Justyna Strużewska-Smirnow
Mateusz Wieczerza

Ustawowe uprawnienia operacyjno-rozpoznawcze i dochodzeniowo-śledcze służb specjalnych w zakresie wykrywania zagrożeń bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych z perspektywy międzynarodowej

I. REPUBLIKA FEDERALNA NIEMIEC

W ramach uprawnień operacyjno-rozpoznawczych i dochodzeniowo-śledczych realizowanych w celu wykrywania zagrożeń bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych, przeprowadzanych przez niemieckie służby policyjne i informacyjne, należy wymienić następujące instrumenty monitoringu:

- bezpośrednią kontrolę telekomunikacji, tzw. źródła kontroli telekomunikacyjnej,
- przeszukanie online (niem. *Online Durchsuchung*), które umożliwia śledczym dostęp do całościowych systemów komputerowych. To rozwiązanie pozwala na włamanie się za pomocą środków technicznych do systemu informacyjno-technicznego, na przykład do sieci komputerowej lub pojedynczego urządzenia, które są w użytkowaniu osoby podejrzanej, bez jej wiedzy[1]. W tym wypadku komputery mogą być sprawdzone jeden raz (przejrzenie – niem. *Online-Durchsicht*) lub sprawdzone, czy też nadzorowane w jakimś określonym czasie (niem. *Online -Überwachung*), bez wiedzy użytkownika[2].

Zasadniczą różnicą w przypadku obuwymienionych metod jest zasięg gromadzenia danych. W przypadku przeszukania online można – również bez wiedzy osoby zainteresowanej – pozyskać pozostałe dane znajdujące się w komputerze, które wykraczają poza bieżącą komunikację[3].

Najbardziej spektakularnym osiągnięciem tego rozwiązania jest możliwość monitorowania usług programów typu Messenger, takich jak WhatsApp, przed lub po ich zaszyfrowaniu[4]. Służy temu zainstalowanie określonego typu oprogramowania trojańskiego[5]. Takie

[1] www.fr.de/kultur/netz-tv-kritik-medien/netz/neues-gesetz-whatsapp-ueberwachung-durch-die-hintertuer-a-1300626 [dostęp: 22 VI 2017].

[2] www.tagesschau.de/inland/faqtrojaner100.html [dostęp: 12 X 2011].

[3] www.wiwo.de/technologie/digitale-welt/whatsapp-was-die-ueberwachung-der-messenger-bedeutet/19972834.html [dostęp: 29 VI 2017].

[4] W tym celu musi zostać zainstalowany i będzie używany program monitorowania telekomunikacji źródłowej (również monitorowanie telekomunikacji na komputerze przed jej zaszyfrowaniem), podczas gdy przy klasycznym monitorowaniu telekomunikacji treść pozostaje zaszyfrowana.

[5] Oprogramowanie trojańskie (tzw. trojan) to program przeprowadzający określone funkcje na komputerze w sposób niejawny lub jako program użytkowy w zakamuflowanej formie, na które użytkownik nie wyraził zgody i ich nie kontroluje. Sam trojan nie musi być szkodliwy. Zwykle współdziała z innym wrogim oprogramowaniem lub umożliwia takiemu oprogramowaniu dostać się do komputera. Nie należy utożsamiać trojana z wirusem komputerowym, wirus bowiem usiłuje się rozprzestrzenić na coraz większą liczbę plików i na cały komputer, a ponadto wirus stara się sam siebie kopiować. Trojan sam się nie kopiuje, ale może zostać połączony z wirusem. Zob. także: www.fr.de/kultur/netz-tv-kritik-medien/netz/neues-gesetz-whatsapp-ueberwachung

działanie może być podjęte za zgodą sądu w celu czynnej obrony lub zbierania informacji wywiadowczych i tym różni się od kontroli telekomunikacji, że nie dotyczy spraw związanych z przesyłem danych, ale z bieżącą komunikacją osoby docelowej, która jest monitorowana przez oprogramowanie szpiegowskie bezpośrednio na urządzeniu końcowym (komputer, telefon komórkowy). To rozwiązanie umożliwia ominięcie szyfrowania transferu danych[6].

Jak już wspomniano, opisywana metoda wymaga zainstalowania szkodliwego oprogramowania zwanego oprogramowaniem trojańskim. W języku potocznym jest ono określane mianem „trojana publicznego" („*Staatstrojaner*", „*Bundestrojaner*"), w branży IT natomiast pojawiają się także inne określenia, m.in. „*Schadsoftware*" (szkodliwe oprogramowanie) lub „*Govware*" (od angielskiego słowa *government* – rząd[7])[8]. Działanie tego specyficznego oprogramowania trojańskiego jest związane z wykorzystaniem urządzenia rejestrującego pracę na komputerze (tzw. Keylogger, który umożliwia śledzenie pracy na klawiaturze i w ten sposób uzyskiwanie np. haseł do skrzynek poczty elektronicznej). Na ogół to narzędzie występuje w wersji programowej, rzadziej w sprzętowej, która musi być zamontowana bezpośrednio na komputerze podejrzanego[9].

Trojan wypełnia rozkazy, które są przekazywane z innego komputera. Te komendy w sposób niezaszyfrowany są wysyłane do programu. Nadawca nie musi ich uwierzytelniać. W ten sposób powstaje pewna luka trybu bezpieczeństwa, gdyż zainfekowany trojanami komputer może zostać przejęty przez osoby trzecie, które mogą wgrać wrogie oprogramowanie[10]. Trojan znajduje się pomiędzy nadawcą a adresatem (w branży IT jest spotykane określenie „*Man in the Middle*").

Przemycanie trojanów na prywatne komputery może być skutkiem załadowania pliku (np. zdjęć, tekstu lub aktualizacji), odwiedzin na zainfekowanej stronie lub otwarcia zmanipulowanego załącznika do maila. Należy zaznaczyć, że jedyną możliwością obrony przed takim atakiem jest korzystanie z komputera, który nie jest podłączony do Internetu. Oprogramowanie typy „*firewall*" oraz programy antywirusowe znajdują przede wszystkim wirusy i wrogie oprogramowanie, które już jest im znane lub które mają typowe sposoby działania, potrzebują zatem uaktualnianych list wirusów. Z uwagi na to, że trojany są „produkcją jednostkową", istnieją niewielkie szanse na ich wykrycie[11].

Organy śledcze mają uprawnienie do niejawnego przegrywania wrogiego oprogramowania na prywatne komputery, laptopy, telefony komórkowe i tablety w celu odczytywania bezpośrednio u źródła, w czasie rzeczywistym, bieżącej komunikacji. Istnieje również możliwość odczytania całego twardego dysku[12]. W ocenie niemieckich prawników kontrowersyjne jest zagadnienie, czy przeszukanie online jest przeszukaniem w prawnym sensie tego słowa oraz w jakim stopniu odpowiada przeszukaniu mieszkania lub domu (tym samym spełniając konstytucyjny wymóg ustawowego uprawnienia do interwencji w podstawowe prawo do mieszkania, np. zgodnie z niemieckim Kodeksem postępowania karnego – Strafprozessordnung)[13].

-durch-die-hintertuer-a-1300626 [dostęp: 22 VI 2017].

[6] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

[7] Taki skrót wskazuje, że przeszukanie online odbywa się na polecenie rządu.

[8] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VII 2017].

[9] www.tagesschau.de/inland/faqtrojaner100.html [dostęp: 12 X 2011].

[10] www.tagesschau.de/inland/faqtrojaner100.html [dostęp:12 X 2011].

[11] www.tagesschau.de/inland/faqtrojaner100.html [dostęp:12 X 2011].

[12] https://deutsche-wirtschafts-nachrichten.de/2017/06/22/bundestag-will-heimlich-weitreichende-ueberwachung-beschliessen/ [dostęp:22 VI 2017].

[13] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

Istotne znaczenie dla opisanych powyżej zastrzeżeń miał wyrok Federalnego Trybunału Sprawiedliwości (Bundesgerichtshof – BGH) z 31 stycznia 2007 r., który podważył dokonywane przez policję przeszukania online ze względu na brak właściwych przepisów prawnych w niemieckim Kodeksie postępowania karnego. Trybunał nie znalazł podstaw do autoryzacji takich działań w § 102[14] oraz § 105[15] kpk. Te paragrafy, w ocenie Trybunału, nie są podstawą do przeprowadzenia takich działań w przypadku braku zezwolenia. Zgodnie z argumentacją Trybunału niejawność przeszukania online nie odpowiada systematyce otwartych przeszukiwań, dla których podstawę stanowi Kodeks postępowania karnego[16].

Federalny Trybunał Sprawiedliwości odrzucił także § 100a[17] niemieckiego kpk jako podstawę prawną do przeszukania online, argumentując, że przy przeszukaniu online (zachowywaniu danych z komputera lub bieżącym śledzeniu pracy osoby podejrzanej) nie dochodzi do monitorowania telekomunikacji, a więc przepływu komunikacyjnego podejrzanego z osobą trzecią. Co istotne – wyrok Trybunału nie dotyczył jednak metod wykorzystywanych przez służby specjalne, których działania są uprawnione na podstawie ustaw. Zgodnie ze stanowiskiem Rządu Federalnego podstawą prawną jest w tym wypadku np. zarządzenie organu stosującego dany środek operacyjno-rozpoznawczy[18].

Doniesienia pojawiające się w niemieckich mediach potwierdzają, że niemieckie służby specjalne, m.in. Federalny Urząd Ochrony Konstytucji (Bundesamt fur Verfassungsschutz – BFV) oraz Federalna Służba Wywiadowcza (Bundesnachrichtendienst – BND) wykorzystują opisane powyżej metody w celu wykonywania ustawowych zadań. Prawdopodobnie początki stosowania wrogich technik teleinformatycznych na potrzeby ochrony bezpieczeństwa państwa sięgają 2005 r.[19] Chociaż służy specjalne nie upubliczniają danych liczbowych związanych ze stosowaniem opisanych powyżej metod, w 2009 r. w mediach niemieckich pojawiła się informacja, że w 2008 r. BND dokonała przeszukania online poza granicami Republiki Federalnej Niemiec przynajmniej

[14] § 102 – „W przypadku osoby podejrzanej o popełnienie przestępstwa lub uczestnika przestępstwa lub zbierania danych, udzielania pomocy sprawcy, utrudniania postępowania karnego lub paserstwa może być przeprowadzone przeszukanie mieszkania i innych pomieszczeń jak również osoby oraz należących do niej rzeczy zarówno w celu zajęcia jak również po tym fakcie, jeżeli zachodzą powody do przypuszczenia, że przeszukanie doprowadzi do odkrycia dowodów" (wszystkie tłum. aut.), https://www.gesetze-im-internet.de/stpo/_102.html [dostęp: 17 VIII 2017].

[15] § 105 ust. 1 – „Przeszukanie może być nakazane tylko przez sędziego, w nagłych przypadkach także przez prokuraturę i śledczych (zgodnie z § 152 ustawy o Sądzie Apelacyjnym). Sędziowie zarządzają przeszukania zgodnie z § 103 ust. 1 zdanie 2. prokuratura jest do tego uprawniona w nagłych wypadkach", https://www.gesetze-im-internet.de/stpo/_105.html [dostęp: 21 VIII 2017].

[16] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

[17] § 100a ust. 1 – „Telekomunikacja może być również monitorowana i rejestrowana bez wiedzy zainteresowanych osób jeżeli:

1) niektóre okoliczności faktyczne uzasadniają podejrzenie, że ktoś jako sprawca lub uczestnik popełnił poważne przestępstwo, o którym mowa w ust. 2, w przypadkach w których karane jest usiłowanie lub przygotowania do przestępstwa poprzez popełnienie przestępstwa,
2) czyn ten jest poważny również w indywidualnych przypadkach,
3) badanie faktów lub określenie miejsca pobytu oskarżonego w inny sposób byłoby znacznie trudniejsze lub daremne", https://www.gesetze-im-internet.de/stpo/__100a.html [dostęp: 21 VIII 2017].

[18] https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland)#cite_note-5 [dostęp: 17 VIII 2017].

[19] W marcu 2005 r. ówczesny Federalny Minister Spraw Wewnętrznych Otto Schily (Socjaldemokratyczna Partia Niemiec, Sozialdemokratische Partei Deutschlands – SPD) został poproszony przez Prezydenta Federalnego Urzędu Ochrony Konstytucji Heinza Fromma o opracowanie metody niejawnego szpiegowania komputerów osób podejrzanych. Według Petera Altmeiera (Unia Chrześcijańsko-Demokratyczna, Christlich Demokratische Union – CDU) parlamentarnego Sekretarza Stanu w MSW od 2005 r. było możliwe dokonywanie przeszukania online. Parlamentarna Komisja Kontrolna została o tym poinformowana w lipcu 2005 r. https://de.wikipedia.org/wiki/Online-Durchsuchung_(Deutschland) [dostęp:17 VIII 2017].

2500 razy. Działania obejmowały zarówno kopiowanie zawartości twardych dysków, jak i montowanie urządzenia Keylogger[20].

Zgodnie z wynikami audytu wewnętrznego w BND przedstawionymi Parlamentarnej Komisji Kontrolnej przez ówczesnego koordynatora służb specjalnych Klausa Dietera Fritschego, BND śledziła m.in. ruch pocztowy pomiędzy afgańskim ministrem Aminem Farhangiem a dziennikarzem tygodnika „ Der Spiegel". Celem działań BND był też pakistański naukowiec atomowy Abdul Quadir Khan oraz sieci komputerowe w Iraku. Śledzono również ruch poczty elektronicznej biura w Afganistanie prowadzonego przez organizację Welthungerhilfe[21].

Ta informacja ponownie wywołała polityczną dyskusję dotyczącą podstaw prawnych takich działań. Była nią bowiem zgoda wydana przez szefa BND. Po ujawnieniu tych informacji eksperci z koalicji rządowej, a także politycy opozycyjni zażądali regulacji ustawowych w tej materii. Ówczesny przewodniczący Parlamentarnej Komisji Kontrolnej Max Stadler (Wolna Partia Demokratyczna, *Freie Demokratische Partei* – FDP) stwierdził, że standardy państwa prawa w tym zakresie powinny być na nowo zdefiniowane w ustawie. Pojawiły się stwierdzenia, że przeszukanie online powinno być stosowane wyłącznie zgodnie z zasadą proporcjonalności, kontrolę zaś nad tymi działaniami powinien sprawować urzędnik mający kompetencje urzędu sądowego. Ogólne pełnomocnictwo ustawowe, na które – zgodnie z przytoczonym wcześniej stanowiskiem Rządu Federalnego – powoływało się BND, nie pozostawiało miejsca na debatę, od czasu wyroku Trybunału Konstytucyjnego w 2007 r.[22]

Federalny Sąd Konstytucyjny ponownie wypowiedział się w sprawie przeszukania online w wyroku z 27 lutego 2008 r. Dopuścił w nim takie działanie w odniesieniu do ochrony dóbr konstytucyjnych tylko pod ściśle określonymi warunkami, tj.: musi istnieć konkretne zagrożenie dla dobra prawnie chronionego, przesłanką może być np.: zabójstwo, atak terrorystyczny lub przetrzymywanie zakładników. Ponadto muszą zostać spełnione także wymogi formalne: wymagana jest zgodna sądu, zagwarantowana musi zostać również szczególna ochrona danych osobowych i integralność systemów informacyjno-technicznych[23].

Wyrok Sądu wpłynął na kształt nowelizacji ustawy o Federalnej Policji Kryminalnej (Bundeskriminalamt – BKA), nad którą prace odbywały się w 2008 r. Federalna Policja Kryminalna otrzymała kolejne uprawnienia, m.in. w treści ustawy zostały uregulowane również kontrowersyjne przeszukania online, jednak – jak wszystkie uprawnienia BKA charakteryzujące się wysokim stopniem ingerencji – podlegają one kontroli sądowej. Nowe przepisy weszły w życie 1 stycznia 2009 r., jednak już 27 stycznia 2009 r. ustawa została zaskarżona do Federalnego Sądu Konstytucyjnego[24]. Wyrokiem z 20 kwietnia

[20] www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html [dostęp: 7 III 2009].

[21] Niemiecka organizacja pozarządowa zajmująca się zwalczaniem głodu na świecie. Informację na ten temat zob. www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html [dostęp: 7 III 2009].

[22] www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html [dostęp: 7 III 2009].

[23] www.tagesschau.de/inland/faqtrojaner100.html [dostęp: 12 X 2011].

[24] Nowelizacja ustawy o BKA w 2008 r. była przedmiotem szerokiej dyskusji społecznej, podnoszono m.in. że przez dodanie nowych uprawnień BKA, zarezerwowanych dotychczas dla służb specjalnych, narusza się zasadę separacji tajnych służb od policji. Rząd federalny i władze policyjne uzasadniały natomiast konieczność wprowadzenia nowych metod walki ze szczególnie poważną przestępczością, w związku z korzystaniem przez przestępców z zaawansowanych technik. Podczas wysłuchania przed Komitetem Wewnętrznym Bundestagu, ówczesny prezydent Federalnego Urzędu Policji Kryminalnej stwierdził, że przeszukania online są nieodzownym instrumentem

2016 r. ustawa została uznana za niekonstytucyjną. Sąd sformułował także wiele wytycznych dotyczących przyszłej regulacji związanych z ingerencją w podstawowe prawo do samostanowienia informacyjnego[25], m.in. zakaz prowadzenia stałego monitorowania w ramach przeszukania online oraz zapewnienie szczególnej ochrony osobom wykonującym zawody zaufania publicznego, takim jak np. adwokaci lub lekarze[26].

Stosowne zmiany w niemieckim ustawodawstwie zostały wprowadzone w 2017 r. W dniu 22 czerwca 2017 r.[27] w Bundestagu uchwalono dwie ustawy, które umożliwiają Federalnej Policji Kryminalnej dokonywanie przeszukań online w celu zwalczania najcięższych przestępstw[28], tj. terroryzmu, prania pieniędzy, korupcji osób zajmujących wysokie stanowiska, pornografii dziecięcej, zabójstw oraz przestępczości zorganizowanej, a także wprowadzają odpowiednie zmiany w niemieckim procesie karnym.

Podstawę prawną przeszukania online jest § 20k ustawy z 7 lipca 1997 r. o Federalnej Policji Kryminalnej oraz współpracy pomiędzy Federacją i krajami związkowymi w sprawach karnych (*Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*) dotyczący ukrytej interwencji w systemach technologii informacyjnych. Zgodnie z § 20k ust. 1:

Federalna Policja Kryminalna może bez wiedzy osoby zainteresowanej interweniować w środki techniczne w systemach informatycznych wykorzystywanych przez tę osobę oraz pozyskiwać z nich dane, jeśli określone fakty uzasadniają przypuszczenie, że istnieje niebezpieczeństwo:

1) dla nietykalności cielesnej, życia lub wolności osoby,
2) dla dóbr powszechnych, których zagrożenie narusza podstawy lub istnienie państwa lub narusza podstawy egzystencji społecznej.

Zastosowanie środków, o których mowa w zdaniu 1, jest również dopuszczalne, jeżeli z wystarczającym prawdopodobieństwem nie daje się ustalić, że bez zastosowania tych środków w niedalekiej przyszłości wystąpi szkoda, pod warunkiem, że określone fakty odnoszą się do określonego przypadku stwarzania przez osobę zagrożenia dla dóbr wskazanych w zdaniu pierwszym. Te środki mogą być wdrożone tylko, gdy jest to konieczne do wykonania zadań, o których mowa w § 4a[29] (ustawy o BKA), a w przeciw-

zapobiegania atakom terrorystycznym https://de.wikipedia.org/wiki/Bundeskriminalamtgesetz [dostęp: 7 IX 2017].

[25] Jest to prawo jednostki do decydowania o udzielaniu i wykorzystaniu danych jej dotyczących.

[26] https://de.wikipedia.org/wiki/Bundeskriminalamtgesetz [dostęp: 7 IX 2017].

[27] https//ddiv.de/download/CY4a139399X15cd3c8b94dX4b0f/Plenarprotokoll 18-240_22.06.2017.pdf [dostęp: 26 VI 2017].

[28] Ustawa z 22 czerwca 2017 r. dotycząca skutecznego i dostosowanego do praktyki wytaczania postępowania karnego (*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*) oraz ustawa z 22 czerwca 2017 r. o zmianach Kodeksu karnego, ustawy o sądach dla nieletnich, Kodeksu postępowania karnego oraz innych ustaw (*Gesetz zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze*).

[29] § 4a ust. 1 – "BKA może wykonywać zadania z zakresu obrony przeciwko międzynarodowemu terroryzmowi, w przypadkach gdy:

1) zachodzi niebezpieczeństwo zagrażające terytorium całego kraju,
2) odpowiedzialność nie znajduje się w gestii policji działającej na terytorium kraju związkowego,
3) wyższy organ państwowy żąda przejęcia,
4) w takich przypadkach może również zapobiegać przestępstwom, o których mowa w art. 129a ust. 1 i 2 Kodeksu karnego i do tego celu są przeznaczone, aby zastraszyć ludność w znaczący sposób, organ władzy państwowej lub organizację międzynarodową niezgodnie z prawem przez użycie siły lub groźby użycia siły, albo polityczne, konstytucyjne, ekonomiczne lub społeczne podstawy państwa lub organizacji międzynarodowej wyeliminować lub znacząco zredukować ich wpływ, a przez sposób popełnienia tych czynów lub ich skutków może państwu lub organizacji międzynarodowej poważnie szkodzić", www.gesetze-im-internet.de/bkag_1997/20k.html [dostęp: 29 VI 2017].

nym razie byłoby bezcelowe lub zasadniczo utrudnione[30].

Istotne uprawnienie zawarte zostało w § 20l ust. 2 pkt 2 ustawy o Federalnej Policji Kryminalnej w myśl którego, w razie konieczności monitorowanie i zapisywanie telekomunikacji może również odbywać się w takiej formie, że za pomocą środków technicznych nastąpi ingerencja w informacyjno-techniczne systemy osoby będącej w kręgu podejrzeń, po to aby umożliwić monitorowanie i nagrywanie szczególnie w formie niezaszyfrowanej[31].

Natomiast w § 20l ust. 2 pkt 5 zdanie 1 ustawodawca wskazał, że (...) *na podstawie zarządzenia* (sądu – przyp. aut.) *każdy, kto wykonuje usługi telekomunikacyjne musi umożliwić Federalnej Policji Kryminalnej zastosowanie środków określonych w ust. 1* (związanych z przechwytywaniem komunikacji – przyp. aut.) *i niezwłocznie udzielić wymaganych informacji*[32].

Taki zapis oznacza, że podmioty oferujące usługi telekomunikacyjne nie mogą blokować kontroli zarządzonej przez sąd, prokuraturę lub śledczego funkcjonariusza policji. Wymienionym organom należy umożliwić przeprowadzenie takiej kontroli[33]. Jak stwierdził jeden z komentatorów: *Przedsiębiorstwa działające w przestrzeni cyfrowej muszą zastanowić się, czy chcą prowadzić swoją działalność w Niemczech, gdyż ich procedury handlowe mogą być nadzorowane przez Rząd Federalny*[34].

Rozwiązania w zakresie uprawnień operacyjno-rozpoznawczych realizowanych w celu wykrywania zagrożeń dla bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych nadal jest przedmiotem dyskusji społecznej Co istotne – działania, jakie aktualnie mogą być podejmowane przez organy śledcze, mają bardzo szeroki zasięg i nie są rozpoznawalne przez użytkownika. Zwolennicy uważają nowe rozwiązania ustawowe za konieczne w walce z terroryzmem i innymi poważnymi przejawami przestępczości. Krytycy natomiast mówią o najdalej idącej kontroli w historii Niemiec.

II. SZWAJCARIA

Ustawowe uprawnienia operacyjno-rozpoznawcze i dochodzeniowo-śledcze służb specjalnych w zakresie wykrywania zagrożeń bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych

W obliczu wciąż wzrastającego zagrożenia terroryzmem w niektórych krajach europejskich służby specjalne dopiero teraz uzyskują nowe możliwości, aby skutecznie chronić obywateli przed ewoluującymi przejawami przestępczości. Najbardziej aktualna zmiana prawa, poprzedzona długą debatą społeczną, miała miejsce w Szwajcarii. W dniu 1 września 2017 r. weszła w życie nowa ustawa z 25 września 2015 r. o Federalnej Służbie Informacyjnej Szwajcarii (*Bundesgesetz über den Nachrichtendienst*)[35], która

[30] www.gesetze-im-internet.de/bkag_1997/20k.html [dostęp: 29 VI 2017].

[31] www.gesetze-im-internet.de/bkag_1997/20l.html [dostęp: 29 VI 2017].

[32] www.gesetze-im-internet.de/bkag_1997/20l.html [dostęp: 29 VI 2017.].

[33] www.fr.de/kultur/netz-tv-kritik-medien/netz/neues-gesetz-whatsapp-ueberwachung-durch-die-hintertuer-a-1300626 [dostęp: 22 VI 2017].

[34] https://deutsche-wirtschafts-nachrichten.de/2017/06/22/bundestag-will-heimlich-weitreichende-ueberwachung-beschliessen/ [dostęp: 22 VI 2017].

[35] https://www.admin.ch/opc/de/classified-compilation/20120872/index.html [dostęp: 11 IX 2017].

znacznie poszerza kompetencje tej służby w zakresie wykonywania uprawnień operacyjno -rozpoznawczych, także przy wykorzystaniu systemów i sieci teleinformatycznych.

Próby wzmocnienia służb specjalnych przez umożliwienie im stosowania szerokiego spektrum metod o charakterze operacyjnym sięgają 2007 r. Wówczas to Rada Federalna[36] przyjęła projekt zmian w ustawie o bezpieczeństwie wewnętrznym i przekazała do dalszych prac na forum parlamentarnym. Konieczność zmian w prawie była argumentowana przyjęciem odpowiednich metod walki z terroryzmem. Zgodnie z założeniami tego projektu służby specjalne miały uzyskać prawo do instalowania podsłuchów oraz nadzoru wizyjnego w prywatnych pomieszczeniach, a także zapobiegawczego monitorowania poczty, telefonów, korespondencji elektronicznej oraz dysków komputerowych. Służby uzyskałyby także możliwość rejestrowania i analizowania emisji elektromagnetycznych, pochodzących z systemów technicznych oraz telekomunikacyjnych (zwłaszcza znajdujących się za granicą). Te uprawnienia określono zbiorczą nazwą „specjalne środki pozyskiwania informacji". W myśl projektu ustawy ich wykorzystanie miało być ograniczone do walki z wybranymi przejawami przestępczości, takimi jak: terroryzm, szpiegostwo, rozprzestrzenianie broni masowego rażenia oraz materiałów promieniotwórczych, a także walki z nielegalnym transferem technologii[37].

W ramach ofensywnych działań służb przy wykorzystaniu sieci teleinformatycznych pojawił się także szwajcarski wariant przeszukania online[38]. Ta prerogatywa, określona jako „tajne przeglądanie systemu przetwarzania danych", miała być wykorzystana, gdy konkretne i aktualne zdarzenia pozwalałyby przypuszczać, że osoba podejrzewana o stwarzanie zagrożenia używa dostępnego dla niej systemu danych, który jest szczególnie chroniony. W przypadku podejrzenia, że dochodzi do rozprzestrzenienia materiałów propagandowych w Internecie, których treść dotyczy nawoływania do przemocy, szwajcarskie służby miały mieć możliwość usunięcia takiej strony. Jeśli te treści nie znajdowałyby się na szwajcarskim serwerze, wówczas stosowny dokument miał być przedłożony szwajcarskiemu dostawcy usług, po zatwierdzeniu zlecenia dotyczącego blokady strony internetowej[39].

Ówczesny szef Federalnego Departamentu Sprawiedliwości i Policji[40] Christoph Blocher popierał wprowadzenie przedstawionych powyżej zmian. W jego ocenie stanowiły one dopasowanie możliwości działań szwajcarskich służb specjalnych do standardów europejskich i miały poprawić pozyskiwanie informacji niezbędnych do walki z islamskim terroryzmem. Argumentował także, że nowe rozwiązania nie stały w sprzeczności z porządkiem konstytucyjnym. Jednak większość prawicowych i lewicowych deputowanych zagłosowała przeciw projektowi, a plany nowelizacji prawa zostały zawieszone[41].

[36] Jest to najwyższy organ władzy wykonawczej, składający się z siedmiu członków wybieranych na cztery lata przez Zgromadzenie Federalne.

[37] https://www.heise.de/newsticker/meldung/Schweizer-Regierung-beschliesst-heimliche-Online-Durchsuchungen-140396.html [dostęp: 16 VI 2007].

[38] Jest to metoda operacyjno-rozpoznawcza polegająca na włamaniu się za pomocą środków technicznych do systemu informacyjno-technicznego, na przykład sieci komputerowej, lub do pojedynczego urządzenia, które są w użytkowaniu osoby podejrzanej, bez jej wiedzy. Szczegółowe informacje na temat tego typu czynności zostały opisane w części artykułu poświęconej rozwiązaniom stosowanym w RFN.

[39] https://www.heise.de/newsticker/meldung/Schweizer-Regierung-beschliesst-heimliche-Online-Durchsuchungen-140396.html [dostęp: 16 VI 2007].

[40] Jest to odpowiednik ministerstwa.

[41] https://www.heise.de/newsticker/meldung/Schweizer-Regierung-beschliesst-heimliche-Online-Durchsuchungen-140396.html [dostęp: 16 VI 2007].

Ponownie prace nad nowelizacją prawa rozpoczęły się w 2014 r. W poprzednim projekcie z 2007 r. uwzględniono dualizm służb specjalnych, zadania wywiadowcze i kontrwywiadowcze były bowiem realizowane przez osobne urzędy. Od 1 stycznia 2010 r. te urzędy zostały połączone, tworząc Federalną Służbę Informacyjną (Nachrichtendienst des Bundes – NDB). Jednak zarówno działające do 2010 r. służby, jak i NDB nie miały uprawnień do korzystania ze specjalnych środków pozyskiwania informacji. Nawet w przypadku działań związanych z podejrzeniem o aktywność terrorystyczną lub szpiegostwo NDB miała bardzo ograniczone możliwości działania, np. osoba podejrzana mogła być monitorowana jedynie w miejscach publicznych[42].

W ustawie o NDB, która weszła w życie 1 września 2017 r., zostały dopuszczone nowe metody, dostosowane – jak podkreślali zwolennicy ustawy – do aktualnych możliwości technicznych Nowe metody mogą być realizowane nie tylko w przestrzeni publicznej. Są to:

- monitorowanie ruchu pocztowego i telekomunikacyjnego,
- korzystanie z urządzeń monitorujących,
- penetracja systemów komputerowych i sieci komputerowych[43],
- korzystanie z urządzeń pozycjonujących,
- przeszukiwanie pomieszczeń, pojazdów itp.

Zgodnie z art. 27 ustawy nowe metody znajdują zastosowanie w związku z występującymi aktualnie zagrożeniami, jedynie w wyjątkowych sytuacjach. Mają one służyć do wykrywania szpiegów, zwalczania terroryzmu, handlu bronią lub materiałami promieniotwórczymi, ataków na infrastrukturę krytyczną, a także ochrony innych istotnych interesów narodowych[44]. Szczególnie istotne znaczenie, w ocenie projektodawców, ma nowy instrument określony w rozdziale 4 ustawy o NDB, którym jest „monitorowanie komunikacji przez łącza" (niem. *Kabelaufklärung*), ważne bowiem informacje znacznie częściej są rozprzestrzeniane przez Internet niż za pośrednictwem tradycyjnych metod komunikacji.

W myśl art. 39 ust. 1 NDB może zlecić służbie prowadzącej daną sprawę, aby uzyskała informacje dotyczące istotnych spraw odnoszących się do polityki i bezpieczeństwa wewnętrznego za granicą (art. 6 ust. 1 lit.b), bądź też aby zarejestrowała transgraniczne sygnały z sieci telekomunikacyjnych w celu ochrony innych ważnych interesów krajowych wynikających z art. 3[45]. Ten instrument może jednak znaleźć zastosowanie jedynie wtedy, gdy jeden z partnerów komunikacyjnych znajduje się za granicą. Jeżeli natomiast zarówno nadawca, jak i odbiorca znajdują się na terytorium Szwajcarii, to wówczas nie ma możliwości wykorzystania tej metody. Jeśli służba prowadząca sprawę nie jest w stanie takich sygnałów usunąć w trakcie rejestracji, należy zebrane dane zniszczyć, gdy okaże się że pochodzą z krajowych źródeł[46].

---

[42] https://www.heise.de/newsticker/meldung/Schweizer-Staatsschutz-soll-Telefone-und-Datenstroeme-ueberwachen-duerfen-2120228.html [dostęp:21 II 2014].

[43] Art. 26 ust. 1 lit. d ustawy wskazuje dwie formy takich działań:

1) dostarczanie informacji, które są dostępne w systemach lub za ich pośrednictwem przesyłane,
2) zapobieganie, utrudnianie lub spowalnianie dostępu do informacji, gdy atak za pośrednictwem systemów i sieci komputerowych skierowany jest przeciwko infrastrukturze krytycznej.

[44] W ustawie wyłączone jest natomiast stosowanie specjalnych środków pozyskiwania informacji w celu obrony przed tzw. brutalnym ekstremizmem. To wyłączenie ma skutkować uniknięciem stosowania kontroli wobec osób ze względu na ich przekonania polityczne.

[45] Ochrona porządku konstytucyjnego Szwajcarii, wspieranie szwajcarskiej polityki zagranicznej, ochrona szwajcarskich interesów gospodarczych i finansowych.

[46] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwa-

Istotne znaczenie ma jednak to, że na terenie Szwajcarii większość przepływu danych odbywa się za pośrednictwem zagranicznych serwerów i sieci, zatem komunikacja wszystkich krajowych użytkowników Internetu może być potencjalnie obiektem rozpoznania za pośrednictwem łączy. Ponadto, na mocy nowych rozwiązań, dostawcy Internetu i poczty są zobowiązani do przekazywania odpowiednich danych[47] do powiązanego z organami wojskowymi Centrum Operacji Elektronicznych (Zentrum für elektronische Operationen – ZEO), które następnie dokonuje, przy wykorzystaniu licznych haseł, oceny danych dla NDB[48]. W przypadku gdy treść danych pochodzących z zarejestrowania sygnałów odpowiada słowom kluczowym[49], które stanowią kryterium wyszukiwania, wówczas te dane mogą zostać przekazane wyłącznie do NDB. Do NDB przekazane zostają wyłącznie dane, które zawierają informacje dotyczące realizacji zlecenia związanego ze słowami kluczowymi. NDB odpowiada za ich ocenę kontrwywiadowczą[50].

W wyjątkowych sytuacjach do NDB mogą także zostać przekazane informacje dotyczące osób znajdujących się na terenie Szwajcarii. Art. 42 ust. 2 i 3 określa, że jest to dopuszczalne, gdy te dane:

1) są niezbędne do wyjaśnienia postępowania za granicą, a wcześniej zostały one zanonimizowane,
2) zawierają informacje odnoszące się do działań w kraju lub za granicą, które wskazują na konkretne zagrożenie bezpieczeństwa wewnętrznego zgodnie z art. 6 ust. 1 lit a.

Jednocześnie, w art. 42 ust. 4 ustawodawca podkreśla, że dane, które nie zawierają takich informacji, a dotyczą osób znajdujących się na terenie kraju, powinny zostać jak najszybciej zniszczone.

W myśl art. 39 ust. 4 ustawy sprawy związane z: dopuszczalnymi obszarami śledztw, w których przypadku może być stosowana opisana powyżej metoda, organizację czynności związanych z monitorowaniem komunikacji przez łącza, a także maksymalny czas przechowywania przez służbę prowadzącą zarejestrowanych danych określa rząd federalny. Zebrane dane mogą być także wymieniane z zagranicznymi służbami wywiadowczymi i organami bezpieczeństwa[51].

Dopuszczenie szerokiego spektrum środków pozwalających na gromadzenie danych zostało zrównoważone przez ustawodawcę wieloetapową procedurą, pozwalająca na ich zastosowanie. Zezwolenie na podjęcie działań, zgodnie z art. 30 ustawy, ma następujący przebieg: NDB kieruje stosowny wniosek do Federalnego Sądu Administracyjnego, po zatwierdzeniu wniosku przez sąd, zgody na przeprowadzenie działań udziela szef Federalnego Departamentu Obrony, Ochrony Ludności i Sportu[52], po wcześniejszej konsultacji z szefem Federalnego Departamentu Spraw Zagranicznych oraz szefem Federalnego De-

chungsarsenal-3331327.html [dostęp:26 IX 2016].

[47] Zgodnie z art. 43 ust. 3 i 4 operatorzy sieci telekomunikacyjnych są zobowiązania do zachowania tajemnicy. Operatorom są wypłacane rekompensaty, których wysokość ustanawia rząd federalny według kosztów dostarczenia sygnałów służbie prowadzącej.

[48] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[49] Słowa kluczowe należy tak zdefiniować, aby ich wykorzystanie w jak najmniejszym stopniu było związane z naruszeniem sfery prywatnej osób fizycznych. Ustawowo zakazane jest formułowanie słów kluczy w taki sposób, aby zawierały dane osób fizycznych lub prawnych (źródło: art. 39 ust. 3 ustawy o NDB).

[50] Art. 42 ust. 5 ustawy o NDB.

[51] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[52] NDB jest organizacyjnie umiejscowiona w tym Departamencie.

partamentu Sprawiedliwości i Policji. Sprawy o szczególnym znaczeniu mogą być przedkładane Radzie Federalnej. Procedura konsultacji odbywa się w formie pisemnej.

Osoby, w stosunku do których dopuszczone zostało zastosowanie specjalnych środków pozyskiwania informacji, są po zakończeniu operacji informowane o przyczynie, rodzaju i okresie zastosowania danej metody. Można jednak zrezygnować z tego obowiązku informacyjnego, jeśli zagrażałoby to toczącemu się postępowaniu, bezpieczeństwu wewnętrznemu, zewnętrznemu lub stwarzało zagrożenie dla osób trzecich[53].

Z uwagi na stały wzrost cyberzagrożeń[54] w NDB został założony nowy wydział, określany w mediach jako „Cyber-NDB". Utworzeniu nowej jednostki towarzyszyły społeczne obawy, że mogłaby ona podjąć aktywne czynności operacyjne bez podstawy prawnej. Do czasu przyjęcia nowej ustawy były to jedynie działania profilaktyczne ukierunkowane na ochronę. Aktualnie Cyber-NDB może również podejmować metody ofensywne związane z przenikaniem do systemów i sieci komputerowych. W celu realizacji zadań Cyber-NDB ściśle współpracuje z różnymi agencjami federalnymi, takimi jak: MELANI[55]i KOBIK[56], a także z Wojskową Służbą Informacyjną (Militaerischer Nachrichtendienst – MND)[57].

Nowa ustawa o Federalnej Służbie Informacyjnej budzi społeczne kontrowersje[58], jednak w referendum, które odbyło się we wrześniu 2016 r., 65,5 proc. obywateli Szwajcarii opowiedziało się za przyjęciem nowych ustawowych rozwiązań. W okresie poprzedzającym referendum krytyczną opinię na temat niektórych aspektów nowej ustawy wyraził Federalny Inspektor Ochrony Danych i Informacji Adrian Lobsiger. Wykazywał on, że nowe uprawnienia NDB stwarzają ryzyko naruszenia sfery prywatnej obywateli. Jako problematyczną, z punktu widzenia ochrony danych, ocenił m.in. możliwość infiltracji systemów i sieci komputerowych w celu ingerencji, przeszkodzenia lub spowolnienia w dostępie do informacji. Ponadto NDB została zwolniona z obowiązku podawania informacji do publicznej wiadomości, co może spowodować, że dostęp do niektórych dokumentów urzędowych może być niemożliwy. W ocenie Federalnego Inspektora Ochrony Danych i Informacji istnieje ryzyko, że opinia publiczna nie będzie w pełni informowana o zakresie działań służb[59].

---

[53] Art. 33 ustawy o NDB.

[54] W 2013 r. takie zalecenie wydał w raporcie rocznym Federalny Urząd ds. Zarządzania Teleinformatyką. Była to odpowiedź na cele określone przez Radę Federalną w ramach Narodowej Strategii Ochrony Szwajcarii przeciwko Cyberzagrożeniom. W ramach Strategii zidentyfikowano 16 metod, które pozwolą na wzmocnienie działań mających na celu zwalczanie cyberprzestępczości. Tych 16 metod zostało przyporządkowanych do czterech obszarów: zapobieganie, reagowanie, zapewnienie ciągłości pracy, procesy wspomagające, za: https://www.heise.de/newsticker/meldung/Neuer-Cyber-Geheimdienst-fuer-die-Schweiz-2183874.html [dostęp: 6 V 2014].

[55] Melde- und Analysestelle Informationssicherung (Centrum Raportowania i Analizy w zakresie Bezpieczeństwa Informacji). Celem działania MELANI jest identyfikowanie i przezwyciężanie niebezpieczeństw oraz pomoc operatorom infrastruktury krytycznej w kryzysowych sytuacjach, za: https://www.melani.admin.ch/melani/en/home.html [dostęp: 13 IX 2017].

[56] Jednostka Koordynująca do spraw Zwalczania Przestępczości Internetowej (Koordinationsstelle zur Bekampfung der Internetkriminalitat) odpowiedzialna za sektor cywilny, za: https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html [dostęp: 13 IX 2017].

[57] https://www.heise.de/newsticker/meldung/Neuer-Cyber-Geheimdienst-fuer-die-Schweiz-2183874.html [dostęp: 6 V 2014].

[58] Podpisy za przeprowadzeniem referendum zbierali przeciwnicy nowych rozwiązań, m.in.: Partia Zielonych, Juso – młodzieżowa sekcja Partii Socjalistycznej, cześć członków Socjaldemokratycznej Partii Szwajcarii, Partia Piratów, a także takie organizacje, jak: Społeczeństwo Cyfrowe oraz Prawa Podstawowe, za: https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[59] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwa-

W obliczu takich wątpliwości istotne znaczenie ma właściwy mechanizm niezależnej kontroli nad działalnością służb, a szczególnie nad wykorzystaniem dyskusyjnych metod operacyjno-rozpoznawczych. Ustawodawca położył szczególny nacisk na niezależną kontrolę instancyjną nad monitorowaniem komunikacji przez łącza oraz rejestrowaniem i analizowaniem emisji elektromagnetycznych[60]. Zadania w tym zakresie wypełnia niezależna, wewnątrzadministracyjna instancja kontrolna, której członkowie są wybierani przez Radę Federalną na cztery lata. Rada wykonuje nadzór nad zgodnością z prawem tych metod oraz nad prawidłowością dopuszczenia zastosowania. Sprawdza także, czy sposób, w jaki informacje są opracowywane i przekazywane do NDB, jest zgodny z ustawą. Jeżeli wyniki tej kontroli okażą się niekorzystne, może zostać wydane zalecenie dla Federalnego Departamentu Obrony, Ochrony Ludności i Sportu dotyczące zakończenia działań związanych z rejestracją i monitoringiem oraz usunięcia zgromadzonych informacji. Wszelkie zalecenia, wnioski i raporty opracowywane przez organ kontrolny są niejawne.

W okresie prac nad ustawą przewidywano, że nowe metody będą wykorzystywane na poziomie około 10 przypadków rocznie. NDB nie zakłada jednak ustalonej liczby czynności, dlatego też możliwy jest wzrost korzystania z nowych uprawnień w obliczu globalnych zagrożeń, powyżej założeń przedstawionych podczas prac parlamentarnych[61]. Istotne znaczenie dla utrzymania wysokiego poziomu zaufania społecznego dla misji realizowanej przez NDB ma właściwy nadzór nad działalnością tej służby[62].

W art. 76 ustawy określono, że Rada Federalna tworzy niezależny organ nadzorujący NDB, jego przewodniczący zaś jest powoływany na sześć lat, na wniosek szefa Federalnego Departamentu Obrony, Ochrony Ludności i Sportu. Niezależny organ sprawuje nadzór nad działalnością NDB, uprawnionymi służbami w kantonach, a także innymi urzędami, które współdziałają z NDB przy wykonywaniu ustawowych uprawnień. Ten organ sprawdza działalność służby pod względem zgodności z prawem, celowości oraz skuteczności.

W celu realizacji uprawnień organ nadzorujący ma dostęp do wszelkich informacji oraz dokumentów, a także posiada dostęp do wszelkich pomieszczeń jednostek nadzoro-

chungsarsenal-3331327.html [dostęp: 26 IX 2016].

[60] Art. 79 ustawy o NDB.

[61] https://www.heise.de/newsticker/meldung/Schweizer-erlauben-Geheimdienst-umfangreiches-Ueberwachungsarsenal-3331327.html [dostęp: 26 IX 2016].

[62] W ocenie komentatorów na wynik referendum niewątpliwie miały wpływ wydarzenia ostatnich lat – ataki terrorystyczne w Europie oraz liczne gwałtowne działania związane z przemocą. Kilka lat wcześniej wynik referendum prawdopodobnie byłby niepomyślny dla projektodawców nowej ustawy o NDB. Do niedawna szwajcarskie społeczeństwo pozostawało bowiem pod negatywnym wrażeniem dwóch skandali związanych z gromadzeniem informacji o obywatelach.

Pierwszy z nich miał miejsce pod koniec lat 80. XX w., gdy ujawniono, że władze państwowe oraz Policja w kantonach utworzyły w latach 1900–1990 około 900 tys. rejestracji w celu ochrony państwa. Zarejestrowano osoby, organizacje i wydarzenia. Rejestracje osobowe dotyczyły: zagranicznych anarchistów, szwajcarskich socjalistów oraz związkowców, niechcianych uchodźców politycznych oraz cudzoziemców, którzy zostali zgłoszeni. Rejestracje dotyczyły także ruchów nacjonalistycznych i faszystowskich. Wraz z pojawieniem się antykomunizmu obserwowano przede wszystkim polityków lewicowych i członków związków zawodowych. Szacuje się, że co dwudziesty obywatel szwajcarski oraz co trzeci cudzoziemiec został odnotowany w tej kartotece.

Drugi skandal miał miejsce latem 2010 r., gdy Parlamentarna Komisja Kontrolna została poinformowana o kolejnym masowym gromadzeniu danych przez służby specjalne. Około 200 tys. osób zostało zarejestrowanych bezpośrednio lub jako osoby trzecie, w większości bez odpowiedniej podstawy prawnej, za: https://de.wikipedia.org/wiki/Fischenskandal [dostęp: 11 IX 2017].

wanych. W ramach swoich nadzorczych kompetencji może on domagać się informacji oraz wglądu do akt w innych jednostkach organizacyjnych na szczeblu centralnym oraz w kantonach, jeśli tylko przedmiotowe informacje wykazują związek ze współpracą tych komórek z nadzorowanymi jednostkami. W celu wypełnienia swojej działalności organ kontrolny może mieć również dostęp do wszelkich systemów informacyjnych oraz zbiorów baz danych jednostek nadzorowanych[63]. Nad dzielnością NDB i jednostek organizacyjnych działających w poszczególnych kantonach prowadzony jest również zwierzchni nadzór parlamentarny[64].

III. ALGORYTM AUTOMATYCZNEGO PRZETWARZANIA DANYCH (TZW. CZARNE SKRZYNKI) JAKO INSTRUMENT WYKRYWANIA ZAGROŻEŃ W SYSTEMACH I SIECIACH TELEINFORMATYCZNYCH W REPUBLICE FRANCUSKIEJ

System „czarnych skrzynek" (fr. *boîtes noires*) – wprowadzony we Francji na podstawie art. L 851-3 ustawy o wywiadzie[65] – ma na celu pozyskiwanie informacji przez służby wywiadowcze przez nałożenie na operatorów telekomunikacyjnych obowiązku zainstalowania w zarządzanych przez nich sieciach algorytmów umożliwiających zidentyfikowanie połączeń mogących wskazywać na zagrożenie terrorystyczne. Te urządzenia analizują metadane komunikacyjne w celu wykrycia tzw. sygnałów słabych (fr. *signaux bas*), które mogą wykazywać określone cechy typowe dla sposobów komunikacji osób prowadzących działalność o charakterze terrorystycznym. Ten algorytm może być stosowany wyłącznie w celu zapobiegania zagrożeniom terrorystycznym. Przyjęcie ustawy wywołało we Francji liczne kontrowersje. Do najważniejszych argumentów krytycznych należy zagrożenie, jakie ten akt niesie za sobą dla prawa do prywatności, zarzut, że przewidziane mechanizmy kontrolne są niewystarczające, oraz stwierdzenie, że przyjęcie tego rodzaju norm stanowi legalizację niezgodnych z prawem działań służb wywiadowczych i jest kopią amerykańskich programów wykorzystywanych przez Agencję Bezpieczeństwa Narodowego (NSA)[66].

Algorytm stanowi jeden z najbardziej kontrowersyjnych elementów ustawy o wywiadzie. *Ratio legis* wprowadzenia tego przepisu stanowiło stworzenie instrumentu pozwalającego służbom specjalnym na skuteczną identyfikację zagrożeń terrorystycznych będących wynikiem działalności zarówno zorganizowanych komórek, jak i działalności tzw. samotnych wilków – osób nienależących w sensie formalno-organizacyjnym do żadnej struktury o charakterze terrorystycznym, prowadzących działania w sposób autonomiczny i niezależny[67]. Monitorowanie ich działalności jest nie-

[63] Art. 78 ustawy o NDB.

[64] Art. 81 ustawy o NDB.

[65] *Loi n° 2015-912 du 24 juillet relative au renseignement*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id [dostęp: 20 IX 2017].

[66] www.sous-surveillance.fr/#/ [dostęp: 20 IX 2017].

[67] Przykładem wykorzystania tej taktyki były trzy ataki z użyciem broni palnej wymierzone przeciwko francuskim żołnierzom i osobom pochodzenia żydowskiego w miastach Tuluza i Montabaun w marcu 2012 r. przez Mohammeda Meraha – Francuza pochodzenia algierskiego powiązanego z terroryzmem islamskim. Pomimo stosowania wobec Meraha środków kontroli operacyjnej i obserwacji przez służby specjalne (DGSI, DPSD) oraz zgromadzenia o nim znacznej wiedzy (m.in. o pobytach w Afganistanie i Pakistanie),

zwykle utrudnione. W przypadku gdy komórka terrorystyczna jest złożona z jednej lub dwóch osób, jej wykrycie, analiza metodologii działań i identyfikacja jej potencjalnych celów jest procesem skomplikowanym i rozłożonym w czasie. Zdolność właściwych organów do rozpoznawania i zapobiegania zagrożeniom tego typu jest ograniczona również z uwagi na znacznie mniejszy wyciek informacji na zewnątrz komórki, niż ma to miejsce w przypadku grup liczących kilkanaście lub kilkadziesiąt osób.

Przepis ustanawiający algorytm czarnych skrzynek został wprowadzony na czas określony – zgodnie z art. 25 ustawy o wywiadzie jej art. L 851-3 jest stosowany do 31 grudnia 2018 r. Do 30 czerwca 2018 r. rząd został zobowiązany do przedstawienia parlamentowi raportu dotyczącego sposobu działania instrumentu. Na uwagę zasługuje to, że system nie został dotychczas aktywowany we Francji, aktualnie jest stosowany wyłącznie w odniesieniu do danych, które nie mogą być powiązane z jej terytorium[68].

Na wstępie należy zaznaczyć, że ani opinia Rady Państwa (Conseil d'État) o projekcie ustawy o wywiadzie z 12 marca 2015 r.[69], ani decyzja Rady Konstytucyjnej 2015-713 DC z 23 lipca 2015 r. co do zgodności ustawy o wywiadzie z Konstytucją[70] nie uznały przepisów przewidujących system „czarnych skrzynek" za niezgodne z ustawą zasadniczą. Zdaniem obydwu organów istniejące w ustawie mechanizmy zabezpieczające i środki odwoławcze sprawiają, że te przepisy nie naruszają Konstytucji ani zasad demokratycznego państwa prawnego.

1. Podstawy prawne

Zgodnie z art. 851-3 kodeksu bezpieczeństwa wewnętrznego po uzyskaniu zgody premiera, wydanej po uzyskaniu zgody Narodowej Komisji Kontroli Technik Pozyskiwania Informacji (CNCTR), operatorzy telekomunikacyjni oraz osoby zajmujące się dostarczaniem usług komunikacji elektronicznej, wymienione w ustawach kodeks pocztowy i telekomunikacyjny[71] oraz w ustawie o zaufaniu do gospodarki cyfrowej[72], mogą zostać zobowiązani do wprowadzenia w administrowanych przez nich sieciach automatycznego przetwarzania danych[73] tzw. czarnych skrzynek, zgodnie z kryteriami opisanymi w autoryzacji, w celu wykrycia połączeń mogących wskazywać na zagrożenie terrorystyczne. „Czarne skrzynki" analizują w sposób masowy przepływ danych komunikacyjnych przesyłanych za pośrednictwem kabli optycznych w celu wykrycia

zapobieżenie atakowi okazało się niemożliwe.

[68] *Renseignement: des boites noires dèjà activées à l'échelle internationale*, Marc Rees, https://www.nextinpact.com/news/105039-renseignement-des-boites-noires-deja-activees-a-echelle-internationale.htm [dostęp: 20 IX 2017].

[69] *Conseil d'État, Avis sur un projet de loi relatif au renseignement, N°389.754*, www.legifrance.gouv.fr/Media/Droit-framcais/Les-avis-du-Conseil-d Etat-rendus-sur les-projets-de-loi/2015/avis_ce_prmx1504410L_cm_19_03_2015 [dostęp: 15 IX 2017].

[70] *Décision n° 2015-713 DC du 23 juillet 2015*, www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc-du-23-juillet-2015.144138.html [dostęp: 21 IX 2017].

[71] *Code des postes et des communications électroniques*, www.legifrance.gouv.fr/affichCode.do;jsessionid=DC13EAA7D9C8685F8B507A74EE79EF70.tpdila20v_1?cidTexte=LEGITEXT000006070987&dateTexte=20170920 [dostęp: 20 IX 2017].

[72] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000000801164&idArticle=LEGIARTI000006421546&dateTexte=&categorieLien=cid [dostęp: 20 IX 2017].

[73] Użyte w ustawie pojęcie automatyczne przetwarzanie (fr. *traitements automatisés*) należy rozumieć jako urządzenia lub algorytmy służące do takiego przetwarzania.

tzw. sygnałów niskich mogących świadczyć o wystąpieniu elementów charakterystycznych dla zagrożeń związanych z terroryzmem.

Omawiana technika może być wykorzystywana wyłącznie w celu przeciwdziałania i zapobiegania terroryzmowi. Zbieranie danych w tym trybie musi spełniać kryteria zawarte w autoryzacji określającej w sposób wyczerpujący dane, które mają być pozyskane oraz ich parametry techniczne. Zgodę na jej zastosowanie wydaje premier, po zasięgnięciu opinii CNCTR.

Do katalogu danych zbieranych przy wykorzystaniu „czarnych skrzynek" ustawodawca zalicza wyłącznie informacje wymienione w art. L 851-1. Powyższy katalog został szerzej opisany dalej, w części poświęconej kontrowersjom związanym z ustawą.

Narodowa Komisja Technik Pozyskiwania Informacji wydaje opinię na temat wniosku o udzielenie autoryzacji wykorzystania tej techniki. Posiada ona stały, bezpośredni i nieograniczony dostęp do systemów automatycznego przetwarzania danych, a także do informacji zebranych i przechowywanych przy wykorzystaniu systemu. Komisja jest informowana o wszelkich modyfikacjach sposobów, w jakich dane są przetwarzane. Może wydawać w tym zakresie rekomendacje (art. L 851-3 II).

W fazie początkowej autoryzacja jest udzielana na dwa miesiące (z możliwością przedłużenia). Wniosek o przedłużenie zawiera wykaz określający wykrytą liczbę identyfikatorów charakterystycznych dla działań terrorystycznych wskazanych przez system wraz z analizą ich znaczenia oraz możliwości realnego występowania ewentualnych powiązań tych elementów z działaniami terrorystycznymi.

W sytuacji gdy mechanizm wykryje elementy wskazujące na zagrożenie terrorystyczne (np. wyszukiwanie słów powiązanych z terroryzmem, działalność na portalach społecznościowych), premier lub upoważniona przez niego osoba może zezwolić, po uprzednim zasięgnięciu opinii Komisji, na identyfikację osoby fizycznej, która w świetle zebranych danych może być uważana za powiązaną z działaniami o charakterze terrorystycznym, i na zgromadzenie innych informacji jej dotyczących. Te dane są przetwarzane przez 60 dni od chwili ich zebrania. Po upływie tego okresu podlegają zniszczeniu, z wyłączeniem sytuacji wystąpienia poważnych przesłanek wskazujących na zagrożenie terrorystyczne związane z jedną lub większą liczbą osób, których dotyczą zgromadzone informacje.

Identyfikacji osoby wskazanej przez system dokonuje Międzyresortowy Zespół Kontroli (Groupement interministériel de contrôle)[74]. Ten organ zwraca się do operatora usług internetowych o dostarczenie informacji o wskazanej osobie fizycznej. Kolejnym etapem, w zależności od specyfiki konkretnej sytuacji, może być prowadzenie dalszych działań operacyjno-rozpoznawczych bądź wszczęcie śledztwa lub dochodzenia.

[74] Groupement interministériel de contrôle – Międzyresortowy Zespół Kontroli, organ podległy premierowi odpowiedzialny m.in. za:

1) rejestrację wniosków o wykorzystanie technik pozyskiwania informacji;
2) rejestrację autoryzacji wykorzystania technik pozyskiwania informacji;
3) zbieranie i przechowywanie informacji i dokumentów związanych z wykorzystywaniem technik pozyskiwania informacji;
4) centralizację przechwytywania informacji ze względów bezpieczeństwa, ich transkrypcję i inne czynności związane z przetwarzaniem przechwyconych informacji;
5) działania związane z centralizacją informacji wywiadowczych.

2. Uzasadnienie stworzenia mechanizmu *boîtes noires* [75]

Do chwili przyjęcia ustawy o wywiadzie sposób wykorzystywania przez służby wywiadowcze instrumentów technicznych pozwalających na przechwytywanie danych (fr. *captation des données*) nie został we Francji uregulowany w żadnym powszechnie obowiązującym akcie normatywnym.

Charakter współczesnych zagrożeń bezpieczeństwa państwa, zarówno w wymiarze wewnętrznym, jak i zewnętrznym, wymaga efektywnych i dostosowanych do ich specyfiki instrumentów pozwalających na jak najszersze pozyskiwanie informacji, dzięki którym możliwe będzie efektywne przeciwdziałanie i zapobieganie tym zagrożeniom. Tego typu działania są dodatkowo utrudnione przez intensywny rozwój środków komunikacji elektronicznej.

Przywołany dokument wskazuje, że w stanie prawnym poprzedzającym przyjęcie ustawy o wywiadzie nie istniały jakiekolwiek podstawy prawne pozwalające na przechwytywanie, transmisję czy rejestrowanie treści rozmów ani na przesyłanie i rejestrowanie danych informatycznych przesyłanych za pośrednictwem zautomatyzowanego systemu przetwarzania danych lub danych przechowywanych w takim systemie. Potwierdza to podnoszone wielokrotnie, zarówno przez organy władzy publicznej, jak i podmioty prywatne, zarzuty, że działalność służb wywiadowczych jest prowadzona we Francji w obszarze „para-legalnym" czy „ekstra-legalnym"[76]. Należy jednak podkreślić, że studium skutków ewentualnego przyjęcia ustawy o wywiadzie odnosi się prawdopodobnie do braku tego rodzaju instrumentów w sferze operacyjno-rozpoznawczej (w dalszej części dokumentu zaznaczono, że od 2011 r. we francuskim porządku prawnym obowiązują przepisy kodeksu karnego pozwalające na przechwytywanie danych informatycznych).

Nadrzędnym celem ustawy było zatem wyposażenie organów właściwych w zakresie ochrony bezpieczeństwa państwa instrumentów pozwalających na skuteczną realizacje ich ustawowych zadań przy jednoczesnym stworzeniu mechanizmów gwarancyjnych, neutralizujących ryzyko związane z ich głęboką ingerencją w prawo do prywatności.

Zgodnie z danymi przedstawionymi w dokumencie przed wejściem w życie ustawy liczbę wniosków o udostępnienie danych o połączeniach szacowano na 350 000 w skali roku. Przyjęcie omawianego aktu normatywnego spowoduje trudny do wyrażenia w wartościach liczbowych wzrost wniosków kierowanych do operatorów telekomunikacyjnych i podmiotów utrzymujących serwery informatyczne.

Kolejnym, wartym podkreślenia argumentem jest to, że analogiczne przepisy prawne funkcjonują w większości państw demokratycznych – jako przykładowy dokument wymienia brytyjską ustawę *Regulation of Investigatory Powers Act 2000*[77] czy włoską ustawę z 2007 r.[78]

---

[75] Opracowano na podstawie dokumentu *Projet de loi relatif au renseignement, Etude d'Impat, 18 Mars 2015* dostępnego na stronie: www.assemblee-nationale.fr/14/projets/pl2669-ei.asp#P1241 200428 [dostęp: 19 IX 2017].

[76] *Conseil Constitutionnel, Décisions n° 2015-713 DC et 2015-714 DC du 23 juillet 2015 – Commentaire*, s. 2, www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2015713DC2015713dc_ccc.pdf [dostęp: 21 IX 2017].

[77] *Regulation of Investigatory Powers Act 2000*, www.legislation.gov.uk/ukpga/2000/23 [dostęp: 20 IX 2017].

[78] *Legge 3 agosto 2007, n.124 – Sistema di informazione per la sicurezza della Repubblica e nuova disci-*

Przyjęcie omawianych regulacji ma niezwykle istotne znaczenie w kontekście coraz szerszych możliwości utrzymywania niezwykle trudnych do wykrycia kontaktów przez ugrupowania terrorystyczne czy zorganizowane grupy przestępcze. Wymiana informacji przez tego rodzaju podmioty jest prowadzona za pośrednictwem zaszyfrowanych środków komunikacji elektronicznej, forów internetowych, zapisywania danych na serwerze, do których dostęp jest uzależniony od znajomości hasła czy na urządzeniu USB. Informacje mogą być przekazywane również za pomocą komputerów znajdujących się w kawiarenkach internetowych.

Kolejnym czynnikiem utrudniającym efektywną realizację zadań służb odpowiedzialnych za wywiad czy bezpieczeństwo wewnętrzne jest coraz większa dywersyfikacja środków komunikacji – zarówno telefonów, jak również komunikatorów internetowych takich jak Skype, Telegram, WhatsApp, Signal czy innych – oraz coraz wyższy stopień zaawansowania technologicznego tych urządzeń. Tradycyjne, ukierunkowane metody przechwytywania treści komunikacji określonej osoby nie są dostosowane do współczesnych zagrożeń i nie pozwalają na spójne i nieprzerwane prowadzenie czynności operacyjno-rozpoznawczych, w sytuacji gdy określona osoba posługuje się różnymi środkami komunikacji czy zmienia dane umożliwiające jej identyfikację (np. numer telefonu, adres poczty elektronicznej).

Pozyskiwanie przez służby danych informatycznych ma szczególne znaczenie w zapobieganiu i zwalczaniu zagrożeń o charakterze terrorystycznym. Masowe wykorzystywanie nowych środków komunikacji przez takie podmioty, jak tzw. Państwo Islamskie sprawia, że na przestrzeni kilku ostatnich lat znacznie wzrosła ilość danych (np. zdjęcia, pliki wideo, prywatne wiadomości), których francuskie służby nie mogą zdobyć zarówno ze względu na ograniczenia natury technologicznej, jak i prawnej. Przechwytywanie danych informatycznych dotyczących odwiedzanych stron internetowych, metadanych o komunikacji elektronicznej czy danych dotyczących zakupów dokonywanych za pośrednictwem sklepów internetowych jest, według twórców dokumentu, niezbędne do ustalenia np. zamiaru wyjazdu określonej osoby do stref działania ugrupowań terrorystycznych (Syria, Irak). Pomoże to ujawnić charakterystyczne dla procesu radykalizacji elementy, np. zakup sprzętu paramilitarnego czy utrzymywanie kontaktów z określonymi osobami czy środowiskami.

Kolejnym niezmiernie istotnym zastosowaniem omawianych regulacji będzie zapobieganie i zwalczanie proliferacji broni masowego rażenia przez monitorowanie działalności podmiotów, w większości stworzonych w sposób sztuczny (tzw. *sociétés écrans*) nabywających od podmiotów wysoce zaawansowanych technologicznie, funkcjonujących we Francji czy innych państwach europejskich, przedmioty czy substancje, które mogą służyć do produkcji komponentów takiej broni.

3. Kontrowersje związane z ewentualnym wykorzystywaniem systemu

Sygnalizowane w toku debaty publicznej wątpliwości związane ze zbieraniem przez służby wywiadowcze informacji w trybie opisanym w art. L 851-3, dodanym do ustawy kodeks bezpieczeństwa wewnętrznego przez ustawę o wywiadzie, należy rozpatrywać na dwóch płaszczyznach. Po pierwsze, według osób i podmiotów prezentujących krytyczne wobec ustawy stanowisko, niezależnie od korzyści związanych z możliwością

plina del segreto, angielska wersja językowa ustawy dostępna na stronie: www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html [dostęp: 19 IX 2017].

powzięcia w ten sposób informacji o potencjalnych zagrożeniach terrorystycznych, ten instrument pociąga za sobą ryzyko stworzenia systemu masowej inwigilacji, działającego bez dostatecznych mechanizmów ograniczających, które zmniejszałyby ryzyko naruszenia prywatności osób niezwiązanych w żaden sposób z działalnością zagrażającą bezpieczeństwu państwa. Po drugie, ustalenie katalogu danych, do których dostęp będzie możliwy dzięki wykorzystaniu algorytmu, jest zadaniem skomplikowanym z uwagi na sposób sformułowania właściwych przepisów i liczne odesłania ustawowe.

Jako jedno z zagrożeń związanych z systemem „czarnych skrzynek" wskazuje się na działanie tych urządzeń na podstawie algorytmu wykorzystującego sztuczną inteligencję, którego szczegółowy sposób działania jest objęty tajemnicą. Zadaniem mechanizmu jest wykrycie elementów typowych dla działań o charakterze terrorystycznym przez analizę zachowań w Internecie, co w dalszej kolejności może doprowadzić do identyfikacji konkretnej osoby, która może być powiązana z działalnością terrorystyczną. Wątpliwości opinii publicznej budzi brak możliwości ustalenia, jakie konkretnie aspekty wykorzystywania sieci podlegają badaniu i jakie zachowania mogą doprowadzić do tego, że dana osoba zostanie wskazana przez system jako mogąca stwarzać zagrożenie[79].

Niepewność natury interpretacyjnej jest również związana z określeniem, jakie konkretnie dane będą podlegać analizie dokonywanej przez system. Trzeba tu podkreślić, że jego ustalenie wymaga interpretacji nie tylko przepisów ustawy o wywiadzie i kodeksu bezpieczeństwa wewnętrznego, lecz także innych aktów prawnych, co sprawia, że zrozumienie rzeczywistego charakteru „czarnych skrzynek" przez osobę nieposiadającą specjalistycznej wiedzy z zakresu prawa i nowoczesnych technologii, niezależnie od przyjęcia dekretu ze stycznia 2016 r. wyjaśniającego wiele istotnych aspektów problemu, było zadaniem skomplikowanym. Dekret, o którym mowa, został przedstawiony szerzej w dalszej części artykułu.

Punktem wyjścia dla określenia ww. katalogu jest zdanie drugie art. L 851-3 par. I, zgodnie z którym:

> Automatyczne przetwarzanie wykorzystuje wyłącznie informacje lub dokumenty, o których mowa w art. L 851-1, nie zbierając innych danych niż te, które odpowiadają parametrom wyjściowym i w sposób nie pozwalający na identyfikację osób, których te informacje lub dokumenty dotyczą[80].

Zgodnie z art. L 851:

> Na zasadach opisanych w rozdziale I tytule II niniejszej księgi[81] może zostać autoryzowane, za pośrednictwem operatorów komunikacji elektronicznej i osób wymienionych w art. L 34-1 kodeksu poczty i komunikacji elektronicznej[82] jak również osób wymie-

[79] G. Chapeau, *Que feront les boîtes noires de la Loi Renseignement?*, 3 IV 2015 r., www.numerama.com/magazine/32699-que-feront-les-boites-noires-de-la-loi-renseignement.html [dostęp: 20 IX 2017].

[80] Wszystkie tłumaczenia aut.

[81] Rozdział I tytułu II księgi VII ustawy (*De l'autorisation de mise en oeuvre*); kodeks bezpieczeństwa wewnętrznego dotyczy autoryzacji wykorzystywania technik pozyskiwania informacji.

[82] *Code des postes et des communications électroniques*:

Art. L 34-1.

„I. Niniejszy artykuł stosuje się do przetwarzania danych osobowych w toku dostarczania usług komunikacji elektronicznej; stosuje się również do sieci wykorzystujących urządzenia zbierania danych identyfikacyjnych.

nionych w pkt 1 i 2 art. 6 ustawy n°2004-575 z dnia 21 lipca 2004 roku o zaufaniu do gospodarki cyfrowej[83], zbieranie informacji i dokumentów przetwarzanych lub przechowywanych przez określone sieci lub usługi komunikacji elektronicznej, w tym danych technicznych dotyczących identyfikacji numeru abonenta lub danych o połączeniu z usługą komunikacji elektronicznej, danych dotyczących spisu wszystkich numerów abonamentu lub danych o połączeniu wskazanej osoby, danych o lokalizacji używanych przez nią urządzeń końcowych i danych dotyczących komunikacji abonenta obejmujących listę numerów połączeń wychodzących i przychodzących oraz czas trwania i datę połączeń.

Analiza przepisów art. L 851-1 ustawy kodeks bezpieczeństwa wewnętrznego, art. L 34-1 kodeksu poczty i telekomunikacji i art. 6 ustawy o zaufaniu do gospodarki cyfrowej prowadzi do wniosku, że obowiązkiem wynikającym z art. L 851-3 mogą zostać objęci operatorzy komunikacji elektronicznej, dostawcy Internetu w rozumieniu ogólnym oraz podmioty hostingowe (co powoduje, iż „czarne skrzynki" obejmują usługi, takie jak YouTube, Gmail czy Facebook)[84].

Istotne znaczenie ma również pojęcie informacji i dokumentów, którym posługuje się art. L 851-1 i do którego odsyła art. L 851-3. Art. L 851-1 zawiera z kolei odesłanie do art. 34-1 kodeksu poczty i telekomunikacji, którego par. VI stanowi, że:

Dane przechowywane i przetwarzane na warunkach określonych w par. III, IV i V dotyczą wyłącznie identyfikacji osób korzystających z usług dostarczanych przez operatorów, charakterystyki technicznej komunikacji zapewnianej przez tych operatorów oraz lokalizacji urządzeń końcowych. W żadnym wypadku nie mogą one ujawniać treści korespondencji ani informacji, z którymi zapoznano się w jakiejkolwiek formie w toku tej komunikacji.

Wątpliwości interpretacyjne związane z zakresem wymienionych pojęć zostały wyjaśnione przez stworzenie definicji informacji i dokumentów na podstawie *Dekretu nr 2016-67 z dnia 29 stycznia 2016 roku dotyczącego technik pozyskiwania informacji*[85].

II. Operatorzy komunikacji elektronicznej, zwłaszcza osoby, których działalność polega na oferowaniu dostępu do usług komunikacji online, usuwają lub czynią anonimowymi wszystkie dane o ruchu, z zastrzeżeniem par. III, IV, V i VI.

Osoby dostarczające usługi komunikacji elektronicznej wprowadzają, z zastrzeżeniem poprzedniego akapitu, wewnętrzne procedury pozwalające na realizację żądań właściwych organów.

Osoby, które z tytułu głównej lub dodatkowej działalności zawodowej oferują połączenia umożliwiające komunikację online przez dostęp do sieci, również bez wynagrodzenia, podlegają na mocy niniejszego artykułu przepisom mającym zastosowanie do operatorów komunikacji elektronicznej. (…)"

[83] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*:

Art. 6

„I.1. Osoby, których działalność polega na oferowaniu dostępu do usług komunikacji elektronicznej online informują swoich abonentów o istnieniu środków technicznych pozwalających na ograniczenie dostępności niektórych usług lub ich selekcję i proponują im co najmniej jeden taki środek. (…)

2. Osoby fizyczne lub prawne zapewniające, również nieodpłatnie, udostępnienie usług komunikacji elektronicznej online, przechowywanie sygnałów, treści pisemnych, obrazów, dźwięków lub jakichkolwiek wiadomości wygenerowanych przez odbiorców tych usług, nie podlegają odpowiedzialności cywilnej związanej z działalnością lub informacjami przechowywanymi na żądanie odbiorcy tych usług, jeżeli nie posiadali wiedzy o ich przestępczym charakterze lub o faktach i okolicznościach mogące wskazywać na ten charakter, jeżeli, od chwili, w której powzięli tego rodzaju informacje, podjęli niezwłoczne działania w celu usunięcia tych danych i uniemożliwienia dostępu do nich. (…)".

[84] *Que feront les boîtes noires ...*

[85] *Décret n°2016-67 du 29 janvier 2016 relatif aux techniques de renseignement*, www.legifrance.gouv.

Art. R 851-5, dodany na podstawie art. 2 dekretu do kodeksu bezpieczeństwa wewnętrznego, stanowi:

> Art. R 851-5 – I. Informacje i dokumenty, o których mowa w art. L 851-1 obejmują, z wyłączeniem treści wymienianej korespondencji lub informacji, z którymi się zapoznano:
>
> 1. Informacje wymienione w art. R.10-13 i R 10-14 kodeksu poczty i komunikacji elektronicznej oraz w art. 1 dekretu nr 2011-219 z dnia 25 stycznia 2011 dotyczącego przechowywania i przekazywania danych pozwalających na identyfikację osób biorących udział w tworzeniu treści umieszczonych w Internecie;
>
> 2. Dane techniczne inne niż wymienione w pkt 1, które:
>
> a) pozwalają na identyfikację urządzeń końcowych;
> b) dotyczą dostępu do urządzeń końcowych w sieciach i do usług komunikacji on-line;
> c) dotyczą przesyłu/dostarczania komunikacji elektronicznej przez sieci;
> d) dotyczą identyfikacji lub weryfikacji użytkownika połączenia, sieci lub usługi komunikacji on-line;
> e) dotyczą charakterystyki urządzeń końcowych i danych konfiguracji oprogramowania.
>
> II. Wyłącznie informacje i dokumenty wymienione w pkt 1 par. I mogą być zbierane na podstawie art. L 851-1. Zbieranie to ma odbywa się z opóźnieniem.
>
> Informacje wymienione w pkt 2 par. I mogą być zbierane wyłącznie w toku stosowania art. L 851-2 i L 851-3 na zasadach opisanych w tych artykułach i z zastrzeżeniem art. R 851-9.

Zarówno art. L 851-1, jak i L 851-3, a także przywołany przepis R 851-5 wprowadzony na mocy dekretu z 29 stycznia 2016 r. przewidują wyłącznie możliwość zbierania i przetwarzania określonych kategorii danych technicznych informujących o poszczególnych parametrach połączeń, nie pozwalają jednak na identyfikację treści rozmów czy korespondencji. Należy zatem uznać, że analizowane przepisy pozwalają na zbieranie i przetwarzanie przez algorytm wyłącznie metadanych. Żadna z kategorii informacji wymienionych w art. L 851-1 czy w pozostałych cytowanych przepisach nie wskazuje, aby było możliwe uzyskanie dostępu do treści komunikacji. Przeciwnie – art. R 851-5 wyraźnie wyłącza z katalogu pojęć wchodzących w zakres definicji informacji i dokumentów treść wymienianej korespondencji oraz informacje, z którymi się zapoznano.

Odnosząc się do mechanizmów mających na celu ochronę praw i wolności, w tym prawa do prywatności, trzeba zwrócić uwagę na art. R 851-9, który podobnie jak art. R 851-5 został dodany do kodeksu bezpieczeństwa wewnętrznego na mocy przywołanego powyżej dekretu. Zgodnie z art. R 851-9

> Informacje i dokumenty zebrane na podstawie niniejszego tytułu nie mogą, bez autoryzacji, o której mowa w art. L 852-1 i art. L 853-2, być wykorzystywane w celu uzyskania dostępu do treści wymienianej korespondencji lub informacji, z którymi się zapoznano.

fr/affichTexte.do?cidTexte=JORFTEXT00003194088&dateTexte=&categorieLien=id [dostęp: 20 IX 2017].

Cytowane przepisy rzeczywiście pozwalają na odtworzenie wielu aspektów życia prywatnego danej osoby – m.in. na ustalenie osób, z którymi utrzymuje ona regularne kontakty, usługi komunikacji elektronicznej, z których korzysta czy uzyskanie informacji o miejscach, w jakich przebywała w konkretnym czasie. Na marginesie należy wspomnieć, że zgodnie z interpretacją Trybunału Sprawiedliwości Unii Europejskiej, wyrażoną w orzeczeniu Tele2[86], krajowe uregulowania przewidujące uogólnione i niezróżnicowane (nieselektywne) zatrzymywanie przez operatorów telekomunikacyjnych wszystkich danych o ruchu i danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników dla celów zwalczania przestępczości są niezgodne z Kartą Praw Podstawowych Unii Europejskiej i dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady dotyczącej przetwarzania danych osobowych i prywatności w sektorze łączności elektronicznej[87]. Biorąc pod uwagę konstrukcję przepisów dotyczących algorytmu wprowadzonego na mocy ustawy o wywiadzie, nie sposób uznać, że powoduje on „uogólnione" i „niezróżnicowane" czy „nieselektywne" zbieranie danych. Ustawodawca jasno wskazał cel, w jakim instrument ten może być zastosowany (wyłącznie zapobieganie terroryzmowi) oraz ograniczył katalog danych zbieranych przez mechanizm przez odesłanie do art. L 851-1 i do przepisów innych aktów prawnych. Ponadto, stworzył definicję informacji i dokumentów w art. R 851-5. Analiza tych czynników sprawia jednocześnie, że określanie tego mechanizmu mianem środka masowej inwigilacji jest nietrafne, gdyż celem algorytmu nie jest nieselektywne zbieranie wszystkich możliwych informacji, lecz ściśle ukierunkowane zbieranie określonych w ustawie kategorii metadanych i tylko w celu zapobiegania zagrożeniom terrorystycznym.

4. Charakterystyka najważniejszych opinii legislacyjnych i orzeczenia Rady Konstytucyjnej odnośnie do zgodności ustawy o wywiadzie z Konstytucją

4.1. Opinia Narodowej Komisji Informatyki i Wolności (CNIL)

W początkowej fazie procesu legislacyjnego związanego z tworzeniem ustawy o wywiadzie strona rządowa argumentowała, że metadane, które mają być pozyskiwane dzięki stworzeniu systemu, będą anonimowe, przez co nawet ich ewentualna późniejsza analiza nie stwarza zagrożenia dla prywatności. Przeciwny pogląd wyraziła Narodowa Komisja Informatyki i Wolności (CNIL). Zdaniem tego organu analiza metadanych przez opisywany algorytm polega m.in. na przetwarzaniu danych osobowych, w konsekwencji zaś musi być zgodne z zasadą proporcjonalności[88].

Zgodnie z argumentami CNIL przedstawionymi w opinii nr 2015-078 w sprawie projektu ustawy o wywiadzie[89] algorytm przewidziany w ustawie o wywiadzie ma na celu wykrywanie tzw. sygnałów słabych mogących świadczyć o przygotowywaniu aktu

[86] Wyrok Trybunału z 21 XII 2016 r. w połączonych sprawach C-203/15 i C-698/15, www.curia.europa.eu. [dostęp: 20 IX 2017].

[87] *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 roku dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)* – Dz. Urz. Wspólnot Europejskich L 201 z 31 VII 2002 r.

[88] *Bulk Collection: Systematic Government Access to Private-Sector Data*, F.H. Cate, J.X. Dempsey (red.), s. 55–56, www.books.google.pl [dostęp: 15 IX 2017].

[89] *Délibération n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement*, s. 9 www.cnil.fr/sites/default/files/typo/document/D2015-078-PJLRenseignement.pdf [dostęp: 15 IX 2017].

terrorystycznego na podstawie określonych kryteriów technicznych. Pod pojęciem tych sygnałów rozumie się np. dane techniczne mogące świadczyć o zamiarach czy sposobie działania charakterystycznych dla działań terrorystycznych lub pozostawione przez zaangażowane osoby ślady działalności w Internecie, lub informacje o ich komunikacji, których osobna, jednostkowa analiza nie pozwoliłaby na stwierdzenie, że te osoby mogą prowadzić działalność o charakterze terrorystycznym. Na marginesie trzeba zaznaczyć, że opinia CNIL zwraca w tym miejscu uwagę na niezmiernie istotny aspekt zagadnienia wykrywania zagrożeń w systemach i sieciach elektronicznych – w wielu przypadkach wyłącznie pozyskanie określonego zbioru informacji może pozwolić na identyfikację konkretnego zagrożenia, wzorców zachowań czy osób zaangażowanych w działalność terrorystyczną. Informacje określane jako sygnały słabe mogą stworzyć całościowy obraz danego zagrożenia po ich odniesieniu do większej grupy osób, osobno zaś nie będą przedstawiać jakiejkolwiek wartości z punktu widzenia wywiadowczego. Treść raportu CNIL w sposób bardzo precyzyjny ilustruje istotę różnic między instrumentami masowego pozyskiwania danych a tradycyjnymi, zbliżonymi do kontroli operacyjnej narzędziami ukierunkowanymi wykorzystywanymi przez służby. Analogiczne argumenty są podnoszone w przedstawionych w części dotyczącej Wielkiej Brytanii dokumentach charakteryzujących sposób działania tzw. *bulk powers*, wprowadzonych na mocy ustawy *Investigatory Powers Act*.

Komisja CNIL zasugerowała w opinii zwrócenie przez rząd szczególnej uwagi na doniosłe znaczenie prawidłowego i konkretnego sformułowania przepisów wprowadzających omawiany mechanizm, tak aby jego interpretacja miała charakter zawężający, a wykorzystywanie w praktyce ograniczało się do sytuacji rzeczywiście związanych z zagrożeniem terrorystycznym zgodnie z zasadą proporcjonalności. Pomimo że celem algorytmu jest wykrycie elementów wskazujących na możliwość zaistnienia zdarzenia o charakterze terrorystycznym, jego działanie sprowadza się do zbierania i analizy informacji mogących bezpośrednio lub pośrednio identyfikować konkretną osobę. Zdaniem CNIL świadczy o tym przewidziany w ustawie mechanizm wyrażenia przez premiera zgody na identyfikację określonej osoby, po uzyskaniu opinii CNCTR, jeżeli algorytm wykryje czynniki wskazujące na możliwość zagrożenia terrorystycznego. Identyfikacja osoby jest zatem możliwa na podstawie danych zebranych przez „czarne skrzynki". Organ podkreśla, że automatyczne przetwarzanie danych przez opisywany system musi czynić zadość wymogom wynikającym z *Ustawy z dnia 6 stycznia 1978 r. o informatyce, bazach danych i wolnościach obywatelskich*[90]. CNIL nie stwierdza jednak w przywołanej opinii, że wprowadzenie na podstawie aktu prawa powszechnie obowiązującego systemu tzw. czarnych skrzynek stanowi *per se* naruszenie prawa do prywatności, niedające się pogodzić z zasadami demokratycznego państwa prawnego.

4.2. Opinia Rady Państwa

Przywołana opinia Rady Państwa dokonuje na wstępie krótkiej charakterystyki projektu ustawy o wywiadzie. Do jego najważniejszych elementów należy określenie warunków, w jakich służby wywiadowcze mogą posługiwać się – w określonych enumeratywnie celach – technikami pozyskiwania informacji opisanymi w ustawie, oraz wprowadzenie szczególnego trybu autoryzacji ich wykorzystania dokonywanej przez

[90] *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 [dostęp: 15 IX 2017].

premiera po uzyskaniu opinii CNCTR. W opinii podkreślono istotne znaczenie roli Rady Państwa jako organu właściwego do rozpoznawania skarg na zastosowanie technik pozyskiwania informacji wprowadzonych na mocy ustawy o wywiadzie, do których złożenia, zgodnie z art. L 841-1 kodeksu bezpieczeństwa wewnętrznego, uprawnione zarówno osoby fizyczne, jak i CNCTR.

Rada Państwa zaznacza ponadto, że w toku procesu legislacyjnego dążyła do znalezienia odpowiedniej równowagi między względami związanymi z ochroną bezpieczeństwa narodowego a poszanowaniem życia prywatnego, zgodnie z art. 2 *Powszechnej Deklaracji Praw Człowieka i Obywatela* oraz art. 8 *Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*. Z dokumentu wynika, że głównym założeniem tego organu było dążenie do wzmocnienia i doprecyzowania przepisów o charakterze gwarancyjnym mających na celu ochronę praw i wolności. Rada Państwa szczególną uwagę przywiązywała do zawarcia w ustawie przepisów przewidujących kontrolę niezależnego organu administracyjnego nad wykorzystywaniem technik pozyskiwania informacji, zarówno w momencie autoryzacji, jak i w czasie ich stosowania, oraz jednocześnie upoważniających Radę Państwa do kontroli sądowej nad stosowaniem przewidzianych w ustawie instrumentów.

Zdaniem organu najważniejszą gwarancją poszanowania praw i wolności obywatelskich w toku wykorzystywania przewidzianych w ustawie ingerujących w prawo do prywatności instrumentów służących gromadzeniu informacji jest zawarcie w ustawie precyzyjnego i zamkniętego katalogu celów, dla których te techniki mogą zostać wykorzystane. Zgodnie z art. L 811-3 ustawy kodeks bezpieczeństwa wewnętrznego, wprowadzonym do tego aktu na mocy art. 2 ustawy o wywiadzie, służby wywiadowcze mogą posługiwać się technikami przewidzianymi w tytule V księgi VIII kodeksu w celu zbierania informacji wywiadowczych istotnych z punktu widzenia obronności i wspierania następujących fundamentalnych interesów państwa:

1. Niepodległości, integralności terytorialnej i obrony narodowej.
2. Istotnych interesów polityki zagranicznej, wykonywania zobowiązań europejskich i międzynarodowych Francji oraz zapobiegania wszelkim formom zagranicznej ingerencji.
3. Istotnych interesów gospodarczych, przemysłowych i naukowych Francji.
4. Zapobiegania terroryzmowi.
5. Zapobiegania:
   1) zamachom na republikańską formę rządów,
   2) działaniom zmierzającym do odtworzenia ugrupowań rozwiązanych na podstawie art. L 212-1[91],

[91] Art. L 212-1 ustawy kodeks bezpieczeństwa wewnętrznego:
Ulegają rozwiązaniu, na mocy dekretu Rady Ministrów, stowarzyszenia i ugrupowania:
1. Prowokujące do zbrojnych manifestacji ulicznych;
2. Posiadające charakter grup zbrojnych lub prywatnych milicji, ze względu na ich formę lub militarny sposób działania;
3. Których celem jest dokonanie zamachu na integralność terytorialną lub siłowa zmiana republikańskiej formy rządów;
4. Których działalność dąży do podważenia legalności rządów republikańskich;
5. Których celem jest pozyskiwanie osób skazanych za współpracę z wrogimi państwami lub propagowanie takiej współpracy;
6. Które prowokują do dyskryminacji, nienawiści lub agresji w stosunku do osób lub grup z uwagi na ich pochodzenie, przynależność do określonej grupy etnicznej, narodu, rasy lub religii lub które propagują idee lub teorie usprawiedliwiające lub zachęcające do takiej dyskryminacji, nienawiści lub przemocy;

3) zbiorowym wystąpieniom z użyciem przemocy stwarzających poważne zagrożenie dla bezpieczeństwa publicznego,

6. Zapobiegania działalności zorganizowanych grup przestępczych.
7. Zapobiegania proliferacji broni masowego rażenia.

Kolejną fundamentalną gwarancją w opinii Rady Państwa jest zawarcie w ustawie przepisów regulujących tryb autoryzacji wykorzystywania instrumentów wprowadzonych na mocy ustawy o wywiadzie. Sposób dokonywania autoryzacji ma szczególne znaczenie w przypadku „czarnych skrzynek" z uwagi na to, że ustawodawca zdecydował się na przyjęcie w tym zakresie przepisów szczególnych powodujących, iż tryb autoryzacji tego instrumentu jest nieco odmienny od pozostałych narzędzi gromadzenia informacji.

Jak już wspomniano, zgodnie z zasadą ogólną wykorzystanie technik pozyskiwania informacji autoryzuje premier, po uprzednim zasięgnięciu opinii CNCTR (art. L 821-1 kodeksu bezpieczeństwa wewnętrznego). Szczegółowe uregulowania dotyczące autoryzacji zostały zawarte w art. L 821-2. Autoryzacja jest wydawana na pisemny i uzasadniony wniosek ministra obrony, spraw wewnętrznych, sprawiedliwości lub ministrów właściwych w zakresie gospodarki, budżetu lub ceł. Minister może upoważnić do składania tego rodzaju wniosków wyłącznie swoich bezpośrednich współpracowników upoważnionych do dostępu do informacji stanowiących tajemnicę obrony narodowej (fr. *secret de la défense nationale*). We wniosku muszą być określone następujące elementy:

1. Technika lub techniki, które mają zostać wykorzystane.
2. Służba, w imieniu której składany jest wniosek o udzielenie autoryzacji.
3. Cel lub cele, które mają zostać osiągnięte dzięki zastosowaniu określonej techniki.
4. Motywy przemawiające za zastosowaniem środków opisanych w autoryzacji.
5. Czas trwania autoryzacji.
6. Osoby, miejsca lub pojazdy, w stosunku do których mają zostać zastosowane techniki pozyskiwania informacji.

Wniosek jest przekazywany przewodniczącemu CNCTR lub, w razie jego nieobecności, jednemu z członków organu, którzy przedstawiają swoją opinię premierowi w ciągu 24 godzin. Jeżeli określony wniosek jest rozpatrywany przez zmniejszony skład lub przez pełny skład Komisji, premier jest o tym informowany, opinia zaś wydawana jest w tym przypadku w ciągu 72 godzin i przekazywana niezwłocznie premierowi. Jeżeli opinia nie zostanie przekazana premierowi w czasie, odpowiednio – 24 lub 72 godzin, wymóg jej uprzedniego uzyskania przed udzieleniem autoryzacji jest uważany za spełniony (art. L 821-3). Autoryzacja na zasadach ogólnych jest udzielana maksymalnie na okres 4 miesięcy (art. L 821-4).

Należy wyróżnić dwie zasadnicze różnice występujące w procesie autoryzacji wykorzystania „czarnych skrzynek" i pozostałych technik pozyskiwania informacji:

1) pierwsza autoryzacja w odniesieniu do tzw. *boîtes noires* może być udzielona na okres dwóch miesięcy. W zakresie ewentualnego przedłużenia art. L 851-3 II odsyła do przepisów ogólnych dotyczących przedłużenia stosowania pozostałych technik pozyskiwania informacji – wynika z tego zatem, że stosowanie „czarnych skrzynek" może zostać przedłużone o kolejne cztery miesiące po upływie początkowego, dwumiesięcznego terminu,

7. Które prowadzą, na terytorium Francji lub poza nim, działania mające na celu dokonanie aktów terrorystycznych we Francji lub za granicą.

2) przesłanką uzasadniającą stosowanie mechanizmu „czarnych skrzynek" jest wyłącznie zapobieganie terroryzmowi.

Ustawodawca wprowadził zatem w sposób expressis verbis daleko idące ograniczenie przesłanek uzasadniających stosowanie omawianego instrumentu. Porównanie norm regulujących funkcjonowanie „czarnych skrzynek" i pozostałych technik pozyskiwania informacji prowadzi zatem do wniosku, że ewentualne użycie tego środka podlega szerokim ograniczeniom przedmiotowym i jest możliwe wyłącznie w celu zapobiegania terroryzmowi. Ustawa nie przewiduje natomiast możliwości jego wykorzystania np. w celach kontrwywiadowczych czy ochrony interesów gospodarczych. Nie można zatem zgodzić się z przedstawianą wielokrotnie we francuskich mediach tezą, że „czarne skrzynki" stanowią nieukierunkowany instrument masowej inwigilacji niepodlegający dostatecznej kontroli. Zarówno przepisy ograniczające cele, w jakich algorytm ten może być wykorzystywany i ograniczenie czasu trwania jego autoryzacji w porównaniu z innymi technikami, jak i opisane w części dotyczącej podstaw prawnych rozgraniczenie między samym stosowaniem mechanizmu a identyfikacją konkretnej osoby przez GIC na podstawie danych zebranych przez „czarne skrzynki" powodują, że pozyskanie za jego pomocą informacji przez służby wywiadowcze jest poddane daleko idącym ograniczeniom.

4.3. Decyzja Rady Konstytucyjnej nr 2015-713 z 13 lipca 2015 r. [92]

Rada Konstytucyjna, zgodnie z art. 61 Konstytucji, w decyzji nr 2015-713 dokonała oceny zgodności ustawy o wywiadzie z Konstytucją[93]. Wniosek o zbadanie konstytucyjności tego aktu złożyli przewodniczący Senatu, prezydent oraz grupa 60 posłów.

Rada Konstytucyjna wydała orzeczenie po uprzednim zbadaniu zgodności ustawy z przepisami Konstytucji, kodeksu obrony, kodeksu karnego, kodeksu bezpieczeństwa wewnętrznego, ustawy o zaufaniu do gospodarki cyfrowej, kodeksu poczty i komunikacji elektronicznej i innych aktów prawnych. Wnioskodawcy zwrócili się o zbadanie zgodności przepisów ustawy o wywiadzie z prawem do poszanowania życia prywatnego, swobody komunikacji, swobody wypowiedzi oraz prawa do wniesienia skutecznego środka odwoławczego.

Charakteryzując treść fundamentalnych zasad francuskiego porządku prawnego – „norm referencyjnych"[94] (fr. *normes de référence*) Rada wskazała, że[95]:

- zgodnie z art. 34 Konstytucji na ustawodawcy ciąży obowiązek stworzenia zasad dotyczących fundamentalnych gwarancji przyznanych obywatelom mających na celu umożliwienie pełnego korzystania z ich praw i wolności, zapewnienia niezbędnej równowagi pomiędzy zapobieganiem zamachom na bezpieczeństwo publiczne, co jest niezbędne dla ochrony praw i nadrzędnych zasad konstytucyjnych, a korzystaniem z gwarantowanych na mocy Konstytucji praw i wolności, do których należą prawo do poszanowania życia prywatnego, nienaruszalność miejsca zamieszkania i tajemnica korespondencji chronione na podstawie art. 2 i 4 Deklaracji Praw Człowieka i Obywatela z 1789 r.;

[92] *Décision n° 2015-713 DC du 23 juillet 2015*, www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc-du-23-juillet-2015.144138.html [dostęp: 21 IX 2017].

[93] *Constitution du 4 octobre 1958*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006071194, [dostęp: 22 IX 2017].

[94] www.lexinter.net/JF/normes_juridiques.htm [dostęp: 22 IX 2017].

[95] Pkt 3, 4 i 5 decyzji 2015-713.

- zgodnie z art. 5 Konstytucji Prezydent Republiki jest gwarantem niepodległości i integralności terytorialnej;
- zgodnie z art. 21 Konstytucji premier kieruje pracami rządu i jest odpowiedzialny za sprawy związane z obroną narodową, sekret obrony narodowej zaś stanowi jeden z elementów mających na celu ochronę fundamentalnych interesów państwa, m.in. niepodległość i integralność terytorialna;
- zgodnie z art. 66 Konstytucji nikt nie może być w sposób arbitralny pozbawiony wolności, a władza sądownicza jest strażnikiem wolności osobistej i zapewnia jej poszanowanie na zasadach przewidzianych w ustawie;
- art. 16 *Deklaracji Praw Człowieka i Obywatela* z 1789 r. gwarantuje prawo do wniesienia skutecznego sądowego środka odwoławczego, prawo do rzetelnego procesu, a także zasadę kontradyktoryjności.

Rozważania Rady Konstytucyjnej odnoszące się do zagadnienia zgodności z Konstytucją przepisu przewidującego wprowadzenie mechanizmu „czarnych skrzynek" sprowadzają się do stwierdzenia, że ten przepis spełnia wymogi konstytucyjności i nie stanowi nieproporcjonalnego zagrożenia prawa do prywatności. Poniżej przedstawiono argumenty Rady zawarte w pkt 58-61 decyzji.

> 58. Biorąc pod uwagę, iż:
>
> – art. L 851-3 kodeksu bezpieczeństwa wewnętrznego stanowi, iż na operatorów telekomunikacyjnych i na osoby wymienione w art. L 851-1 może być nałożony obowiązek zainstalowania urządzeń technicznych służących do automatycznego przetwarzania danych mających na celu, w zależności od parametrów wskazanych w autoryzacji, wykrywanie połączeń mogących świadczyć o zagrożeniu terrorystycznym;
>
> – urządzenia te wykorzystywać będą wyłącznie informacje i dokumenty, o których mowa w art. L 851-1 nie zbierając innych danych niż odpowiadające pierwotnym parametrom i nie zezwalając na identyfikację osób, których te informacje lub dokumenty dotyczą;
>
> – podczas gdy urządzenia służące do automatycznego przetwarzania danych wykryją dane, które mogą wskazywać na istnienie zagrożenia terrorystycznego, identyfikacja tej osoby lub osób i zebranie dotyczących ich danych będą mogły zostać autoryzowane przez Premiera lub przez wyznaczoną przez niego osobę;
>
> 59. Biorąc pod uwagę, iż w opinii deputowanych wnioskujących o zbadanie zgodności przepisów ustawy z Konstytucją, biorąc pod uwagę ilość danych, które mogą potencjalnie podlegać kontroli i niedostateczne gwarancje dotyczące tzw. fałszywych trafień (faux positifs), technika przewidziana przez przedmiotowe przepisy stwarza nieproporcjonalne zagrożenie dla prawa do poszanowania życia prywatnego;
>
> 60. Biorąc pod uwagę, iż:
>
> – pozyskiwanie informacji wywiadowczych w trybie opisanym w art. L 851-3 prowadzone jest w warunkach i z poszanowaniem gwarancji opisanych w motywie 51[96];

[96] 51. Biorąc pod uwagę, że techniki pozyskiwania informacji, o których mowa w art. L 851-1 – L 851-6 oraz w art. L 852-1, są wykorzystywane, z zastrzeżeniem przepisów szczególnych, na zasadach opisanych w rozdziale I tytułu II kodeksu bezpieczeństwa wewnętrznego; iż są autoryzowane przez Premiera, na pisemny i uzasadniony wniosek ministra obrony, ministra spraw wewnętrznych, lub ministra właściwego do spraw gospodarki, budżetu lub ceł, po uzyskaniu uprzedniej opinii Narodowej Komisji Kontroli Technik Pozyskiwania Informacji; iż techniki te mogą być stosowane wyłącznie przez indywidualnie wskazanych i upoważnionych funkcjonariuszy; iż stosowane są pod kontrolą Narodowej Komisji Kontroli Technik Pozyskiwania Informa-

– technika ta może być zastosowana wyłącznie w celu zapobiegania terroryzmowi;

– zarówno samo zastosowanie tej techniki, jak również parametry automatycznego przetwarzania danych podlegają autoryzacji po uprzednim wyrażeniu opinii przez Narodową Komisję Kontroli Technik Pozyskiwania Informacji;

– pierwsza autoryzacja przyznawana jest na ograniczony czas dwóch miesięcy, zaś wniosek o przedłużenie zawierać musi opis liczby identyfikatorów wskazanych przez algorytm oraz analizę ważności informacji wskazanych przez system;

– urządzenia służące do automatycznego przetwarzania danych wykorzystują wyłącznie informacje, o których mowa w art. L 851-1, nie zbierając innych danych niż odpowiadające pierwotnym parametrom i nie zezwalając na identyfikację osób, których te informacje lub dokumenty dotyczą;

– gdy dane wykryte przez algorytm wskazywać będą na możliwość istnienia zagrożenia terrorystycznego, niezbędne będzie wydanie nowej autoryzacji przez Premiera, po uzyskaniu uprzedniej zgody Narodowej Komisji Kontroli Technik Pozyskiwania Informacji w celu identyfikacji określonej osoby;

– dane te przetwarzane są przez 60 dni licząc od momentu ich pozyskania i są niszczone po upływie tego terminu z wyjątkiem wystąpienia poważnych przesłanek świadczących o istnieniu zagrożenia terrorystycznego;

– autoryzacja wykorzystania tej techniki nie może być wydana w trybie pilnym przewidzianym w art. L 821-5;

– w konsekwencji, przepisy te nie stanowią ewidentnie nieproporcjonalnego zagrożenia dla prawa do poszanowania życia prywatnego;

– treść art. L 851-3 kodeksu bezpieczeństwa wewnętrznego musi zostać uznana za zgodną z Konstytucją.

Rada uznała zatem za zgodne z Konstytucją najważniejsze elementy ustawy o wywiadzie, podkreślając, że przewidziane w niej mechanizmy ochronne należy uznać za wystarczające w demokratycznym państwie prawnym. Szczególną uwagę trzeba zwrócić na argumentację Rady, która stanowi swego rodzaju odwrócenie logiki zazwyczaj prezentowanej w orzecznictwie TSUE (np. w cytowanym wyroku w sprawie Tele2 czy w orzeczeniu w sprawie *Digital Rights*[97]). Pomimo że, z oczywistych względów, nie wynika to z samej treści decyzji, za największe zagrożenie dla praw i wolności obywatelskich uznano powtarzające się we Francji zamachy terrorystyczne, nie zaś instrumenty mające na celu przeciwdziałanie tego rodzaju zdarzeniom. Niektórzy komenta-

cji; że skład i organizacja tego niezależnego organu administracyjnego są określone w art. L 833-1 – L 832-5 kodeksu bezpieczeństwa wewnętrznego w sposób zapewniający jego niezależność; iż zadania wymienione w art. L 833-1 – L 833-11 tego kodeksu sformułowane są w sposób zapewniający efektywność jego działań kontrolnych; iż, zgodnie z treścią art. L 841-1 tego kodeksu, zarówno Narodowa Komisja Kontroli Technik Pozyskiwania Informacji, jak również każda osoba może wnieść do Rady Państwa wniosek o zweryfikowanie, czy była wobec niego stosowana w sposób niezgodny z prawem technika pozyskiwania informacji; że w ramach stosowania art. L 871-6 tego kodeksu, działania niezbędne dla wprowadzenia technik wskazanych w art. L 851-1 – L 851-4 oraz L 852-1 mogą być wykonywane wyłącznie przez funkcjonariuszy służb lub podmiotów, nad którymi nadzór sprawuje minister właściwy do spraw komunikacji elektronicznej, operatorów sieci i dostawców usług telekomunikacji (…).

[97] Wyrok Trybunału z 8 IV 2014 r. – *Digital Rights Ireland Ltd przeciwko Minister for Communications*, Marine and Natura Resources, Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Siochana, Irlandii i Attorney General (C-293/12); Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl i in. (C-594-12); sprawy połączone C-293/12 i C-594/12, www.curia.europa.eu/juris/documents.jsf?num=C-293/12, [dostęp: 21 IX 2017].

torzy wskazują, że uznanie większości przepisów ustawy za konstytucyjne świadczyło o pragmatycznym podejściu Rady do problemu i wynikało z woli uniknięcia późniejszych zarzutów, że swoją decyzją ułatwiła działalność terrorystyczną, a jednocześnie – uniemożliwiła lub znacznie utrudniła podejmowanie odpowiednich działań przez pozostałe organy państwa[98].

Dokonana przez ten organ wykładnia polegająca na ocenie konstytucyjności ustawy o wywiadzie przez pryzmat fundamentalnych dla francuskiego porządku prawnego norm może być jednak uznana za próbę dynamicznej interpretacji przepisów w szczególnym kontekście historycznym. Tak zwane instrumenty inwigilacji zostały uznane nie za naruszenie konstytucyjnych praw i wolności, ale za środek stanowiący z jednej strony ingerencję w prawo do prywatności, z drugiej zaś – mający na celu ich ochronę przed innym, dużo poważniejszym zagrożeniem jaki jest terroryzm.

5. Wnioski

Biorąc pod uwagę, że omawiany system zgodnie z dostępnymi powszechnie informacjami nie został jeszcze aktywowany na terytorium Francji i działa tylko w odniesieniu do danych zewnętrznych, wszelkie rozważania dotyczące celowości jego istnienia, skuteczności czy zgodności z normami rangi konstytucyjnej i prawem do prywatności mają charakter wyłącznie teoretyczny. Analiza przepisów ustawy dokonana przez Radę Konstytucyjną wskazuje, że samo istnienie algorytmu „czarnych skrzynek" nie może być uznane za niezgodne z francuską konstytucją i przepisami innych ustaw, przez których pryzmat badano przepisy wprowadzające ten instrument. Jego działalność w rozumieniu przepisów ogranicza się do tzw. metadanych – informacji technicznych o połączeniach, które nie ujawniają treści komunikatów.

Ustawa wprowadza również kompleksowy system kontroli i autoryzacji, do którego najważniejszych elementów należy opinia CNCTR, autoryzacja premiera czy możliwość wniesienia skargi do Rady Państwa. Trzeba też pamiętać, że stosowanie tego rodzaju środków podlega również wewnętrznym przepisom i procedurom (np. dotyczącym ochrony informacji niejawnych czy odpowiedzialności dyscyplinarnej), które obowiązują funkcjonariuszy konkretnej służby. Należy również rozróżnić samą sferę analizy metadanych niepozwalającą na identyfikację konkretnej osoby od postępowania po ewentualnym wykryciu zagrożenia, zmierzającym do ustalenia danych pozwalających na tą identyfikację,, do którego zastosowanie mają kolejne wymogi w postaci chociażby dodatkowej autoryzacji premiera, wydanej po uzyskaniu opinii CNCTR.

Szczegółowe poznanie zasad działania algorytmu jest niemożliwe z uwagi na objęcie tych informacji tajemnicą obrony (fr. *secret défense*). Kompleksowa ocena przynajmniej jawnych aspektów jego funkcjonowania będzie możliwa po aktywowaniu systemu w odniesieniu do informacji przetwarzanych na terytorium Francji oraz po przedstawieniu przez rząd raportu o stosowaniu algorytmu, do czego jest zobowiązany najpóźniej do 30 czerwca 2018 r. (art. 25 ustawy o wywiadzie).

Pomimo wszelkich wątpliwości i braku dostatecznej ilości informacji o sposobie działania automatycznego przetwarzania danych, przewidzianego w art. L 851-3 kodeksu bezpieczeństwa wewnętrznego, należy uznać, że jest to potencjalnie efektywny in-

[98] M. Verpeaux, *La loi sur le renseignement, entre sécurité et libertés; À propos de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015*, s. 8, http://web.lexisnexis.fr/newsletter/avocats/10_2015/pdf3.pdf [dostęp: 21 IX 2017].

strument reagowania na współczesne zagrożenia o charakterze terrorystycznym. Analiza zarówno francuskiego systemu prawnego, jak i prawodawstwa innych państw pokazuje, że katalog instrumentów operacyjno-rozpoznawczych dotyczących stricte rozpoznawania i zapobiegania zagrożeniom terrorystycznym jest w rzeczywistości ograniczony. Charakter poczynań osób zaangażowanych w tego rodzaju działalność sprawia, że skuteczność tradycyjnych, bazujących na czynniku ludzkim metod, jest ograniczona. Metody opierające się chociażby na pozyskiwaniu informacji od informatorów nie pozwoliły na zapobiegnięcie serii zamachów (np. na teatr Bataclan w listopadzie 2015 r.), pomimo że z dużą dozą prawdopodobieństwa można zakładać, że francuskie służby specjalne powinny dysponować szczegółowym rozpoznaniem środowisk składających się z imigrantów pochodzących z państw Afryki Północnej czy Bliskiego Wschodu, z uwagi a strukturę etniczną społeczeństwa i duży odsetek osób pochodzących z tych regionów w stosunku do ogółu populacji.

Pomimo wszystkich wątpliwości dotyczących rzeczywistego sposobu działania algorytmu automatycznego przetwarzania danych, środek ten należy rozpatrywać w kategoriach niejako wymuszonej okolicznościami reakcji organów państwa na eskalację zagrożeń związanych z międzynarodowym terroryzmem. Obserwowane na przestrzeni kilku ostatnich lat mutacje tego zjawiska sprawiają, że zagrożenia, na które muszą reagować organy odpowiedzialne za bezpieczeństwo narodowe uległy daleko idącej ewolucji. Analogicznemu procesowi modyfikacji i adaptacji muszą zatem ulec również instrumenty wykorzystywane w celu ich zwalczania.

IV. STANY ZJEDNOCZONE AMERYKI

Pozyskiwanie zewnętrznych informacji wywiadowczych na przykładzie sekcji 702 ustawy *Foreign Intelligence Surveillance Amendments Act of 2008*[99]

W 2008 r. w USA została przyjęta ustawa *Foreign Intelligence Surveillance Amendments Act of 2008*[100] (dalej: FISA Amendments Act) wprowadzająca zmiany w obowiązującym od 1978 r. podstawowym akcie normatywnym regulującym problematykę prowadzenia działań wywiadowczych poza terytorium USA oraz nadzór nad tym procesem – *Foreign Intelligence Surveillance Act of 1978* (dalej: FISA). Jedną z najważniejszych zmian wynikających z ustawy zmieniającej FISA było wprowadzenie sekcji 702, upoważniającej prokuratora generalnego (Attorney General) i dyrektora Wywiadu Narodowego (Director of National Intelligence) do autoryzacji pozyskiwania, za pośrednictwem operatorów usług komunikacji elektronicznej, zewnętrznych informacji wywiadowczych dotyczących tzw. *non-US persons*, w stosunku do których można przypuszczać, że przebywają poza terytorium Stanów Zjednoczonych.

Przepisy sekcji 702 stanowią podstawę prawną pozyskiwania informacji o zewnętrznych zagrożeniach dla bezpieczeństwa Stanów Zjednoczonych za po-

[99] *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, https://www.intelligence.senate.gov/laws/fisa-amendments-act-2008 [dostęp: 23 IX 2017].

[100] *50 U.S. Code Chapter 36 – Foreign Intelligence Surveillance*, https://www.law.cornell.edu/uscode/text/50/chapter-36 [dostęp: 23 IX 2017].

średnictwem mechanizmów często mylnie określanych jako tzw. masowe programy inwigilacji (ang. *mass surveillance*)[101] wykorzystujących Internet i sieci telekomunikacyjne. Programy oparte na sekcji 702 pozwalają zarówno na uzyskanie metadanych, jak i treści komunikacji. Nie jest wymagane zdobycie indywidualnego nakazu sądu na gromadzenie informacji w tym trybie – kontrola specjalnego sądu utworzonego na mocy ustawy FISA – Foreign Intelligence Surveillance Court (dalej: FISC) ogranicza się do zatwierdzenia ogólnych procedur (procedur ukierunkowania i minimalizacji opisanych dalej), według których właściwe organy będą pozyskiwać zewnętrzne informacje wywiadowcze na podstawie sekcji 702[102]. Rola sądu FISC w odniesieniu do tych czynności jest zatem znacznie bardziej ograniczona niż w przypadku kontroli programu masowego pozyskiwania danych o połączeniach telefonicznych prowadzonego na podstawie sekcji 215 FISA[103].

Działania podejmowane na podstawie tych przepisów przez podmioty wchodzące w skład tzw. wspólnoty wywiadowczej (Intelligence Community), zwłaszcza Agencję Bezpieczeństwa Narodowego (National Security Agency – NSA), były określane wielokrotnie jako mające kluczowe znaczenie z punktu widzenia bezpieczeństwa narodowego USA, zwłaszcza w kontekście zapobiegania zdarzeniom o charakterze terrorystycznym[104]. Według publicznie dostępnych danych statystycznych ponad 25 proc. raportów NSA dotyczących międzynarodowego terroryzmu jest opartych na informacjach zbieranych na podstawie sekcji 702, ta proporcja zaś wykazuje tendencję rosnącą od chwili przyjęcia w 2008 r. FISA Amendments Act. Tego rodzaju dane w znacznym stopniu przyczyniły się do zrozumienia przez organy odpowiedzialne za ochronę bezpieczeństwa narodowego sposobu działania ugrupowań terrorystycznych, ustalenia ich taktyki, priorytetów czy długofalowych celów strategicznych. Jak wskazywano w rozdziałach poświęconych analogicznym instrumentom prawnym funkcjonującym w Wielkiej Brytanii i we Francji, działania w trybie sekcji 702 pozwalają nie tylko na analizę informacji o już znanych zagrożeniach, lecz także często pozwalają na wykrycie nowych przesłanek świadczących o potencjalnych działaniach terrorystycznych wymierzonych w USA i inne państwa oraz zidentyfikowanie osób zaangażowanych w te działania, nieznanych dotychczas amerykańskim służbom wywiadowczym[105].

Celem niniejszego artykułu jest dokonanie charakterystyki najważniejszych postanowień sekcji 702 i próba odpowiedzi na pytanie, czy działania podejmowane na jej podstawie mogą faktycznie być uznane za tzw. masową inwigilację oraz czy stoją one w sprzeczności z zasadami demokratycznego państwa prawnego. Autor przedstawi również argumenty podnoszone w kontekście ewentualnego przedłużenia obowiązywania sekcji 702.

---

[101] We wnioskach przedstawiono argumenty przemawiające za tym, że określenie masowe programy inwigilacji jest nieprawidłowo używane w kontekście działań prowadzonych na podstawie sekcji 702.

[102] https://cdt.org/insight/section-702-what-it-is-how-it-works/ [dostęp: 24 IX 2017].

[103] *Brennan Center for Justice at New York University School of Law, Are They Allowed To Do That*? A Breakdown of Selected Government Surveillance Programs, https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf, [dostęp: 24 IX 2017]; także: https://www.lawfareblog.com/topic/fisa-215-collection [dostęp: 24 IX 2017].

[104] P. Rosenzweig, C. Stimson, D. Shedd, *Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program*, http://www.heritage.org/defense/report/maintaining-americas-ability-collect-foreign-intelligence-the-section-702-program [dostęp: 24 IX 2017].

[105] *Privacy and Civil Liberties Oversight Board: Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014, https://www.nsa.gov/about/civil-liberties/resources/assets/files/pclob_section_702_report.pdf [dostęp: 23.IX.2017].

Biorąc pod uwagę, że przepisy sekcji wygasają z dniem 31 grudnia 2017 r.[106], dyskusja dotycząca ewentualnego przedłużenia ich obowiązywania, modyfikacji lub całościowej zmiany, prowadzona w Stanach Zjednoczonych, będzie mieć niezmiernie istotne znaczenie w odniesieniu do sposobu uregulowania kompetencji służb specjalnych i ich roli w demokratycznym społeczeństwie, a także do interpretacji wspólnej dla wszystkich państw euroatlantyckich konstytucyjnej zasady prawa do prywatności.

1. Najważniejsze postanowienia sekcji 702

Tryb pozyskiwania zewnętrznych informacji wywiadowczych na podstawie ustawy FISA Amendments Act został przewidziany w sekcji 702 (a). W celu zachowania niezbędnej spójności terminologicznej poniżej zamieszczono tłumaczenie najważniejszych elementów tego przepisu oraz definicji zawartych w ustawach FISA oraz FISA Amendments Act. Mając na względzie stopień szczegółowości omawianego aktu prawnego poniższe tłumaczenie jest jedynie odzwierciedleniem jego najistotniejszych elementów, niezbędnych dla zrozumienia całości procesu.

Sekcja 702

(a) Autoryzacja. (…) Prokurator Generalny i Narodowy Dyrektor Wywiadu mogą wspólnie autoryzować, na okres do jednego roku, licząc od daty autoryzacji, prowadzenie działań wobec osób, wobec których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych, w celu pozyskania zewnętrznych informacji wywiadowczych.

(b) Ograniczenia. Pozyskiwanie informacji autoryzowane na podstawie podsekcji (a) –

(1) nie może być celowo ukierunkowane na osoby, o których wiadomo, że w momencie pozyskiwania informacji znajdują się na terytorium Stanów Zjednoczonych;

(2) nie może być celowo ukierunkowane na osoby, w stosunku których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych, jeżeli cel pozyskiwania informacji jest ukierunkowany na osoby, w stosunku do których można racjonalnie przypuszczać, że znajdują się na terytorium Stanów Zjednoczonych;

(3) nie może być celowo ukierunkowane na podmiot USA[107] przebywający poza terytorium Stanów Zjednoczonych;

(c) Prowadzenie czynności polegających na pozyskiwaniu zewnętrznych informacji wywiadowczych

(1) Pozyskiwanie informacji autoryzowane na podstawie podsekcji (a) może być prowadzone wyłącznie, jeżeli jest to zgodne z –

(A) procedurami ukierunkowania i minimalizacji przyjętymi zgodnie z podsekcjami (d) i (e); oraz

(B) po wydaniu certyfikatu zgodnie z podsekcją (g).

(2) Ustalenie – w rozumieniu niniejszej podsekcji, dla celów podsekcji (a) pojęcie to oznacza ustalenie przez Prokuratora Generalnego i Dyrektora Wywiadu Narodo-

[106] H.R. 5949 An Act. *To extend the FISA Amendments Act of 2008 for five years*, https://www.govtrack.us/congress/bills/112/hr5949/text [dostęp: 24 IX 2017].

[107] Zgodnie z definicją zawartą w § 6010 rozdziału 69 tytułu 22 Kodeksu Stanów Zjednoczonych pojęcie United States person – tłumaczone w niniejszym opracowaniu jako podmiot amerykański – oznacza obywatela Stanów Zjednoczonych, cudzoziemca uprawnionego do stałego pobytu oraz korporację, spółkę lub inną organizację utworzoną zgodnie z prawem Stanów Zjednoczonych.

wego, że istnieją okoliczności powodujące, że brak niezwłocznej autoryzacji na podstawie podsekcji (a) spowoduje, że istotne z punktu widzenia bezpieczeństwa narodowego Stanów Zjednoczonych informacje wywiadowcze zostaną utracone lub nie będą mogły być uzyskane w odpowiednim czasie, a względy czasowe nie pozwalają na wydanie nakazu zgodnie z podsekcją (i) (3) przed implementacją takiej autoryzacji.

(d) Procedury ukierunkowania

(1) Prokurator Generalny, w porozumieniu z Dyrektorem Wywiadu Narodowego, przyjmuje procedury ukierunkowania, których celem jest –

(A) zapewnienie, że pozyskiwanie informacji autoryzowane na podstawie podsekcji (a) jest ograniczone do osób, w stosunku do których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych;

(B) zapobieganie celowemu pozyskaniu komunikacji, których nadawca lub wszyscy zamierzeni odbiorcy zgodnie z posiadaną wiedzą w czasie pozyskiwania informacji przebywają na terytorium Stanów Zjednoczonych.

(2) Kontrola sądowa – Procedury przyjęte zgodnie z paragrafem (1) podlegają kontroli sądowej zgodnie z podsekcją (i).

(e) Procedury minimalizacji

(1) Prokurator Generalny, w porozumieniu z Dyrektorem Wywiadu Narodowego, przyjmuje procedury minimalizacji spełniające kryteria przewidziane dla procedur minimalizacji opisane w sekcji 101 (h) i 301 (4) w stosunku do pozyskiwania informacji zgodnie z podsekcją (a).

(2) Kontrola sądowa – Procedury minimalizacji przyjęte zgodnie z paragrafem (1) podlegają kontroli sądowej zgodnie z podsekcją (i).

(…)

(g) Certyfikacja

(A) Z zastrzeżeniem (B), przed implementacją autoryzacji na podstawie podsekcji (a), Prokurator Generalny i Narodowy Dyrektor Wywiadu dostarczają sądowi Foreign Intelligence Surveillance Court pisemny certyfikat i inne oświadczenia, sporządzone pod przysięgą i opatrzone pieczęcią zgodnie z niniejszą podsekcją.

(B) Jeżeli Prokurator Generalny i Narodowy Dyrektor Wywiadu dokonają ustaleń zgodnie z podsekcją (c) (2), a względy czasowe nie pozwalają na złożenie certyfikatu na podstawie niniejszej podsekcji przed implementacją autoryzacji na podstawie podsekcji (a), Prokurator Generalny i Dyrektor Wywiadu Narodowego przedkładają sądowi certyfikat dla takiej autoryzacji tak szybko, jak to możliwe, jednak nie później niż 7 dni po dokonaniu ustaleń.

(2) Wymagania – Certyfikat wydany zgodnie z niniejszą podsekcją powinien –

(A) zaświadczać, że:

(i) istnieją zatwierdzone przez sąd FISC procedury, procedury złożone w celu zatwierdzenia lub takie, które zostaną złożone w celu zatwierdzenia wraz z certyfikatem, których celem jest:

(I) zapewnienie, że pozyskiwanie danych na podstawie podsekcji (a) jest ograniczone do osób, w stosunku do których można racjonalnie przypuszczać, że znajdują się poza terytorium Stanów Zjednoczonych;

(II) zapobieganie celowemu pozyskiwaniu komunikacji, których nadawca lub wszyscy zamierzeni odbiorcy w czasie pozyskania znajdują się na terytorium Stanów Zjednoczonych;

(ii) procedury minimalizacji, które mają być stosowane w odniesieniu do pozyskiwania zewnętrznych informacji wywiadowczych:

(I)spełniają kryteria określone w definicji procedur minimalizacji określone w sekcji 101 (h) oraz 301 (4) oraz;

(II) zostały zatwierdzone przez sąd FISC, złożone w celu zatwierdzenia lub zostaną złożone w celu zatwierdzenia wraz z certyfikatem;

(iv) procedury i wytyczne są zgodne z wymogami czwartej poprawki do Konstytucji Stanów Zjednoczonych;

(v) istotnym celem pozyskiwania jest uzyskanie zewnętrznych informacji wywiadowczych;

(vi) pozyskiwanie odbywa się poprzez uzyskiwanie zewnętrznych informacji wywiadowczych z pomocą operatora usług komunikacji elektronicznej.

(…)

(h) Nakazy i sądowa kontrola nakazów

(1) W odniesieniu do pozyskiwania informacji autoryzowanego na podstawie podsekcji (a) Prokurator Generalny i Dyrektor Wywiadu Narodowego mogą zobowiązać na piśmie dostawcy usług komunikacji elektronicznej do:

(A) niezwłocznego udostępnienia organom rządowym wszystkich informacji, urządzeń lub udzielenia wsparcia niezbędnego do pozyskania informacji w sposób zapewniający ochronę informacji o tym pozyskiwaniu oraz tworzący możliwie najmniejsze zakłócenia usług dostarczanych przez tego dostawcę osobie, w stosunku do której będą prowadzone te czynności;

(B) przechowywania danych dotyczących pozyskiwania informacji i udzielonej właściwym organom pomocy zgodnie z procedurami bezpieczeństwa zatwierdzonymi przez Prokuratora Generalnego i Dyrektora Wywiadu Narodowego.

Przewidziany w sekcji 702 zasięg podmiotowy pozyskiwania informacji został określony w sposób szeroki. Obejmuje on nie tylko osoby fizyczne, lecz także osoby prawne (zob. przyp. 9) Osoby te muszą zgodnie z dostępną wiedzą przebywać poza terytorium Stanów Zjednoczonych. Ustawa posługuje się pojęciem *reasonably believed to be located outside the United States,* nie wyjaśnia jednak w sposób precyzyjny, co należy rozumieć pod tym pojęciem Niemniej jednak sekcja 702 przewiduje przyjęcie tzw. procedur ukierunkowania, dzięki którym pozyskiwanie informacji w omawianym trybie będzie ograniczone do osób przebywających poza terytorium Stanów Zjednoczonych[108].

Przepis dotyczący tzw. procedur ukierunkowania ma istotne znaczenie w kontekście ochrony prawa do prywatności. Mają one zapewnić, że prowadzenie działań opisanych w sekcji 702 będzie obejmować osoby określone w ustawie jako „*non-US persons*" (przebywające poza granicami USA). Dokumenty te określają, jakie konkretnie działania będą podejmowane w tym celu przez właściwe organy. Procedury minimalizacji określają natomiast, jakie działania będą podejmowane, aby ograniczyć wykorzystywanie i przechowywanie danych pozyskiwanych zgodnie z sekcją 702. Te procedury podlegają zatwierdzeniu przez Federal Intelligence Surveillance Court (FISC)[109].

[108] *Privacy and Civil Liberties Oversight Board: Report*…, s. 21.

[109] P. Rosenzweig, C. Stimson, D. Shedd, *Maintaining America's Ability*…

Celem działań podejmowanych w trybie sekcji 702 jest pozyskiwanie zewnętrznych informacji wywiadowczych, które w rozumieniu ustawy FISA oznaczają:

> (...) (1) informacje odnoszące się, lub jeżeli dotyczą podmiotu USA są niezbędne dla zdolności Stanów Zjednoczonych do ochrony przed –
>
> (A) faktycznym lub potencjalnym atakiem lub innymi wrogimi działaniami innego państwa lub jego agenta;
>
> (B) sabotażem, międzynarodowym terroryzmem lub międzynarodową proliferacją broni masowego rażenia dokonanymi przez obce państwo lub jego agenta;
>
> (C) niejawnymi działaniami wywiadowczymi obcych służb wywiadowczych lub siatki stworzonej przez obce państwo lub jego agenta;
>
> (2) informacje dotyczące obcego państwa lub zagranicznego terytorium odnoszące się do, lub jeżeli dotyczą podmiotu USA – niezbędne do:
>
> (A) bezpieczeństwa narodowego lub obronności Stanów Zjednoczonych;
>
> (B) prowadzenia polityki zagranicznej Stanów Zjednoczonych.

2. Najważniejsze programy pozyskiwania informacji stosowane na podstawie sekcji 702

Raport *Privacy and Civil Liberties Oversight Board* z 2014 r. zawiera dokładny opis programów wykorzystywanych na podstawie sekcji 702. Największym problemem związanym z praktycznym funkcjonowaniem tych mechanizmów jest możliwość uzyskania nieautoryzowanego dostępu do informacji o podmiotach amerykańskich w toku działań ukierunkowanych na zdobycie zagranicznych danych wywiadowczych. Wyjaśnienie przyczyn tego zjawiska jest możliwe dopiero jednak po dokonaniu charakterystyki dwóch najważniejszych instrumentów wykorzystywanych na podstawie sekcji 702 – programów typu PRISM oraz *upstream collection*[110].

Zgodnie z opisem poszczególnych etapów procesu pozyskiwania zewnętrznych informacji wywiadowczych (przedstawionym w cytowanym raporcie), po uzyskaniu autoryzacji zgodnie z sekcją 702 właściwe organy rządowe przesyłają do operatorów usług komunikacji elektronicznej nakazy udzielenia pomocy w celu otrzymania danych dotyczących komunikacji określonych osób. Właściwy organ określa tzw. selektor, dzięki któremu jest możliwe oznaczenie konkretnej osoby znajdującej się w zainteresowaniu amerykańskich służb wywiadowczych. Mianem s e l e k t o r a można określić informacje służące identyfikacji komunikacji określonej osoby, może to być np. numer telefonu czy adres poczty elektronicznej. Selektory są przekazywane określonemu dostawcy usług komunikacji elektronicznej, po czym rozpoczyna on proces zbierania informacji odnoszących się do wskazanej osoby. Dalszy sposób postępowania jest uzależniony od tego, przez który ze wskazanych powyżej dwóch programów informacje mają być zbierane – PRISM czy *upstream collection*.

Zbieranie informacji z wykorzystaniem programu PRISM rozpoczyna się od przesłania przez właściwy organ administracji określonego selektora dostawcy usług komunikacji elektronicznej, mającemu siedzibę na terytorium Stanów Zjednoczonych. Ten podmiot jest zobowiązany, zgodnie z sekcją 702, do udostępnienia informacji o komunikacji wysyłanej i odbieranej przez ten selektor. Program PRISM ogranicza się wyłącznie do danych przesyłanych za pośrednictwem Internetu, nie obejmuje natomiast połączeń

[110] Tamże.

telefonicznych – dlatego można domniemywać, że najczęściej wykorzystywanym w tym przypadku selektorem będzie adres poczty elektronicznej. Wszystkie dane zebrane z wykorzystaniem programu PRISM są przekazywane NSA. Dodatkowo, część zebranych informacji trafia również do innych organów – zwłaszcza do CIA oraz FBI[111].

Upstream collection jest programem znacznie różniącym się od PRISM, zarówno pod względem sposobu zbierania danych, jak i katalogu objętych nim danych. W odróżnieniu od PRISM *upstream collection* polega na pozyskiwaniu danych dotyczących zarówno komunikacji internetowej, jak i telefonicznej. Jest on prowadzony za pośrednictwem operatorów zarządzających, tzw. *telecommunications backbone* – sieci przesyłowych skupiających dane przesyłane przez mniejsze, lokalne sieci[112]. W ten sposób NSA uzyskuje dostęp do danych transferowanych przez największe telekomunikacyjne punkty przesyłowe[113]. Uzyskane w tym trybie informacje są przekazywane wyłącznie NSA. Istotne znaczenie mają dwie kolejne różnice między programem *upstream collection* a PRISM:

1) *upstream collection* pozwala na pozyskiwanie komunikacji typu „*about*", czyli takiej, w której selektor dotyczący konkretnej osoby jest zawarty w treści komunikacji prowadzonej przez inne osoby, ona sama jednak niekoniecznie musi być stroną takiej komunikacji. Treści wymieniane przez inne strony dotyczą selektora wskazanego przez właściwy organ; są to informacje „o selektorze", stąd też nazwa „*about communications*";
2) program ten obejmuje tzw. *multiple communications transaction* (MCT) – połączenia internetowe zawierające określoną liczbę odrębnych, indywidualnych połączeń. Jeżeli jedno z nich jest połączeniem „z selsktorem", „do selektora" lub „o selektorze" (*about*), wskazanym przez właściwe organy, wówczas NSA uzyskuje dane o całym połączeniu MCT, również o pozostałych połączeniach wchodzących w jego skład, niedotyczących konkretnego selektora.

Pozyskiwanie danych o połączeniach MCT stanowiło jeden z głównych powodów kontrowersji dotyczących możliwości nieautoryzowanego monitorowania komunikacji podmiotów amerykańskich i w konsekwencji – zgodności z prawem niektórych aspektów programu *upstream collection*. Dla wyjaśnienia dokładnego charakteru połączeń MCT istotne znaczenie mają informacje znajdujące się na stronie fundacji Electronic Frontier Foundation, które zostały przekazane przez Dyrektora Wywiadu Narodowego w czasie konferencji prasowej we wrześniu 2013 r.[114] Odpowiadając na pytanie, co dokładnie należy rozumieć pod pojęciem MCT, udzielił on następującej odpowiedzi, zastrzegając, że będzie ona miała charakter ogólny, gdyż dokładne wyjaśnienie istoty tego pojęcia może dotyczyć wrażliwych kwestii operacyjnych:

> Jeżeli dana osoba posiada konto poczty elektronicznej, jak Gmail lub Hotmail, po zalogowaniu się na konto widoczny jest *screenshot* pokazujący określoną liczba e-maili znajdujących się w skrzynce odbiorczej. W przypadku mojego serwera widoczna jest data wiadomości, nadawca, temat i rozmiar wiadomości. Mogę jednak otrzymać 15 różnych [wiadomości] naraz.

[111] *Privacy and Civil Liberties Oversight Board: Report*…, s. 7.

[112] http://searchtelecom.techtarget.com/definition/backbone [dostęp: 24 IX 2017].

[113] *Intelligence Attorney on How „Multi-Communication Transactions" Allowed for Domestic Surveillance"*, https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed [dostęp: 24 IX 2017].

[114] Tamże.

> Wszystkie przesyłane są przez Internet jako jedno połączenie, pomimo że po otwarciu konta wymienionych jest 15 oddzielnych wiadomości. Z przyczyn technicznych NSA nie była i w dalszym ciągu nie jest w stanie podzielić takiej informacji na jej indywidualne komponenty.
>
> Jeżeli zatem jeden z tych maili odnosił się w temacie wiadomości do maila, do którego pierwotnie zamierzano uzyskać dostęp, zebrane zostaną dane o wszystkich wiadomościach znajdujących się w skrzynce. Działa to na zasadzie *screenshot'u*. (…)
>
> Niektóre [z tych e-maili] mogą być wyłącznie wiadomościami wewnętrznymi. Na przykład, jeżeli działania ukierunkowane są na podmiot zewnętrzny, a podmiot ten komunikuje się z podmiotem amerykańskim, możliwe jest uzyskanie całego *screenshot'u* podmiotu amerykańskiego. (…)[115].

Wątpliwości dotyczące rzeczywistego sposobu funkcjonowania programu *upstream collection* oraz możliwość naruszenia prawa do prywatności podmiotów amerykańskich, z uwagi na specyfikę technologiczną tego instrumentu, doprowadziły do podjęcia przez NSA decyzji o wstrzymaniu jego wykorzystywania w odniesieniu do komunikacji „*about*". Zgodnie z oświadczeniem z 28 kwietnia 2017 r. ten organ zdecydował, że z uwagi na kilkukrotne przypadki stosowania programu w sposób niezgodny z wymogami ustanowionymi w sekcji 702, które wynikały z trudności natury technologicznej, czynności NSA prowadzone na podstawie sekcji 702 nie będą obejmować komunikacji typu „*about*". Będą natomiast ograniczone wyłącznie do informacji przesyłanych „do" lub „z" określonego selektora wykorzystywanego przez osobę stanowiącą cel zewnętrznych działań wywiadowczych. Ten zabieg ma zmniejszyć ryzyko naruszania prawa do prywatności podmiotów amerykańskich przez ograniczenie czynności operacyjno-rozpoznawczych prowadzonych przez NSA wyłącznie do osób pozostających w bezpośrednim kontakcie z cudzoziemcami przebywającymi poza terytorium USA, znajdującymi się w zainteresowaniu służb wywiadowczych[116].

3. Wnioski

Określanie programu PRISM i *upstream collection* mianem instrumentów masowej inwigilacji elektronicznej jest pewnego rodzaju nadużyciem. Nie jest to program typu „*bulk*" działający na zasadzie pozyskiwania określonego zbioru informacji, z których potem są odfiltrowywane informacje mogące mieć znaczenie dla bezpieczeństwa narodowego[117]. Omawiane programy działają na zasadzie wykorzystywania konkretnych selektorów identyfikujących komunikację określonej osoby fizycznej znajdującej się poza terytorium USA i niebędącej tzw. *US person*. Sekcja 702 zawiera zatem dwie przesłanki negatywne powodujące, że te programy nie mają w rzeczywistości charakteru masowe-

[115] Tamże.

[116] *NSA Stops Certain Section 702 „Upstream" Activities*, April 28, 2017, https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml [dostęp: 24 IX 2017]. Więcej informacji na temat wstrzymania działań typu „*upstream collection"* przez NSA znajduje się w artykułach prasowych na stronach dzienników „New York Times" i „The Washington Post", https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html?mcubz=1 oraz https://www.washingtonpost.com/world/national-security/nsa-halts-controversial-email-collection-practice-to-preserve-larger-surveillance-program/2017/04/28/e2ddf9a0-2c3f-11e7-be51-b3fc6ff7faee_story.html?utm_term=.bf621de0b542 [dostęp: 24 IX 2017].

[117] Więcej na temat instrumentów typu „*bulk*" w części poświęconej Wielkiej Brytanii.

go pozyskiwania danych, lecz są ukierunkowane na ściśle określone osoby spełniające powyższe warunki. Ponadto ustawa zobowiązuje prokuratora generalnego i dyrektora Wywiadu Narodowego do opracowania dokumentów przewidujących konkretne działania, jakie organy administracji będą podejmować w celu wykluczenia pozyskiwania informacji o podmiotach amerykańskich (procedury minimalizacji i ukierunkowania).

Nie powinno budzić wątpliwości, że programy pozyskiwania informacji, prowadzone na podstawie sekcji 702, są nowoczesnymi i wykazującymi niezwykle wysoki stopień zaawansowania technologicznego instrumentami służącymi do wykrywania zewnętrznych zagrożeń bezpieczeństwa narodowego USA. Krytycy ustawy i przedstawiciele środowisk zaangażowanych w ochronę prawa do prywatności argumentują, że przepisy tej sekcji w aktualnym kształcie stwarzają liczne problemy, do których – jako najważniejsze – należy zaliczyć:

- ograniczony nadzór sądowy,
- niezamierzone zbieranie danych o podmiotach amerykańskich, w przypadku gdy komunikują się oni z cudzoziemcami stanowiącymi cel działań amerykańskich służb wywiadowczych, co stoi w sprzeczności z sekcją 702,
- FBI i inne organy mające uprawnienia dochodzeniowo-śledcze są uprawnione do przeszukiwania danych zebranych w sposób niezamierzony dla celów prowadzenia postępowań niemających związku z terroryzmem czy szpiegostwem, co nie odpowiada pierwotnym założeniom ustawy FISA i stanowi naruszenie czwartej poprawki do Konstytucji Stanów Zjednoczonych,
- nieznaną liczbę podmiotów amerykańskich, których dane zostały pozyskane w toku wykorzystywania programów działających na podstawie sekcji 702,
- kontrowersje związane z tzw. komunikacją *about*,
- masową inwigilację obywateli innych państw, co przyczynia się do pogorszenia opinii wspólnoty międzynarodowej o USA, utrudnia prowadzenie bieżącej polityki zagranicznej oraz powoduje straty dla amerykańskich podmiotów gospodarczych.

Zgodnie z oficjalnym stanowiskiem Białego Domu administracja prezydenta Donalda Trumpa będzie dążyć do utrzymania przepisów sekcji 702 w niezmienionym stanie, biorąc pod uwagę istotne znaczenie wykorzystywanych na jej podstawie programów dla bezpieczeństwa narodowego[118]. Prokurator generalny Jeff Sessions oraz dyrektor Wywiadu Narodowego Dan Coats w liście z 7 września 2017 r. skierowanym do liderów Partii Demokratycznej i Partii Republikańskiej określili reautoryzację przez Kongres przepisów sekcji 702 jako najważniejszy cel legislacyjny Departamentu Sprawiedliwości i Wspólnoty Wywiadowczej[119].

Kontrowersje związane z tzw. masową inwigilacją i kierowane głównie pod adresem NSA zarzuty o niezgodne z prawem praktyki, polegające na niczym nieograniczonym pozyskiwaniem danych przesyłanych za pośrednictwem środków komunikacji elektronicznej czy rozmów telefonicznych, w dużej mierze wynikają z niejawności szczegółowych zasad działania tych programów, sama zaś analiza przepisów ustaw FISA czy FISA Amendments Act nie pozwala na ich dokładne zrozumienie. Jak wskazano w części poświęconej programom PRISM czy *upstream collection*, incydenty zwią-

[118] D. Volz, S. Holland, *White House supports renewal of spy law without reforms: official*, https://www.reuters.com/article/us-usa-trump-fisa/white-house-supports-renewal-of-spy-law-without-reforms-official-idUSKBN16855P [dostęp: 24 IX 2017].

[119] K. Bo Williams, *Sessions, Coats push for permanent renewal of controversial surveillance law*, http://thehill.com/policy/national-security/350155-sessions-coats-push-for-permanent-702-renewal [dostęp: 24 IX 2017].

zane z uzyskaniem danych podmiotów amerykańskich w sposób niezgodny z sekcją 702 wynikają z obiektywnych trudności technologicznych, immanentnie związanych ze sposobem funkcjonowania Internetu i międzynarodowych sieci telekomunikacyjnych. Należy zwrócić uwagę na to, że zaprzestanie przez NSA pozyskiwania komunikacji typu „*about*" w ramach programu *upstream collection* pokazuje, że system nadzoru nad rzeczywistym wykorzystywaniem tego rodzaju instrumentów, zarówno w ramach samej NSA, jak i sprawowanego przez inne organy, jest na tyle efektywny, że jest w stanie wykryć zagrażające prawu do prywatności nieprawidłowości i podjąć odpowiednie środki zaradcze. Pomimo wielu wątpliwości co do dalszego istnienia sekcji 702 po 31 grudnia 2017 r., całkowite usunięcie jej przepisów z amerykańskiego systemu prawnego należy uznać za mało prawdopodobne. Ponadto byłoby to zjawisko szkodliwe zarówno z punktu widzenia bezpieczeństwa narodowego, jak i ochrony prywatności.

Brak zgody Kongresu na przedłużenie obowiązywania sekcji 702 skutkowałby, po pierwsze, powstaniem luki prawnej powodującej, że służby wywiadowcze byłyby zmuszone do działania w obszarze nieuregulowanym jakimkolwiek aktem normatywnym, po drugie zaś – przestałyby obowiązywać jakiekolwiek mechanizmy ochronne funkcjonujące na podstawie omawianych ustaw. Najbardziej korzystnym rozwiązaniem z punktu widzenia ochrony obu fundamentalnych wartości – bezpieczeństwa narodowego i prawa do prywatności – byłaby modyfikacja przepisów sekcji 702 w sposób ograniczający ryzyko związane ze stosowaniem programów typu PRISM czy *upstream collection*, np. przez zwiększenie zakresu kontroli sądowej sprawowanej przez sąd FISC czy ograniczenie możliwości korzystania z zebranych w ten sposób informacji przez służby inne niż NSA. Należy też pamiętać, że duża część problemów związanych ze stosowaniem omawianych mechanizmów ma swoje źródło nie w prawie, lecz w aspektach technologicznych związanych zarówno ze sposobem funkcjonowania nowoczesnych środków komunikacji, jak i z ograniczeniami samej NSA. Zorientowane na sferę zewnętrzną działania wywiadowcze, czy szerzej – działania wszystkich służb specjalnych, zmierzające do ochrony bezpieczeństwa narodowego, prowadzą do powstania nieprawidłowości, występujących z różnym nasileniem, naruszających wolności i prawa obywatelskie. Niemniej jednak zgodność przepisów stanowiących ich podstawę normatywną z normami rangi konstytucyjnej należy oceniać przez pryzmat efektywnego systemu nadzoru i kontroli. Trzeba również wziąć pod uwagę, w jakim stopniu te działania przyczyniają się do ochrony innych wartości stanowiących podstawę demokratycznego państwa prawnego – prawa do życia czy prawa do bezpieczeństwa, bez których prawo do prywatności byłoby jedynie teoretyczną, niemożliwą do urzeczywistnienia koncepcją.

V. WIELKA BRYTANIA

Ujawnienie w 2013 r. przez byłego pracownika amerykańskiej Agencji Bezpieczeństwa Narodowego informacji dotyczących istnienia i zasad funkcjonowania programów masowej inwigilacji wykorzystywanych przez USA, Wielką Brytanię i pozostałe państwa tzw. Pięciorga Oczu (*Five Eyes*) dało początek prowadzonej niemal we wszystkich państwach Unii Europejskiej i NATO dyskusji dotyczącej sposobu rozumienia prawa do prywatności, roli służb specjalnych we współczesnym świecie i wykorzystywanych przez nie instrumentów. Sposób realizacji zadań w sferze bezpieczeństwa narodowego przez upraw-

nione do tego organy jest warunkowany dwoma podstawowymi czynnikami: po pierwsze, dogłębną ewolucją charakteru zagrożeń, na jakie muszą reagować tego rodzaju instytucje, oraz – po drugie – bezprecedensowym rozwojem środków komunikacji elektronicznej i stale zwiększającą się rolą Internetu w niemal wszystkich aspektach życia społecznego. Problem charakteru i zakresu uprawnień przyznanych zarówno służbom zorientowanym na zewnętrzne działania wywiadowcze, jak i organów zajmujących się ochroną bezpieczeństwa wewnętrznego państwa jest nierozerwalnie powiązany z koniecznością znalezienia odpowiednich proporcji między bezpieczeństwem a prawem do prywatności.

Pomimo że przepisy prawne zezwalające na wykorzystywanie przez służby tzw. programów masowej inwigilacji (ang. *mass surveillance*) budzą w naturalny sposób liczne wątpliwości co do ich zgodności zarówno ze standardami konstytucyjnymi na gruncie prawa krajowego, jak i z zakresem praw i wolności przyznawanych na mocy aktów prawa międzynarodowego, opinie ograniczające się do uznania tego rodzaju regulacji za z zasady niezgodne z podstawowymi wartościami demokratycznego państwa prawnego byłoby zbyt daleko idącym uproszczeniem. Ocena skutków społecznych tego rodzaju rozwiązań oraz ich implikacji dla funkcjonowania całego porządku prawnego powinna być dokonywana w sposób dynamiczny, uwzględniający ewolucję zagrożeń dla bezpieczeństwa państwa oraz to, że coraz więcej z nich rozwija się w przestrzeni wirtualnej. Istotne znaczenie w tym kontekście ma nie samo istnienie i wykorzystywanie tego rodzaju instrumentów, lecz działający równolegle niezależny od służb sposób nadzoru umożliwiający weryfikację ich faktycznego działania i zapobieganie ewentualnym naruszeniom.

Celem niniejszego artykułu jest dokonanie charakterystyki niektórych aspektów funkcjonowania w Wielkiej Brytanii dwóch instrumentów przewidzianych w ustawie *Investigatory Powers Act 2016,* która została przyjętej w listopadzie 2016 r.[120] – *Bulk Interception* (masowe przechwytywanie komunikacji zagranicznej) oraz *Bulk Equipment Interference* (masowa ingerencja w urządzenia informatyczne). Analiza rozwiązań brytyjskich w zakresie uprawnień operacyjno-rozpoznawczych może mieć istotne znaczenie w kontekście dyskusji nad sposobami przeciwdziałania obserwowanej intensyfikacji zagrożeń o charakterze terrorystycznym. Głównym aspektem przywołanych instrumentów jest to, że stanowią one nowoczesne środki zdobywania informacji umożliwiające służbom dostęp do ogromnych ilości informacji wymienianych za pośrednictwem środków komunikacji elektronicznej. Te instrumenty wykorzystują równocześnie narzędzia filtrowania i segregacji danych, odrzucając elementy nieprzydatne z punktu widzenia bezpieczeństwa państwa. Wykorzystywanie tego rodzaju instrumentów należy postrzegać nie w kategoriach bezprawnego i nieuzasadnionego zamachu na prawa i wolności obywatelskie czy dążenia brytyjskich służb do niekontrolowanego pozyskiwania informacji o obywatelach, lecz jako próbę dostosowania nieprzystających często do rzeczywistych wyzwań narzędzi wykorzystywanych przez te podmioty w toku realizacji ich ustawowych zadań. Zasadne wydaje się uznanie, że przyjęcie tego rodzaju rozwiązań legislacyjnych i nadanie formalnoprawnych ram działaniom operacyjno-rozpoznawczym w sferze informatyki i telekomunikacji jest wyrazem dążenia do zrównania możliwości działania państwa w zestawieniu z osobami bądź ugrupowaniami stwarzającymi zagrożenie dla podstaw jego funkcjonowania.

Analiza przywołanych rozwiązań legislacyjnych i obserwowana na przestrzeni kilku ostatnich lat ewolucja katalogu instrumentów operacyjno-rozpoznawczych[121]

[120] *Investigatory Powers Act 2016*, www.legislation.gov.uk/ukpga/2016/25/contents/enacted [dostęp: 22 VIII 2017].

[121] Oprócz opisywanych rozwiązań brytyjskich dobrym przykładem w kontekście ewolucji rozwiązań

wykorzystywanych przez służby państw UE i NATO wskazuje, że państwa, które są najbardziej narażone na zagrożenia o charakterze terrorystycznym, konsekwentnie wprowadzają środki umożliwiające skuteczne gromadzenie danych za pośrednictwem systemów i sieci informatycznych. Tendencja ta prawdopodobnie będzie prowadzić do stopniowego ograniczania wykorzystywania tradycyjnych metod pozyskiwania informacji, przy jednoczesnym poszerzaniu sposobu i zakresu wykorzystywania inwigilacji elektronicznej.

1. *Bulk interception*

Bulk interception (masowe przechwytywanie) jest instrumentem umożliwiającym zdobywanie zewnętrznych informacji wywiadowczych (ang. *foreign-focused intelligence*) oraz identyfikację osób, grup oraz organizacji mogących stanowić zagrożenie dla bezpieczeństwa Wielkiej Brytanii. Ten mechanizm polega na przechwytywaniu komunikacji (zarówno treści, jak i danych telekomunikacyjnych) osób przebywających poza jej terytorium oraz filtrowaniu i analizie materiału mogącego mieć znaczenie wywiadowcze. Istota masowych instrumentów pozyskiwania informacji, w tym *bulk interception*, polega na gromadzeniu dużych ilości informacji, z których jedynie część będzie dotyczyć osób mogących stwarzać potencjalne zagrożenie dla bezpieczeństwa narodowego.

Opisywany mechanizm to jeden z podstawowych komponentów działań ukierunkowanych na pozyskiwanie informacji o zdarzeniach wykazujących powiązania z osobami lub podmiotami znajdującymi się poza terytorium Wielkiej Brytanii zagrażających bezpieczeństwu Wielkiej Brytanii. W większości przypadków wiedza służb odpowiedzialnych za ochronę bezpieczeństwa narodowego o ewentualnych zagrożeniach zewnętrznych, stwarzanych przez osoby lub ugrupowania znajdujące się poza jej terytorium, ma charakter wysoce fragmentaryczny i nieweryfikowalny. Ponadto – mając na względzie wykorzystywanie coraz bardziej wyrafinowanych metod komunikacji elektronicznej przez osoby powiązane z działalnością terrorystyczną, zagraniczne służby wywiadowcze, członków transgranicznych zorganizowanych grup przestępczych, a także brak możliwości dokładnego ustalenia technicznych aspektów przesyłu określonej wiadomości spowodowany strukturą zależności i powiązań internetowych metod komunikacji – w wielu sytuacjach masowe przechwytywanie jest jedyną metodą pozwalającą na wykrycie i skuteczne przeciwdziałanie określonemu zagrożenia. Masowe pozyskiwanie danych pozwala na dokonanie ich całościowej analizy, identyfikację połączeń pomiędzy osobami stwarzającymi zagrożenie i podjęcie odpowiednich działań zapobiegawczych.

Założeniem masowego przechwytywania nie jest jednak próba uzyskania dostępu do całości ruchu internetowego. Działanie tego rodzaju nie mogłoby w efektywny sposób realizować faktycznych potrzeb wywiadowczych ani też nie spełniałoby kryterium proporcjonalności. Wykorzystywane przez służbę GCHQ[122] systemy masowego przechwytywania komunikacji ograniczają się do bardzo zawężonej części globalnej infrastruktury sieci Internet. Dokonują one filtrowania ruchu internetowego na podstawie szeregu kryteriów

prawnych dotyczących instrumentów operacyjno-rozpoznawczych było przyjęcie we Francji ustawy o wywiadzie z 24 lipca 2015 r. (*Loi n°2015-912 du 24 juillet relative au renseignement*), www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id [dostęp: 22 VIII 2017].

[122] Government Communications Headquarters (Centrala Łączności Rządowej) – zgodnie z ustawą *Investigatory Powers Act* jest jedyną brytyjską służbą uprawnioną do prowadzenia masowego przechwytywania (ang. *bulk interception*).

(tzw. selektorów) pozwalających na ustalenie konkretnych priorytetów odpowiadających najważniejszym celom operacyjnym służby. Przechwycona komunikacja podlega dalszej analizie po spełnieniu warunków wynikających z przepisów wewnętrznych i tylko wtedy, gdy jest to niezbędne i proporcjonalne dla realizacji zadań służby[123].

1.1. Podstawy prawne

Masowe przechwytywanie zostało uregulowane w rozdziale 1 części 6 ustawy *Investigatory Powers Act* 2016 z 29 listopada 2016 r.[124] (dalej: IPA). Omawiany akt utrzymał najistotniejsze postanowienia ustawy *Regulation of Investigatory Powers Act* z 2000 r. (dalej: RIPA), które odnosiły się do omawianego instrumentu, wprowadzając jednocześnie dodatkowe mechanizmy ochronne mające na celu zwiększenie kontroli nad wykorzystywaniem masowego przechwytywania w praktyce i wzmocnienie instrumentów chroniących prawo do prywatności.

Analogicznie do przepisów ustawy RIPA nakazy autoryzujące masowe przechwytywanie będą wydawane w dalszym ciągu przez Sekretarza Stanu; jednak w myśl ustawy IPA będą podlegać zatwierdzeniu przez Komisarza (Judicial Commissioner) – organu oceniającego niezbędność, proporcjonalność i celowość wydania nakazu w konkretnym przypadku. Wprowadzona przez ustawę IPA procedura dwustopniowej autoryzacji nakazów (ang. *double lock*), obowiązująca nie tylko w przypadku masowego przechwytywania, lecz także w odniesieniu do innych instrumentów zdobywania informacji opisanych w ustawie, jest jedną z najbardziej doniosłych zmian w brytyjskim systemie przepisów prawnych regulujących sferę funkcjonowania służb specjalnych i wykorzystywania przez nie środków niejawnego pozyskiwania informacji. Ciężar oceny, czy charakter określonej sytuacji rzeczywiście uzasadnia wykorzystanie mechanizmów charakteryzujących się wysokim stopniem inwazyjności i potencjalnie mogących stwarzać poważne zagrożenia dla konstytucyjnych praw i wolności, został rozłożony pomiędzy organ władzy wykonawczej (Sekretarz Stanu) i organ o charakterze quasi-sądowym (Komisarz). Pomimo iż szczegółowa analiza systemu kontroli sądowej nad procesem stosowania środków przewidzianych w ustawie wspomnieć w tym miejscu należy, że skargi w zakresie ich niezgodnego z prawem stosowania rozpatruje Investigatory Powers Tribunal utworzony na podstawie sekcji 65 ustawy RIPA. Należy podkreślić, że ustawa IPA wprowadziła możliwość odwołania się od orzeczeń Trybunału do innego sądu krajowego (sekcja 242 IPA).

Ustawa stworzyła również instytucję Investigatory Powers Commissioner – organ nadzorczy skupiający w sobie kompetencje realizowane dotychczas przez trzy oddzielne podmioty (Chief Surveillance Commissioner, Interception of Communications Commissioner and Intelligence Services Commissioner). Dnia 1 września 2017 r. na to stanowisko został powołany sir Adrian Fulford[125]. Zgodnie z art. 229 IPA organ ten kontroluje, przez audyt, inspekcje i inne czynności wyjaśniające, wykonywanie przez organy władzy publicznej zadań związanych z przechwytywaniem komunikacji, pozyskiwaniem i retencją danych komunikacyjnych, pozyskiwaniem danych wtórnych lub związanych z nimi danych systemowych oraz ingerencją w urządzenia.

---

[123] *Investigatory Powers Bill: Operational Case for Bulk Powers*, 1 March 2016, par. 7.1–7.3, s. 26, www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents; [dostęp: 24 VII 2017].

[124] www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm [dostęp: 24 VII 2014].

[125] https://www.gov.uk/government/news/investigatory-powers-commissioner-establishes-oversight-regime, http://ipco.org.uk/ [dostęp: 22 IX 2017].

Zgodnie z sekcją 136 ustawy IPA nakaz masowego przechwytywania (ang. *bulk interception warrant*) musi spełniać dwa warunki.

Warunek A. Głównym celem nakazu jest przechwycenie zagranicznej łączności lub zdobycie za jej pośrednictwem tzw. danych wtórnych (ang. *secondary data*). Pojęcie zagranicznej łączności (ang. *overseas-related communications*) oznacza komunikację wysyłaną lub odbieraną przez osoby znajdujące się poza terytorium Wysp Brytyjskich (podsekcja 3). Dane wtórne, w kontekście łączności przesyłanej z wykorzystaniem systemu telekomunikacyjnego, oznaczają dane opisane w sekcji 137 (4) i (5), które mają następujące cechy:

1) są to dane systemowe[126] dołączone do określonego komunikatu, logicznie z nim powiązane lub stanowiące jego część (przez nadawcę lub w inny sposób);
2) są to dane identyfikujące[127] posiadające następujące cechy:
   – są dołączone do określonego komunikatu, logicznie z nim powiązane lub stanowiące jego część (przez nadawcę lub w inny sposób),
   – mogą być logicznie odłączone od reszty komunikatu,
   – w razie odłączenia nie ujawniłyby niczego, co może w rozsądny sposób zostać uznane za mające znaczenie dla komunikatu, pomijając znaczenie wynikające z samej komunikacji lub jakichkolwiek danych dotyczących przesyłu komunikatu.

Pozyskiwanie danych wtórnych jest możliwe zarówno w fazie przesyłu komunikatu, jak i w każdym czasie, gdy jest on przechowywany w systemie lub przez ten system, zarówno przed, jak i po dokonaniu przesyłu [sekcja 137 (2)].

Warunek B. Nakaz zobowiązuje osobę, do której jest skierowany, do realizacji czynności w nim opisanych lub autoryzuje ich dokonanie przez podjęcie następujących działań:

1) przechwycenie, w trakcie przesyłu za pośrednictwem systemu telekomunikacyjnego, łączności opisanej w nakazie,
2) uzyskanie opisanych w nakazie danych wtórnych pochodzących z łączności przesyłanej z wykorzystaniem takiego systemu,
3) dokonanie w sposób opisany w nakazie selekcji przechwyconej treści komunikatów lub danych wtórnych uzyskanych na podstawie nakazu,
4) ujawnienie w sposób opisany w nakazie informacji uzyskanych na jego podstawie osobom, do których skierowany jest nakaz lub osobom działającym w ich imieniu.

Nakaz masowego przechwytywania autoryzuje również dokonanie dodatkowych czynności nieprzewidzianych wprost w treści dokumentu, niezbędnych dla realizacji głównego celu wymienionego w nakazie, z uwzględnieniem przechwycenia łączności niewyszczególnionej w nakazie i uzyskania pochodzących z niej danych wtórnych, zobowiązanie innych osób do udzielenia pomocy w realizacji nakazu, a także uzyskanie od operatora telekomunikacyjnego powiązanych danych systemowych[128].

---

[126] Sekcja 263 (4) IPA– „Dane systemowe w rozumieniu ustawy oznaczają jakiekolwiek dane ułatwiające lub umożliwiające identyfikację wszelkich elementów umożliwiających lub ułatwiających funkcjonowanie –

a) usług pocztowych;
b) systemu telekomunikacyjnego (z uwzględnieniem wszystkich urządzeń stanowiących jego cześć);
c) usługi telekomunikacyjnej dostarczanej za pośrednictwem systemu telekomunikacyjnego;
d) systemu przechowującego dane o komunikacji i inne informacje;
e) usług dostarczanych przez system przechowujący dane o komunikacji i inne informacje".

[127] Sekcja 263 (2) – „Dane identyfikujące w rozumieniu ustawy oznaczają dane ułatwiające lub umożliwiające identyfikację osoby, urządzenia, systemu lub usługi, zdarzenia, lokalizacji osoby, zdarzenia lub innego elementu" (wszystkie tłum. aut.).

[128] Powiązane dane systemowe (ang. *related systems data*), zgodnie z sekcją 136 (6), oznaczają dane systemowe dotyczące łączności będącej przedmiotem nakazu, jej nadawcy, odbiorcy lub zamierzonego odbiorcy, niezależnie od tego, czy jest to osoba fizyczna.

1.2. Rodzaje nakazów przechwytywania danych – najważniejsze różnice pomiędzy tzw. nakazami ukierunkowanymi (*targeted interception warrant*) a nakazami *bulk interception*[129]

Ustawa IPA rozróżnia następujące rodzaje nakazów przechwytywania danych: nakazy ukierunkowane, nakazy masowego przechwytywania danych, nakazy selekcji materiału zebranego za pomocą *bulk interception* do dalszej analizy oraz nakazy wydawane w ramach realizacji wniosku o współpracę wydanego przez właściwe organy innych państw (ang. *mutual assistance warrant*). Pomimo że celem niniejszego opracowania jest charakterystyka instrumentów typu „*bulk*", niezbędne jest wskazanie najważniejszych różnic pomiędzy masowymi a ukierunkowanymi nakazami przechwytywania informacji.

- Nakaz ukierunkowany [sekcja 15 (2)] – autoryzuje podjęcie przez osobę, do której jest skierowany, czynności polegających na przechwyceniu komunikacji wskazanej w nakazie lub pozyskania danych wtórnych.
- Nakaz selekcji materiału zebranego za pomocą *bulk interception* do dalszej analizy [sekcja 15 (3)] – autoryzuje podjęcie przez osobę, do której jest skierowany, czynności polegających na wstępnym oszacowaniu materiału zebranego w toku masowego przechwytywania danych i selekcji wybranych elementów do dalszej analizy. Ten nakaz musi być wydany wówczas, gdy treść przechwyconej komunikacji ma zostać poddana analizie na podstawie kryteriów dotyczących osoby, która według dostępnych informacji przebywa na terytorium Wielkiej Brytanii w chwili selekcji materiału do dalszej analizy. Wydanie tego rodzaju nakazu znosi ustanowiony na podstawie sekcji 152 (4) zakaz selekcji do dalszej analizy treści komunikacji, jeżeli kryteria wykorzystane w celu selekcji przechwyconego materiału odnoszą się do osoby znajdującej się według dostępnej wiedzy na terytorium Wysp Brytyjskich lub jeżeli te kryteria zastosowano w celu zidentyfikowania treści komunikacji wysłanej lub odebranej przez taką osobę.
- Nakaz masowego przechwytywania (sekcja 136) – jego głównym celem jest przechwycenie zagranicznej komunikacji lub uzyskanie danych wtórnych pochodzących z tej komunikacji. Autoryzuje on jednorazowe lub wielokrotne przechwycenie komunikacji, uzyskanie danych wtórnych oraz selekcję przechwyconego materiału do dalszej analizy. Może on dotyczyć również wyłącznie danych wtórnych. W odróżnieniu od nakazów o charakterze ukierunkowanym może on dotyczyć komunikacji określonego zbioru osób, nie zaś indywidualnie wskazanego podmiotu. Druga zasadnicza różnica między nakazem ukierunkowanym a masowym polega na odmiennym zakresie przedmiotowym obu nakazów – sekcja 136 dotyczy przechwytywania zagranicznej komunikacji i pozyskiwania związanych z nią danych wtórnych, *a contrario* – należy zatem wnioskować, że nakaz ukierunkowany dotyczy przechwytywania komunikacji prowadzonej na terytorium Wielkiej Brytanii i zdobywania związanych z nią danych wtórnych.

[129] *Interception of Communications – Draft Code of Practice* s. 12–13, www.gov.uk/government/consultations/investigatory-powers-act-2016-codes-of-practice [dostęp: 17 VIII 2017].

1.3. Proces wydawania nakazu masowego przechwytywania (sekcja 138)

Jak wskazano na wstępie, proces wydawania nakazu dokonania czynności związanych z masowym przechwytywaniem danych ma charakter dwustopniowy. W celu wzmocnienia standardów ochrony prywatności cała konstrukcja wykorzystywania środków opisanych w ustawie IPA została oparta na modelu *double lock* zakładającym powierzenie autoryzacji wniosków dwóm niezależnym od siebie organom dokonującym autoryzacji wniosków – Sekretarzowi Stanu i Komisarzowi.

Na wstępie należy wskazać, że mechanizm masowego przechwytywania jest ściśle powiązany ze sferą ochrony bezpieczeństwa narodowego. Zgodnie z sekcja 138 (1) (b) Sekretarz Stanu może, na wniosek szefa jednej ze służb wywiadowczych[130], wydać omawiany nakaz, jeżeli jest to niezbędne:

- w celu ochrony interesu bezpieczeństwa narodowego,
- w tym celu i w którymkolwiek z celów opisanych w podsekcji (2).

Przedstawiony powyżej sposób sformułowania sekcji 138 sprawia, że ustawodawca wprowadził bezwzględny wymóg istnienia związku dwóch pozostałych przesłanek, – zapobiegania i wykrywania poważnej przestępczości oraz ochrony interesów ekonomicznych UK – z bezpieczeństwem narodowym.

Ustawodawca wprowadził ponadto dalsze mechanizmy ograniczające możliwość wykorzystania *bulk interception* w praktyce. Wydanie nakazu w celu ochrony interesów ekonomicznych jest możliwe tylko wtedy, gdy informacje, które mają zostać uzyskane dzięki zastosowaniu mechanizmu, dotyczą działań lub zamierzeń osób znajdujących się poza terytorium Wysp Brytyjskich [sekcja 138 (3)]. Ustawa wyklucza możliwość wydania nakazu, jeżeli ma on służyć wyłącznie pozyskiwaniu dowodów dla celów postępowania karnego [sekcja 138 (4)]. Biorąc pod uwagę konstrukcję przepisów sekcji 138 określających przesłanki materialne stosowania masowego przechwytywania w praktyce, należy zwrócić uwagę na to, że ustawodawca znacznie ograniczył możliwość wykorzystywania tego instrumentu w celu ścigania przestępczości. Przepis sekcji 138 (1) (b) w zw. z podsekcją (2) (a) oraz (4) sprawia, że mechanizm *bulk interception* będzie mógł być stosowany wyłącznie w odniesieniu do wąskiej kategorii przestępstw uznawanych za zagrażające bezpieczeństwu narodowemu (np. przestępstwo szpiegostwa, terroryzmu oraz czyny zabronione związane z proliferacją broni masowego rażenia). Wyłączenie możliwości wykorzystania masowego przechwytywania jedynie w celu zbierania dowodów dla celów postępowania karnego sprawia, że ten instrument będzie miał zastosowanie na etapie rozpoznawania i wykrywania przestępstw zagrażających bezpieczeństwu narodowemu, nie zaś na etapie ewentualnego postępowania sądowego. Opisane powyżej elementy sprawiają, że *bulk interception* należy traktować jako środek o charakterze stricte wywiadowczym, jego zaś rolę w procesie zwalczania przestępczości należy uznać za pomocniczą.

Oprócz wymienionych powyżej przesłanek materialnych sekcja 138 przewiduje następujące warunki wydania nakazu masowego przechwytywania, stanowiąc, że jest to możliwe, jeżeli w opinii Sekretarza Stanu:

- głównym celem nakazu jest przechwycenie zagranicznej łączności (ang. *overseas -related communications*) lub uzyskanie pochodzących z niej danych wtórnych,

[130] Sekcja 263 (1) – „Pojęcie *h e a d* , w odniesieniu do służb wywiadowczych, oznacza –
a) w odniesieniu do Security Service – Dyrektora Generalnego,
b) w odniesieniu do Secret Intelligence Service – Szefa,
c) w odniesieniu do GCHQ – Dyrektora".

- działania autoryzowane na podstawie nakazu są proporcjonalne do zakładanego celu,
- wszystkie wskazane we wniosku o wydanie nakazu cele operacyjne[131] są celami, dla których analiza przechwyconej treści komunikatów lub danych wtórnych jest lub może być konieczna,
- analiza przechwyconej treści komunikatów lub danych wtórnych jest niezbędna w kontekście wszystkich celów operacyjnych z jakichkolwiek powodów, dla których Sekretarz Stanu uznaje wydanie nakazu za niezbędne,
- istnieją wystarczające środki zabezpieczające odnoszące się m.in. do procedur związanych z wykorzystywaniem przechwyconego materiału, jego dalszym ujawnieniem i innymi aspektami dotyczącymi jego ochrony,
- wydanie nakazu zostało zatwierdzone przez Komisarza.
- Jeżeli w opinii Sekretarza Stanu jest prawdopodobne, że realizacja nakazu będzie wymagała pomocy operatora telekomunikacyjnego działającego poza Wielką Brytanią, ustawa nakłada na Sekretarza Stanu obligatoryjny wymóg przeprowadzenia konsultacji z tym operatorem oraz dokonania oceny, przed wydaniem nakazu, m.in. liczby użytkowników usług telekomunikacyjnych dostarczanych przez operatora objętych masowym przechwytywaniem, możliwości technicznych operatora co do udzielenia przez niego pomocy w realizacji nakazu, koszt takiej pomocy i inne ewentualne skutki wykonania nakazu dla operatora (sekcja 139).

1.4. Zatwierdzenie nakazu przez Komisarza

Przy dokonywaniu oceny decyzji o wydaniu nakazu (sekcja 140) Komisarz weryfikuje wnioski Sekretarza Stanu dotyczące:

- konieczności wydania nakazu w związku z przesłankami wymienionymi w sekcji 138 (1) (b) – bezpieczeństwem narodowym, zapobieganiem i wykrywaniem poważnej przestępczości oraz ochroną interesów ekonomicznych istotnych z punktu widzenia bezpieczeństwa narodowego,
- proporcjonalności czynności opisanych w nakazie do zakładanego celu,
- sprawdzenia, czy wskazane w nakazie cele operacyjne mogą zostać uznane za cele, dla których realizacji dalsza analiza przechwyconych treści komunikatów lub danych wtórnych jest lub może być niezbędna,
- weryfikacji, czy analiza przechwyconych treści komunikatów lub danych wtórnych jest niezbędna dla realizacji każdego z ww. celów.

W razie odmowy zatwierdzenia decyzji o wydaniu nakazu Komisarz informuje o tym pisemnie Sekretarza Stanu.

1.5. Wymogi formalne nakazu

Zgodnie z sekcją 142 nakaz masowego przechwytywania musi spełniać określone kryteria formalne. Do najważniejszych z nich należą:

- wzmianka identyfikująca dokument jako nakaz masowego przechwytywania,

[131] Sekcja 142 – „Cele operacyjne wskazane w nakazie muszą odpowiadać celom wymienionym na liście prowadzonej przez szefów służb wywiadowczych (lista celów operacyjnych) jako cele, dla których przechwycona treść lub dane wtórne na podstawie nakazu masowego przechwytywania mogą być poddane dalszej analizie".

- nakaz musi być adresowany do szefa służby wywiadowczej, który złożył wniosek o wydanie nakazu lub w którego imieniu taki wniosek został złożony,
- nakaz musi wymieniać cele operacyjne, dla których przechwycone treści komunikatów lub dane wtórne mogą być poddane dalszej analizie,
- cele operacyjne wskazane w nakazie muszą być uwzględnione w prowadzonej przez szefów służb wywiadowczych tzw. liście celów operacyjnych (ang. *list of operational purposes*) jako cele uzasadniające dalszą analizę treści przechwyconych komunikatów lub danych wtórnych uzyskanych na podstawie nakazu *bulk interception*.

1.6. Czas trwania, modyfikacje i unieważnienie nakazu

Nakaz traci moc po upływie sześciu miesięcy, licząc od dnia jego wydania lub, w razie jego przedłużenia, w dniu następującym po dniu, w którym utraciłby moc, gdyby nie został przedłużony (sekcja 143). Możliwe jest przedłużenie nakazu przez Sekretarza Stanu za zgodą Komisarza, jeżeli w dalszym ciągu istnieją przesłanki, które uzasadniały jego pierwotne wydanie. Przedłużenie jest możliwe w czasie trwania tzw. okresu przedłużenia (ang. *renewal period*) obejmującym 30 dni przed upływem ważności nakazu, z czego ostatni dzień obowiązywania nakazu jest równocześnie ostatnim dniem okresu przedłużenia.

Nakaz może również zostać zmodyfikowany na zasadach opisanych w sekcji 145. Zmiana może obejmować dodanie, modyfikację lub usunięcie któregoś z celów operacyjnych, wskazanych w nakazie, uzasadniających poddanie przechwyconej treści komunikatów lub danych wtórnych dalszej analizie lub stwierdzenie, że nakaz nie autoryzuje już przechwytywania treści komunikatów w czasie ich przesyłu za pomocą systemu telekomunikacyjnego lub pozyskania danych wtórnych. Możliwość zmiany treści nakazu należy traktować jako element umożliwiający dynamiczne reagowanie na bieżącą sytuację operacyjną oraz dowodzi, że nie w każdym przypadku treść przechwytywanych komunikatów i dane wtórne są ze sobą nierozerwalnie powiązane. Przeciwnie – pozyskiwanie ww. typów danych może mieć charakter alternatywny, na co wskazuje raport[132] o wykorzystywaniu tzw. *bulk powers* opracowany przez niezależny organ – Niezależnego Sprawozdawcę ds. Prawa Antyterrorystycznego (*Independent Reviewer of Terrorism Legislation*). Wskazuje on, że możliwość ograniczenia nakazu masowego przechwytywania wyłącznie do danych wtórnych jest jednym z instrumentów pozwalających na zdobywanie przez służby informacji w sposób w mniejszym stopniu ingerujący w prawo do prywatności.

Jeżeli prowadzenie czynności opisanych w nakazie przestało być niezbędne dla ochrony bezpieczeństwa narodowego, jeżeli przestały one mieć proporcjonalny charakter w stosunku do zakładanych celów lub jeżeli analiza przechwyconych na podstawie nakazu treści komunikatów lub danych wtórnych nie jest już konieczna dla realizacji celów operacyjnych, Sekretarz Stanu lub działający z jego upoważnienia urzędnik szczebla kierowniczego (ang. *senior official*) może stwierdzić wygaśnięcie nakazu w dowolnym momencie jego obowiązywania (sekcja 148).

[132] *Report of the Bulk Powers Review by David Anderson Q.C Independent Reviewer of Terrorism Legislation*, August 2016, pkt 2.9, s. 22 dostęp na stronie https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf [dostęp: 21 IX 2017].

1.7. Praktyczne aspekty działania *bulk interception*

Masowe przechwytywanie można zdefiniować jako gromadzenie, w trakcie ich przesyłu, informacji o komunikacji (prowadzonej poza granicami UK) za pośrednictwem sieci telekomunikacyjnych w taki sposób, że ich treść staje się dostępna dla osób innych niż nadawca lub odbiorca. Instrument *bulk interception* służy wykrywaniu zagrożeń bezpieczeństwa narodowego w dwóch ściśle określonych przypadkach:

1) monitorowania komunikacji osób, które zostały już wcześniej zidentyfikowane jako stwarzające potencjalne zagrożenie,
2) wyszukiwania informacji prowadzących do wygenerowania nowych tropów wywiadowczych (ang. *intelligence leads*) dotyczących sytuacji nieznanych do tej pory właściwym organom, np. nowych zagrożeń terrorystycznych czy cyberataków[133].

Pomimo licznych doniesień medialnych odnoszących się do tzw. programów masowej inwigilacji wykorzystywanych przez służby wywiadowcze państw tzw. Pięciorga Oczu, argumenty przedstawione zarówno przez rząd, jak i przez właściwe organy parlamentarne Wielkiej Brytanii zdają się zaprzeczać tezie, że te służby (np. GCHQ) prowadziły tak naprawdę działania polegające na nieselektywnym i ogólnym monitorowaniu całości komunikacji internetowej, naruszając tym samym prawo do prywatności nieokreślonej liczby osób niestwarzających żadnego zagrożenia dla bezpieczeństwa narodowego. Raport Komisji ds. Wywiadu i Bezpieczeństwa (dalej: komisja ISC) z 2015 r. wskazuje, że masowe przechwytywanie nie może dotyczyć całości komunikacji internetowej z uwagi na ograniczenia natury prawnej, technologicznej oraz praktycznej. Konieczność dokonywania szczegółowych czynności analitycznych dotyczących tak dużej ilości danych byłoby zadaniem przekraczającym możliwości GCHQ. Twórcy raportu wskazują, że ta służba może teoretycznie uzyskać dostęp do niewielkiej części z ok. 100 000 przekaźników[134], stanowiących podstawowy element składowy infrastruktury globalnej sieci Internet. Służba określa przekaźniki, przez które prawdopodobnie mogą być przesyłane dane o istotnym znaczeniu wywiadowczym. Niemniej jednak, z uwagi na to, że przetwarzanie tak ogromnych ilości danych wymaga znacznego nakładu środków i pracy analitycznej, GCHQ przechwytuje komunikację przesyłaną jedynie przez niewielką część tych przekaźników, do których ma teoretycznie dostęp. Co więcej – nie oznacza to, że GCHQ gromadzi i przechowuje całą komunikację przesyłaną przez te przekaźniki, informacje te są następnie poddawane selekcji znacznie zmniejszającej ilość danych, do których służba ta fizycznie uzyskuje dostęp i poddaje analizie[135]. W tym kontekście niezmiernie istotne znaczenie ma zawarta w cytowanym raporcie komisji ISC uwaga, pomimo pojawiających się w debacie publicznej zarzutów, iż *bulk interception* prowadzi do masowego i nieselektywnego pozyskiwania danych, w istocie rzeczy instrument ten ma charakter ukierunkowany – GCHQ wybiera przekaźniki, do których dostęp, z jej punktu widzenia, jest najbardziej korzystny, następnie zaś stosuje tzw. selektory w celu wyodrębnienia komunikacji konkretnych osób[136]. *Bulk interception* nie zbiera zatem wszystkich informacji, lecz ich ściśle wyselekcjonowaną część, co powoduje, że wskazane powyżej zarzuty

[133] *Privacy and Security: a modern and transparent legal framework*; Intelligence and Security Committee of Parliament, 12 March 2015, s. 28, www.isc.independent.gov.uk/news-archive/12March2015 [dostęp: 22 VIII 2017].

[134] Twórcy omawianych raportów posługują się pojęciem *b e a r e r* (tłum. własne aut.).

[135] *Privacy and Security*…, s. 27.

[136] Tamże, s.28–29.

dotyczące powszechnego i systematycznego łamania prawa do prywatności oparte są na niewłaściwych przesłankach.

Zgodnie z informacjami zawartymi w cytowanych powyżej raportach Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego oraz parlamentarnej komisji ISC proces masowego przechwytywania można – w ujęciu ogólnym – podzielić na trzy zasadnicze fazy: zbierania informacji (ang. *collection*), wstępnej selekcji (ang. *filtering*) oraz wyboru, które z informacji nieodrzuconych na poprzednim etapie zostaną faktycznie poddane dalszej analizie (ang. *selection for examination*).

Faza pierwsza – collection

Proces faktycznego zbierania informacji rozpoczyna się od dokonania oceny przewidywanej wartości wywiadowczej danych przesyłanych przez poszczególne przekaźniki oraz wyboru przekaźników, które GCHQ zamierza w danym momencie wykorzystać. Wybór ma charakter wysoce ocenny, opiera się prawdopodobnie na określonych założeniach wypracowywanych na podstawie, po pierwsze, specjalistycznej wiedzy technicznej dotyczącej sposobu przepływu informacji w Internecie oraz, po drugie, na informacjach uzyskanych z innych rodzajów źródeł, np. źródeł osobowych.

Jak wskazano powyżej, GCHQ nie dysponuje możliwościami technicznymi pozwalającymi na jednoczesne pozyskiwanie informacji ze wszystkich najważniejszych przekaźników tworzących globalną sieć Internet. Służba ta ogranicza zatem zakres swoich działań do tych jej elementów składowych, w stosunku do których istnieją uzasadnione przesłanki, by sądzić, że mogą przynieść rzeczywiste korzyści wywiadowcze. Według publicznie dostępnych informacji zawartych w cytowanych raportach liczba przekaźników, z których w danym momencie GCHQ zdobywa informacje, jest niewielka (jest określana np. jako: *a tiny fraction of all the bearers in the world*[137], czyli: niewielka część wszystkich przekaźników na świecie – tłum. wł. aut.) Informacje o dokładnej liczbie przekaźników, do których służba ma dostęp, zostały zawarte w raporcie ISC, ale zostały usunięte z publicznie dostępnej wersji dokumentu. Są to zatem informacje niejawne[138].

Faza druga – wstępna selekcja (filtering)

Wykorzystywane przez GCHQ systemy przetwarzania danych badają ruch internetowy przepływający przez przekaźniki, do których służba ma dostęp. W dalszej kolejności są wykorzystywane instrumenty tzw. filtrowania danych umożliwiające wyselekcjonowanie danych mogących potencjalnie przynieść korzyści wywiadowcze. Jednocześnie odrzuceniu ulegają informacje, których znaczenie, zgodnie z zastosowanymi kryteriami wyboru, jest niewielkie.

Już na etapie wstępnej selekcji odrzuceniu ulega znaczna część danych przesyłanych przez przekaźniki wybrane przez GCHQ. Proces tzw. filtrowania należy trak-

[137] Tamże.

[138] „GCHQ could theoretically assess a small percentage (***%) of the 100.000 bearers which make up the Internet, but in practice they access only a fraction of these (***) (…) GCHQ do not therefore have „blanket coverage of all internet communications, as has been alleged – they have neither the legal authority, the technical capacity nor the resources to do so". (Działania GCHQ nie obejmują zatem w sposób kompleksowy całej komunikacji internetowej, jak zarzucano – nie ma ona ku temu podstaw prawnych, zdolności ani zasobów – tłum. wł. aut.), za: *Privacy and Security*…, s. 28.

tować z jednej strony jako narzędzie pozwalające na skoncentrowanie późniejszych działań analitycznych na informacjach mogących mieć faktycznie znaczenie z punktu widzenia wywiadowczego, z drugiej zaś jest to jeden z etapów złożonego i wielostopniowego procesu selekcji przyczyniający się w znacznej mierze do ochrony prywatności i zminimalizowania negatywnych skutków masowego przechwytywania dla osób niepowiązanych w żaden sposób z działalnością mogącą stanowić zagrożenie dla bezpieczeństwa narodowego. Jest to również argument przemawiający na niekorzyść tezy, że systemy masowego pozyskiwania danych wykorzystywane m.in. przez GCHQ mają charakter zupełnie nieselektywny, wykorzystujące je służby dążą zaś do totalnej inwigilacji wszystkich użytkowników Internetu czy innych systemów komunikacji.

Faza trzecia – wybór informacji do dalszej analizy (selection for examination)

Dane nieodrzucone na etapie wstępnej selekcji są poddawane kwerendom (prostym i złożonym) w celu wyodrębnienia komunikacji mogącej mieć znaczenie wywiadowcze. Raport Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego wskazuje, że GHCQ wykorzystuje dwa zasadnicze, odrębne mechanizmy mające na celu ocenę informacji zbieranych w toku masowego przechwytywania – proces selektorów silnych (ang. *strong selector process*) i proces kwerend złożonych (ang. *complex query process*).

1.8. Proces selektorów silnych

Proces związany z wykorzystaniem selektorów silnych jest przykładem kwerendy prostej, polegającej na wyszukiwaniu informacji na podstawie elementów dających wysokie prawdopodobieństwo jednoznacznej identyfikacji konkretnej osoby. Przykładem selektora silnego jest np. numer telefonu oraz adres poczty elektronicznej. Kwerendy złożone prowadzone są natomiast na podstawie kryteriów wykorzystujących selektory o mniejszej mocy, których nie można jednoznacznie przyporządkować do konkretnej osoby. W połączeniu pozwalają one jednak na znaczne zredukowanie ryzyka tzw. fałszywych trafień (ang. *false positive*) mogących prowadzić do analizy danych dotyczących osoby przypadkowej, niezwiązanej z zainteresowaniami służby[139].

Można domniemywać, że kwerendy proste, wykorzystujące mechanizm selektorów silnych, mają charakter bardziej ukierunkowany i są stosowane wówczas, gdy służba dysponuje stosunkowo dużą ilością informacji o danej osobie czy o konkretnej sytuacji operacyjnej. Ten proces sprawdza się, jeśli weźmie się pod uwagę linię chronologicznego rozwoju danego zagrożenia, na jego dalszych etapach, gdy posiadane przez służbę informacje pozwalają na określenie zaangażowanych osób, wykorzystywanych przez nie środków komunikacji, miejsca ich pobytu czy innych elementów. Można zatem przyjąć, że efektywność procesu selektorów silnych jest najwyższa, jesli doszło do indywidualizacji elementów składowych konkretnej sytuacji mogącej stanowić zagrożenie dla bezpieczeństwa narodowego.

Z technicznego punktu widzenia ten system porównuje dane przepływające przez konkretny przekaźnik z listą selektorów silnych dotyczących konkretnych celów operacyjnych[140]. Zgodnie z informacjami przedstawionymi w cytowanym raporcie komisji ISC, uzyskanymi od służby GCHQ, wszystkie komunikaty i dane wtórne odpowiadające

[139] *Report of the Bulk Powers Review*…, s. 24.

[140] Liczba aktualnie wykorzystywanych przez GCHQ selektorów i indywidualnych celów operacyjnych została usunięta z raportu komisji ISC, *Privacy and Security: a modern and transparent*…, s. 28.

konkretnym selektorom silnym są automatycznie zbierane w czasie zbliżonym do czasu rzeczywistego, podczas gdy pozostałe informacje są odrzucane. Informacje o ilości oraz proporcjach zbieranych i odrzucanych danych nie zostały uwzględnione w publicznie dostępnej wersji raportu.

Komisja zwraca uwagę, że mechanizm *bulk interception* – pomimo że jest zaliczany przez ustawę IPA do kategorii *bulk powers*, rozumianych jako instrumenty masowego pozyskiwania danych – jak wskazano powyżej, w gruncie rzeczy w praktyce jest on ściśle skoncentrowany na określonych osobach, o czym świadczy stosowanie selektorów pozwalających na odrzucenie danych nieprzedstawiających wartości wywiadowczej.

1.9. Proces kwerend złożonych

W przeciwieństwie do opisanego powyżej procesu wykorzystującego selektory silne wykorzystujące czynniki, takie jak np. adres poczty elektronicznej, kwerendy złożone polegają na zastosowaniu większej liczby (np. trzech lub czterech) znacznie bardziej kompleksowych kryteriów selekcji informacji. Ten proces jest prowadzony na podstawie niewielkiej liczby przekaźników (mniejszej niż w przypadku procesu selektorów silnych), w których przypadku najbardziej jest prawdopodobne, że przesyłają one informacje mogące mieć istotne znaczenie[141].

Systemy przetwarzania danych GCHQ stosują w pierwszej kolejności tzw. zasady selekcji (ang. *selection rules*) zezwalające na odrzucenie większości danych przepływających przez dany przekaźnik. Zbierają one równocześnie informacje, które w opinii służby mogą mieć znaczenie z punktu widzenia wywiadowczego. W dalszej kolejności systemy informatyczne dokonują automatycznych sprawdzeń zgromadzonych w ten sposób danych przy użyciu kompleksowych kryteriów wyszukiwania, co pozwala na odrzucenie znacznej części fałszywych trafień (ang. *false positive*). Pomimo że analitycy mogą dokonywać dodatkowych sprawdzeń, korzystając ze złożonych kryteriów wyszukiwania, wewnętrzne regulacje GCHQ i sposób działania systemów analitycznych nie pozwalają im na dokonywanie dowolnych wyszukiwań, nieopartych na istniejących potrzebach operacyjnych.

Proces masowego przechwytywania z wykorzystaniem kompleksowych kryteriów wyszukiwań jest w istocie bliższy koncepcji *bulk interception*, niż pozyskiwanie informacji na podstawie selektorów silnych z uwagi na to, że specyfika jego funkcjonowania zakłada zbieranie niewyselekcjonowanych danych, zarówno treści komunikatów, jak i danych wtórnych. Niemniej jednak pozwala on na dokonywanie kompleksowych kwerend informacji zgromadzonych dzięki kombinacji kilku selektorów, co w znacznej mierze przyczynia się do oddzielenia informacji mogących mieć znaczenie z punktu widzenia bezpieczeństwa narodowego od tych, które nie mają żadnego związku z celami działań służby[142].

Analiza przedstawionych różnic między masowym przechwytywaniem prowadzonym z wykorzystaniem selektorów silnych a procesem kwerend złożonych prowadzi do wniosku, że są to dwa komplementarne i wzajemnie się uzupełniające instrumenty. Skuteczność jednego bądź drugiego mechanizmu w danym przypadku jest uzależniona od odpowiedniego doboru właściwego procesu do konkretnych uwarunkowań operacyjnych. Mechanizm związany z użyciem selektorów silnych, jak wskazano powyżej, jest

[141] Tamże, s. 29.

[142] *Report of the Bulk Powers Review*…, s. 25.

najskuteczniejszy w sytuacji posiadania przez służby innych informacji wskazujących na istnienie określonego zagrożenia, pozwalających na indywidualizację osób zaangażowanych w działania zagrażające bezpieczeństwu narodowemu i wykorzystywanych przez nie środków komunikacji, jak telefony, komunikatory internetowe czy poczta elektroniczna. Jest to zatem faza następująca po wykryciu określonej sytuacji stanowiącej zagrożenie.

Kwerendy złożone pozwalają natomiast na zdobywanie informacji na wcześniejszym etapie, gdy niemożliwe jest jednoznaczne stwierdzenie, czy daną sytuację należy traktować jako zagrażającą bezpieczeństwu narodowemu. W konsekwencji niemożliwe jest oznaczenie zaangażowanych osób czy określenie innych parametrów sytuacji. Proces analityczny w tym przypadku ma znacznie bardziej dogłębny charakter i pozwala na prześledzenie wzorców komunikacji, jej natężenia czy innych elementów, dzięki którym płynące z niej wnioski i prognozy dotyczące potencjalnych scenariuszy rozwoju sytuacji będą miały charakter komplementarny i będą przedstawiać tło analizowanych wydarzeń, w przeciwieństwie do selektorów silnych skoncentrowanych na ściśle określonych osobach czy parametrach.

1.10. Kryteria decyzji o poddaniu zebranych informacji dalszej analizie

Niezależnie od zastosowanego w danym przypadku mechanizmu, ilość pozyskiwanych danych jest zbyt duża, aby było możliwe dokonanie ich całościowej analizy. W odniesieniu do procesu selektorów silnych, w celu wyselekcjonowania danych mogących mieć największe znaczenie z punktu widzenia realizacji zadań GCHQ, są one poddawane procesowi tzw. segregacji (ang. *triage*). Z informacji przekazanych przez GCHQ komisji ISC wynika, że wskutek tego procesu większość zebranych danych nigdy nie jest poddawana jakimkolwiek czynnościom prowadzonym przez analityków[143].

W przypadku kwerend złożonych służba określa, które z danych przechodzących przez dane przekaźniki mogą mieć istotne znaczenie przez stosowanie zasad selekcji (ang. *selection rules*) oraz kompleksowych wyszukiwań. W rezultacie analitycy otrzymują zestawienie zawierające określoną liczbę spisów (ang. *index*) w formie tabeli przedstawiającej wyniki tych wyszukiwań. Raport komisji ISC powołując się na informacje przekazane przez GCHQ, wskazuje, że (…) *uzyskanie przez analityka pełnego dostępu do zawartości określonej pozycji (item) wymaga jej otwarcia bazując na informacjach zawartych w indeksie*. Ten proces wykazuje pewne zbieżności z mechanizmem działania wyszukiwarek internetowych. Analitycy nie mogą badać wszystkich rezultatów wyszukiwania, muszą polegać na swojej indywidualnej ocenie i doświadczeniu w celu podjęcia decyzji o tym, które informacje są z ich punktu widzenia najbardziej istotne. Służba podała komisji ISC również dokładną liczbę pozycji wybieranych przez analityków w czasie jednego dnia pracy, została jednak usunięta z publicznej wersji omawianego raportu[144].

Zasady dotyczące poddawania przechwyconych danych (zarówno treści, jak i danych wtórnych) zostały określone w sekcji 152 IPA. W celu zapewnienia spójności terminologicznej poniżej przytoczono jej tłumaczenie.

> 152 – Instrumenty zabezpieczające w zakresie analizy przechwyconych informacji
>
> (1) Dla celów sekcji (150), wymogi dotyczące przechwyconej treści komunikatów lub danych wtórnych pozyskanych na podstawie nakazu są spełnione, jeżeli:

[143] *Privacy and Security*…, s. 31.

[144] Tamże.

a) selekcja jakichkolwiek przechwyconych treści lub danych wtórnych do dalszej analizy dokonywana jest wyłącznie dla realizacji ustalonych celów (podsekcja 2);

b) selekcja jakichkolwiek przechwyconych treści lub danych wtórnych do dalszej analizy jest niezbędna i proporcjonalna we wszystkich okolicznościach;

c) selekcja jakichkolwiek przechwyconych treści do dalszej analizy spełnia warunki selekcji (selection conditions) (podsekcja (3)).

(2) Selekcja przechwyconych treści lub danych wtórnych do dalszej analizy dokonywana jest wyłącznie dla ustalonych celów, jeżeli przechwycone treści lub dane wtórne są wybierane do dalszej analizy o tyle, o ile jest to niezbędne dla realizacji celów operacyjnych wyszczególnionych w nakazie, zgodnie z sekcją 142.

„Wyszczególnione w nakazie" oznacza wskazane w nakazie w czasie selekcji przechwyconych treści lub danych wtórnych do dalszej analizy.

(3) Do warunków selekcji, o których mowa w podsekcji (1) (c) zaliczają się następujące elementy:

a) przechwycone dane nie mogą zostać wyselekcjonowane do dalszej analizy, jeżeli naruszają one zakaz, o którym mowa w podsekcji (4), a osoba wykonująca czynności związane z realizacją nakazu sądzi, że wybór określonych danych do dalszej analizy nie narusza zakazu analizy komunikacji osoby znajdującej się na terytorium Wysp Brytyjskich;

b) wybór przechwyconych danych do dalszej analizy z naruszeniem zakazu, o którym mowa powyżej jest uzasadniony na podstawie sekcji 152 (5);

c) wybór przechwyconych danych do dalszej analizy z naruszeniem zakazu, o którym mowa powyżej uzyskał autoryzację w postaci odrębnego nakazu wydawanego na podstawie rozdziału 1 części 2 IPA;

(4) Zakaz, o którym mowa w podsekcji (3)(a) polega na tym, że przechwycona treść nie może w żadnym razie zostać wyselekcjonowana do dalszej analizy, jeżeli:

a) jakiekolwiek kryteria wykorzystane w selekcji dotyczą osoby, o której wiadomo, że znajduje się na terytorium Wysp Brytyjskich;

b) wybór tych kryteriów ma na celu zidentyfikowanie treści komunikacji wysłanej lub skierowanej do tej osoby;

(5) Wybór przechwyconej treści komunikatów do dalszej analizy jest dopuszczalny na podstawie niniejszej podsekcji jeżeli:

a) kryteria odnoszące się do danej osoby są lub były używane w celu selekcji przechwyconej treści komunikatów w okolicznościach, o których mowa w podsekcji (3) (a) i (b);

b) w którymkolwiek momencie osoba realizująca nakaz sądzi, że zaistniała istotna zmiana okoliczności dotyczących określonej osoby (podsekcja 6) sprawiająca, że wybór przechwyconej treści komunikatów do dalszej analizy naruszałby zakaz, o którym mowa w podsekcji (4);

c) wydany został pisemny nakaz analizy przechwyconej treści komunikatów z wykorzystaniem tych kryteriów przez osobę pełniącą funkcje kierownicze (*senior officer*);

d) wybór przechwyconej treści komunikatów został dokonany przed upływem okresu, o którym mowa w podsekcji (7).

(6) Dla celów podsekcji (5)(b) istotna zmiana okoliczności dotyczących określonej osoby ma miejsce, jeżeli:

a) osoba ta znalazła się na terytorium Wysp Brytyjskich lub

b) przeświadczenie osoby realizującej nakaz, że osoba znajduje się poza terytorium Wysp Brytyjskich okazało się błędne.

(7) W podsekcji (5) –

a) „osoba pełniąca funkcje kierownicze", w odniesieniu do nakazu skierowanego do szefa służby wywiadowczej, oznacza funkcjonariusza tej służby, który:

b) jest członkiem Wyższej Służby Cywilnej (Senior Civil Service) lub członkiem Wyższej Struktury Kierowniczej Służby Dyplomatycznej Jej Królewskiej Mości (Senior Management Structure of Her Majesty's Diplomatic Service) lub

c) zajmuje analogiczne stanowisko w służbie wywiadowczej. (…)

1.11. Wnioski

Instrument masowego przechwytywania należy traktować jako jedno z podstawowych narzędzi wykorzystywanych przez brytyjskie służby wywiadowcze. Umożliwia on wykrywanie zagrożeń dla bezpieczeństwa narodowego na wczesnym etapie ich powstawania, odkrywanie powiązań między fragmentarycznymi informacjami dotyczącymi konkretnych zagrożeń oraz badanie wzorców komunikacji osób mogących stwarzać potencjalne zagrożenie bezpieczeństwa narodowego. W odróżnieniu od tzw. ukierunkowanych metod pozyskiwania informacji skupionych na jednej osobie lub grupie osób, o których działalności służby mają duży zasób wiedzy, *bulk interception* ma kluczowe znaczenie dla wykrywania nieznanych wcześniej, dopiero powstających zagrożeń[145]. Z chronologicznego punktu widzenia – im bardziej zaawansowany jest etap rozwoju konkretnej sytuacji mogącej potencjalnie zagrażać bezpieczeństwu narodowemu, tym większe znaczenie mają metody ukierunkowane. Mechanizmy masowego pozyskiwania danych, w tym *bulk interception*, znajdują największe zastosowanie w pierwszych fazach procesu wykrywania zagrożeń, gdy zagrożenie ma charakter mglisty i nie jest potwierdzone przez informacje pochodząc z innych źródeł, np. ze źródeł osobowych.

Zawarty w raporcie Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego skrótowy opis cyklu działań służb wywiadowczych również zdaje się sugerować, że masowe przechwytywanie należy uznać za instrument realnie przyczyniający się do neutralizacji zagrożeń dla bezpieczeństwa narodowego[146]. Ten cykl składa się z trzech zasadniczych etapów: wykrywania zagrożeń, zrozumienia ich natury i podjęcia odpowiednich działań. Opisywany model należy traktować jako uproszczenie, a czynności realizowane na poszczególnych etapach są ze sobą ściśle powiązane. Nie są one również podejmowane w sposób linearny – niekiedy działania wdrażane w fazach wykrywania i zrozumienia ulegają, w zależności od stopnia intensywności danego zagrożenia, ograniczeniu na rzecz działań operacyjnych, które mogą okazać się konieczne nawet w razie braku pełnej wiedzy o charakterystyce określonej sytuacji.

Zgodnie z informacjami zawartymi w przywołanym powyżej raporcie, do najważniejszych typów czynności analitycznych prowadzonych na różnych etapach cyklu działań służb wywiadowczych należą:

- identyfikacja celu – ustalenie osób, które mogą stać się przedmiotem zainteresowania służb,
- pogłębienie informacji o celu – pozyskiwanie dalszych informacji o potencjalnym celu (m.in. kontaktach czy codziennych aktywnościach), aby ocenić, czy

[145] *Privacy and Security*…, s. 32.

[146] *Report of the Bulk Powers Review*…, s. 142.

może on stwarzać zagrożenie lub czy z innych powodów może stać się przedmiotem zainteresowania,
- wykrycie anomalii – proces technologiczny zmierzający do wykrycia określonych wzorców w zbiorach danych, których analiza może przyczynić się do identyfikacji zagrożenia,
- analiza sieci – proces technologiczny, dzięki któremu analiza informacji uzyskanych przez przechwytywanie może dostarczyć istotnych informacji dotyczących struktury najbliższego otoczenia osoby znajdującej się w zainteresowaniu służb oraz umiejscowić pozyskane dane w odpowiednim kontekście,
- segregacja i przyznanie pierwszeństwa (priorytetyzacja) – proces polegający na oddzieleniu informacji istotnych od nieistotnych[147].

Biorąc pod uwagę charakterystykę *bulk interception*, wydaje się, że uzyskiwane za pośrednictwem tego instrumentu dane mogą mieć niezwykle istotne znaczenie w identyfikacji oraz pogłębianiu informacji o celu oraz w wykrywaniu anomalii w zbiorach danych, co może doprowadzić do odkrycia elementów charakterystycznych dla ataków terrorystycznych czy cybernetycznych.

Pomimo licznych wątpliwości natury etycznej i prawnej dotyczących stosowania masowego przechwytywania, informacje przedłożone przez brytyjskie służby specjalne, przedstawicieli władzy ustawodawczej i wykonawczej pozwalają na sformułowanie wniosku, że nie sposób zanegować pozytywnego wpływu tego mechanizmu na możliwości neutralizacji najbardziej kompleksowych zagrożeń dla bezpieczeństwa narodowego (terroryzm i cyberprzestępczość) oraz, w ograniczonym zakresie i w ściśle określonych przypadkach, zwalczania przestępczości. Przedstawione poniżej przykłady hipotetycznych sytuacji związanych z wykorzystaniem *bulk interception* przemawiają za tym, że podjęcie skutecznych działań neutralizujących określone zagrożenie nie byłoby możliwe lub byłoby znacznie utrudnione bez zastosowania tego instrumentu. Te przykłady to ogólne streszczenie trzech spraw prowadzonych przez brytyjskie służby specjalne w najbardziej wrażliwych obszarach – zwalczania terroryzmu, ścigania sprawców przestępstw związanych z pedofilią[148] oraz ochrony przed cyberatakami[149].

Sprawa nr 1. Zwalczanie terroryzmu

Prowadzone przez brytyjskie służby specjalne analizy danych zgromadzonych dzięki *bulk interception* doprowadziły do zidentyfikowania nieznanej im wcześniej osoby podejrzewanej o planowanie ataków terrorystycznych na terenie państw UE i NATO.

[147] *Report of the Bulk Powers Review*…, s. 143.

[148] W poprzednim stanie prawnym (sekcja 5 ustawy *Regulation of Investigatory Powers Act* 2000) przesłanki wydania przez Sekretarza Stanu nakazu przechwycenia komunikacji (ang. *interception warrant*) były określone w sposób szerszy niż w ustawie IPA. Było to możliwe m.in. w celu ochrony interesów bezpieczeństwa narodowego oraz zapobiegania i wykrywania poważnej przestępczości. Ustawa nie wymagała jednak, aby przesłanka związana z zapobieganiem i wykrywaniem poważnej przestępczości była połączona z bezpieczeństwem narodowym. W ustawie RIPA zwalczanie przestępczości mogło zatem stanowić samoistną przesłankę wydania nakazu przechwytywania. Zgodnie z sekcją 138 ustawy IPA Sekretarz Stanu może wydać nakaz masowego przechwytywania, jeżeli jest to niezbędne z punktu widzenia ochrony interesów bezpieczeństwa narodowego oraz zapobiegania lub wykrywania poważnej przestępczości lub w celu ochrony interesów gospodarczych.

[149] Opis przywołanych spraw (ang. *case studies*) znajduje się dokumencie *Operational Case for Bulk Powers*, s. 28–29, www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents [dostęp: 3 VIII 2017].

Utrzymywała ona kontakty ze współpracującymi z Państwem Islamskim ugrupowaniami o charakterze ekstremistycznym, działającymi na terenie Syrii. Biorąc pod uwagę, że podejrzewana osoba przebywała poza granicami Wielkiej Brytanii, wykrycie prowadzonej przez nią działalności za pomocą innych instrumentów wywiadowczych było mało prawdopodobne. Pomimo podejmowanych przez nią działań, mających na celu maskowanie działalności terrorystycznej, służby dzięki wykorzystaniu danych pozyskanych przez masowe przechwytywanie, były w stanie wykryć, że podejrzewana osoba znalazła się na terytorium jednego z państw europejskich. Brytyjskie służby poinformowały właściwe organy tego państwa, które następnie przerwały proces przygotowywania ataku terrorystycznego i przejęły kilka tzw. improwizowanych ładunków wybuchowych.

Przytoczona sprawa pokazuje, jak istotne znaczenie dla zagwarantowania bezpieczeństwa wewnętrznego może mieć masowe przechwytywanie komunikacji prowadzonej przez osoby znajdujące się poza granicami danego państwa lub w sytuacji, gdy jedna ze stron (nadawca lub odbiorca) znajduje się poza jego granicami. Ten przykład jest dowodem na jedną z najważniejszych tez przemawiających za stosowaniem *bulk interception* – w wielu przypadkach jest to jedyny instrument realnie pozwalający na wykrycie zagrożenia w sytuacji, w której pozyskanie niezbędnych informacji nie jest możliwe za pośrednictwem jakichkolwiek innych metod wywiadowczych. Brytyjskie służby wskazały, że podejrzany o działalność terrorystyczną przebywał poza granicami Wielkiej Brytanii i nie był im wcześniej znany. Zdobycie wyprzedzających informacji o jego planach nie byłoby możliwe przy użyciu innych metod, np. źródeł osobowych, inwigilacji ukierunkowanej czy informacji uzyskanych od organów innych państw. Omawiany przypadek potwierdza również to, że podstawową funkcją masowego przechwytywania jest wykrywanie zagrożeń na wczesnym etapie ich powstawania, wówczas gdy stopień konkretyzacji informacji posiadanych przez służby jest niewielki lub gdy nie dysponują one w ogóle wiedzą o danej sytuacji.

Sprawa nr 2. Zwalczanie przestępstw związanych z pedofilią i wykorzystywaniem seksualnym małoletnich

W 2013 r. służby specjalne Wielkiej Brytanii prowadziły analizy danych uzyskanych dzięki *bulk interception* w celu określenia wzorców komunikacji i korzystania z Internetu osób dopuszczających się czynów zabronionych, związanych z wykorzystywaniem seksualnym małoletnich. Prace te doprowadziły do identyfikacji brytyjskiego obywatela odwiedzającego stronę sprzedającą zdjęcia przedstawiające wymienione czynności. Ta strona znajdowała się na serwerze państwa, które niechętnie współpracowało z organami brytyjskimi w sferze ścigania przestępczości. Bez analizy tych danych działalność tej osoby nie mogłaby zostać w żaden sposób wykryta i nie mogłaby ona zostać pociągnięta do odpowiedzialności. W toku dalszych czynności ustalono, że miejsce pracy podejrzanego zapewniało mu kontakt z dziećmi i małoletnimi oraz że figurował on w specjalnym rejestrze osób skazanych za ten rodzaj przestępstw (*UK Violent and Sexual Offenders Register*). Dzięki wykorzystaniu danych zdobytych dzięki zastosowaniu *bulk interception*, sprawca został skazany na trzy lata pozbawienia wolności i poddany instrumentowi zakazującemu zbliżania się do dzieci i małoletnich, uniemożliwiające mu wykonywanie pracy związanej z kontaktem z nimi lub przewidującemu inne instrumenty ochronne.

Sprawa nr 3. Ochrona przed cyberatakami

Jednym z najbardziej powszechnych zastosowań masowego przechwytywania w Wielkiej Brytanii jest wykrywanie ataków cybernetycznych, m.in. kradzieży danych, oszustw internetowych, wrogich operacji służb wywiadowczych innych państw i ugrupowań terrorystycznych. Wykorzystując informacje, które można porównać do elektronicznych odcisków palców (ang. *electronic signatures*), służby badają techniczne aspekty komunikacji internetowej w celu wykrycia elementów świadczących o możliwości dokonania ataku cybernetycznego wymierzonego w Wielką Brytanię. Tego rodzaju działania umożliwiają identyfikację złośliwego oprogramowania oraz wykrycie nowych, nieznanych wcześniej służbom, form cyberataków. Jeśli weźmie się pod uwagę tempo ewolucji technologicznej i skalę ilości danych funkcjonujących w cyberprzestrzeni, to instrument *bulk interception* jest jedną z niewielu skutecznych metod pozwalających na monitorowanie tego rodzaju ataków na wszystkich etapach, na co nie pozwala specyfika funkcjonowania instrumentów ukierunkowanych.

2. *Bulk equipment interference*

Pojęcie *bulk equimpent interference* (dalej: *bulk EI)* odnosi się do zbioru działań uprawnionych służb, których celem jest pozyskanie określonych informacji (np. treści komunikatów czy danych o urządzeniu) przez ingerencję w funkcjonowanie określonego urządzenia, np. komputera czy telefonu komórkowego. Te czynności mogą być prowadzone w sposób zdalny lub bezpośredni, np. przez fizyczne wpływanie na działalność danego urządzenia. Opisywane operacje mogą charakteryzować się różnym stopniem złożoności w zależności od zamierzonego celu czy poziomu zabezpieczeń urządzeń. Mniej skomplikowane działania mogą polegać np. na zgraniu określonych danych z urządzenia czy wykorzystaniu hasła lub loginu użytkownika w celu uzyskania dostępu do informacji zapisanych w pamięci urządzenia. Większy stopień złożoności wykazują działania polegające na wykorzystywaniu słabych punktów określonego oprogramowania służące przejęciu kontroli nad urządzeniem lub siecią, co umożliwia zdalne przekazywanie za ich pośrednictwem określonych informacji lub monitorowanie aktywności użytkownika[150]. W najbardziej powszechnym rozumieniu ten mechanizm można określić jako prowadzenie czynności o charakterze hakerskim przez służby specjalne[151].

Sposób funkcjonowania *bulk EI* i korzyści operacyjne dla służb specjalnych płynące z wykorzystywania tego sposobu – w kontekście zwalczania zagrożeń dla bezpieczeństwa narodowego oraz ewentualne naruszenia prawa do prywatności i innych dóbr prawnie chronionych – należy rozważać na płaszczyźnie coraz wyraźniej rysującego się w porządkach prawnych niektórych państw UE i NATO podziału na dwa typy mechanizmów pozyskiwania danych: masowych (*bulk*) oraz ukierunkowanych (*targeted*). Podczas gdy instrumenty ukierunkowane w dalszym ciągu mają kluczowe znaczenie z punktu widzenia reagowania na zagrożenia wpisujące się w sferę działalności służb specjalnych – z uwagi na to, że pozwalają one na zdobycie informacji o planach czy działaniach określo-

[150] *Equipment Interference – Draft Code of Practice*, Home Office, Autumn 2016, s. 8, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557861/IP_Bill_-_Draft_EI_code_of_practice.pdf [dostęp: 21 IX 2017].

[151] *Report of the Bulk Powers Review*…, s. 34.

nego, zidentyfikowanego już podmiotu – możliwości ich wykorzystania zawierają immanentne ograniczenia natury strukturalnej, które są spotęgowane bezprecedensowym rozwojem nowoczesnych technologii informatycznych czy telekomunikacyjnych.

Zobrazowanie przedstawionej powyżej tezy wymaga szczegółowych informacji dotyczących, z jednej strony, charakterystyki współczesnych zagrożeń bezpieczeństwa narodowego (cyberataki, terroryzm, zjawisko *foreign fighters* czy niezwykle trudny do zidentyfikowania i przerwania proces tzw. *homegrown radicalisation*[152]), z drugiej zaś – sposobu funkcjonowania i rozwiązań technologicznych wykorzystywanych przez nowoczesne środki komunikacji. Te czynniki sprawiają, że dogłębnej redefinicji muszą ulec również instrumenty wykorzystywane przez służby specjalne. W wielu sytuacjach tradycyjne, wysoce ukierunkowane i zindywidualizowane metody pozyskiwania informacji (źródła osobowe, obserwacja, kontrola operacyjna, sprawdzenia w bazach danych itd.) rozmijają się z rzeczywistymi potrzebami i charakterystyką działań stwarzających zagrożenie dla bezpieczeństwa narodowego. Przykładem jest sytuacja, w której w razie rozwijającego się zagrożenia o charakterze terrorystycznym, funkcjonariusze służb nie mogą zakładać, że osoby zaangażowane w realizację hipotetycznego ataku będą komunikować się wyłącznie przy użyciu określonego numeru telefonu czy komunikatora internetowego. Niemożliwe jest również poczynienie założenia, że dane uzyskane dzięki instrumentom ukierunkowanym będą zawierać wszystkie istotne informacje i że za ich pośrednictwem będzie możliwe całościowe odtworzenie zamierzonych działań. Ponadto profesjonalnie działające podmioty, zarówno państwowe (obce służby specjalne), jak i pozapaństwowe (grupy terrorystyczne), korzystają z zaszyfrowanych metod komunikacji, co uniemożliwia lub znacznie utrudnia proces zdobycia informacji mogących zapobiec eskalacji danego zagrożenia. Organy odpowiedzialne za ochronę bezpieczeństwa narodowego będą zatem dysponować coraz bardzie fragmentarycznymi informacjami, natura zaś samych zagrożeń i związanych z nimi podmiotów będzie coraz bardziej nieprzejrzysta. Próby przeciwdziałania opisanym powyżej trendom wymagają dostosowania zbioru instrumentów operacyjno-rozpoznawczych do zmieniających się warunków oraz stworzenia katalogu komplementarnych i wzajemnie oddziałujących środków pozwalających na pozyskiwanie informacji o zagrożeniach na różnych etapach ich rozwoju – zarówno w fazie ich powstawania, jak i w fazie eskalacji[153].

2.1. Podstawy prawne

Przepisy dotyczące sposobu i zasad wykorzystywania *bulk EI* zostały zawarte w rozdziale 3 części 6 IPA. Regulacje dotyczące tego instrumentu należy określić jako analogiczne w stosunku do mechanizmu *bulk interception*. Proces wydawania nakazu

[152] Pojęcie *homegrown radicalisation* odnosi się do procesu radykalizacji osób na stałe przebywających w państwach tzw. świata zachodniego. Takie osoby zaczęły prezentować radykalne, związane z ultrakonserwatywnymi odłamami islamu poglądy z uwagi na fakt obcowania z tego rodzaju ideologią np. w meczetach, szkołach czy przez różnego rodzaju źródła internetowe. Omawiany proces jest niezwykle trudny do wykrycia z uwagi na to, że te osoby pozornie nie stwarzają jasno zarysowanego zagrożenia z punktu widzenia służb – nie podejmowały działań charakterystycznych dla tzw. *foreign fighters*, nie wyjeżdżały do obozów szkoleniowych Państwa Islamskiego w Syrii czy Iraku, nie utrzymują kontaktów z zagranicznymi bojownikami itd. *Homegrown radicalisation* należy uznać za proces jednostkowy i osobniczy, rozwijający się w oderwaniu od ustalonych struktur, grup czy organizacji. Największą rolę odgrywają w nim indywidualne aspekty psychologiczne określonej osoby.

[153] *Equipment Interference – Draft Code of Practice*…, s. 30.

zastosowania *bulk EI* oraz ewentualnych modyfikacji nakazu został poddany systemowi podwójnego nadzoru (*double lock*) ze strony Sekretarza Stanu i Komisarza.

Zgodnie z sekcją 176 pod pojęciem nakazu zastosowania omawianego instrumentu (ang. *bulk equimpent interference warrant*) rozumie się nakaz wydany na podstawie rozdziału 3 części 6 IPA, autoryzujący lub nakazujący osobie, do której jest skierowany, przeprowadzenie działań polegających na ingerencji w funkcjonowanie jakiegokolwiek urządzenia w celu uzyskania treści komunikatów (ang. *communications*), danych o urządzeniu (ang. *equipment data*) lub jakichkolwiek innych informacji. Sekcja 176(c) wskazuje natomiast, że głównym celem nakazu powinno być pozyskiwanie informacji, jeżeli wykazują one powiązania zagraniczne[154]. Ten warunek sprawia, że niemożliwe jest prowadzenie czynności związanych z ingerencją w urządzenia informatyczne, jeżeli jej głównym celem miałoby być zdobywanie informacji dotyczących osób znajdujących się na terytorium Wysp Brytyjskich[155]. Pomimo wyraźnego zastrzeżenia, że *bulk EI* powinno koncentrować się na sferze zewnętrznej, ustawodawca nie wykluczył możliwości prowadzenia działań polegających na ingerencji w funkcjonowanie urządzeń w wymiarze wewnętrznym. Analiza materiału dotyczącego osób znajdujących się na terytorium Wysp Brytyjskich wymaga jednak odrębnego nakazu wydawanego zgodnie z zasadami *double lock*[156].

Definicja komunikacji zagranicznej (ang. *overseas-related communications*) oznacza, analogicznie jak w przypadku przepisów dotyczących masowego przechwytywania, komunikację wysyłaną lub odbieraną przez osoby znajdujące się poza terytorium Wielkiej Brytanii. Na zasadzie analogii – pojęcie *overseas-related information* oznacza informację o osobach znajdujących się poza terytorium tego kraju.

Zgodnie z sekcją 177 pojęcie danych o urządzeniu (*equipment data*) oznacza dane systemowe lub dane identyfikujące (ang. *identifying data*), które:

- są dołączone do określonego komunikatu, logicznie z nim powiązane lub stanowiące jego część (przez nadawcę lub w inny sposób),
- mogą być logicznie odłączone od reszty komunikatu,
- w razie odłączenia nie ujawniłyby niczego, co może w rozsądny sposób zostać uznane za mające znaczenie dla komunikatu, pomijając znaczenie wynikające z samej komunikacji lub jakichkolwiek danych dotyczących przesyłu komunikatu.

Dane o urządzeniu zostało w ustawie [sekcja 176 (3)] określone jako wykazujące powiązania zagraniczne (ang. *overseas-related equipment data*), jeżeli:

- stanowią część lub są połączone z komunikacją zagraniczną lub informacjami o osobach znajdujących się za granicą (*overseas-related information*);
- mogą pomóc w ustaleniu istnienia lub nieistnienia komunikacji zagranicznej lub informacji o osobach znajdujących się za granicą, lub w ich uzyskaniu;
- mogą pomóc w wypracowaniu metod pozwalających na uzyskanie komunikacji zagranicznej lub informacji o osobach znajdujących się za granicą.

[154] Sekcja 176 (c) – „(…) the main purpose of the warrant is to obtain one or more of the following –
i) overseas-related communications;
ii) overseas-related information;
iii) overseas-related equipment data".

[155] *Draft Equipment Interference Code of Practice*, Home Office, February 2017, s. 65, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593753/IP_Act_-_Draft_EI_code_of_practice_Feb2017_FINAL_WEB.pdf [dostęp: 7 VIII 2017].

[156] Tamże.

Nakaz musi zezwalać osobie, do której jest skierowany, uzyskanie komunikacji, danych o sprzęcie lub innych informacji, lub autoryzować dokonanie przez nią czynności, których nakaz dotyczy. Może również zezwalać lub zobowiązywać do selekcji materiału uzyskanego zgodnie z nakazem do dalszej analizy lub do ujawnienia tego materiału osobie, do której nakaz jest skierowany, lub osobie działającej w jej imieniu [sekcja 176 (4)].

2.2. Rodzaje *equipment interference* – najważniejsze różnice między tzw. nakazami ukierunkowanymi (ang. *targeted equimpent interference*) a nakazami *bulk equipment inteference*

Analogicznie jak w przypadku masowego przechwytywania, ustawa IPA wprowadza rozróżnienie między stosowaniem ingerencji w sprzęt w sposób ukierunkowany (*targeted*) oraz prowadzeniem tych czynności w sposób masowy (*bulk*). Ukierunkowana ingerencja w sprzęt jest regulowana w części 5 ustawy (*Equipment Interference*), podczas gdy podstawą prawną wariantu polegającego na prowadzeniu czynności związanych z masowa ingerencją w sprzęt (*bulk EI*) jest rozdział 3 części 6.

Nakazy *EI* w rozumieniu ustawy dzielą się na następujące typy[157]:

- ukierunkowany nakaz ingerencji w urządzenia (ang. *targeted equipment interference warrant*) [sekcja 99 (2)] – autoryzuje podjęcie przez osobę, do której jest skierowany, czynności polegających na ingerencji w urządzenia w celu uzyskania komunikacji, danych o urządzeniu lub innych informacji. Zezwala on również na podjęcie wszelkich czynności niezbędnych dla wykonania nakazu;
- ukierunkowany nakaz analizy materiału (ang. *targeted examination warrant*) [sekcja 99 (9)] – autoryzuje podjęcie czynności polegających na selekcji materiału uzyskanego na podstawie *bulk EI* do analizy, niezależnie od sekcji 193 (4), zakazującej identyfikacji komunikacji lub informacji o charakterze prywatnym dotyczących osób znajdujących się na terytorium Wysp Brytyjskich. Tego rodzaju nakaz musi być uzyskany wtedy, gdy zebrany w powyższy sposób materiał ma zostać poddany dalszej analizie na podstawie kryteriów odnoszących się do osoby, co do której składający wniosek o wydanie nakazu wie, że w chwili wyboru materiału do analizy znajduje się na terytorium Wysp Brytyjskich;
- nakaz masowej ingerencji w sprzęt (ang. *bulk equipment interference warrant*) (sekcja 176) – nakaz, którego głównym celem jest uzyskanie zagranicznej komunikacji, danych o urządzeniu lub innych informacji. Autoryzuje on zdobycie treści zagranicznej komunikacji, danych o urządzeniu oraz innych informacji oraz wybór zebranego materiału do dalszej analizy.

Analogicznie jak w przypadku przechwytywania danych (ang. *interception*), ukierunkowaną ingerencję w sprzęt można zastosować wówczas, gdy właściwe organy mają dostateczną wiedzę pozwalającą na indywidualizację i stosunkowo dokładne określenie osób stwarzających potencjalne zagrożenie i wykorzystywanych przez nich urządzeń. Ingerencja o charakterze masowym ma z kolei zastosowanie, gdy zagrożenie ma charakter nieokreślony, jego zaś charakter i skala nie mogą być sprecyzowane przed wydaniem nakazu.

[157] Tamże, s. 22.

Nakaz ukierunkowany może zostać wydany, jeżeli organ wnioskujący jest w stanie w dostatecznie precyzyjny sposób określić skalę ingerencji w dane urządzenia, przy uwzględnieniu szacunkowej ilości informacji pobocznych, niemających związku z celem wydania nakazu, do których organ, prowadząc czynności, uzyska w sposób naturalny dostęp oraz dzięki czemu oceni proporcjonalność i niezbędność ingerencji. W tym wypadku nie są zatem konieczne dodatkowe ograniczenia i restrykcje stanowiące immanentną cechę reżimu regulującego sposób wykorzystywania masowych środków gromadzenia informacji. Jeżeli natomiast niemożliwe jest dokonanie oceny niezbędności, proporcjonalności i skali ingerencji w czasie wydawania nakazu lub jeżeli zastosowanie ingerencji ukierunkowanej byłoby w danym wypadku niepraktyczne lub niewystarczające, powinien zostać wydany nakaz typu „*bulk*", w ramach którego są przewidziane dodatkowe środki ochronne, np. wielostopniowe ograniczenia dostępu do pozyskanego materiału[158].

2.3. Proces wydawania nakazu *bulk equipment interference* (sekcja 176 i następne)

Elementy proceduralne związane z wydawaniem nakazu *bulk EI* zostały uregulowane na zasadzie analogicznej, jak w przypadku masowego przechwytywania. Do najważniejszych elementów należy zaliczyć dwuetapowy proces zatwierdzania nakazu przez Sekretarza Stanu i Komisarza (*double lock*) oraz wymóg wykazania proporcjonalności i niezbędności wydania nakazu w danym przypadku (sekcja 178). W ten sam sposób zostały uregulowane również przesłanki przedmiotowe warunkujące możliwość zastosowania tego instrumentu. Sekretarz Stanu może wydać nakaz, jeżeli w jego opinii jest to niezbędne w interesie bezpieczeństwa narodowego oraz w celu zapobiegania lub wykrywania poważnej przestępczości lub ochrony interesów ekonomicznych Wielkiej Brytanii i jeżeli te przesłanki mają związek z bezpieczeństwem narodowym. Przesłanka związana z ochroną interesów ekonomicznych może uzasadniać zastosowanie *bulk EI*, jeśli wydanie nakazu jest niezbędne dla pozyskania informacji dotyczących działań lub zamiarów osób znajdujących się poza terytorium Wysp Brytyjskich. Podobnie jak w przypadku masowego przechwytywania, obie pozostałe przesłanki (zwalczanie poważnej przestępczości i ochrona interesów ekonomicznych) muszą pozostawać w koniunkcji z przesłanką ochrony interesów bezpieczeństwa narodowego. Ten mechanizm należy uznać za jeden z wielu elementów wchodzących w skład katalogu środków ograniczających możliwość stosowania instrumentów masowego gromadzenia danych, zarówno masowego przechwytywania, jak i masowej ingerencji w urządzenia informatyczne, których celem jest ochrona prawa do prywatności i minimalizacja możliwości wyrządzenia szkody osobom, które nie stanowią zagrożenia dla bezpieczeństwa narodowego.

Sekretarz Stanu może wydać nakaz, jeżeli, w jego opinii, wskazane we wniosku o wydanie nakazu cele operacyjne uzasadniają analizę materiału zgromadzonego w czasie realizacji czynności autoryzowanych na podstawie nakazu oraz jeżeli sądzi on, że ta analiza jest niezbędna w związku z którymkolwiek z celów, z których powodu Sekretarz Stanu uważa, że wydanie nakazu jest w danym wypadku niezbędne [sekcja 178 (2)]. Przykładem jest następująca sytuacja – jeśli nakaz został wydany w związku z ochroną bezpieczeństwa narodowego oraz zapobiegania i zwalczania poważnej przestępczości, to wybór danych do dalszej analizy musi być niezbędny w kontekście jednej lub obu wymienionych przesłanek[159].

[158] *Draft Equimpent Interference Code of Practice*…, s. 36.
[159] Tamże, s. 69.

Po wydaniu nakazu przez Sekretarza Stanu Komisarz dokonuje wszechstronnej oceny zasadności wykorzystania *bulk EI* w konkretnej sytuacji. Bada on m.in. niezbędność, proporcjonalność oraz to, czy wskazane we wniosku cele operacyjne uzasadniają późniejszą analizę zebranego materiału (sekcja 179). W razie odmowy zatwierdzenia nakazu Komisarz informuje o tym na piśmie Sekretarza Stanu wraz z podaniem przyczyn uzasadniających odmowę.

Przepisy dotyczące kryteriów formalnych nakazu *bulk EI* zostały skonstruowane w sposób analogiczny, jak w przypadku masowego przechwytywania (patrz wyżej).

2.4. Nakazy *bulk EI* wydawane w trybie pilnym

Mając na uwadze specyfikę zagrożeń cybernetycznych i dynamikę ewentualnych wrogich działań prowadzonych z wykorzystaniem narzędzi informatycznych, ustawodawca przewidział wyjątek od zasady *double lock*. Zgodnie z sekcją 180 Sekretarz Stanu może wydać nakaz zastosowania *bulk EI,* jeżeli w jego opinii zachodzi nagła potrzeba wykorzystania tego instrumentu. Jest on zobowiązany do poinformowania o tym Komisarza.

Ocena, czy w danym przypadku rzeczywiście zachodzi konieczność zastosowania trybu pilnego, musi uwzględnić, czy uzyskanie zgody Komisarza – biorąc pod uwagę okoliczności sprawy i konieczność realizacji określonych celów operacyjnych – byłoby praktycznie możliwe i rozsądne. Co do zasady, nakazy wydawane w trybie pilnym powinny wiązać się z co najmniej jedną z poniższych przesłanek:

- bezpośrednim zagrożeniem dla życia lub zdrowia (np. jeżeli występuje bezpośrednie zagrożenie atakiem terrorystycznym, który może być powstrzymany lub którego skutki mogą zostać zminimalizowane dzięki zastosowaniu *bulk EI*),
- ograniczoną czasowo możliwością użycia masowej ingerencji w urządzenia informatyczne w celu wykorzystania okazji pozyskania informacji wywiadowczych lub mogących mieć istotne znaczenie w toku ewentualnego śledztwa (np. sytuacja, w której służby dysponują wiedzą, że grupa o charakterze terrorystycznym działa w określonym rejonie geograficznym, ale zamierza wkrótce przemieścić się w inne miejsce)[160];

Komisarz podejmuje decyzję o utrzymaniu nakazu w mocy w terminie trzech dni roboczych od czasu wydania nakazu oraz zawiadamia o jej treści Sekretarza Stanu. Nakaz przestaje obowiązywać i nie może zostać przedłużony, jeżeli Komisarz odmówi utrzymania nakazu w mocy.

W razie odmowy utrzymania nakazu w mocy osoby realizujące czynności pierwotnie autoryzowane w trybie nagłym przez Sekretarza Stanu są zobowiązane do zaprzestania, tak szybko jak to możliwe, wszelkich czynności związanych z ingerencją w urządzenia informatyczne. W celu zniwelowania negatywnych skutków tych działań Komisarz może wyrazić zgodę na dalszą ingerencję po to, aby osoba realizująca powyższe czynności była w stanie zapewnić, że wszelkie działania związane z pierwotnym nakazem ustały tak szybko, jak to możliwe. Może on również nakazać zniszczenie materiałów uzyskanych w trakcie realizacji czynności lub określić warunki dotyczące ewentualnego użycia lub retencji tego materiału.

[160] Tamże, s. 71.

Ustawa przyznaje Sekretarzowi Stanu możliwość odwołania się od negatywnej decyzji Komisarza do Investigatory Powers Commissioner[161] – organu mogącego utrzymać decyzję Komisarza lub mogącego wydać samoistną decyzję w tej sprawie [sekcja 181 (7)].

Uchylenie nakazu wydanego w trybie pilnym nie pociąga za sobą bezprawności czynności dokonanych w okresie między wydaniem nakazu przez Sekretarza Stanu a jego ewentualnym uchyleniem [sekcja 181 (8)].

Najważniejsze przepisy dotyczące czasu trwania nakazu, jego ewentualnego przedłużenia lub modyfikacji zostały skonstruowane w sposób analogiczny do regulacji dotyczących masowego przechwytywania. Istotną różnicą jest krótszy ustawowy czas trwania nakazu wydanego w trybie pilnym – wynosi on pięć dni roboczych licząc od dnia, w którym nakaz został wydany [sekcja 184 (2) (a)].

2.5. Aspekty praktyczne i rola *bulk EI* w działalności służb specjalnych

Pozyskiwanie danych dzięki zastosowaniu *bulk EI* może być instrumentem pozwalającym organom odpowiedzialnym za ochronę bezpieczeństwa narodowego na przezwyciężenie zagrożeń związanych z ich zmniejszającą się zdolnością skutecznego reagowania na zagrożenia. Może to być spowodowane coraz wyższym poziomem zabezpieczeń technologicznych i szyfrowania urządzeń końcowych (ang. *end-to-end*), stosowanych w narzędziach komunikacji w celu zwiększenia poziomu bezpieczeństwa i prywatności użytkowników. Były dyrektor Federalnego Biura Śledczego (FBI) James Comey określił ten problem jako „*going dark*"[162]. To zjawisko jest jednym z aspektów poruszanych w ramach toczącej się w wielu krajach UE i NATO debaty publicznej, dotyczącej konieczności określenia nowych paradygmatów w zakresie wzajemnych relacji między sposobem wykorzystywania nowoczesnych instrumentów komunikacji a potrzebą wyposażenia właściwych organów w instrumenty dostosowane do nowych uwarunkowań i pozwalające na rzeczywistą realizację zadań przez te organy.

Obserwowany na przestrzeni ostatnich lat bezprecedensowy rozwój technologiczny wywiera w istocie dwojakiego rodzaju wpływ na proces zwalczania przestępczości i innych zagrożeń bezpieczeństwa. Z jednej strony organy realizujące czynności o charakterze operacyjno-rozpoznawczym czy dochodzeniowo-śledczym mogą, dzięki badaniu poszczególnych aspektów wykorzystywania nowoczesnych metod komunikacji, teoretycznie uzyskać dostęp do rozbudowanego katalogu informacji, które pozwalają na wykrywanie ewentualnych zagrożeń. Z drugiej zaś strony – tempo ewolucji nowych technologii sprawia, że stałe i systematyczne dostosowywanie do nich instrumentów, wykorzystywanych przez wspomniane organy, jest niemożliwe. W konsekwencji może dojść do sytuacji, w której z powodu np. zaawansowanych metod szyfrowania informacji wykorzystywanych przez niektóre komunikatory internetowe dostęp organów o charakterze policyjnym czy innych służb do niezbędnych im informacji, mimo zgodności tych działań z powszechnie obowiązującymi przepisami prawa, będzie niewykonalny

[161] Investigatory Powers Commissioner, zgodnie z sekcją 229, prowadzi nadzór nad wykonywaniem przez inne organy publiczne w ich ustawowych zadań w zakresie przechwytywania komunikacji, pozyskiwania lub retencji danych telekomunikacyjnych, pozyskiwania danych wtórnych lub danych systemowych zgodnie z rozdziałem 1 cześci 2 lub rozdziałem 1 części 6 IPA oraz nad prowadzeniem czynności związanych z ingerencją w urządzenia informatyczne (ang. *equipment interference*).

[162] J.B. Comey, *Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?* Director, Federal Bureau of Investigation, Brookings Institution, Washington, D.C. October 16, 2014, www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [dostęp: 8 VIII 2017].

z technicznego punktu widzenia. Szyfrowanie jest jedynie jednym z aspektów problemu *going dark*, stanowi ono jednak główny element opisanej powyżej debaty z uwagi na to, że w wielu wypadkach pociąga za sobą fizyczne wyłączenie możliwości uzyskania przez podmiot publiczny dostępu do informacji, który przysługuje mu na mocy odpowiednich aktów normatywnych bądź indywidualnego aktu kompetentnego organu (np. sądu), autoryzującego tego rodzaju dostęp[163].

Niektóre z przedsiębiorstw informatycznych wskazują również na to, że nie dysponują możliwościami technicznymi, które umożliwiają uzyskanie dostępu do informacji zgromadzonych w pamięci urządzeń. Ten problem pojawił się w kontekście prowadzenia przez FBI czynności mających na celu wyjaśnienie okoliczności i zebranie materiału dowodowego w sprawie zdarzeń w San Bernardino (Kalifornia) z 2 grudnia 2015 r. W ich wyniku śmierć poniosło 14 osób, a 22 zostały ranne.[164] Departament Sprawiedliwości zamierzał, na podstawie nakazu wydanego przez sąd, uzyskać informacje mogące mieć istotne znaczenie dla toczącego się śledztwa przez uzyskanie dostępu do danych zgromadzonych w pamięci urządzenia iPhone należącego do jednego ze sprawców ataku. Nakaz zobowiązywał przedsiębiorstwo Apple do dezaktywacji właściwości technicznej urządzenia, polegającej na automatycznym usuwaniu wszystkich zgromadzonych w nim danych po 10 nieudanych próbach wpisania hasła dostępu. W ten sposób byłoby możliwe obejście zabezpieczeń urządzenia przez próby wpisania określonej liczby kombinacji haseł, bez ryzyka usunięcia danych mających istotne znaczenie dla śledztwa. Przedstawiciele Apple argumentowali, że parametry techniczne i oprogramowanie telefonu sprawiają, że nie są oni w stanie odblokować urządzenia ani wyłączyć funkcji automatycznie usuwającej dane po nieudanych próbach wpisania hasła. Taką możliwość ma wyłącznie użytkownik lub osoba znająca oryginalne hasło[165].

Spór pomiędzy Apple a FBI i Departamentem Sprawiedliwości pokazuje, jak dalece możliwości organów odpowiadających za zwalczanie przestępczości i zagwarantowanie bezpieczeństwa są ograniczone w konfrontacji z osobami korzystającymi z nowoczesnych metod komunikacji. Przedstawiciele FBI wskazywali, że zaszyfrowane dane znajdujące się w pamięci telefonu jednego ze sprawców ataku, Syeda Rizwana Farooka, oraz zbiór koordynatów GPS wskazujących lokalizacje, w których przebywał on przed dokonaniem ataku, mogą zawierać niezwykle istotne informacje dotyczące kontaktów Farooka i jego żony, Tashfeen Malik, z osobami należącymi do Państwa Islamskiego[166].

Pojawiające się w kontekście sprawy San Bernardino interdyscyplinarne problemy prawne i technologiczne wskazują, że zjawisko *going dark* ma niezwykle istotne znaczenie w zwalczaniu terroryzmu. Niemożność uzyskania dostępu do danych przesyłanych za pośrednictwem środków komunikacji elektronicznej lub znajdujących się w pamięci urządzeń w wielu wypadkach może całkowicie uniemożliwić podejmowanie skutecznych działań zapobiegawczych w tej sferze lub odbywających się na późniejszym etapie czynności śledczych. Naturę problemu ilustrują zacytowane w przywoły-

[163] K. Finklea, *Encryption and the „Going Dark" Debate*, July 20, 2016, www.fas.org/sgp/crs/misc/R44481.pdf [dostęp: 8 VIII 2017].

[164] www.edition.cnn.com/2015/12/04/us/san-bernardino-shooting/index.html [dostęp: 8 VIII 2017].

[165] www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.f0ff02bab120 [dostęp: 8 VIII 2017].

[166] www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html [dostęp: 8 VIII 2017]. Także: www.washingtonpost.com/news/post-nation/wp/2015/12/08/both-san-bernardino-attackers-pledged-allegiance-to-the-islamic-state-officlals-say/?utm_term=.093527772da99 [dostęp: 8 VIII 2017].

wanym wcześniej raporcie Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego (*A Question of Trust – Report of the Investigatory Powers Review*) słowa dyrektora Europolu, który stwierdził, że szyfrowanie jest (…) *największym problemem dla policji i służb bezpieczeństwa w sprawach dotyczących zwalczania terroryzmu* (…) *Zmieniło ono samą naturę działań antyterrorystycznych – w przeszłości czynności te opierały się na skutecznym monitorowaniu komunikacji, podczas gdy obecnie nie jest to już możliwe*[167].

Specyfika funkcjonowania instrumentu *bulk EI* sprawia, że jest on w stanie zneutralizować jedno z najważniejszych obecnie wyzwań, z jakim mierzą się służby specjalne i organy o charakterze policyjnym w większości państw UE i NATO. Tym wyzwaniem jest brak technicznych możliwości uzyskania dostępu do zaszyfrowanych informacji zgromadzonych w pamięci urządzeń lub przesyłanych za pomocą środków komunikacji elektronicznej, mimo że tego rodzaju czynności są zgodne z prawem i mieszczą się w katalogu ustawowych kompetencji tych podmiotów. Zaprezentowane poniżej przykłady[168] hipotetycznych sytuacji, w których jest możliwe wykorzystanie *bulk EI*, wskazują, że potencjalne zastosowania tego instrumentu mają charakter komplementarny i mogą obejmować szerokie spektrum zagrożeń bezpieczeństwa.

Przykład nr 1. Przeciwdziałanie i zapobieganie terroryzmowi

Służby wywiadowcze z powodzeniem zastosowały ukierunkowaną ingerencję w urządzenia telekomunikacyjne wykorzystywane przez członków ugrupowania o charakterze terrorystycznym, przebywających w bazie treningowej poza granicami Wielkiej Brytanii. Zgromadziły tym samym informacje o planowanym przez grupę ataku na pochodzących z państw zachodnich turystów w jednym z głównych miast tego samego państwa, w którym była zlokalizowana baza treningowa, nie wiedziały jednak, kiedy atak ma zostać dokonany. Następnie grupa zaprzestała jakiegokolwiek wykorzystywania urządzeń, wobec których zastosowano *bulk EI*, co prawdopodobnie było spowodowane nabyciem nowych urządzeń i rozpoczęciem przygotowań do przeprowadzenia ataku. Służby nie miały również informacji o tym, jakiego typu urządzenia są obecnie wykorzystywane przez ugrupowanie. Biorąc pod uwagę okoliczności sprawy i realne zagrożenie zamachem terrorystycznym, zastosowano masową ingerencję w celu pozyskania informacji za pośrednictwem wszystkich lub znacznej części urządzeń znajdujących się w docelowym mieście, co miało doprowadzić do zidentyfikowania nowych urządzeń członków grupy. Jeżeli urządzenia te zostaną zidentyfikowane dostatecznie szybko, będzie możliwe zapobieżenie potencjalnemu zamachowi.

Przytoczony przykład w jasny sposób charakteryzuje możliwości związane z poprawnym wykorzystaniem *bulk EI*. Hipotetyczna sytuacja, w której zakłada się stosowanie ukierunkowanej ingerencji w sprzęt znajdujący się w posiadaniu zidentyfikowanej grupy przebywającej poza granicami Wielkiej Brytanii oraz nietypowe przejście od techniki ukierunkowanej do masowej, warunkowane dynamiką sytuacji, pokazuje, że zastosowany instrument może być skutecznie wykorzystany w szybko zmieniającej się sytuacji operacyjnej, charakteryzującej się dużą ilością zmiennych parametrów. Należy zwrócić uwagę, że przewidziany w ustawie IPA ogólny podział technik pozyskiwania informacji na ukierunkowane i masowe trzeba traktować jako

[167] *A Question of Trust*, s. 194-195.

[168] Przykłady te znajdują się dokumencie *Operational Case for Bulk Powers*, s. 35–36, www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents [dostęp: 8 VIII 2017].

zestaw komplementarnych instrumentów wykorzystywanych w różnych fazach działań operacyjno-rozpoznawczych, nie zaś jako zbiór niezależnych od siebie i całkowicie odrębnych instrumentów. Te zależności dowodzą również, że nowoczesny system gromadzenia informacji za pomocą narzędzi informatycznych będzie wykazywał się odpowiednią skutecznością, jeżeli wchodzące w jego skład komponenty będą wykazywać niezbędny stopień wewnętrznej harmonii i zgodności. Stosowanie technik wyłącznie masowych lub wyłącznie ukierunkowanych spowoduje, że możliwe będzie ich łatwe obejście, chociażby przez regularne zmiany wykorzystywanych telefonów, laptopów czy innych urządzeń. Brytyjski system – zarówno w odniesieniu do *equimpent interference*, jak i *interception* – pozwala na dynamiczną zmianę stosowania poszczególnych technik zdobywania informacji na różnych etapach danej sytuacji operacyjnej.

Przykład nr 2. Przeciwdziałanie proliferacji broni masowego rażenia

Hipotetyczne państwo o ustroju totalitarnym ma własny system poczty elektronicznej wykorzystywany przez część jego obywateli, w tym przez naukowców zaangażowanych w program rozwoju broni biologicznej i w rozprzestrzenianie technologii wojskowej. Liczba użytkowników systemu jest liczona w tysiącach. Służby wywiadowcze innych państw, w celu zdobycia wiarygodnych informacji o ewentualnym zagrożeniu proliferacją broni biologicznej, są w stanie zdobyć jedynie fragmentaryczne informacje pochodzące z innych źródeł wywiadowczych (np. z przechwytywania komunikacji), co oznacza, że niemożliwe jest zidentyfikowanie indywidualnych kont poczty internetowej należących do osób zaangażowanych w rozwój programu. Technika masowej ingerencji w sprzęt może w tym wypadku pozwolić na zdobycie ograniczonej liczby informacji o większej liczbie lub o wszystkich użytkownikach systemu, pozwalającej na określenie osób, w stosunku do których będzie konieczne prowadzenie dalszych działań wywiadowczych przez wykorzystanie ukierunkowanych technik pozyskiwania informacji.

Sytuacja opisana w przykładzie nr 2 akcentuje kilka niezmiernie istotnych aspektów sposobu działania *bulk EI*. Po pierwsze, w przeciwieństwie do sytuacji opisanej w przykładzie nr 1 ilustruje ona typowy dla tego rodzaju operacji przebieg konwersji techniki masowej w ukierunkowaną. Po identyfikacji, którzy z użytkowników systemu poczty elektronicznej mogą być zaangażowani w prace nad programem rozwoju broni masowego rażenia, będzie możliwe skoncentrowanie działań wywiadowczych wyłącznie na tych osobach i wykorzystywanych przez nich urządzeniach. Po drugie – ten casus pokazuje, że identyfikacja konkretnych osób spośród dużej liczby użytkowników danego systemu (w tym wypadku poczty elektronicznej) wymaga uzyskania dostępu do niewielkiej ilości danych o dużej liczbie urządzeń i ich użytkowników. Ten proces – pomimo że jego zakres podmiotowy (użytkownicy i urządzenia) jest szeroki, jego zasięg przedmiotowy (ilość i charakter informacji, do których należy uzyskać dostęp) jest spłycony i powierzchowny – dotyczy bardzo ograniczonego katalogu danych. Po trzecie – omawiana technika jest skuteczna w stosunku do zamkniętych i hermetycznych środowisk operacyjnych (jak np. krąg osób zaangażowanych w program proliferacji broni masowego rażenia w państwie totalitarnym), w odniesieniu do których inne metody wywiadowcze nie mogłyby przynieść spodziewanego rezultatu.

Przykład nr 3. Cyberbezpieczeństwo

Kontrolowany przez inne państwo podmiot zapewnia infrastrukturę (komputery, oprogramowanie i inne elementy) dla analogicznych do *bulk EI* programów, wymierzonych w organy rządowe i podmioty gospodarcze Wielkiej Brytanii. Brytyjskie organy wywiadowcze dążą do identyfikacji tego podmiotu w celu ustalenia, jakie konkretnie urządzenia czy oprogramowanie dostarcza on użytkownikom. Aby to osiągnąć, służby mogą posłużyć się masową ingerencją w urządzenia w celu monitorowania miejsca, z którego prawdopodobnie jest dostarczany zmanipulowany sprzęt. Zadaniem służb jest odkrycie charakterystycznych parametrów działalności dostawców. Wykrycie osób zaangażowanych w tego rodzaju działania będzie wymagać zgromadzenia dużych ilości danych pozwalających na ich identyfikację, co umożliwi późniejsze zastosowanie ukierunkowanych technik pozyskiwania informacji.

Zapobieganie i przeciwdziałanie atakom cybernetycznym jest jedną z podstawowych funkcji masowej ingerencji w urządzenia. Powyższy przykład opisuje sytuację, w której stan zaawansowania rozwoju sytuacji stwarzającej zagrożenie dla bezpieczeństwa narodowego jest wysoki (podmioty dostarczające sprzęt i oprogramowanie prowadzą już zakrojone na szeroką skalę działania), poziom wiedzy służb jest natomiast stosunkowo niski. Posiadają one informację o samym istnieniu zagrożenia i jego skutkach, a także ograniczoną wiedzę dotyczącą metod wykorzystywanych w toku tego procesu, nie są jednak w stanie dokładnie określić jego sprawców. *Bulk EI* może w tym wypadku przyczynić się do neutralizacji zagrożenia przez monitorowanie sposobu wykorzystywania urządzeń teleinformatycznych we wskazanej w przykładzie lokalizacji, będącej prawdopodobnie głównym miejscem działań grupy. Wykrycie osób zaangażowanych w opisane działania wymaga jednak ingerencji we wszystkie urządzenia znajdujące się w tym obiekcie. Na podstawie informacji podanych w przykładzie można założyć, że jest to prawdopodobnie miejsce dystrybucji sprzętu informatycznego. Złośliwe oprogramowanie będzie zatem zainstalowane nie we wszystkich urządzeniach dystrybuowanych za jego pośrednictwem, lecz w wybranych elementach, które następnie trafią do brytyjskich podmiotów będących przedmiotem zainteresowania obcych służb. Określenie, w których urządzeniach to oprogramowanie zostało faktycznie zainstalowane, wymaga więc ingerencji we wszystkie przedmioty sprzedawane bądź udostępniane przez ten punkt.

Neutralizacja zagrożenia będzie wymagać analizy dużej ilości bardziej szczegółowych niż w przykładzie nr 2 danych. Tamta sytuacja zakładała jedynie identyfikację określonych użytkowników systemu, tutaj zaś wykrycie złośliwego oprogramowania znajdującego się w urządzeniach dostarczanych przez opisany powyżej podmiot będzie prawdopodobnie wymagać bardziej zaawansowanych i dogłębnych czynności. W tej sytuacji, podobnie jak w przykładzie nr 2, zakłada się również przejście od zastosowanej początkowo techniki masowej do techniki ukierunkowanej na identyfikację osób zaangażowanych w wymierzone przeciwko brytyjskim podmiotom działania. Należy zwrócić uwagę na to, że przydatność *bulk EI* wynika w tym przypadku z potencjalnie wysokiej skuteczności tego mechanizmu w sytuacjach dynamicznych, w których uwarunkowania operacyjne podlegają częstym fluktuacjom. Niemożliwe jest bowiem stworzenie wyczerpującej listy podmiotów, do których trafił zainfekowany sprzęt informatyczny lub złośliwe oprogramowanie. Niemożliwe jest również, bez dokładnej znajomości sposobu działania tego oprogramowania, precyzyjne oszacowanie szkód, na jakie są narażone brytyjskie podmioty, i określenia, jakie informacje, trafiły do obcych służb

w wyniku tego rodzaju operacji. Przewaga masowej ingerencji w sprzęt nad innymi, tradycyjnymi technikami zdobywania informacji przejawia się również w szybkości działania tego mechanizmu. Ewentualne zdobycie osobowego źródła wśród pracowników podmiotu prowadzącego wrogą działalność byłoby procesem czasochłonnym i obarczonym wysokim stopniem ryzyka. Tak jak w pozostałych przykładach, zaletami *bulk EI* jest duża elastyczność tego mechanizmu oraz to, że stwarza on możliwość dotarcia do informacji nieosiągalnych innymi metodami.

2.6. Wnioski

Wyróżniającą cechą tzw. *bulk powers* na tle innych metod pozyskiwania informacji wykorzystywanych przez służby bezpieczeństwa i ochrony porządku publicznego jest umożliwienie im zdobywania dużych ilości danych przesyłanych za pośrednictwem Internetu oraz środków komunikacji elektronicznej, w celu wykrycia zagrożeń bezpieczeństwa narodowego. Większość zdobytych w ten sposób informacji nie dotyczy osób mogących stwarzać realne zagrożenie, jednak sposób wykorzystywania tych instrumentów, ograniczenia natury technologicznej i prawnej (ograniczenia dostępu, opisane w poprzednich częściach procesy selekcji informacji) oraz konieczność skupienia działań służb na informacjach mogących mieć istotne znaczenie wywiadowcze prowadzi do wniosku, że stworzony w Wielkiej Brytanii system *bulk powers* jest rozwiązaniem optymalnym z punktu widzenia konieczności przeciwdziałania i zwalczania nowych rodzajów zagrożeń bezpieczeństwa narodowego.

Przywoływane w niniejszym opracowaniu raporty brytyjskiego Niezależnego Sprawozdawcy ds. Prawa Antyterrorystycznego („*Bulk Powers Review*" oraz „*A Question of Trust*") słusznie wskazują, że na podstawie orzecznictwa Europejskiego Trybunału Praw Człowieka nie sposób uznać, że samo wykorzystywanie instrumentów masowego zdobywania danych, przy założeniu, że spełnia ono określone warunki (m.in. istnienie odpowiedniego systemu nadzoru, ograniczenia dostępu do zdobytych informacji) jest nieproporcjonalne i niedające się uzasadnić w demokratycznym społeczeństwie naruszeniem prawa do prywatności. W wydanym w sprawie Weber vs. Germany[169] orzeczeniu Europejski Trybunał Praw Człowieka uznał, że instrument tzw. strategicznego monitorowania komunikacji (ang. *strategic monitoring*) analizowany w toku postępowania, występujący w prawie niemieckim, nie stanowi *per se* nieproporcjonalnego naruszenia prawa do prywatności z uwagi na to, że ten środek może być wykorzystywany w ściśle określonych przypadkach, mechanizmy zabezpieczające prawo do prywatności i ograniczenia proceduralne są zaś wystarczające dla zagwarantowania przestrzegania praw obywatelskich.

Podobną linię orzeczniczą ETPCz przyjął w sprawie Liberty and others vs. the United Kingdom[170], że przepisy brytyjskiej ustawy *The Interception of Communications Act* z 1985 r., podlegające wykładni Trybunału, nie precyzowały w sposób wystarczająco jasny zakresu i sposobu korzystania z przyznanych właściwym organom kompetencji do przechwytywania i analizowania komunikacji zewnętrznej (gdy adresat, nadawca lub obydwoje znajdują się za granicą). Organy brytyjskie nie udostępniły opinii publicznej informacji o tym, w jaki sposób jest dokonywana selekcja przechwyconych informacji

[169] European Couurt of Human Rights, Decision as to the admissibility of application no. 54394/00 by Gabriele Weber and Cesar Richard Saravia v. Germany, 29 June 2006.

[170] European Court of Human Rights, Case of Liberty and others v. the United Kingdom, application no. 58243/00, Judgment, Strasbourg, 1 July 2008.

do dalszej analizy ani o zasadach dalszego udostępniania, przechowywania czy niszczenia przechwyconego materiału. Pomimo wskazania wad poszczególnych przepisów prawa brytyjskiego Trybunał nie wykazał systemowej niezgodności instrumentów masowego pozyskiwania danych z przepisami *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*. Należy zatem zgodzić się z postawioną w raporcie *A Question of Trust* tezą, że instrumenty typu „*bulk*" nie są same w sobie nieproporcjonalnym naruszeniem prawa do prywatności, niemniej jednak, z uwagi na ich charakter i inwazyjność, muszą podlegać ocenie według bardziej rygorystycznych standardów, niż ma to miejsce w przypadku instrumentów ukierunkowanych, dotyczących konkretnie wskazanej osoby fizycznej.

Porównując przepisy ustawy *Investigatory Powers Act* z instrumentami o charakterze operacyjno-rozpoznawczym, wymienionymi w *Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[171] oraz w *Ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[172] należy wskazać, że polski porządek prawny nie zawiera uregulowań zezwalających służbom specjalnym na wykorzystywanie instrumentów typu „*bulk*", pozwalających na masowe zdobywanie danych w celu rozpoznawania, zapobiegania i zwalczania zagrożeń bezpieczeństwa państwa. Charakter uprawnień Agencji Bezpieczeństwa Wewnętrznego w zakresie rozpoznawania zagrożeń w systemach i sieciach informatycznych należy określić jako defensywny i zorientowany w głównej mierze na zabezpieczenie przed atakami informatycznymi systemów teleinformatycznych, istotnych z punktu widzenia funkcjonowania państwa[173].

Tego rodzaju sposób ustawowego uregulowania zakresu kompetencji ABW i pozostających w jej dyspozycji instrumentów, służących realizacji zadań opisanych w art. 5 ustawy, wynika częściowo z ustrojowej roli tej instytucji, polegającej na łącznym wykonywaniu zadań zarówno w sferze informacyjnej (uprawnienia operacyjno-rozpoznawcze), jak i w sferze procesowej (uprawnienia dochodzeniowo-śledcze). Najbardziej charakterystycznym przykładem wskazanej powyżej dychotomii jest sposób, w jaki zostało uregulowane w ustawie o ABW oraz AW zagadnienie kontroli operacyjnej. Zgodnie z art. 27 tej ustawy sąd, na pisemny wniosek szefa ABW, złożony po uzyskaniu pisemnej zgody prokuratora generalnego, może, w drodze postanowienia, zarządzić kontrolę operacyjną, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez ABW w celu rozpoznawania, zapobiegania i wykrywania określonych przestępstw (m.in. szpiegostwa, terroryzmu oraz przestępstw w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeni strategicznym dla bezpieczeństwa państwa). Kontrola operacyjna pozwala na prowadzenie stosunkowo szerokiego katalogu czynności, m.in. uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych (art. 27 ust. 6 pkt 4).

Po pierwsze, należy wskazać, że kontrola operacyjna jest instrumentem ściśle związanym ze sferą zwalczania przestępczości, nie zaś ze sferą informacyjną sprowadzającą się do wykrywania zagrożeń bezpieczeństwa państwa. Analiza przepisu art. 27 ustawy prowadzi do wniosku, że w przeciwieństwie do środków pozyskiwania informacji wprowadzonych na podstawie *Investigatory Powers Act* w Wielkiej Brytanii, za-

[171] T.j.: Dz.U. z 2016 poz. 1897 – przyp. red.
[172] Dz.U. z 2016 r. poz. 904 – przyp. red.
[173] Art. 5 pkt 2a ustawy o ABW oraz AW.

równo masowych, jak i ukierunkowanych, kontrola operacyjna nie może być uznana za środek prospektywny, służący wykrywaniu zagrożeń bezpieczeństwa narodowego na wczesnym etapie ich rozwoju. Przeciwnie, konstrukcja art. 27 ustawy powoduje, że jego zastosowanie jest możliwe na późniejszym etapie. Świadczy o tym chociażby katalog informacji, które powinien zawierać wniosek o zastosowanie kontroli operacyjnej – opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej czy dane osoby lub inne dane pozwalające na jednoznacznie określenie podmiotu lub przedmiotu, wobec którego będzie stosowana kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania (art. 27 ust. 7). Te elementy sprawiają, że kontrola operacyjna może mieć zastosowanie wówczas, gdy ABW ma informacje umożliwiające dokonanie stosunkowo dokładnej rekonstrukcji działań osób, w stosunku do których ma być prowadzona kontrola operacyjna, nie zaś np. na pozyskanie informacji o samym procesie powstawania nowych zagrożeń, co umożliwia chociażby instrument *equipment interference*.

Po drugie, kontrola operacyjna w myśl ustawy o ABW jest środkiem wyłącznie ukierunkowanym, o wysokim stopniu indywidualizacji. Świadczy o tym zawarte w art. 27 ust. 7 pkt 4 ustawy sformułowanie (…) *dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego będzie stosowana kontrola operacyjna*. Porównanie *equipment interference* z uzyskiwaniem i utrwalaniem danych w myśl art. 27 ust. 6 pkt 4 prowadzi do wniosku, że ustawa o ABW nie zezwala na prowadzenie czynności polegających na ingerencji w urządzenia informatyczne, jeżeli w danej sytuacji nie jest możliwe jednoznaczne określenie osoby lub osób prowadzących działania, o których mowa w przywołanym artykule czy podanie kwalifikacji prawnej przestępstwa. Niemożliwe zatem na gruncie aktualnie obowiązujących przepisów byłoby zdobywanie informacji o zagrożeniach za pośrednictwem urządzeń i sieci informatycznych w przypadku, w którym ABW posiadałaby fragmentaryczne informacje o zagrożeniu niepozwalające na dokładne określenie zaangażowanych w nie osób.

Przeanalizowanie powyższych elementów prowadzi do wniosku, że w przeciwieństwie do systemu brytyjskiego, zorientowanego na prowadzenie działań służących wykrywaniu zagrożeń na wczesnym etapie ich powstawania z wykorzystaniem instrumentów informatycznych, kontrola operacyjna – w myśl ustawy o ABW oraz AW – jest instrumentem zbliżonym raczej do sfery czynności procesowych niż działań wywiadowczych służących wykrywaniu zagrożeń bezpieczeństwa państwa. Nie podważając niezbędności istnienia tego rodzaju instrumentu, należy zwrócić uwagę na to, że w porównaniu z analogicznymi regulacjami funkcjonującymi w Wielkiej Brytanii w polskim systemie prawnym brakuje przepisów upoważniających właściwe podmioty do prowadzenia czynności typu „*bulk interception*" czy „*bulk equipment interferencje*", umożliwiających wczesne wykrywanie zagrożeń i podejmowanie odpowiednich działań zapobiegawczych. Pomimo że wykorzystywanie instrumentów masowego pozyskiwania informacji jest poważną ingerencją w prawa i wolności gwarantowane na mocy zarówno prawa międzynarodowego, jak i krajowego, samo ich istnienie nie może być uznane za sprzeczne z zasadami demokratycznego państwa prawnego. Wpływ tego rodzaju sposobów działania służb na prawo do prywatności należy rozpatrywać przez pryzmat mechanizmów zabezpieczających, pozwalających na gromadzenie i analizę tylko tych informacji, które mogą mieć istotne znaczenie z punktu widzenia bezpieczeństwa narodowego oraz dostatecznej precyzji i jasności przepisów normujących sposób i zakres ich praktycznego wykorzystywania.

Przyjęcie w Wielkiej Brytanii ustawy IPA należy rozpatrywać w dwóch kontekstach. Po pierwsze – jako próbę stworzenia rozwiązań legislacyjnych umożliwiających skuteczną realizację jednej z podstawowych funkcji państwa – zagwarantowania prawa do bezpieczeństwa. Po drugie, pomimo że ten akt wprowadza instrumenty pozwalające na daleko idącą ingerencję w prawo do prywatności, zawarte w ustawie szczegółowe przepisy dotyczące sposobu i trybu ich wykorzystywania przyczyniają się do zwiększenia pewności prawa i ograniczenia pojawiających się – chociażby w kontekście sprawy ujawnienia dokumentów NSA przez Edwarda Snowdena – wątpliwości dotyczących realnego zakresu kompetencji służb specjalnych i dopuszczalnego przez prawo stopnia ich ingerencji w prawa i wolności obywatelskie. Biorąc pod uwagę występujące w niektórych państwach UE i NATO (np. w Wielkiej Brytanii czy Francji) kierunki zmian legislacyjnych dotyczących katalogu instrumentów wykorzystywanych przez służby wywiadowcze oraz służby odpowiedzialne za ochronę bezpieczeństwa wewnętrznego państwa, można wyraźnie zaobserwować coraz większą liczbę aktów normatywnych wprowadzających instrumenty pozwalające na pozyskiwanie informacji za pośrednictwem systemów i sieci teleinformatycznych.

Pomimo że Polska nie jest priorytetowym celem działań międzynarodowych grup terrorystycznych, utrzymujące się na wysokim poziomie w większości państw Europy Zachodniej zagrożenie terrorystyczne oraz istotna zmiana paradygmatów bezpieczeństwa państw Unii Europejskiej i NATO, związana m.in. z coraz bardziej agresywnymi działaniami Federacji Rosyjskiej w sferze międzynarodowej, skłaniają do refleksji nad kształtem ustawowego uregulowania zakresu kompetencji i uprawnień polskich służb specjalnych. Katalog instrumentów operacyjno-rozpoznawczych przewidzianych w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu był tworzony z myślą o zwalczaniu rozumianych tradycyjnie zagrożeń bezpieczeństwa państwa, takich jak szpiegostwo, terroryzm (istniejący w ówczesnej postaci) oraz działalność zorganizowanych grup przestępczych o zasięgu międzynarodowym. Nieznane były wówczas zjawiska typu: zagrożenia hybrydowe, ataki terrorystyczne dokonywane w Europie przez *foreign fighters* czy przez osoby przechodzące proces tzw. *homegrown radicalisation*, a także wielowymiarowe zagrożenia związane z nasilonym w ostatnich latach procesem migracji. Mniejsze znaczenie miało również wykorzystywanie zaszyfrowanych środków komunikacji elektronicznej i Internetu.

Nawet pobieżna analiza wzorców ataków terrorystycznych dokonywanych w państwach Europy Zachodniej na przestrzeni lat 2015–2017 prowadzi do wniosku, że utrzymujące się na wysokim poziomie bezpieczeństwo Polski jest odpowiednim momentem na zainicjowanie procesu dostosowywania sposobu działania polskich służb specjalnych do nowych zagrożeń. Opisane w artykule wzorce brytyjskie mogą być punktem odniesienia dla pokazania perspektywy organów legislacyjnych państwa niejednokrotnie dotkniętego w przeszłości zjawiskiem terroryzmu.