niejawnych, to jej przepisy mają zastosowanie do organów administracji rządowej, a centralnym organem administracji rządowej, właściwym w sprawach ochrony bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa i porządku publicznego, jest m.in. Komendant Główny Policji, podległy ministrowi właściwemu do spraw wewnętrznych (art. 5 ust. 2 pkt c uPol). Ustawę stosuje się także do jednostek organizacyjnych podległych organom władzy publicznej (art. 5 ust. 2 pkt 5 uPol), a więc Komendanta Centralnego Biura Śledczego Policji (art. 5a ust. 2 uPol), Komendanta Biura Spraw Wewnętrznych Policji (art. 5a ust. 2 uPol) i Komendanta Centralnego Biura Zwalczania Cyberprzestępczości (art. 5d ust. 2 uPol), jako organom Policji podległym Komendantowi Głównemu Policji. Zakres podmiotowy ustawy stanowi ponadto, że jej przepisy mają zastosowanie do jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy (art. 1 ust. 2 u pkt 2 u.o.i.n.). Zgodnie z art. 6 ust. 1 pkt 1–3 uPol organami administracji rządowej na obszarze województwa w sprawach ochrony bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa i porządku publicznego jest komendant wojewódzki Policji działający w imieniu własnym w określonych sprawach (m.in. wykonywania czynności operacyjno-rozpoznawczych i dochodzeniowo–śledczych), komendant powiatowy (miejski) Policji i komendant

[44] Pogląd taki został ugruntowany w orzecznictwie Naczelnego Sądu Administracyjnego i doktrynie prawniczej. „Dla zakwalifikowania danej informacji do informacji niejawnej, wystarczy element materialny, tzn. istnienie takiej jej cechy, poprzez którą to stanowi ona informację, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczpospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie jej opracowywania oraz niezależnie od formy i sposobu jej wyrażania (art. 1 ust. 1 u.o.i.n.). Informacja niejawna chroniona jest zatem bez względu na to, czy osoba uprawniona uznała za stosowne oznaczyć ją odpowiednia klauzulą. Jest ona bowiem niejawna z uwagi na zagrożenia wynikające z jej treści lub sposobu jej uzyskania, a nie w następstwie klasyfikacji" (w:) uzasadnienie do wyroku z dnia 25 kwietnia 2019 r. Naczelnego Sądu Administracyjnego, sygn. I OSK 2344/18, LEX nr 2677192; podobnie: wyrok Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., sygn. I OSK 668/16, LEX nr 2475548, wyrok Naczelnego Sądu Administracyjnego z dnia 21 września 2012 r., sygn. I OSK 1393/12, ONSA-iWSA 2013, nr 6, poz. 108; zob. też: T. S z e w c, Ochrona informacji niejawnych. Komentarz, Warszawa 2007, s. 115–117.

[45] Stanowisko Szefa CBA przytoczone w wyroku Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., sygn. I OSK 668/16, LEX nr 2475548.

komisariatu Policji. Zakres podmiotowy ustawy o ochronie informacji niejawnych obejmuje także pozostałe organy, które występują z wnioskiem o zastosowanie kontroli operacyjnej; np. w przypadku Szefa Centralnego Biura Antykorupcyjnego art. 5 ust. 2 uCBA stanowi, że jest on centralnym organem administracji rządowej.

Obowiązek „utajnienia" narzędzi stosowanych do realizacji kontroli operacyjnej przez Centralne Biuro Antykorupcyjne wynika wprost z art. 24 ust. 1 uCBA; przepis brzmi następująco: „W związku z wykonywaniem swoich zadań CBA zapewnia ochronę środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy CBA"[46]. Dlatego w sprawie rozpoznawanej przez Naczelny Sąd Administracyjny i dotyczącej skargi jednej z Fundacji na Szefa Centralnego Biura Antykorupcyjnego o nieudzieleniu informacji w ramach dostępu do informacji publicznej, Szef CBA wskazał, że ochronie przewidzianej dla informacji niejawnych podlegają wszystkie informacje, których ujawnienie utrudni wykonywanie służbom ich zadań, w tym wykonywanie czynności operacyjno-rozpoznawczych bez względu na to, czy dotyczą one konkretnych postępowań. Informacja o technicznych możliwościach CBA, tj. o posiadaniu narzędzi do automatycznej lub półautomatycznej analizy danych telekomunikacyjnych, danych o lokalizacji osób lub urządzeń za pomocą informacji o logowaniach do stacji BTS, czy też narzędzi, których przeznaczeniem jest automatyczne lub półautomatyczne przeszukiwanie zasobów sieci Internet pod kątem zdefiniowanych słów kluczowych, jak również bezzałogowych statków powietrznych (dronów) i innych narzędzi jest – zdaniem Szefa CBA – szczegółową informacją dotyczącą organizacji, form i metod pracy operacyjnej służby i podlega zasadom ochrony informacji niejawnych[47]. Sąd przychylił się do tak sformułowanego stanowiska i stwierdził, że bez wątpienia skierowane do CBA pytania dotyczyły możliwości technicznych, jakimi dysponuje ta służba, gdyż odnosiły się do narzędzi (urządzeń i oprogramowania) i do bezzałogowych statków powietrznych, które są ewentualnie wykorzystywane przez CBA. Udzielenie informacji w tym zakresie przyczyniłoby się niewątpliwie do ujawnienia poziomu zaawansowania organizacyjnego, technicznego czy innowacyjności stosowanych metod, form czy środków pracy operacyjnej. Wskazane urządzenia mogą być bowiem ponad wszelką wątpliwość wykorzystywane w pracy operacyjnej wykonywanej przez agentów tej służby.

[46] Podobne regulacje zawierają pozostałe ustawy kompetencyjne służb przewidujące procedurę realizacji kontroli operacyjnej; chodzi m.in. o art. 20a ust. 1 ustawy o Policji, art. 35 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego, art. 9c ust. 1 ustawy o Straży Granicznej, art. 131 ust. 1 ustawy o Krajowej Administracji Skarbowej, art. 40 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

[47] Stanowisko Szefa CBA przytoczone w wyroku Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., sygn. I OSK 668/16, LEX nr 2475548.

To zaś spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, co pozwala uznać takie informacje za podlegające reżimowi przewidzianemu dla ochrony informacji niejawnych, bez względu na to, czy nadano im klauzulę tajności. Udostępnienie tych informacji byłoby zagrożeniem realnym, stanowiącym możliwość wyrządzenia określonej w ustawie o ochronie informacji niejawnych szkody[48]. Stanowisko Sądu I instancji podtrzymał Naczelny Sąd Administracyjny stwierdzając m.in., że chociaż działalność służb specjalnych podlega społecznej kontroli, to tylko w obszarach, które nie ograniczają możliwości skutecznej realizacji ich zadań i nie dotyczą konkretnych prowadzonych postępowań oraz stosowanych w nich metod operacyjnych[49].

Podsumowując stwierdzić należy, że o ile ustawa o ochronie informacji niejawnych zakazuje ujawnienia narzędzi służących do realizacji metod pracy operacyjnej osobom nieuprawnionym, to art. 24 ust. 1 uCBA stanowi zabezpieczenie jeszcze dale idące, gdyż uzależnia ujawnienie „środków, form i metod realizacji zadań" przez Biuro od decyzji Szefa CBA. Mowa bowiem o tzw. kuchni pracy służb, najbardziej strzeżonych „technikaliach", które muszą być zgodne z zarządzoną przez sąd, i znaną sądowi, metodą realizacji konkretnej kontroli operacyjnej, ale niekoniecznie opisywane we wniosku o zarządzenie kontroli.

Nie sposób zatem zgodzić się ze stanowiskiem D. Szumiło-Kulczyckiej; Autorka postuluje, aby postanowienie sądu o zarządzeniu kontroli operacyjnej zawierało m.in. „wskazanie jaki rodzaj środków technicznych lub typu oprogramowania, jakie może być stosowane podczas realizacji danej kontroli operacyjnej"[50]. Zdaniem D. Szumiło-Kulczyckiej brak takiego wskazania powoduje, że „w konsekwencji sądy nie są często świadome rodzaju używanego ostatecznie przez służby środka technicznego lub oprogramowania, ani możliwości jakie on służbom w rzeczywistości daje"[51]. W podobnym duchu wypowiadają się A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek twierdząc, że sąd musi wejść w posiadanie wszelkich informacji pozwalających miarodajnie ustalić, jak działa instrument, na użycie którego ma wyrazić zgodę. Bezpodstawne jest przy tym stanowisko, że opi-

[48] Uzasadnienie do wyroku Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., sygn. I OSK 668/16, LEX nr 2475548.

[49] Uzasadnienie do wyroku Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., sygn. I OSK 668/16, LEX nr 2475548.; podobnie: wyrok NSA z dnia 28 kwietnia 2016 r., sygn. I OSK 2620/14. Szczególne regulacje dotyczącą udzielania informacji o czynnościach operacyjnych dotyczą sytuacji wyjątkowych, związanych np. z popełnieniem przestępstwa (zob. m.in. art. 20b ust. 1 i 3 uPol), ale ich treść nie wiąże się bezpośrednio w przedmiotem artykułu.

[50] D. Szumiło-Kulczycka, Opinia sporządzona na zlecenie Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz Reformy Służb Specjalnych, Kraków 26 sierpnia 2022 r., s. 7.

[51] Tamże, s. 6.

sane informacje nie muszą być przekazane sądowi z powodu konieczności ochrony przez służby informacji o używanych przez nie środkach technicznych i metodach ich pracy operacyjnej, ponieważ dostateczną ochronę wskazanych informacji zapewnia „oklauzulowanie" wniosku o zastosowanie kontroli operacyjnej, zaś samo postępowanie w przedmiocie jego rozpoznania toczy się przy zachowaniu rygorów przewidzianych dla przetwarzania informacji niejawnych. Co więcej – piszą dalej przywołani Autorzy – jeśli materiał zgromadzony w toku kontroli zostanie procesowo wykorzystany w postępowaniu karnym, wówczas i tak będzie możliwe ustalenie formy przeprowadzenia konkretnych czynności operacyjno-rozpoznawczych[52].

Oczywistym jest, że zarówno sąd rozpatrujący wniosek o zarządzenie kontroli operacyjne, jak i strony postępowania karnego, jeśli materiały z „podsłuchu" trafią do procesu, poznają „formę przeprowadzenia konkretnych czynności operacyjno-rozpoznawczych" w tym znaczeniu, że we wniosku musi znaleźć się literalny zapis któreś z metod ujętych w art. 19 ust. 6 pkt 1–5 uPol. Metoda wskazuje wprost, jak uzyskano dane bez konieczności precyzowania użytego narzędzia np. zastosowanego programu komputerowego. Nie do końca wiadomo zresztą na czym miałoby polegać zamieszczenie we wniosku „wszelkich informacji pozwalających miarodajnie ustalić, jak działa instrument". Na oznaczeniu nazwy oprogramowania? Sama nazwa nie mówi przecież, jak funkcjonuje program komputerowy, więc należałoby opisać szczegółowo algorytmy wykorzystywane przez narzędzie, jak procesor wykonuje instrukcje programu. Otóż, wbrew pozorom, takie szczegółowe zapisy nakładałyby na sąd, ale także na prokuratora, obowiązek posiadania wiadomości specjalnych z zakresu informatyki i w konsekwencji nie ułatwiały oceny podstaw faktycznych i prawnych wniosku, ale czyniły ją iluzoryczną. Jeśli Policja lub służba wnioskuje o zarządzenie kontroli operacyjnej polegającej na „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych" to wynika z tego jednoznacznie, że chodzi o dane informatyczne znajdujące się wewnątrz urządzenia, że ich akwizycja ma charakter pasywny (służba nie może kreować nowego, merytorycznego co do treści, zapisu lub zmieniać istniejącego), a kontrola nie dotyczy rejestracji obrazu lub dźwięku za pomocą kamery i mikrofonu zamontowanych w telefonie. Na sądzie nie ciąży obowiązek badania, a nawet nie posiada do tego kompetencji, czy rzeczywiście program komputerowy będzie funkcjonował z zachowaniem wymienionych rygorów, bo to wynika z opisanej metody pozyskiwania danych. Jeśli sędzia stwierdzi jednak, że chciałby uzyskać więcej informacji o wskazanej we wniosku metodzie kontroli, ma prawo wyznaczyć posiedzenie

[52] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych…, s. 42.

i przesłuchać funkcjonariusza Policji, czy Centralnego Biura Antykorupcyjnego na okoliczności sprawy.

Szczegółowa charakterystyka narzędzi pracy operacyjnej (w uzasadnieniu wniosku, a następnie postanowieniu sądu), oprócz tego, że jest niecelowa, to groziłaby ujawnieniem techniki stosowanej do realizacji czynności operacyjno-rozpoznawczych. Nie ma znaczenia, że wniosek o zarządzenie kontroli operacyjnej jest „oklauzulowany", bo i tak podejrzany i jego obrońca mają prawo zapoznać się z nim najdalej w trakcie końcowego zaznajomienia z materiałami postępowania przygotowawczego. Co więcej, autorowi znana jest praktyka, kiedy sądy wydają zgody na zdjęcie klauzuli z postanowienia o zarządzeniu kontroli operacyjnej bez konsultacji z wytwórcą wniosku. Wynika z tego, że umieszczenie w dokumentach, dotyczących zarządzenia kontroli, informacji o narzędziach stosowanych np. przez Centralne Biuro Antykorupcyjne groziłoby ujawnieniem tych narzędzi i w konsekwencji brakiem faktycznych możliwości realizacji przez CBA ustawowego obowiązku wynikającego z art. 24 ust. 1 uCBA, a co za tym idzie, demontażem tej służby. W tym kontekście warto przywołać stanowisko rządu Belgi, który na zapytanie jednej z komisji Parlamentu Europejskiego, czy tamtejsze służby używają programów szpiegujących, odpowiedział, że nie będzie informować o jakichkolwiek środkach technicznych użytkowanych przez belgijską policję[53]. Jak słusznie stwierdził były szef Służby Kontrwywiadu Wojskowego: „Przeciwnik – zawsze mówimy o jakimś przeciwniku, czy to jest przestępca, czy to jest obcy wywiad – powinien mieć jak najmniejszą wiedzę o naszych możliwościach technicznych"[54].

6. Podsumowanie

Kontrola operacyjna urządzenia końcowego, jako metoda pracy operacyjnej, przewidziana jest w każdej z dziesięciu ustaw dopuszczających stosowanie takiej kontroli. Treść zapisu: „uzyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych" pozwala na uzyskiwanie i utrwalanie tylko i wyłącznie danych zapisanych w urządzeniu, a nie obrazu i dźwięku z otoczenia telefonu. Nie należy zatem łączyć stosowania urządzenia końcowego na telefon z funkcjonalnością zdalnego włączenia mikrofonu i kamery tego telefonu. Co do zasady nie do-

[53] DRAFT REPORT of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)), data odczytu: 25 lutego 2023 r.

[54] Wypowiedź P. Pytla, Szefa Służby Kontrwywiadu Wojskowego w latach 2014–2015, z posiedzenia Komisji Nadzwyczajnej X kadencji Senatu RP do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczpospolitej Polskiej oraz reformy służb specjalnych, zapis stenograficzny, Warszawa 2022.

tyczy także danych umieszczonych w chmurze, z którymi aparat łączy się. Kontrola taka musi być prowadzona pasywnie, tj. nie modyfikować pierwotnej treści informacji, a więc zapisu stanowiącego merytoryczną treść, znajdujących się w pamięci urządzenia końcowego. Ponadto „brak podstaw, by wykluczyć dopuszczalność pozyskiwania danych z pamięci urządzenia, które zostały wytworzone przed datą postanowienia sądowego o udzieleniu zgody na stosowanie kontroli operacyjnej”[55].

Kontrolę zarządza sąd posiadając sprecyzowaną informację o osobie, wobec której kontrola ma być stosowana oraz literalnie przytoczone brzmienie metody kontroli wraz z przywołaniem jej podstawy prawnej i indywidualizacją urządzenia (środka technicznego), którego kontrola będzie dotyczyć. Trybunał Konstytucyjny uznał za wystarczające dla urzeczywistnienia gwarancji konstytucyjnych przyjęcie takiej wykładni przepisów, że organ zarządzający kontrolę operacyjną jest obowiązany do zindywidualizowania w każdej sprawie środka technicznego, jaki ma być stosowany. Z punktu widzenia wymagań konstytucyjnych dopuszczalne jest zastosowanie tylko takiego środka, który przewidziany został przez prawo i może być stosowany przez organ wnoszący o zarządzenie kontroli operacyjnej[56].

Nie jest zatem realne, aby wniosek o zastosowanie kontroli operacyjnej mógł zostać w jakikolwiek sposób „zanonimizowany”. Brak bowiem elementów konstrukcyjnych wniosku powodowałby negatywną decyzję sądu w przedmiocie zarządzenia kontroli operacyjnej, a wcześniej brak zgody prokuratora na wystąpienie z wnioskiem. Przed podjęciem decyzji w sprawie sąd ma obowiązek zapoznać się z materiałami uzasadniającymi potrzebę zastosowania kontroli operacyjnej, może żądać od wnioskodawcy uzupełnienia tych materiałów, a także wyznaczyć posiedzenie niejawne i przesłuchać funkcjonariusza służby, co do szczegółów realizacji planowanej kontroli. Prawo nakazuje więc przedłożenie przez wnioskodawcę takich materiałów, po lekturze których wszystkie organy uczestniczące w procedurze zarządzania kontroli operacyjnej będą w stanie dokonać formalnej i merytorycznej oceny tak w zakresie występowania przesłanek formalnych, jak i materialnych dopuszczalności zastosowania omawianej metody[57]. We wniosku o zarządzenie kontroli nie umieszcza się natomiast szczegółowych informacji o narzędziach, które mają posłużyć do wdrożenia kontroli, ponieważ metoda jednoznacznie wskazuje, jak będą gromadzone dane, a sąd nie musi oceniać szczegółów działania nowoczesnych

[55] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych…, *op. cit*., s. 38.

[56] Uzasadnienie do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11.

[57] T. Łodziana, Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika, Palestra 2022, nr 9, https://palestra.pl, data odczytu: 25 lutego 2023 r.

rozwiązań teleinformatycznych. Jeśli informacje uzyskane w trakcie realizacji kontroli zostaną wykorzystane w postępowaniu karnym, to ocena, czy dana forma pracy operacyjnej była zgodna z prawem, następuje *in concreto*, tj. na podstawie okoliczności faktycznych konkretnej sprawy. Trybunał Konstytucyjny podkreślił, że ustrojowa pozycja sądów, jako organów niezależnych od władzy wykonawczej oraz postawionych na straży konstytucyjnych wolności i praw podmiotowych (art. 10, art. 77 ust. 2 Konstytucji) predestynuje je do przeprowadzania kompleksowej oceny wniosków o zarządzenie kontroli operacyjnej[58].

Jeżeliby w konkretnych sprawach zgody na prowadzenie kontroli w formie „uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych" wydawałyby sądy w tym m.in. Sąd Okręgowy w Warszawie, Wojskowy Sąd Okręgowy w Warszawie, Sąd Apelacyjny w Warszawie lub Sąd Najwyższy, to wtedy decyzje w tym zakresie podejmowaliby sędziowie z ogromną wiedzą i nietuzinkowym doświadczeniem zawodowym. Co ważne, we wniosku o przedłużenie stosowania kontroli operacyjnej przytacza się wprost lub opisuje informacje uzyskane z urządzenia końcowego, a więc sąd rozpatrujący taki wniosek miałby świadomość, skąd pochodzą informacje oraz jak zostały uzyskane. Zatem sugestie, że sędzia zarządzający, przedłużający lub wyrażający zgodę na kontynuację kontroli nie wiedziałby, jakiej metody ona dotyczy, godzą w powagę urzędu sędziowskiego, tym bardziej, że sędzia ma ustawowy obowiązek zapoznania się z materiałami zgromadzonymi w toku prowadzonej kontroli[59].

Kontrola operacyjna urządzenia końcowego *in abstracto* nie jest ani mniej, ani bardziej ofensywnym środkiem uzyskiwania danych w trakcie działań pozaprocesowych, aniżeli przechwytywanie treści rozmów telefonicznych, czy zawartości skrzynki e–mail. Z raportu Komisji Śledczej Parlamentu Europejskiego ds. Pegasusa[60] wynika, że zaawansowane narzędzia hakerskie do kontroli operacyjnej urządzeń końcowych posiadają niemal wszystkie kraje Unii Europejskiej w tym Niemcy, Francja, Holandia czy Hiszpania. Narzędzia takie stosowane są także w Stanach Zjednoczonych Ameryki[61]. Dzisiaj bowiem nie sposób walczyć z poważną przestępczością zorganizowaną, korupcją na najwyższych szczeblach instytucjonalnych,

[58] Uzasadnienie do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11.

[59] P. O p i t e k, Poważnie kontrolować można nie tylko terrorystów, Rzeczpospolita z dnia 20 stycznia 2022 r.

[60] DRAFT REPORT of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, *op. cit*.

[61] Wiretap Report 2021, United States Courts, https://www.uscourts.gov/statistics–reports/wiretap–report–2021, data odczytu: 25 lutego 2023 r.

czy praniem pieniędzy bez kontroli operacyjnej opartej na zaawansowanych narzędziach teleinformatycznych.

Bibliografia

Literatura

1. Grabowski M., Zając A., Dane, informacja, wiedza – próba definicji, Zeszyty Naukowe. Uniwersytet Ekonomiczny w Krakowie 2009, nr 798.
2. Kozielewicz W., Środek techniczny umożliwiający uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie – kilka uwag o wykładni art. 19 ust. 6 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji, (w:) A. R. Pach, Z. Rau, M. Wągrowski (red.), Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa. Szanse i zagrożenia, Wydawnictwo Wolters Kluwer Polska, Warszawa 2013.
3. Kwiatek B., Nośnik dokumentu elektronicznego, (w:) Dokument elektroniczny w ogólnym postępowaniu administracyjnym, WKP 2020, LEX.
4. Łodziana T., Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika,
5. Martyniak Z., Metody organizacji i zarządzania, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków 1999.
6. Palestra 2022, nr 9, https://palestra.pl, data odczytu: 25 lutego 2023 r.
7. Opitek, Nadzór prokuratora nad realizacją kontroli operacyjnej, cz. I, Prokuratura i Prawo 2021, nr 12.
8. Opitek P., Poważnie kontrolować można nie tylko terrorystów, Rzeczpospolita z dnia 20 stycznia 2022 r.
9. Radoniewicz F., Odpowiedzialność karna za przestępstwo hackingu, Prawo w Działaniu 2013, nr 13.

Akty prawne

1. Konwencja Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728.).
2. Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (tekst jedn. Dz. U. z 2023 r., poz. 66, z 2022 r., poz. 2600, z 2023 r., poz. 240).
3. Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (tekst jedn. Dz. U. z 2022 r., poz. 813, 835, 1079 z późn. zm.).
4. Ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze (tekst jedn. Dz. U. z 2022 r., poz. 1247, 1259, 2582, z 2023 r., poz. 240).
5. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jedn. Dz. U. z 2019 r., poz. 742, z 2022 r., poz. 655, 1933).
6. Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej (tekst jedn. Dz. U. z 2022 r., poz. 2470, z 2023 r., poz. 240).

7. Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz. U. z 2022 r., poz. 1900, z 2023 r., poz. 240).
8. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (tekst jedn. Dz. U. z 2023 r., poz. 81).
9. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jedn. Dz. U. z 2022 r., poz. 1648, 1933, 2581).
10. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. Dz. U. z 2022 r., poz. 557, 1488, 2185, z 2023 r., poz. 240).
11. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jedn. Dz. U. z 2021 r., poz. 1214, z 2022 r., poz. 655, 1488, 2600).
12. Ustawa z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (tekst jedn. Dz. U. z 2022 r., poz. 2487, 2600).
13. Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz.U. z 2020 r., poz. 305 ze zm.).
14. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2020 r., poz. 360 ze zm.).
15. Rozporządzenie Ministra Sprawiedliwości z dnia 13 lutego 2017 r. w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi (Dz. U. z 2017 r., poz. 292).

Orzecznictwo

1. Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. K 23/11, OTK-A 2014, nr 7, poz. 80.
2. Postanowienie Sądu Najwyższego Izba Karna z dnia 5 października 2015 r., sygn. V KK 171/15.
3. Wyrok z dnia 25 kwietnia 2019 r. Naczelnego Sądu Administracyjnego, sygn. I OSK 2344/18, LEX nr 2677192.
4. Wyrok Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., sygn. I OSK 668/16, LEX nr 2475548.

Inne materiały

1. Barczak-Oplustil A., Małecki M., Tarapata S., Behan A., Zontek W., Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casusu Pegasusa), Krakowski Instytut Prawa Karnego, data publikacji: 15 lutego 2022 r.
2. Szumiło-Kulczycka D., Opinia sporządzona na zlecenie Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz Reformy Służb Specjalnych, Kraków 26 sierpnia 2022 r.

3. DRAFT REPORT of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, *op. cit*.
4. Wiretap Report 2021, United States Courts, https://www.uscourts.gov/statistics–reports/wiretap–report–2021, data odczytu: 25 lutego 2023 r.
5. Projekt ustawy z 2008 r. o czynnościach operacyjno-rozpoznawczych, http://orka.sejm.gov.pl/proc6.nsf/projekty/353_p.htm, data odczytu: 25 lutego 2023 r.
6. Https://eur–lex.europa.eu/legal–content/PL/TXT/?uri=CELEX%3A32013L0040, data odczytu: 25 lutego 2023 r.
7. Stanowisko Szefa CBA przytoczone w wyroku Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., sygn. I OSK 668/16, LEX nr 2475548.

End device wiretapping

Abstract

This paper addresses one of the wiretapping methods that are used as part of operational reconnaissance to monitor electronic devices such as telephones or laptops. A definition of the wiretapping method is provided, which method consists of "obtaining and preserving data from digital data carriers, ICT end devices, and information and tele-information systems". Clarified is the meaning of each term used in the definition and legal and factual conditions that need to be met for wiretapping to supply valuable evidence. "Forms", "methods", "technical means", and "tools" used in operations are described. Views of legal academic and commentators relating to lawfulness of, and conditions for "tapping" end devices are challenged with the argument that tapping is a lawful method of information gathering in extra-judicial operations. The paper ends with a summary of the research topic.

Key words

Wiretapping, tapping, special service, crime, IT data, digital traces, evidence, electronic data carrier.