Krzysztof Krełowski

Kontratyp w uprawnieniach ABW i MI5

Nie czyni bezprawia, kto spełnia swą powinność

Artykuł 235 kodeksu karnego[1] penalizuje działanie polegające na podstępnym doprowadzeniu do wszczęcia postępowania karnego. Z takiej perspektywy można spojrzeć na ogół czynności operacyjnych podejmowanych przez służby kontrwywiadowcze. Posługiwanie się dokumentami legalizacyjnymi, legendowanie działań, kontrola operacyjna, działanie pod przykryciem itd. to swego rodzaju podstęp ukierunkowany na wszczęcie postępowania karnego. Każde z wymienionych wyżej działań wyczerpuje dodatkowo formalne znamiona odrębnych czynów zabronionych przez kodeks karny, jak np. posługiwanie się dokumentami stwierdzającymi nieprawdę, udział w grupie przestępczej itp.

W tym kontekście rodzi się pytanie, jakie przepisy bądź konstrukcje prawne „przywracają" legalność działań funkcjonariuszy wypełniających formalne znamiona przepisów ustawy karnej.

Okoliczności wyłączające bezprawność czynu noszą w nauce nazwę kontratypów. Czyn noszący formalne znamiona przestępstwa nie jest bezprawny w pewnych, określonych, okolicznościach.

Można więc postawić tezę, że podstawą pracy służb policyjnych i specjalnych w ujęciu prawnokarnym jest konstrukcja kontratypu.

Kontratypy można podzielić na kodeksowe – unormowane przez kodeks karny – oraz pozakodeksowe. Kontratypy kodeksowe to obrona konieczna, stan wyższej konieczności, eksperyment naukowy, udział w zawodach sportowych, błąd co do prawa i błąd, co do okoliczności faktycznych. Jako kontratyp można potraktować także brak winy bądź szkodliwości społecznej czynu. Z punktu widzenia działania służb istotniejsze są jednak kontratypy pozakodeksowe, wśród których pierwszorzędne znaczenie ma kontratyp działania w ramach szczególnych uprawnień i zezwoleń (na ten temat szeroko wypowiedzieli się W. Wolter oraz W. Wróbel i A. Zoll)[2].

Policjant stosujący środki przymusu bezpośredniego, posługujący się na przykład pałką lub paralizatorem, nie popełnia przestępstwa, jeśli działa w warunkach określonych prawem. Odpowiedzialność karną wyłącza tu fakt działania w ramach uprawnień. Ustawy określające uprawnienia funkcjonariuszy są przepisami szczególnymi w stosunku do kodeksu karnego i przez to, na zasadzie *lex specialis derogat legi generali*[3] – wyłączają jego działanie.

---

[1] Ustawa z dn. 6 czerwca 1997 r., Dz.U. Nr 88, poz. 553 ze zm.

[2] W. Wolter, *Zarys systemu prawa karnego. Część ogólna*, Kraków 1933, s. 135 oraz W. Wróbel i A. Zoll, *Polskie prawo karn*e. *Część ogólna*, Kraków 2010, s. 373.

[3] *Lex specialis derogat legi generali* – łac. 'ustawa szczególna uchyla ustawę ogólną'.

W praktyce sprawa ta nie wygląda jednak tak prosto. Kontratyp w ustawie o ABW oraz AW[4] (dalej *Ustawa*) skonstruowany jest w sposób niejednolity.

Nie czyni bezprawia, kto spełnia swą powinność

Przykładem poprawnie skonstruowanego kontratypu są następujące przepisy *Ustawy*:

1) art. 23 – wydawanie poleceń określonego zachowania, zatrzymywanie osób, przeszukanie osób i pomieszczeń, kontrola osobista, przeglądanie bagażu oraz obserwowanie i rejestrowanie zdarzeń,
2) art. 25 – użycie środków przymusu bezpośredniego,
3) art. 26 – użycie broni palnej,
4) art. 27 – kontrola operacyjna.

Ustawa nadaje we wskazanych przepisach określone uprawnienia, które tym samym wyłączają stosowanie kodeksu karnego. Regułę tę wyraża rzymska paremia: *Non facit fraudem, qui facit, quod debet* (nie czyni bezprawia, kto spełnia swą powinność).

Podwójna garda?

Nieprawidłowe z legislacyjnego i logicznego punktu widzenia są przepisy art. 32 ust. 1 i art. 35 ust. 6 *Ustawy*. Artykuł 32 ust. 1 brzmi:

„Nie popełnia przestępstwa, kto, będąc do tego uprawnionym, wykonuje czynności określone w art. 29 ust. 1, jeżeli zostały zachowane warunki określone w art. 29 ust. 3, a także kto wykonuje czynności określone w art. 30 ust. 1".

W art. 29 jest mowa o zakupie kontrolowanym, w art. 30 zaś o przesyłce niejawnie nadzorowanej.

Artykuł 35 dotyczy posługiwania się dokumentami legalizacyjnymi. Ustęp 6 tego przepisu brzmi:

„6. Nie popełnia przestępstwa:
   1) kto poleca sporządzenie lub kieruje sporządzeniem dokumentów, o których mowa w ust. 2 i 3,
   2) kto sporządza dokumenty, o których mowa w ust. 2 i 3,
   3) kto udziela pomocy w sporządzeniu dokumentów, o których mowa w ust. 2 i 3,
   4) funkcjonariusz Agencji lub osoba wymieniona w ust. 3, posługujący się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami, o których mowa w ust. 2 i 3".

Konstrukcja polegająca na przyznaniu w jednym przepisie określonych uprawnień, w następnym zaś depenalizująca takie działanie oznacza de facto, że za korzystanie z uprawnień można zostać ukaranym. W państwie prawa to samo działanie nie może być jednocześnie dozwolone przez prawo i nielegalne, a tym bardziej karalne.

Działanie pod przykryciem, czyli udział w grupie przestępczej

Z drugiej strony mamy instytucje niekorzystające z podwójnego zabezpieczenia, a nawet takie, których legalność wynika z ustawy jedynie pośrednio. Legalność funkcjonowania w grupie przestępczej pod przykryciem wynika z przepisów regulujących instytucję zakupu kontrolowanego (art. 29 *Ustawy*). Choć artykuł ten nie zezwala

[4] Ustawa z dn. 24 maja 2002 r., Dz.U. z 2010 r. Nr 29, poz. 154 ze zm.

wprost na prowadzenie pozorowanej działalności przestępczej, to należy konstatować, że przepis prawa musi być możliwy do wykonania, a możliwość taką daje właśnie działanie pod przykryciem. Jest to jednak tylko interpretacja.

Autoryzacja określonych działań

Zgodnie z *Ustawą* zgoda osobnego organu jest wymagana w przypadkach:

1) stosowania kontroli operacyjnej – konieczna jest tu zgoda sądu (art. 27),
2) zakupu kontrolowanego – wymagana jest pisemna zgoda Prokuratora Generalnego (art. 29),
3) przesyłki niejawnie nadzorowanej – w tym przypadku przepis nakłada obowiązek poinformowania Prokuratora Generalnego, który może nakazać zaniechanie tych czynności (art. 30).

Zgoda niezależnego organu jest potrzebna w sytuacji, kiedy określone działania szczególnie głęboko ingerują w konstytucyjne prawa jednostki i jednocześnie nie są to działania nagłe, będące bezpośrednią odpowiedzią na czyn przestępczy. Konieczne są tu dwa elementy: działanie na podstawie ustawy i zgoda podmiotu zewnętrznego. Podmiotem tym będzie sąd lub prokurator.

W polskiej tradycji prawnej istnieje jednak przykład autoryzowania określonych działań przez organ administracji. Legalizację działań pod przykryciem zawierał już przepis art. 2 rozporządzenia prezydenta RP z 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu państwa[5], którego konstrukcja była następująca:

„Art. 2. Działanie nie jest bezprawne wtedy tylko, gdy podjęto je za zezwoleniem udzielonem:

a) przez Ministra Spraw Wojskowych lub upoważnione przez niego organa państwowe – w związku z wykonywaniem zadań ochrony bezpieczeństwa Państwa Polskiego;
b) przez właściwą władzę naczelną lub upoważnione przez nią organa podległe – w związku z wykonywaniem innych zadań państwowych".

Przepis ten, jak widać, nie wyszczególniał działań wypełniających znamiona przestępstwa, które miały być legalizowane przez wydanie zezwolenia. Trzeba jednak zauważyć, że jest on skonstruowany precyzyjnie – nie pozostawia funkcjonariuszom wątpliwości, które działanie jest zgodne z prawem.

Zezwolenie jako podstawa legalizacji określonych działań w legislacji brytyjskiej

Autoryzacja określonych działań przez organ administracji jest podstawą pracy operacyjnej służb brytyjskich. Podstawowym aktem prawnym regulującym tę materię jest *Regulation of Investigatory Powers Act 2000* (*Ustawa o uprawnieniach operacyjnych z 2000 roku,* dalej RIPA). Ustawa ta została uchwalona w odpowiedzi na rozwój nowoczesnych technologii związanych z Internetem i przesyłaniem danych. W miarę precyzyjnie określiła też stosowanie innych, bardziej tradycyjnych metod pozyskiwania informacji, takich jak stosowanie obserwacji, rejestrowanie obrazów i zapisów sytuacji w miejscach publicznych i prywatnych czy prace z osobowymi źródłami informacji. Akt ten jest podstawą pracy operacyjnej przede wszystkim Security Service (MI5),

[5] Dz.U. Nr 94, poz. 851.

Goverment Communications Headquarters (GCHQ) oraz innych formacji, w tym Secret Intelligence Service (MI6), choć ta ostatnia służba działa w pewnej mierze, opierając się na swojej własnej ustawie (*The Intelligence Services Act 1994*), która uwzględnia specyfikę funkcjonowania wywiadu – np. naruszenie własności rzeczy położonej poza terytorium Wielkiej Brytanii. W polskiej ustawie brak takiego zapisu, a miałby on znaczenie istotne – polską ustawę karną stosuje się także wobec obywatela polskiego, który popełnił przestępstwo za granicą (art. 109 kk).

Niniejsze opracowanie dotyczy jedynie uprawnień określonych w RIPA. Jest to tematyka niezmiernie obszerna – RIPA to akt liczący ponad sto stron, do którego dochodzą wydawane na jego mocy przez sekretarzy stanu *Orders*, tj. akty zbliżone do polskich rozporządzeń, zawierające uzupełnienie przepisów ustawy, i wreszcie *Codes of Practice*, tj. *Zasady postępowania* – mające moc prawną dokumenty przeznaczone do praktycznego wykorzystywania przez urzędników dokonujących autoryzacji określonych działań. W sumie jest to kilkaset stron uregulowań dotyczących pracy operacyjnej. W niniejszej publikacji z konieczności ograniczono się jedynie do kilku wybranych kwestii.

Definicja przestępstwa telekomunikacyjnego

Artykuł 1 RIPA definiuje przestępstwo telekomunikacyjne: „Kto umyślnie i bez zgody uprawnionego organu władzy narusza na terenie Zjednoczonego Królestwa tajemnicę komunikowania się…" ("It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication…"). Przepis ten sam w sobie zawiera kontratyp, którym jest działanie w ramach uprawnienia. We wcześniejszych uwagach zawartych w niniejszej publikacji został wyrażony pogląd, że działanie w ramach uprawnień w każdym przypadku będzie wyłączać bezprawność czynu. Jak się jednak wydaje, w zapisie tym chodzi o podkreślenie konieczności uzyskania stosownego zezwolenia określonej władzy dla danego działania, co jest istotą RIPA.

Przestępstwo wymienione w artykule 1 RIPA odpowiada czynowi stypizowanemu w art. 267 polskiego kodeksu karnego, ale RIPA opisuje je dużo szerzej i bardziej szczegółowo. Jest to istotne z punktu widzenia zasady zawężającego interpretowania przepisów karnych i zakazu stosowania analogii. Prawo karne jest instrumentem surowym, stąd jego wszelkie interpretacje winny być ograniczane do minimum. Artykuł 1 ust. 3 RIPA stanowi przykładowo, że naruszenie systemu telekomunikacyjnego polegające na uzyskaniu dostępu do przekazu ogólnie dostępnego nie stanowi przestępstwa („References in this Act to the interception of communication do not include references to the interception of any communication broadcast for general reception"). Polska ustawa karna nie zawierała takiego zapisu, a problem był istotny i wymagał ostatecznie rozstrzygnięcia go przez Sąd Najwyższy, co nastąpiło w orzeczeniu z 22 stycznia 2003 r. (IKZP 43/02): „Działanie sprawcy polegające na bezprawnym podłączeniu odbiornika telewizyjnego do sieci kablowej godzi w prawa majątkowe nadawcy programu, nie wyczerpuje jednak znamion przestępstwa określonego w art. 267 kodeksu karnego".

Przestępstwo nieudzielenia informacji uprawnionemu organowi

Instytucją nieznaną w prawie polskim jest przestępstwo polegające na odmowie udzielenia informacji niejawnej funkcjonariuszowi posiadającemu stosowne zezwolenia

– art. 53 *Ustawy*. Informacje niejawne w ujęciu tego przepisu to informacje chronione w sposób dowolny – poprzez zakodowanie itp. Zgodnie z art. 49 tejże *Ustawy* organem wydającym nakaz udzielenia informacji niejawnych jest sąd, co jest pewnego rodzaju wyjątkiem – zasadą bowiem jest wydawanie zezwoleń przez organ administracyjny. Obowiązek ten obejmuje wydanie kodów, programów deszyfrujących itd., tj. narzędzi umożliwiających dostęp do informacji. Skorelowana z tym rozwiązaniem jest konstrukcja przestępstwa nieujawnienia informacji, przewidziana w art. 53. Jest to niewątpliwie narzędzie użyteczne w pracy operacyjnej.

Konstrukcja kontratypu w RIPA

Jak już zostało powiedziane, legalizacja działań służb brytyjskich polega na udzieleniu zezwolenia określanego jako *authorisation* (bądź *warrant* – w najpoważniejszych przypadkach, typu naruszenie własności) przez określony organ administracyjny.

RIPA określa: po pierwsze metodę działania, po drugie cel, któremu ma ona służyć, oraz po trzecie przyporządkowuje tej metodzie rodzaj uprawnienia (ranga podmiotu dokonującego autoryzacji) nadający takiemu działaniu walor legalności. W pewnym uproszczeniu model ten obrazuje poniższa tabela.

Tabela. Konstrukcja kontratypu w RIPA.

Metoda	Cel	Poziom autoryzacji
Kontrola korespondencji i telekomunikacji – *Interception of communication*	Bezpieczeństwo narodowe, prewencja i wykrywanie poważnych przestępstw (definicja poważnego przestępstwa poniżej tabeli), bezpieczeństwo ekonomiczne Wielkiej Brytanii	*Warrant* udzielony przez sekretarza stanu dla Home Office (w Szkocji – Cabinet Secretary for Justice)
Dane telekomunikacyjne (bilingi) – *Use of communication data*	Bezpieczeństwo narodowe, prewencja i wykrywanie przestępstw, zapobieganie zamieszkom, bezpieczeństwo ekonomiczne Wielkiej Brytanii, bezpieczeństwo publiczne, zapobieganie czynnikom niebezpiecznym dla zdrowia powszechnego, odzyskiwanie należności podatkowych i innych danin publicznych, oraz jeśli czyn może skutkować śmiercią lub rozstrojem zdrowia	urzędnik wysokiej rangi danej instytucji (*senior member of that authority*) – RIPA definiuje to pojęcie w odniesieniu do każdej formacji
Obserwacja (śledzenie osób) – *Directed surveillance*	Bezpieczeństwo narodowe, prewencja i wykrywanie przestępstw, zapobieganie zamieszkom, bezpieczeństwo ekonomiczne Wielkiej Brytanii, bezpieczeństwo publiczne, zapobieganie czynnikom niebezpiecznym dla zdrowia powszechnego, odzyskiwanie należności podatkowych i innych danin publicznych	urzędnik wysokiej rangi danej instytucji (*senior member of that authority*)

Osobowe źródła informacji – *Covert human intelligence sources*	Bezpieczeństwo narodowe, prewencja i wykrywanie przestępstw, zapobieganie zamieszkom, bezpieczeństwo ekonomiczne Wielkiej Brytanii, bezpieczeństwo publiczne, zapobieganie czynnikom niebezpiecznym dla zdrowia powszechnego, odzyskiwanie należności podatkowych i innych danin publicznych	urzędnik wysokiej rangi danej instytucji (*senior member of that authority*)
Inwigilacja – ukryta aparatura rejestrująca dźwięk i obraz oraz możliwość naruszania własności – *Intrusive surveillance*	Bezpieczeństwo narodowe, prewencja i wykrywanie poważnych przestępstw, bezpieczeństwo ekonomiczne Wielkiej Brytanii	sekretarz stanu dla Home Office (w Szkocji – Cabinet Secretary for Justice) (możliwość taką posiadają również liczne służby, w pierwszej kolejności policja, a także formacje o charakterze skarbowym lub policji militarnej, najczęściej na podstawie zgody szefa służby, zatwierdzanej przez Komisarza ds. Inwigilacji).

Źródło: Opracowanie własne autora.

RIPA definiuje pojęcie „poważnego przestępstwa" (*serious crime*): zgodnie z tym dokumentem „poważne przestępstwo" wiąże się z użyciem przemocy bądź skutkuje dużymi stratami finansowymi lub jest popełnione przez wiele osób działających we wspólnym celu albo też jest to przestępstwo, w którego przypadku istnieje duże prawdopodobieństwo, że osoba, które je popełniła, mająca ukończone 21 lat, wcześniej nie karana, zostanie skazana na karę co najmniej 3 lat pozbawienia wolności.

Przestępstwo ujawnienia informacji dotyczącej udzielonej autoryzacji

Ustawa brytyjska w odrębny sposób penalizuje czyn polegający na ujawnieniu danych dotyczących autoryzacji, tj. na jaki okres została wydana, komu, w związku z jaką sprawą itd.

Komisarze

RIPA sankcjonuje istnienie niezależnych, choć działających w ramach administracji, organów nadzorczych, którymi są Komisarz ds. Służb Specjalnych oraz Komisarz ds. Ingerencji Telekomunikacyjnych (*Intellegence Services Commissioner* oraz *Interception of Communications Commissioner*). Statuuje też funkcjonowanie Komisarza ds. Uprawnień Operacyjnych dla Irlandii Północnej (*Investigatory Powers Commissioner for Northern Ireland*) oraz rozszerza zakres kompetencji Głównego Komisarza ds. Inwigilacji (*Chief Surveillance Commissioner*) powołanego na mocy ustawy o Policji z 1997 r. Do zadań tych Komisarzy należy nadzór nad wydawaniem zezwoleń dotyczących stosowania określonych metod. W przypadkach ingerencji sięgających najdalej w sferę praw jednostkowych (np. naruszenie własności) zaś konieczne jest uprzednie wyrażenie zgody przez właściwego Komisarza. Komisarze rokrocznie

składają premierowi sprawozdania, które zawierają podstawę prawną i zakres ich kompetencji, opis wykonanych przez nich czynności – liczbę i datę spotkań z przedstawicielami służb, ich przedmiot, liczbę stwierdzonych uchybień (*errors*), studium poszczególnych przypadków i wreszcie ogólną ocenę funkcjonowania służb. Instytucja Komisarzy odgrywa więc istotną rolę w zapewnieniu ochrony praw jednostki przed nieuzasadnioną ingerencją ze strony państwa.

Trybunał do spraw Operacyjnych

RIPA statuuje też istnienie wyspecjalizowanego organu sądowego właściwego w sprawach skarg na czynności operacyjno-rozpoznawcze, które mogłyby naruszyć prawa jednostkowe, w tym zwłaszcza w sprawach związanych z naruszeniem własności bądź tajemnicy telekomunikacyjnej, tj. Investigatory Powers Tribunal (Trybunał do spraw Operacyjnych). Każdy, kto uzna, że jego prawa zostały naruszone, ma prawo wnieść skargę do tego Trybunału. Komisarze obowiązani są świadczyć pomoc w wyjaśnianiu spraw będących przedmiotem prac Trybunału do spraw Operacyjnych.

Zasady postępowania – *Codes of Practice*

Na mocy RIPA oraz innych ustaw (ustawa o Policji z 1997 r.) są wydawane *Zasady postępowania* (*Codes of Practice*). Zgodnie z nazwą mają one wymiar stricte praktyczny – określają przystępnym językiem, w jakich sytuacjach należy wystąpić o jaki rodzaj autoryzacji i jak rozumieć poszczególne terminy. Tekst jest przeplatany przykładami, które jednak, zgodnie z informacją zamieszczoną na początku, nie mają mocy prawnej. *Zasady postępowania* to zbiór publikacji dotyczących naruszania tajemnicy telekomunikacyjnej, tajemnicy korespondencji, naruszania własności nieruchomości i rzeczy ruchomych, stosowania środków umożliwiających rejestrację obrazów miejsc i zdarzeń itd. Są one skierowane do funkcjonariuszy realizujących uprawnienia operacyjne, ale są powszechnie dostępne, w tym na stronach internetowych. Na marginesie mówiąc, zgodnie z informacjami zamieszczonymi na stronach Home Office ambicją tej instytucji jest bycie najbardziej transparentną strukturą o tym charakterze na świecie.

Niejawne osobowe źródła informacji

RIPA inaczej niż art. 36 ustawy o ABW oraz AW definiuje pojęcie osobowych źródeł informacji. Nie ogranicza się w tym jedynie do osób niebędących funkcjonariuszami, jak czyni to *Ustawa*. Rozwiązuje tym samym problem działania funkcjonariuszy działających pod przykryciem. Zgodnie z art. 26 ust. 8 RIPA niejawnym osobowym źródłem informacji (*covert human intelligence source* – dalej CHIS) jest osoba, która:

a) nawiązuje lub utrzymuje osobiste lub inne relacje z drugą osobą w niejawnym celu określonym w punktach „b" lub „c" poniżej,
b) w sposób niejawny wykorzystuje takie relacje do zdobywania informacji lub umożliwienia dostępu do takich informacji innym osobom,
c) w niejawny sposób przekazuje informacje uzyskane przy wykorzystaniu takich relacji.

Zdobywanie informacji poprzez CHIS wymaga zezwolenia. Ustawodawca brytyjski wychodzi z założenia, że kształtowanie relacji międzyludzkich przez organ państwa

jest daleko posuniętą ingerencją w sferę prywatności, wobec czego dopuszczalne jest jedynie w wyjątkowych okolicznościach poprzez autoryzowanie takich działań. Zezwolenie wydawane jest, co do zasady, na okres 12 miesięcy. W szczególnych przypadkach – korzystanie z pomocy osób nieletnich, „podatnych na zranienie" (chodzi o osoby, którym byłaby przynależna pomoc społeczna w związku z niedomaganiem psychicznym lub fizycznym) – autoryzacja jest wydawana wyjątkowo i jedynie na okres jednego miesiąca.

RIPA przewiduje dwa rodzaje autoryzacji w odniesieniu do CHIS, tj. autoryzację wykorzystania osobowego źródła informacji, która ma znaczenie dla władzy publicznej sięgającej po taki środek (*use of a covert human intelligence source*) oraz autoryzację poszczególnych działań (*conduc tof a covert human intelligence source*), która ma znaczenie dla CHIS, jako akt kontratypizujący określone działania. Autoryzacja działania (*conduct authorisation*) nie musi się przy tym odnosić do każdej czynności. Chodzi tu bardziej o autoryzację działań w określonym celu. CHIS nie może więc być wykorzystywane w każdym celu. Nawiasem mówiąc, w pewnych sytuacjach funkcjonariusze sami mogą autoryzować swoje działania. W takich jednak przypadkach obowiązani są umieścić stosowną notatkę w rejestrze autoryzacji prowadzonym przez każdą z upoważnionych formacji. Tego typu autoryzacje podlegają szczególnemu nadzorowi ze strony Komisarzy.

Ograniczenia w korzystaniu z CHIS

System brytyjski nie zawiera ograniczeń podmiotowych dotyczących funkcjonariuszy państwa, z którymi współpraca jest zabroniona. Katalog taki zawiera natomiast art. 37 ustawy o ABW oraz AW. Zbiór ten jest szeroki i obejmuje przedstawicieli wszystkich trzech władz oraz mediów. Zwłaszcza ta ostatnia kwestia, a mianowicie zakaz tajnej współpracy z dziennikarzami, nastręcza wielu problemów. Czy osoba sporadycznie publikująca teksty w czasopiśmie hobbistycznym jest dziennikarzem, czy nie? Sprawa jest o tyle istotna, że ustawa o ABW oraz AW przewiduje sankcję karną za nieuprawnione podejmowanie tajnej współpracy z dziennikarzami.

Ustawodawstwo brytyjskie idzie w innym kierunku. RIPA kładzie nacisk na ochronę jednostki przed działaniem służb. Przykładowo *The Regulation of Investigatory Powers (Juveniles) Order 2000* – akt prawny wydany przez sekretarza stanu – określa warunki wykorzystania nieletnich CHIS. Zgodnie z nim dozwolone jest korzystanie z pomocy CHIS, które ukończyły 16 rok życia. W wyjątkowych sytuacjach możliwe jest wykorzystanie CHIS poniżej tej granicy. W takim wypadku konieczne jest zapewnienie udziału dorosłego opiekuna w jego spotkaniach z funkcjonariuszem. W odniesieniu do CHIS poniżej 18 roku życia na pierwszy plan wysuwa się kwestia uniknięcia „zranień psychicznych" takiej osoby oraz wyczerpującego przedstawienia różnego rodzaju ryzyka związanego z taką działalnością. Niedopuszczalne jest zdobywanie od CHIS informacji dotyczących jego rodziców i najbliższej rodziny.

Możliwość wykorzystania informacji zdobytych przez CHIS w postępowaniu karnym

RIPA dopuszcza wykorzystywanie informacji zdobytych przez CHIS w postępowaniu karnym, wprowadzając przy tym jednak wiele ograniczeń. Będą one dotyczyły np. informacji uzyskanych od nieletnich CHIS czy poufnych materiałów

dziennikarskich. Szeroki opis „wrażliwych" informacji wyłączonych z wykorzystania w procesie karnym zawiera rozdział 4 *Zasad postępowania* dotyczący niejawnej inwigilacji i naruszeń własności (*Codes of Practice – Covert Surveilance and Property Interference*).

Działanie pod przykryciem

Wracając zaś do funkcjonariuszy działających pod przykryciem, należy zaznaczyć, że zarówno sam ich udział w grupie przestępczej, jak i możliwość dokonywania przez nich określonych działań są legalizowane poprzez kombinacje autoryzacji ich wykorzystania (*use*) i działania (*conduct*) w określonych kierunkach.

Kontratyp cywilny

RIPA wyłącza odpowiedzialność cywilną CHIS za szkody będące przypadkową konsekwencją ich działania na podstawie wydanej autoryzacji lub innego działania zgodnego z prawem.

Luki w systemie

Prawo brytyjskie reguluje kwestie dotyczące pracy operacyjnej znacznie obszerniej i bardziej wyczerpująco niż legislacja polska. Pomimo to, co jakiś czas są podnoszone postulaty na temat dopracowywania systemu. Jako ciekawostkę można przytoczyć sprawę Marka Kennedy'ego, funkcjonariusza Metropolitan Police, działającego przez wiele lat pod przykryciem w środowisku ekologów – ekstremistów, których działania nierzadko miały charakter przestępczy. Kennedy wszedł w to środowisko i głęboko je rozpracowywał, często utrzymując zażyłe kontakty z wieloma działaczami. Mając żonę i dwoje dzieci, żył na przykład w bliskim związku z jedną z aktywistek tego środowiska (według niektórych miał zresztą wiele romansów). Wreszcie wraz z kilkudziesięcioma innymi osobami został podczas jednej z akcji aresztowany i zdekonspirowany (pozostali uczestnicy zdarzenia chcieli wspólnie skorzystać z usług jednego adwokata, a tylko Kennedy domagał się innego prawnika. To wzbudziło podejrzenia grupy). Po różnych perypetiach odmówił jednak składania zeznań na niekorzyść ekologów. Sprawa odbiła się szerokim echem nie tylko w Wielkiej Brytanii. Również w Polsce ukazało się kilka artykułów prasowych na ten temat. Ich mottem przewodnim było pytanie o aspekt moralny i legalność takiego postępowania. Działanie Kennedy'ego było przedmiotem raportu Głównego Komisarza ds. Inwigilacji, który badał, czy i jakich autoryzacji mu udzielono i czy jego działanie mieściło się w ich zakresie.

Sprawa okazała się jednak bardziej kłopotliwa. Kennedy pozwał Metropolitan Police o to, że ta, będąc obowiązana do opieki nad CHIS, nie zapobiegła jego zaangażowaniu się w głęboki związek uczuciowy z jedną z aktywistek – przełożeni akceptowali fakt utrzymywania przez niego intymnych relacji. Po ujawnieniu szczegółów jego działalności rozpadło się jego małżeństwo, a on sam utracił cześć i dobre imię. Na fali doniesień prasowych do Metropolitan Police wpłynęły kolejne pozwy, tym razem od kobiet, które twierdziły, że oficerowie działający pod przykryciem utrzymywali z nimi długie i w efekcie wyniszczające je psychicznie intymne stosunki. Jedna ze spraw okazała się szczególnie bulwersująca, ponieważ w wyniku takich relacji jedna z aktywistek zaszła w ciążę, po czym ojciec dziecka zniknął z jej życia. Na podstawie znanych jej danych

osobowych tego mężczyzny dotarła do jego, jak sądziła, rodziny. Wówczas okazało się, że Metropolitan Police, budując legendę dla swoich funkcjonariuszy, wykorzystała dane zmarłych dzieci. W wyniku tych incydentów obecnie są podnoszone postulaty dotyczące zmiany prawa regulującego działanie funkcjonariuszy pod przykryciem, w celu uniknięcia podobnych sytuacji. Dnia 1 marca 2013 r. w „The Guardian" ukazał się artykuł autorstwa Roba Evansa i Paula Lewisa pod tytułem: *Konieczne nowe prawo dla policji pod przykryciem – Metropolitan Police* (*New law needed for undercover police – MPs*).

Pozwy wniesione w sprawach podobnych do wyżej opisanych są badane przez Trybunał ds. Operacyjnych.

Różnice między legislacją polską a brytyjską

Różnice między legislacją polską a brytyjską w zakresie stosowania poszczególnych metod operacyjnych (oprócz różnic przedstawionych powyżej) przedstawiają się następująco:

1. Zasadą RIPA jest autoryzowanie działań przez organ administracji. Ustawa brytyjska nie przewiduje (poza wydawaniem nakazu ujawnienia informacji) wydawania zezwolenia przez niezawisły sąd bądź prokuratora. Na pierwszy rzut oka może się zdawać, że model polski zabezpiecza prawa jednostki w sposób pełniejszy. RIPA wymaga jednak autoryzacji dla zdecydowanie większej liczby działań, nadzór prowadzony w trybie administracyjnym zaś pozwala na bieżąco modyfikować bądź cofać autoryzacje w razie ustania takiej potrzeby. A należy pamiętać, że każde działanie operacyjne jest związane z naruszaniem praw jednostkowych. Ingerencja w te sfery powinna ograniczać się do niezbędnego minimum. Niezawisły sąd czy prokurator mają mniejsze możliwości prowadzenia bieżącego nadzoru nad faktycznym wykorzystaniem danego instrumentu.
2. Obserwowanie i rejestrowanie obrazu i dźwięku zdarzeń w miejscach publicznych jest w polskim i brytyjskim porządkach prawnych uregulowane ustawowo. Przepisy brytyjskie jednak oprócz zdefiniowania podmiotu uprawnionego do podejmowania decyzji w tym zakresie szczegółowo określają w *Code of Practice*, jakie miejsca należy uznać za publiczne. Będą to np. klatki schodowe. W przypadku jednak, gdy w takim miejscu zamieszka bez tytułu prawnego jakakolwiek osoba (np. bezdomny), to miejsce takie staje się pomieszczeniem prywatnym i umieszczenie tam aparatury rejestrującej obraz i dźwięk wymaga już uzyskania stosownego zezwolenia.
3. RIPA reguluje kwestie związane z wykorzystaniem dodatkowych informacji uzyskanych w trakcie prowadzenia czynności operacyjnych w postępowaniach sądowych i innych.
4. Istotną różnicą między legislacją polską a brytyjską jest możliwość naruszania własności (bądź ograniczonych praw rzeczowych – najem, posiadanie, użytkowanie rzeczy) nieruchomości i ruchomości w trakcie prowadzenia czynności operacyjno-rozpoznawczych. Ustawa o ABW oraz AW nie przewiduje takiej możliwości. Tym samym brak jest ustawowego kontratypu dla przestępstwa określonego w art. 193 kk („Kto wdziera się do cudzego mieszkania, lokalu, pomieszczenia albo ogrodzonego terenu albo wbrew żądaniu uprawnionej osoby miejsca takiego nie opuszcza podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku") oraz dla przepisów karnych chroniących mienie. Brak takiej regulacji często uniemożliwia wykonanie postanowienia sądowego dotyczącego zgody na

zastosowanie kontroli operacyjnej, co jest przecież ważnym instrumentem walki z przestępczością. Trzeba tu podkreślić, że *Codes of Practice* reguluje tę materię bardzo szczegółowo. Przykładowo, zdjęcie odcisków palców z telefonu publicznego nie wymaga autoryzacji. Pozyskanie telefonu prywatnego w tym celu zaś wymaga już jednak stosownej zgody. Naruszenie nieruchomości wymaga *warrantu*, ale w razie ryzyka zdekonspirowania obserwacji jest możliwe chwilowe naruszenie nieruchomości sąsiedzkiej bez autoryzacji.

5. RIPA definiuje jako niejawne osobowe źródła informacji zarówno funkcjonariuszy działających pod przykryciem, jak i osoby niebędące funkcjonariuszami. Działanie obu tych kategorii źródeł wymaga autoryzacji. RIPA narzuca ograniczenia w zakresie korzystania z CHIS będących osobami niepełnoletnimi lub ułomnymi. Przewiduje też wprost możliwość wykorzystania w procesie karnym informacji i materiałów uzyskanych przez CHIS z określonymi wyjątkami. Ustawa o ABW oraz AW nie określa procedury autoryzacji wykorzystania osobowych źródeł informacji, tak w zakresie samej współpracy, jak i w zakresie poszczególnych działań.
6. Artykuł 37 ustawy o ABW oraz AW jest jedynym ograniczeniem dotyczącym podmiotów współpracujących ze służbami. Zawiera on szeroki katalog osób, z którymi podejmowanie współpracy jest zabronione z uwagi na ochronę państwa przed wpływem służb. Ustawa brytyjska nie zawiera takich ograniczeń, kładzie natomiast nacisk na ochronę jednostki.

Wnioski końcowe

1. Przepisy art. 32 oraz art. 35 ust. 6 *Ustawy* winny zostać usunięte. Ustęp 2 w art. 35 powinien otrzymać brzmienie: „Przy wykonywaniu czynności operacyjno-rozpoznawczych funkcjonariusze Agencji mogą **sporządzać** dokumenty, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza oraz środków, którymi posługuje się przy wykonywaniu zadań służbowych, i posługiwać się nimi".
2. *Ustawa* powinna regulować działania pod przykryciem poprzez szersze zdefiniowanie osobowego źródła informacji bądź poprzez dopuszczenie expressis verbis prowadzenia pozorowanej działalności przestępczej w celu realizacji zadań ustawowych służb. Przy tej okazji należałoby wprowadzić instytucję kontratypu cywilnego.
3. *Ustawa* powinna szczegółowo określać sposób postępowania z wszelkimi materiałami uzyskanymi w trakcie działań operacyjno-rozpoznawczych (a nie tylko zgromadzonymi podczas kontroli operacyjnej) tak w procesie karnym dotyczącym danego zagadnienia, jak i w innych działaniach procesowych i operacyjnych.
4. Zasadne wydaje się wskazanie w *Ustawie* podmiotów wydających zgodę na podjęcie określonych działań (np. że na działanie pod przykryciem zgodę wydaje szef służby, na prowadzenie obserwacji – szef bądź upoważniony przez niego kierownik jednostki organizacyjnej itd.).
5. *Ustawa* powinna przewidywać możliwość naruszania własności (bądź ograniczonego prawa rzeczowego) w celu realizacji kontroli operacyjnej oraz w innych celach (np. pobranie odcisków palców). Przepis taki winien być skonstruowany podobnie do regulacji dotyczącej kontroli operacyjnej. W sytuacji zagrożenia poważnymi przestępstwami zgodę na naruszenie własności powinien wydawać sąd (lub inny organ, np. minister spraw wewnętrznych lub minister koordynator).
6. Kodeks karny dzieli przestępstwa na występki i zbrodnie. Można więc przyjąć, że naruszenie, o którym mowa wyżej, jest możliwe tylko w przypadku zbrodni.

Powinien to być jednak instrument ostateczny – zgoda byłaby udzielana tylko w sytuacji, gdyby określonego celu nie można było osiągnąć inaczej. Pewną odrębność musiałby jednak zachować wywiad. Naruszenie własności poza granicami kraju powinno być autoryzowane przez szefa służby.

7. Duże znaczenie miałoby opracowanie dokumentów na wzór *Codes of Practice*, które szczegółowo przedstawiałyby praktyczne rozumienie pojęć i procedur ustawowych, a przy tym miałyby charakter aktu prawnego. Regulacje dotyczące uprawnień operacyjnych powinny być zrozumiałe przede wszystkim dla funkcjonariuszy wykonujących przepisy, ale także dla reszty obywateli.

Przedstawiona problematyka ma znaczenie fundamentalne. Prawidłowe określenie sfery działań funkcjonariuszy to z jednej strony gwarancja ich bezpieczeństwa określona przepisami karnymi, z drugiej zaś gwarancja ochrony praw jednostki. Służby realizujące zadania z zakresu bezpieczeństwa powinny być wyposażone w instrumentarium odpowiednie do znaczenia takich zadań. Jako przykład szerokich uprawnień przy jednoczesnym zapewnieniu transparentnej i głębokiej (choć w pewnych aspektach niepełnej) kontroli nad służbami może posłużyć model brytyjski.

Sprawa ma dodatkowe znaczenie w świetle toczących się aktualnie dyskusji nad wprowadzeniem regulacji dyskwalifikującej możliwość wykorzystania w procesie karnym dowodów pozyskanych w wyniku czynu zabronionego (tzw. owoce trującego drzewa – *fruits of poisoneous tree*). W judykaturze amerykańskiej przykładem takich praktyk jest nieuprawnione przeszukanie pomieszczeń, w którego trakcie uzyskano dowód popełnienia przestępstwa. Dowód taki, podobnie jak i dowody pochodne – „trujące drzewo" i jego „owoce" – nie będą brane pod uwagę w postępowaniu sądowym. Prace nad nowelizacją są w toku i trudno wyrokować, jak materia ta zostanie ostatecznie uregulowana. Niemniej jednak przy niniejszych rozważaniach kwestii tej nie można tracić z pola widzenia.

Abstrakt

Artykuł ma postać felietonu prawniczego. Jako cel stawia sobie zrozumiałe zaprezentowanie uprawnień ABW i MI5 jako kontratypu, czyli okoliczności wyłączających odpowiedzialność karną za działania noszące formalne znamiona przestępstwa. Większość metod pracy operacyjnej, których istotę można ująć jako podstępne doprowadzanie do wszczęcia postępowania karnego, oraz metod pracy śledczej, takich jak zatrzymanie, stosowanie środków przymusu bezpośredniego itd., to działania wypełniające formalne znamiona przestępstwa. Rodzi się wobec tego pytanie, jakie przepisy bądź konstrukcje prawne przywracają legalność takich działań funkcjonariuszy. Analiza tego typu konstrukcji zawartych w ustawie o ABW oraz AW stanowi pierwszą część artykułu.

W części drugiej artykuł przedstawia uregulowania dotyczące czynności operacyjno-rozpoznawczych w legislacji brytyjskiej, koncentrując się przy tym na przepisach zawartych w *Regulation of Investigatory Powers Act 2000*, ustawy będącej podstawą pracy operacyjnej wielu brytyjskich służb, między innymi MI5. Model brytyjski opiera się na autoryzacji określonych działań przez określone podmioty. Tak więc uzyskanie stosownego zezwolenia będzie okolicznością przywracającą legalność działaniu noszącemu formalne znamiona przestępstwa.

W artykule zanalizowano również zakres uprawnień służb brytyjskich i sposób ich nadzorowania. Wskazano, że istotną rolę w zakresie nadzoru pełnią tu Komisarze:

do spraw Służb, Inwigilacji oraz Naruszeń Komunikacyjnych. W systemie brytyjskim funkcjonuje wreszcie wyspecjalizowany organ sądowy, którego zadaniem jest rozpatrywanie skarg osób uważających, że ich prawa jednostkowe zostały poprzez działania służb naruszone. Uprawnienia służb brytyjskich są zdecydowanie szersze niż uprawnienia służb polskich, ale jednocześnie są zrównoważone ich pełnym i transparentnym nadzorowaniem.

Na koniec porównano legislację polską i brytyjską oraz postawiono wnioski *de lege ferenda*.

Abstract

The aim of the article is to analyze the powers of special services from the point of view of the penal law. The article presents a view that most operational work methods that might be referred to as deceitful attempts to launch criminal proceedings, as well as most investigative methods, such as arrest, use of coercive measures, etc., are activities that fit the definition of a crime. This raises a question about the provisions of law or legal measures that would reestablish the legitimacy of such activities performed by officers. The first section of the article offers an analysis of such provisions contained in the Act on ABW and AW.

The second section of the article provides an overview of regulations on surveillance and investigation operations in the British law based on the provisions of the Regulation of Investigatory Powers Act 2000. The Act is the basis for operation of many British services, including MI5. The analysis of the regulations shows that the British model is based on the authorization of specific operational activities carried out by specific bodies. Authorization of specific activities makes those actions that formally fit the definition of a crime legitimate.

The author also examines the scope of powers granted to British services and how they are controlled. The analysis indicates that Commissioner play an important role in the supervision. There are commissioners responsible for the affairs of the service, surveillance, and communications violations. The British system includes a judicial court unit that is responsible for examining complaints of persons who believe that activities taken by services infringed upon their rights. The powers of British services are much more extensive than the powers of Polish services. However, they are subject to comprehensive and transparent control system.

The last section of the article contains a comparison of the Polish and English legislation and conclusions *de lege ferenda*.