Kazimierz Pawelec*

Centralne Biuro Zwalczania Cyberprzestępczości i jego wybrane uprawnienia. Kilka refleksji

Streszczenie

Z dniem 12 stycznia 2022 roku weszła w życie ustawa z 17 grudnia 2021 roku o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości. Publikacja omawia jej najważniejsze fragmenty związane z przeprowadzaniem czynności operacyjno-rozpoznawczych zarówno w stadium czynności poprzedzających wszczęcie postępowania karnego, jak i po jego wszczęciu, ich znaczenie dowodowe, wskazuje kontrowersje związane z zakresem przedmiotowym uchwalonej ustawy, w tym zamkniętym katalogiem czynów zabronionych oraz innych z nimi niezwiązanych immunitetami, tajemnicami zawodowymi, gwarancjami osób, wobec których służby podjęły określone niejawne czynności. Nie pomija także kwestii kontrowersyjnych, a związanych z oceną dowodów pośrednio nielegalnych oraz konsekwencji naruszenia obowiązującej procedury, w tym kwestii oddania prokuratorowi do oceny wykorzystania informacji uzyskanych z naruszeniem procedury w sytuacji, gdy powyższe może należeć wyłącznie do sądu. Wreszcie przedstawia propozycje ustawodawcze mające charakter postulatów *de lege ferenda* dających sądowi uprawnienia do badania legalności czynności operacyjno-rozpoznawczych, w tym również w zakresie proceduralnych dyrektyw w każdym stadium postępowania, a nie tylko po jego wszczęciu.

Słowa kluczowe: Centralne Biuro Zwalczania Cyberprzestępczości, czynności operacyjno-rozpoznawcze, tajemnice zawodowe

* Dr Kazimierz Pawelec, Instytut Nauk o Bezpieczeństwie, UPH w Siedlcach, e-mail: pawelec.kancelaria@op.pl, ORCID: 000-0001-8669-0249.

Wstęp

12 stycznia 2022 roku weszła w życie ustawa z 17 grudnia 2021 roku o zmianie niektóry ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (CBZC)[1]. Utworzone Biuro będzie realizowało następujące zadania: rozpoznawanie, zapobieganie oraz zwalczanie przestępczości popełnionej przy użyciu systemów teleinformatycznych lub sieci teleinformatycznej. Z powyższym będzie wiązało się również wykrywanie tego rodzaju przestępczości, a także wspieranie pozostałych jednostek organizacyjnych policji we wskazanym wyżej zakresie. *Ratio legis* uchwalonej ustawy były wyzwania stawiane cyberbezpieczeństwu we współczesności. Są one związane z rozwojem technologii informatycznych, wręcz zależności od niej życia codziennego, w tym Internetu, a także anonimowości w cyberprzestrzeni. Powyższego nie sposób nie powiązać z podnoszeniem jakości działania służb porządku publicznego i ich możliwości operacyjnych w zakresie realizacji ustawowych zadań. Powszechny dostęp do Internetu w kontekście globalnego charakteru cyberprzestrzeni i jednocześnie stosunkowo duże możliwości zachowania *incognito* osób komunikujących w tej przestrzeni sprzyjają powstaniu różnego rodzaju zagrożeń nie tylko bezpieczeństwa systemów informatycznych, lecz także sprzyjają podejmowaniu działań o charakterze przestępczym, zwłaszcza przestępstw przeciwko mieniu, gospodarczych, narkotykowych czy pedofilskich. Nie sposób nie zauważyć, że osiągnięcia związane z rozwojem technologicznym stają się częstokroć narzędziami wykorzystywanymi do popełniania przestępstw, a także celem samej działalności przestępczej. Tym samym stanowią poważne wyzwanie dla organów państwa w kontekście ich ujawniania, wykrywania oraz zwalczania. Stąd przyjęto, że niezbędne było utworzenie ogólnokrajowej jednostki organizacyjnej policji i ustanowienie nowej służby odpowiedzialnej za rozpoznanie, zapobieganie oraz zwalczanie cyberprzestępczości.

Nowo uchwalona ustawa, aczkolwiek nawiązuje do ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, dotyczy jednak innych kwestii niż należących do Agencji Bezpieczeństwa Wewnętrznego, gdyż zjawisko cyberprzestępczości jest czym innym niż bezpieczeństwo systemów

1 Ustawa z dnia 17 grudnia 2021 r. o zmianie niektóry ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, Dz.U. 2021, poz. 2449.

teleinformatycznych, które stało się przedmiotem działania nowej jednostki policji, jak wynika z uzasadnienia projektu ustawy.

W dalszej kolejności twórcy ustawy w uzasadnieniu zwrócili uwagę, na podstawie danych statystycznych, że w latach 2013–2020 liczba przestępstw popełnionych w cyberprzestrzeni oraz wykorzystujących Internet wzrosła z 52 291 do 107 518. Najwięcej popełniono w następujących kategoriach: przeciwko mieniu, w tym gospodarczych, prawom autorskim i pokrewnym, wolności seksualnej i obyczajności, ochronie informacji, wiarygodności dokumentów, własności przemysłowej, wolności oraz czci i nietykalności cielesnej. W praktyce powszechnie rozumiana cyberprzestępczość zwykle nie tworzy nowego rodzaju przestępstw, lecz dostarcza nowych metod i środków, a także stanowi nową przestrzeń do ich popełniania. Dlatego też wymaga specjalistycznego podejścia do rozpoznania środowiska internetowego, identyfikowania pojawiających się w nim nowych zagrożeń oraz skutecznego reagowania na zjawiska należące jeszcze do przedpola czynów zabronionych[2].

Zamierzeniem autora nie było absolutnie podważenie zasadności uchwalonej ustawy czy jej szczegółowego omówienia, w tym także w zakresie zapewnienia fachowego obsadzenia nowo tworzonego Biura. Uwagę poświęcił kontrowersyjnym kwestiom, które ustawa może wywołać w systemie obowiązującego porządku prawnego. Powyższe znajduje uzasadnienie, gdyż brakuje aktów wykonawczych, zwłaszcza rozporządzenia dotyczącego sposobów sporządzania dokumentacji w związku z zarządzeniem kontroli operacyjnej, jej dokumentowania, przechowywania, przekazywania wniosków oraz zarządzeń, a także przechowywania, przekazywania, kopiowania i niszczenia materiałów uzyskanych podczas tej kontroli, zakresu danych gromadzonych w rejestrach, o których mowa w art. 16a–16c, oraz wzorów stosowanych dokumentów i rejestrów, mając na względzie zapewnienie niejawnego charakteru podejmowanych czynności i uzyskanych materiałów.

W dalszej kolejności autor skupił się na zakresie przedmiotowym podejmowanych przez CBZC czynnościom operacyjno-rozpoznawczym (art. 19 ust. 1 pkt 2 ustawy), ich przełożenia na materiał procesowy w związku z przyznaniem Biuru uprawnień do prowadzenia czynności dochodzeniowo-śledczych, oceny i konsekwencji naruszeń procedury karnej we wskazanym zakresie, a także możliwości uzyskania informacji przez obywateli czy inne organa

2 Por. Ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości. Ocena skutków regulacji, Lex/el.

o prowadzonych wobec nich czynnościach operacyjno-rozpoznawczych, w tym kwestiach związanych z immunitetami, tajemnicami zawodowymi, także bezwzględnie obowiązującymi. Są to kwestie ważne, zwłaszcza w demokratycznym państwie prawa szanującym tajemnice korespondencji, komunikowania, prawa do prywatności oraz podstawowych gwarancji procesowych.

Czynności operacyjno-rozpoznawcze. Zagadnienia podstawowe

Czynności operacyjno-rozpoznawcze należą do niejawnych i polegają na kontroli korespondencji, przesyłek oraz stosowaniu środków technicznych umożliwiających uzyskanie w sposób niejawny informacji, dowodów oraz ich utrwalania, w szczególności rozmów telefonicznych i innych informacji przesyłanych za pomocą sieci telekomunikacyjnych czy internetowych. Obejmują również możliwość dyskretnego wejścia do pomieszczeń w celu zainstalowania urządzeń umożliwiających podgląd i podsłuch. Przewidują także możliwość zastosowania prowokacji, przesyłki niejawnie nadzorowanej lub zakupu kontrolowanego czy kontrolowanej łapówki. Tego rodzaju działania, ze względu na ich tajny charakter oraz utajnienie większości aktów prawnych wykonawczych, mogą budzić poważne wątpliwości, czy były prowadzone zgodnie z uprawnieniami przysługującymi organom państwa[3].

Czynności operacyjno-rozpoznawcze można prowadzić zarówno na etapie przedprocesowym, jak i w trakcie postępowania przygotowawczego. Wykluczone jest ich przeprowadzanie na etapie postępowania sądowego, z wyjątkiem możliwości zarządzenia przeprowadzenia podsłuchu procesowego na podstawie treści art. 237 i następnych k.p.k.[4].

3 Por.: S. Waltoś, *Tajny agent policji na obrzeżach odpowiedzialności karnej*, „Państwo i Prawo" 1993, nr 11, s. 28–29; A. Taracha, *Działania operacyjno-rozpoznawcze prowadzone w ramach uprawnień jako kontratyp – wybrane zagadnienia* [w:] *Współzależność prawa karnego i procesowego*, red. Z. Ćwiąkalski, G. Artymiak, Warszawa 2009, s. 461; K.J. Pawelec, *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010, s. 94; H. Pracki, *Nowe instytucje prawne w ustawach policyjnych*, „Prokuratura i Prawo" 1996, nr 2–3, s. 46; D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 225 i nast.; P. Herbowski, *Poufne osobowe źródła informacji. Aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2018, s. 194–263 oraz podana literatura.

4 Por.: A. Marek, *Komentarz do kodeksu karnego*, Warszawa 1999, s. 60; idem, *Kodeks karny. Praktyczny komentarz*, Warszawa 2006, s. 65–66.

Zakres podmiotowy czynności operacyjno-rozpoznawczych może obejmować osoby zarówno podejrzewane, podejrzane, oskarżone, pokrzywdzone, jak i inne mające związek z ujawnionym przestępstwem bądź mogącym być popełnionym (o ile przygotowanie do popełnienia owego przestępstwa zostało wskazane w k.k. jako czyn karalny) czy też, z którymi mogą się kontaktować wymienione (art. 237 par. 4 k.p.k. *in fine*) lub mogące mieć związek z przestępstwem (należy sądzić, że będą to współsprawcy, podżegacze czy pomocnicy, a także inni mogący mieć o nim wiedzę).

Rozważając zakres czynności operacyjno-rozpoznawczych, nie można pominąć istotnej kwestii związanej z możliwością podejmowania tych czynności w stosunku do osób korzystających z immunitetów (np. sędziowskiego, prokuratorskiego, poselskiego, senatorskiego), a także dyplomatycznych, o których mowa w art. 578 i następnych k.p.k. Analiza przedmiotowa poszczególnych immunitetów może prowadzić do wniosku, że osoby z nich korzystające nie mogą być pociągnięte do odpowiedzialności bez zgody właściwych organów bądź nie podlegają orzecznictwu polskich sądów. Nie oznacza to, że w razie istnienia uzasadnionego podejrzenia popełnienia przestępstwa wobec nich nie mogą być prowadzone rzetelne czynności operacyjno-rozpoznawcze, ale nie pozostające w związku z wykonywaniem czynności zawodowych. Możliwość wykorzystania uzyskanych materiałów będzie uzależniona dopiero od uzyskania zgody właściwego organu zezwalającego na pociągnięcie do odpowiedzialności karnej. Brak takiej zgody będzie determinował konieczność zniszczenia uzyskanych materiałów[5].

Odrębnego potraktowania wymaga problematyka zastosowania czynności operacyjno-rozpoznawczych w stosunku do osób korzystających z tajemnic zawodowych, tj. adwokackiej, radcy prawnego, doradcy podatkowego, mediatora, lekarskiej, dziennikarskiej, notarialnej, komorniczej czy statystycznej. Analizując tę kwestię, trzeba odróżnić sytuację, kiedy czynności operacyjno-rozpoznawcze były związane z wykonywanym zawodem, od tej, kiedy nie miały one związku z pracą i tajemnicą z nią związaną. Jeżeli chodzi o czynności objęte tajemnicą zawodową, to zastosowanie czynności operacyjno-rozpoznawczych było możliwe w razie zaistnienia okoliczności przedmiotowych

5 Por.: K. Eichstaed, *Czynności sądu w postępowaniu przygotowawczym w polskim prawie karnym*, Warszawa 2008, s. 55–56; S. Hoc, *Refleksje na marginesie art. 10 ustawy o Urzędzie Ochrony Państwa*, „Wojskowy Przegląd Prawniczy" 1992, nr 3–4, s. 34–35; B. Kurzępa, *Kontrola i utrwalanie rozmów według kodeksu postępowania karnego*, „Prokuratura i Prawo" 1999, nr 3, s. 82.

wskazanych w art. 19 ust. 1 pkt 2 ustawy o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, o czym będzie mowa w dalszej części opracowania, a także art. 20 ust. 9 powołanej ustawy oraz w sytuacji, gdy zaszły okoliczności umożliwiające złożenie wniosku o zwolnienie z tej tajemnicy, a wskazane w art. 180 par. 2 i 3 k.p.k.[6].

Nie jest możliwe zastosowanie czynności operacyjno-rozpoznawczych w stosunku do osób korzystających z tzw. bezwzględnej tajemnicy zawodowej określonej w art. 178 pkt 1 i 2 k.p.k.[7].

Rozważenia wymaga, czy czynności operacyjno-rozpoznawcze mogą być przeprowadzone podczas czynności sprawdzających oraz tzw. niecierpiących zwłoki. W piśmiennictwie Waldemar Osiecki dopuszczał taką możliwość, nie widział jej jednak podczas czynności sprawdzających, ponieważ – jego zdaniem – nie miały one charakteru procesowego. Pogląd ten podzielił Ryszard A. Stefański, a także Bolesław Kurzępa[8].

Przywołani autorzy nie mieli racji, argumentując, że wykonywanie czynności operacyjno-rozpoznawczych było niedopuszczalne podczas postępowania sprawdzającego. Ich charakter był zupełnie inny – zmierzający m.in. do ujawnienia zaplanowanego czy przygotowywanego przestępstwa i zapobieżenia jego popełnieniu. Rację należało przyznać Michałowi Błońskiemu, który uznał wykonywanie tego rodzaju czynności za dopuszczalne[9].

6 Por.: K.J. Pawelec, [w:] *Praktyczny komentarz do zmian procedury karnej*, red. W. Cieślak i in., Warszawa 2017, s. 188–190; K.J. Pawelec, *Tajemnica zawodowa notariusza w znowelizowanym kodeksie postępowania karnego. Zagadnienia podstawowe*, „Rejent" 2015, nr 9, s. 88–101; M. Bartnik, M. Karpiuk, W. Lis, K.J. Pawelec, I. Tuleya, *Ustawa o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego. Komentarz* [w:] *Prawo bezpieczeństwa. Komentarze*, t. 1, red. M. Karpiuk, Olszyn 2017, s. 150–157 oraz podana literatura i orzecznictwo.

7 Por.: J. Machlańska, *Dowód z podsłuchu procesowego a ochrona tajemnicy obrończej*, „Palestra" 2016, nr 1–2, s. 74–82; P. Kardas, *Ochrona tajemnicy obrończej. Kilka uwag o kontroli i utrwalaniu treści rozmów oraz przekazów informacji realizowanych przy użyciu środków technicznych pomiędzy obrońcą a mandantem*, „e-Czasopismo Prawa Karnego i Nauk Penalnych" 2011, nr 4, s. 5–35.

8 Zob.: W. Osiecki, *Kontrola rozmów telefonicznych w ustawodawstwie polskim*, „Nowe Prawo" 1987, nr 9, s. 98–99; R.A. Stefański, [w:] *Kodeks postępowania karnego. Komentarz*, t. 1, red. Z. Gostyński, Warszawa 1998, s. 601; B. Kurzępa, op. cit., s. 84–85.

9 Więcej zob. M. Błoński, *Zakres przedmiotowy podsłuchu procesowego*, „Palestra" 2012, nr 7–8, s. 82–90. Por.: Postanowienie SN z 1 czerwca 2010, WZ 20/10, „Orzecznictwo Sądu Najwyższego w Sprawach Karnych" 2010, nr 1, poz. 1146; Postanowienie SA w Krakowie z dnia 5 lutego 2009, II AKa 6/09, „Krakowskie Zeszyty Sądowe" 2009, nr 2, poz. 41.

Zakres przedmiotowy czynności operacyjno-rozpoznawczych przysługujących CBZC

Artykuł 19 ust. 1 pkt 2 ustawy o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości określa jego zakres przedmiotowy. Wymienia przestępstwa, do których Biuro może zastosować techniki operacyjno-rozpoznawcze, a także w ramach powierzonych mu zadań dochodzeniowo-śledczych. Są to przestępstwa określone w artykułach: 134, 135 par. 1, 136 par. 1, 156 par. 1 i 3, 163 par. 1 i 3, 164 par. 1, 165 par. 1 i 3, 166, 167, 173 par. 1 i 3, 189, 189a, 200a, 200b, 211a, 223, 224a, 228 par. 1 i 3–5, 222 par. 1 i 3–5, 230 par. 1, 230a par. 1, 231 par. 2, 232, 233 par. 1, 1a, 4 i 6, 234, 235, 236 par. 1, 238, 239 par. 1, 240 par. 1, 245, 246, 252 par. 1–3, 258, 267 par. 1–4, 268a par. 1 i 2, 269, 269a, 269b par. 1, 270a par. 1 i 2, 271a par. 1 i 2, 277a par. 1, 273 par. 1, 280–282, 285 par. 1, 286 par. 1, 287 par. 1, 296a par. 1, 2 i 4, 299 par. 1–6 oraz art. 310 par. 1, 2 i 4 k.k. Patrząc na wymienione przestępstwa, można dojść do wniosku, że ich wybór był dość przypadkowy w odniesieniu do zagrożeń wskazanych w uzasadnieniu uchwalonej ustawy, danych statystycznych, a także oceny regulacji. W tej materii brak jest jakiegokolwiek uzasadnienia.

Poważne wątpliwości może budzić regulacja wymieniona w art. 20 ust. 9 ustawy. Pomijając już, że wskazany przepis dający uprawnienie CBZC do wykonywania czynności operacyjno-rozpoznawczych w zakresie typowych czynności cywilno-prawnych, tj. umów, czyli takich, które nie mają wiele wspólnego z regulacją art. 19 ust. 1 pkt 2, razi również ogólnością dającą możliwość podejmowania wskazanych czynności zawierających w sobie fundamentalne zasady swobody zawierania umów, działalności gospodarczej czy też tajemnicy przedsiębiorstwa. Powołany przepis daje CBZC przyzwolenie na sekretne obserwowanie umów o świadczeniu usług płatniczych zawieranych z osobami fizycznymi, prawnymi lub jednostkami organizacyjnymi, które nie mają osobowości prawnej. Przepis przyznaje nowo powołanemu Biuru możliwość weryfikacji tych umów, czasu ich obowiązywania, a także pozyskiwania danych teleadresowych umożliwiających nawiązanie kontaktu z ich stronami. Powyższy przepis może stwarzać pokusę ingerencji w sfery cywilistyczne, które wszak znajdują się we właściwości sądów cywilnych oraz gospodarczych. *Ratio legis* art. 20 ust. 9 nie zawiera uzasadnienia, co *de facto* uniemożliwia dokonanie jego wykładni autentycznej.

Zauważyć także należy, że wprowadzenie do procesu karnego wyników czynności operacyjno-rozpoznawczych możliwe jest dopiero po wszczęciu postępowania karnego, więc wszelkie sekretne poczynania służb we wcześniejszych etapach pozostają poza wszelką kontrolą, w tym również sądową.

Dowodowa ocena wyników czynności operacyjno-rozpoznawczych

Wprowadzenie do procesu karnego wyników czynności operacyjno-rozpoznawczych ma miejsce na podstawie art. 167 k.p.k., z zastosowaniem, o ile zaszły takie okoliczności, m.in. art. 168a i 168b k.p.k., a w odniesieniu do postępowania przygotowawczego także art. 297 k.p.k., po uwzględnieniu również bezwzględnych oraz względnych zakazów dowodowych[10].

Istotną przy tym kwestią o charakterze merytorycznym, dotychczas nie rozwiązaną, będzie problematyka związana z inaczej unormowanymi zagadnieniami kontroli operacyjnej w chwili jej podjęcia, a odmiennej w stadium wyrokowania. W tej materii przekonywające stanowisko zaprezentował Sąd Najwyższy w uchwale siedmiu sędziów SN z 23 marca 2011 roku (I KZP 32/10, OSNKW 2011, nr 3, poz. 22), w której wątpliwości co do interpretacji „zgody następczej" odnosiły się do konieczności zastosowania art. 237a k.p.k., a także podsłuchów stosowanych przed wejściem w życie zmian dokonanych w rozdziale 25 k.p.k. Z uzasadnienia rządowego projektu poprzedzającego zmiany dokonane ustawą z 4 lutego 2011 roku[11] wynikało, że zostały one przygotowane w związku z koniecznością pilnej zmiany przepisów regulujących zarówno procesową kontrolę rozmów, jak i sferę czynności operacyjnych poddanych kontroli sądu lub prokuratora. Zasada rządów prawa zakłada, że ingerencja ze strony organów władzy wykonawczej w prawa jednostki powinna być przedmiotem skutecznej kontroli, która musi być przeprowadzona przez organy sądowe. To one dają najlepszą gwarancję niezależności, bezstronności oraz

10 Więcej zob.: K.J. Pawelec, [w:] *Praktyczny komentarz…*, s. 180–182, 186–190 oraz podana literatura i orzecznictwo; M. Gabriel-Węglowski, [w:] *Praktyczny komentarz…*, s. 279–282; K.J. Pawelec, *Substytuowanie dowodowe nielegalnych czynności operacyjno-rozpoznawczych. Zagadnienia podstawowe*, „Przegląd Sądowy" 2018, nr 3, s. 77.

11 Ustawa z dnia 4 lutego 2011 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw, Dz.U. 2011, nr 53, poz. 273.

stosowania właściwej procedury, a realizacja tej zasady nie powinna być ograniczona czasem dokonywanej czynności operacyjnej[12].

Ustawodawca mimo licznych nowelizacji procedury karnej nie dał wyraźnego przyzwolenia na dopuszczalność przyjęcia każdego źródła dowodowego jako podstawy ustaleń faktycznych. Procedura karna w tej materii zawiera liczne ograniczenia, w tym także w zakresie czynności operacyjno-rozpoznawczych. Stąd kwestia wprowadzenia i wykorzystania w toczącym się postępowaniu karnym należy wyłącznie do sądu, w zależności od ich znaczenia dla prowadzonego postępowania[13].

Pamiętać należy, że w polskiej procedurze karnej istnieją przepisy określające warunki przeprowadzania czynności operacyjno-rozpoznawczych, brakuje zaś regulujących losy dowodów uzyskanych w następstwie czynności dokonanych z naruszeniem prawa. Zgodnie z zasadą swobodnej oceny dowodów dopuszczalne jest przeprowadzanie wszelkich czynności dowodowych, z wyjątkiem czynności objętych zakazem ich przeprowadzania[14].

Nie został przy tym określony zakaz wykorzystywania tzw. owoców zakazanego drzewa, oceny dowodów pozyskanych nielegalnie, w inny, częstokroć pośredni sposób. Rozważenie przedłożonych trudnych, częstokroć kontrowersyjnych kwestii wykracza poza zakres niniejszej publikacji[15].

Zakończenie

Niewątpliwie zagrożenie przestępczością z wykorzystaniem cyberprzestrzeni będzie wzrastać. Świadczyć może o tym choćby postęp nauk informatycznych, technicznych, tworzenie coraz to nowych, nowocześniejszych technologii. Dlatego utworzenie Centralnego Biura Zwalczania Cyberprzestępczości wydaje się dobrym pomysłem. Jednakże zakres jego uprawnień określony w art. 19 ust. 2 ustawy o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości wydaje się zbyt duży. Zakres przedmiotowy powołanego przepisu odbiega od przedłożonego Sejmowi,

12 Por. Postanowienie SN z 26 kwietnia 2007 r., I KZP 6/07, „Orzecznictwo Sądu Najwyższego w Sprawach Karnych" 2007, nr 5, poz. 37.

13 Por. Postanowienie SN z 8 grudnia 2010 r., WZ 50/10, ibidem 2010, nr 1, poz. 2476; Postanowienie SN z 8 grudnia 2010 r., WZ 49/10, ibidem, poz. 2475.

14 Por. Wyrok SN z 2 lutego 2016 r., IV KK 346/15, ibidem 2016, nr 7, poz. 43.

15 Więcej zob. K.J. Pawelec, *Substytuowanie dowodowe…*, s. 79–85 oraz przywołane orzecznictwo i literatura.

Senatowi i Prezydentowi RP projektu regulacji oraz jego uzasadnienia. Nie wszystkie wymienione w art. 19 ust. 2 ustawy przestępstwa były ujawniane przez praktykę jako wykorzystujące cyberprzestrzeń. I dalej, poważny niepokój może wzbudzać możliwość wykorzystywania instrumentów operacyjno-rozpoznawczych podczas zawierania umów cywilno-prawnych zarówno przez osoby fizyczne, jak i podmioty gospodarcze. Ingerencja w te sfery, wybitnie gospodarcze, związane ze swobodą zawierania umów, raczej nie powinna interesować powołanego Biura.

Jednakże nie jest to najważniejsze. Niezwykle obszerny katalog możliwości stosowania przez CBZC niejawnych czynności operacyjno-rozpoznawczych może stwarzać pokusę podsłuchiwania, śledzenia, prowokowania itp. obywateli, którzy mają czyste sumienie. Takie osoby nie mają szans dowiedzieć się, że wobec nich były stosowane sekretne czynności służb. Szansę taką mogły uzyskać dopiero po wszczęciu postępowania karnego, ale i tak w bardzo ograniczonym zakresie. W obowiązującym stanie prawnym obywatel mający uzasadnione przypuszczenie, że jest w „zainteresowaniu służb", może jedynie wystąpić do nich z pytaniem, w trybie dostępu do informacji publicznej, czy faktycznie miało to miejsce. Jednakże skazany jest na porażkę, ponieważ pytana służba, powołując się na klauzulę niejawności, odmówi udzielenia odpowiedzi. Z kolei praktyka sądów administracyjnych wskazuje, że tego rodzaju skargi obywateli są oddalane. Tymczasem Konstytucja RP przewiduje gwarancję ochrony prawa do prywatności, miru domowego, tajemnicy korespondencji i autonomii informacyjnej. Dlatego też realizacja zadań przez służby specjalne powinna odbywać się z poszanowaniem wartości konstytucyjnych, z przestrzeganiem zasady legalizmu, trójpodziału władz oraz poszanowania konstytucyjnych praw i wolności jednostki. W Polsce w dalszym ciągu brakuje niezależnego organu, który sprawowałby nadzór nad tymi służbami. Aktualnie nadzór ten jest tylko fragmentaryczny i nie pozwala na skuteczne, bezstronne i niezależne od polityki weryfikowanie ich działań. Wobec tego autor przedkłada do rozważenia propozycję *de lege ferenda* oddania wyodrębnionemu wydziałowi Sądu Okręgowego w Warszawie rozpatrywanie wniosków oraz skarg obywateli na działania służb, w tym także w odniesieniu do podejmowanych działań operacyjno-rozpoznawczych, zanim zostało wszczęte postępowanie karne. Propozycja ta odbiega od opracowania Biura Rzecznika Praw

Obywatelskich pt. „Osiodłać Pegaza”[16]. Jest znacznie prostsza, a wykorzystuje zarówno doświadczenia zawodowe sędziów, jak i ich pozycję ustrojową. Wskazany specjalny wydział powinien zostać wyposażony w prawo do sprawdzania działania służb, w tym jego materiałów operacyjno-rozpoznawczych zastosowanych wobec osób wnoszących o to także w zakresie przed wszczęciem postępowania, oraz wypowiadać się co do ich legalności oraz zgodności z prawem. Podobne uprawnienia powinien posiadać po wszczęciu postępowania, jeżeli strona uprawniona zgłosi tego rodzaju wniosek.

Bibliografia

Bartnik M., Karpiuk M., Lis W., Pawelec K.J., Tuleya I., *Ustawa o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego. Komentarz* [w:] *Prawo bezpieczeństwa. Komentarze*, t. 1, red. M. Karpiuk, Olszyn 2017.

Błoński M., *Zakres przedmiotowy podsłuchu procesowego*, „Palestra” 2012, nr 7–8.

Bodnar A. i in., *„Osiodłać Pegaza”. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy*, Warszawa 2019.

Eichstaed K., *Czynności sądu w postępowaniu przygotowawczym w polskim prawie karnym*, Warszawa 2008.

Herbowski P., *Poufne osobowe źródła informacji. Aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2018.

Hoc S., *Refleksje na marginesie art. 10 ustawy o Urzędzie Ochrony Państwa*, „Wojskowy Przegląd Prawniczy” 1992, nr 3–4.

Kardas P., *Ochrona tajemnicy obrończej. Kilka uwag o kontroli i utrwalaniu treści rozmów oraz przekazów informacji realizowanych przy użyciu środków technicznych pomiędzy obrońcą a mandantem*, „e-Czasopismo Prawa Karnego i Nauk Penalnych” 2011, nr 4.

Kodeks postępowania karnego. Komentarz, t. 1, red. Z. Gostyński, Warszawa 1998.

Kurzępa B., *Kontrola i utrwalanie rozmów według kodeksu postępowania karnego*, „Prokuratura i Prawo” 1999, nr 3.

Machlańska J., *Dowód z podsłuchu procesowego a ochrona tajemnicy obrończej*, „Palestra” 2016, nr 1–2.

Marek A., *Kodeks karny. Praktyczny komentarz*, Warszawa 2006.

Marek A., *Komentarz do kodeksu karnego*, Warszawa 1999.

Osiecki W., *Kontrola rozmów telefonicznych w ustawodawstwie polskim*, „Nowe Prawo” 1987, nr 9.

Pawelec K.J., *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010.

Pawelec K.J., *Substytuowanie dowodowe nielegalnych czynności operacyjno-rozpoznawczych. Zagadnienia podstawowe*, „Przegląd Sądowy” 2018, nr 3.

Pawelec K.J., *Tajemnica zawodowa notariusza w znowelizowanym kodeksie postępowania karnego. Zagadnienia podstawowe*, „Rejent” 2015, nr 9.

Pracki H., *Nowe instytucje prawne w ustawach policyjnych*, „Prokuratura i Prawo” 1996, nr 2–3.

Praktyczny komentarz do zmian procedury karnej, red. W. Cieślak i in., Warszawa 2017.

Szumiło-Kulczycka D., *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012.

16 Zob. A. Bodnar i in., *„Osiodłać Pegaza”. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy*, Warszawa 2019, s. 27–42.

Taracha A., *Działania operacyjno-rozpoznawcze prowadzone w ramach uprawnień jako kontratyp – wybrane zagadnienia* [w:] *Współzależność prawa karnego i procesowego*, red. Z. Ćwiąkalski, G. Artymiak, Warszawa 2009.
Waltoś S., *Tajny agent policji na obrzeżach odpowiedzialności karnej*, „Państwo i Prawo" 1993, nr 11.

The Central Office for Combating Cybercrime and some of its powers. A few remarks

Abstract

The Act of 17 December 2021 amending certain acts in connection with the establishing of the Central Office for Combating Cybercrime entered into force on 12 January 2022. This paper discusses its most important sections dealing with the conduction of investigative operations, both at the stage of operations preceding the institution of criminal proceedings and after their commencement, as well as their evidentiary significance. It also sheds light on some controversies connected with the objective scope of the adopted Act, including a closed list of prohibited acts and other acts not related thereto, immunities, professional secrets, and guarantees offered to persons with regard to whom specific covert activities are undertaken. Other controversial issues related to evaluating the evidence that is considered indirectly unlawful, as well as the consequences of breaching the procedure in force, including the matter of entrusting the prosecutor with assessing the use of information obtained in breach of the procedure, when this can only be done by the court, are also presented. Finally, the article mentions legislative proposals, such as *de lege ferenda* postulates, which grant the court the authority to verify the legality of investigative operations, also as regards procedural directives at every stage of the proceedings, not only after their commencement.

Key words: Central Office for Combating Cybercrime, investigative operations, professional secrets