BEZPIECZEŃSTWO 2010 nr 1–2
TEORIA I PRAKTYKA

**Bogdan Mucha**

# Zakres ingerencji egzekutywy w prawa i wolności obywateli USA w dobie walki z terroryzmem

## Wprowadzenie

Zagadnienie kontroli władz wykonawczych w zakresie prowadzonych działań mających na celu pozyskiwanie informacji obcych służb wywiadowczych w celu zapewnienia większego bezpieczeństwa narodowego stanowi w ostatnim czasie przedmiot dużego zainteresowania opinii publicznej, którą poruszyło ujawnienie przez media prowadzenia przez służby specjalne Stanów Zjednoczonych inwigilacji własnych obywateli.

Rok 2005 zakończył się pod znakiem skandalu związanego z ujawnieniem przez media monitorowania rozmów obywateli z zagranicznymi podmiotami na terenie USA prowadzonego przez Krajową Agencję Bezpieczeństwa (*National Security Agency* – dalej NSA)[1]. Falę oburzenia wywołał fakt prowadzenia tej inwigilacji zaraz po ataku z 11 września 2001 r. bez jakiegokolwiek nadzoru sądowego i, co podkreślała większość specjalistów, wbrew regulacjom prawnym obowiązującym w tej dziedzinie. Odbywała się ona na wyłączne zarządzenie prezydenta G. W. Busha, który co kilkadziesiąt dni upoważniał NSA do dalszego prowadzenia inwigilacji rozmów prowadzonych przez osoby, które podejrzewano o związki z międzynarodowymi organizacjami terrorystycznymi, głównie Al-Kaidą, sprawcami zamachu z 11 września. Jak przyznał sam prezydent[2] przeszło 30 razy odnawiał mandat NSA, opierając się na konstytucyjnym obowiązku obrony Stanów Zjednoczonych i uprawnieniach jako naczelnego

[1] Zob. E. Lichtblau, J. Risen, *Bush lets U.S. Spy on Callers Without Courts*, „New York Times" 16.12.2005, s. A1; S. Shane, *Behind Power One Principle,* „New York Times" 17.12.2005, s. A1; E. Lichtblau, S. Shane, *Files Say Agency Initiated Growth of Spying Effort,* „New York Times" 04.01.2006, s. A1.

[2] George W. Bush, President of the United States, *President's Radio Address* (Dec. 17, 2005); United States Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, Jan. 19, 2006 – www. usdoj.gov.

dowódcy sił zbrojnych w czasie wojny[3] oraz na kongresowym upoważnieniu zawartym w ustawie uchwalonej po zamachu do użycia wszelkich koniecznych i niezbędnych środków w wojnie z międzynarodowym terroryzmem[4].

Legalność decyzji prezydenta opartych na koncepcji inherentnych uprawnień była wielokrotnie podważona przez federalne władze ustawodawcze i sądownicze[5]. Trzeba jednak przyznać, że wiele przedsięwzięć podjętych przez administrację prezydenta Busha zostało *post facto* aprobowanych przez Kongres, zaś federalne sądy oddalały dużą liczbę skarg kierowanych przez środowiska libertariańskie[6].

W związku z tym warto dokonać analizy rozwiązań prawnych obowiązujących w Stanach Zjednoczonych Ameryki i ich ewolucji w odniesieniu do działań podejmowanych w imię zapewnienia większego bezpieczeństwa państwa polegających na ustawodawczej i sądowej kontroli pozyskiwania informacji obcych wywiadów przez szesnaście różnych agencji składających się na amerykańskie służby specjalne[7].

## Tajemnica państwowa i zakres jej stosowania

Realizowany przez NSA w latach 2001–2007 projekt *Total Surveillence Program* (dalej TSP) miał na celu pozyskiwanie informacji będących w posiadaniu agentów obcych państw, do których zalicza się również członków organizacji terrorystycznych, aby zapobiegać aktom terroru i eliminować ukryte komórki terrorystów na terenie Stanów Zjednoczonych i w ten sposób zapewnić wyższy stopień bezpieczeństwa państwowego. W ramach programu prowadzone było podsłuchiwanie rozmów telefonicznych, monitorowanie komunikacji elektronicznej przez Internet, a także przeszukiwanie pomieszczeń osób podejrzanych o współpracę z grupami terrorystycznymi. Jak to ujawniła senacka Komisja Wymiaru Sprawiedliwości, TSP był jednym z około 200 różnych programów inwigilacji elektronicznej realizowanych przez pięćdziesiąt dwie cywilne i wojskowe agencje rządowe[8].

Programy te prowadziły w sposób utajniony między innymi przeszukiwanie baz danych, czyli *data mining*, w celu pozyskiwania informacji i wykrycia ewentualnych zagrożeń dla bezpieczeństwa narodowego. O ich istnieniu dowiedział się Kongres dopiero z mediów, zaś administracja prezydenta G. W. Busha zasłaniała się tajemnicą państwową, której naruszenie mogłoby spowodować niepowetowane szkody dla bezpieczeństwa kraju. Powoływała się na ten przywilej, opierając się na dwóch precedensowych orzeczeniach Sądu Najwyższego (dalej SN).

---

[3] *Ibidem*.

[4] Ustawa *Authorization for the Use of Military Force,* PL 107-40, 115 Stat.224 (2001) – dalej AUMF.

[5] Zob. M. Rosenberg, *Presidential Claims of Executive Privilege*: *History, Law, Practice and Recent Developments*, CRS Report for Congress, Order Code RL 30319, Washington, August 21, 2008.

[6] Ich szerokie omówienie zawarte jest w moim opracowaniu nt. Data mining a *prawo do prywatności w świetle doświadczeń amerykańskich* [w:] *Ochrona bezpieczeństwa państwa a ochrona praw i wolności jednostki we współczesnym świecie*, red. nauk. J. Jaskiernia, Uniwersytet Humanistyczno-Przyrodniczy Jana Kochanowskiego, Kielce 2010 (w druku).

[7] Na ich czele stoi Krajowy Dyrektor Służby Specjalnych (*National Intelligence Service Director*) będący jednocześnie członkiem gabinetu prezydenckiego i koordynatorem cywilnych i wojskowych agencji wywiadu i kontrwywiadu.

[8] *Statement of Senator Edward M. Kennedy,* Senate Judiciary Committee on *„Balancing Privacy and Security*: *The Privacy Implication of Government Data Mining Programs"*, January 10, 2007, www.judiciary.senate.gov/hearings/testimony.

Pierwsze zapadło jeszcze w XIX wieku w sprawie *Totten* v. *United States*[9]. SN oddalił wówczas skargę zatrudnionego przez władze Unii szpiega, który operując na tyłach wojsk konfederackich w czasie wojny domowej 1861–1865, miał donosić o ruchach ich oddziałów w zamian za miesięczne wynagrodzenie, którego wypłaty władze odmówiły. Oddalając skargę, SN uzasadnił, że jej przyjęcie doprowadziłoby do ujawnienia tajnych informacji.

Natomiast drugie orzeczenie zostało wydane w sprawie *United States* v. *Reynolds* w 1953 r.[10] W tym wypadku skargę o odszkodowanie wniosły rodziny osób, które zginęły w wypadku samolotu wojskowego przeprowadzającego testy nowych broni. Skarżący zażądali przedstawienia przez lotnictwo raportu powypadkowego. Władze odmówiły, powołując się na tajemnicę państwową, którą były objęte testy. Jej ujawnienie – zdaniem wojska – mogłoby zagrozić bezpieczeństwu narodowemu. Sąd federalny nakazał przedstawienie go do wglądu wyłącznie sędziemu (*in camera*), ale przedstawiciele lotnictwa odmówili. W tej sytuacji sąd uznał roszczenia rodzin. Władze wniosły apelację, w której podnosiły, iż bezzasadny nakaz przedłożenia sądowi dokumentów ingerował w konstytucyjne uprawnienia władz wykonawczych wynikające z konieczności ochrony bezpieczeństwa państwa poprzez odmowę ujawnienia tajnych dokumentów. Sprawa trafiła do Sądu Najwyższego, który dosyć pobieżnie zapoznał się z nią i orzekł, iż władze słusznie zasłoniły się przywilejem tajemnicy państwowej, który sądy powinny respektować. SN zastrzegł, że nie można go dowolnie stosować w każdej sytuacji.

Po latach okazało się jednak, że władze lotnictwa wojskowego chciały ukryć fakt, iż samolot był niesprawny i nie nadawał się do wykonania zadania[11]. Odtajniony raport wskazał, że nie było w nim nic, co mogłoby być objęte tajemnicą państwową.

Orzeczenie w sprawie *Reynolds* spowodowało, że z chwilą objęcia tajemnicą państwową pewnych dokumentów skarżący musieli polegać wyłącznie na dokumentach jawnych jako dowodach w danej sprawie. W razie ich braku sądy na wniosek władz wykonawczych oddalały pozwy.

Przez 20 lat po wydaniu tego orzeczenia władze stosunkowo rzadko zasłaniały się tajemnicą państwową, nie chcąc dopuścić do ujawnienia dokumentów. W latach 1953–1976 tylko w 11 przypadkach wniesiono o oddalenie skarg. Natomiast poważny wzrost nastąpił w latach 1977–2001, kiedy odnotowano 59 takich przypadków. W okresie prezydentury G. W. Busha w latach 2002–2006 administracja 20 razy zasłaniała się tajemnicą państwową, żądając oddalenia pozwów przez sądy, nie poprzestając tylko na odmowie ujawnienia dokumentów. W trzech przypadkach związanych z prowadzeniem nielegalnych podsłuchów przez NSA sądy odmówiły żądaniom władz[12]. Natomiast w dwóch przypadkach sądy federalne przychyliły się do wniosków, z tym że jeden przypadek dotyczył nielegalnych podsłuchów, zaś drugi nielegalnego zatrzymania i przekazania osoby do wiezienia za granicą (*rendition*)[13].

W piśmiennictwie podkreśla się, że posługiwanie się przez władze wykonawcze immunitetem tajemnicy państwowej jest nieuzasadnioną formą przejmowania upraw-

[9] 92 U.S. 105 (1875).

[10] 345 U.S. 1 (1953).

[11] Zob. L. Fisher, *In the Name of National Security: Unchecked Presidential Power and Reynolds*, 2006.

[12] *Al-Haramain Islamic Foundation, Inc.* v. *Bush,* 451 F.Supp.2d 1215 (D.Ore. 2006); *ACLU* v. *NSA,* 438 F.Supp.2d 754 (E.D. Mich. 2006); *Hepting v. AT&T Corp.*, 439 F.Supp.2d 974 (N.D. Cal. 2006).

[13] *Terkel* v. *AT&T Corp.,* 441 F.Supp.2d 889 (N.D. Ill. 2006);*El-Masri* v. *Tenet,* 437 F.Supp.2d 530 (E.D. Va. 2006).

nień władz sądowniczych[14] i ustawodawczych[15]. Konstytucja Stanów Zjednoczonych w art. III upoważnia Kongres do określenia zakresu spraw rozpatrywanych przez sądownictwo federalne. Stąd wymuszanie na sądach oddalania pozwów stanowi nie tylko ingerencję w kompetencje sądów, ale też w uprawnienia Kongresu. Egzekutywa przeszkadza we współpracy władzy sądowniczej i ustawodawczej, która ma na celu kontrolę jej poczynań. Konstytucyjny podział władz pozwala nie tylko na wzajemne hamowanie i kontrolowanie się władz, ale także na to, żeby dwie władze kontrolowały i hamowały trzecią z nich. W literaturze jest prezentowane dosyć odosobnione stanowisko, zgodnie z którym sądy nie posiadają fachowego przygotowania w sprawach bezpieczeństwa narodowego, stąd powinny odgrywać ograniczoną rolę i oddalać skargi, gdy władze zasłaniają się tajemnicą państwową, której ujawnienie mogłoby spowodować duże szkody dla bezpieczeństwa państwa[16]. Ponadto prezydentowi jako naczelnemu dowódcy przysługują konstytucyjne uprawnienia związane z ochroną bezpieczeństwa państwa.

## Ustawowe ramifikacje i ich adaptacja do zmieniających się warunków funkcjonowania

Wbrew twierdzeniom administracji prezydenta G. W. Busha powołującej się na inherentne uprawnienia prezydenta krytycy podkreślają, że działania polegające na stosowaniu zwłaszcza nielegalnych podsłuchów były niezgodne z obowiązującym prawem, a przede wszystkim z ustawą *Foreign Intelligence Surveillance Act of 1978* (dalej FISA)[17].

W celu lepszego zrozumienia zasad wprowadzonych przez ustawę FISA trzeba przybliżyć reguły rządzące monitorowaniem komunikacji osób na terenie USA dla celów prowadzonych zwykłych postępowań karnych oraz wydarzenia historyczne, które wpłynęły na jej uchwalenie przez Kongres.

Instalowanie podsłuchów telefonicznych oraz kontrola korespondencji w sprawach kryminalnych od początku miały na celu wykrycie sprawców przestępstw już popełnionych lub przeciwdziałanie zamiarom ich dokonania. Ewoluowały one przez całe ubiegłe stulecie. Początkowo organy ścigania wydawały nakazy ich instalowania bez jakiejkolwiek kontroli zewnętrznej, co potwierdził Sąd Najwyższy w orzeczeniu *Olmstead* v. *United States*[18], orzekając, iż nie ma żadnych ograniczeń w stosowaniu podsłuchów, jeśli nie dochodzi do fizycznej ingerencji w domu, budynku lub budowli należących do podejrzanego. SN dokonał interpretacji IV poprawki do Konstytucji Stanów Zjednoczonych, która stanowi, że „prawo ludzi do bezpieczeństwa własnej osoby,

---

[14] Zob. R. M. Chesney, *State Secrets and the Limits of National Security Litigations,* „George Washington Law Review" 2007, t. 75, s. 1249 i nast.

[15] Zob. A. Frost, *The State Secrets Privilege and Separation of Powers*, „Fordham Law Review" 2007, t. 75, s. 1931 i nast.

[16] Zob. J. Yoo, *Courts at War*, „Cornell Law Review" 2006, t. 91, s. 573 i nast.

[17] PL 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §1801–1811). Interesujące spojrzenie na historyczne uwarunkowania przyjęcia tej ustawy zawiera opracowanie jednego z jej autorów – W. Funk, *Electronic Surveillance of Terrorism*: *The Intelligence/Law Enforcement Dilemma-A History*, "Lewis & Clark Law Review" 2007, t. 11, s. 1099–1139.

[18] 277 U.S. 479 (1928) (L. Brandeis, dissenting).

a także domów, dokumentów i majątku ruchomego nie będzie naruszane nieuzasadnionym przeszukaniem czy aresztowaniem, przeto nakazy sądowe zezwalające na takie naruszenie będą wydawane tylko przy uzasadnionym podejrzeniu, wspartym zeznaniami złożonymi pod przysięgą lub przyrzeczeniem i będą szczegółowo określać miejsce do przeszukania oraz osoby lub rzeczy do aresztowania"[19]. Zgodnie z nią, gdy urządzenia służące do podsłuchiwania rozmów telefonicznych instalowano na zewnątrz pomieszczeń zajmowanych przez osobę będącą obiektem inwigilacji zbędne było uzyskanie wcześniejszej zgody sądu. Z taką interpretacją większości składu Sądu Najwyższego nie zgodził się sędzia SN L. Brandeis, który w zdaniu odrębnym podkreślił, że „IV poprawka daje nam prawo do pozostawania w sferze prywatności, które jest najszerszym i najbardziej cenionym prawem cywilizowanych ludzi". Jednocześnie SN zachęcił Kongres do uregulowania tej kwestii w drodze ustawowej.

Realizując te sugestie, Kongres w 1934 r. przyjął ustawę wprowadzającą federalne standardy prowadzenia podsłuchów, kierując się w pewnym stopniu rozwiązaniami przyjmowanymi wcześniej w poszczególnych stanach[20]. Bez zezwolenia sądowego zakazano pozyskiwania informacji w drodze monitorowania komunikacji telefonicznej, telegraficznej oraz radiowej i następnie przekazywania ich treści jakiejkolwiek osobie. Nie obejmowało ono nagrywania rozmów lub słuchania ich treści na żywo. Sąd Najwyższy zabronił później wykorzystywania pozyskanych informacji jako dowodów we wszelkich postępowaniach karnych[21].

Stan prawny nie uległ zmianie aż do późnych lat 60., kiedy ochroną z IV poprawki objęto elektroniczne monitorowanie rozmów w warunkach „uzasadnionego oczekiwania prywatności". W orzeczeniu *Katz* v. *United States*[22] SN orzekł, że w sytuacji istnienia uzasadnionego podejrzenia popełnienia przestępstwa i w warunkach, gdy podmiot inwigilowany spodziewa się prywatności, konieczny jest nakaz sądowy na jej prowadzenie. Jednocześnie nie sprecyzowano, czy te same przesłanki obowiązują we wszelkich inwigilacjach, w tym prowadzonych dla celów ochrony bezpieczeństwa państwowego. Podobne stanowisko SN zajął w odniesieniu do podsłuchów prowadzonych w oparciu o stanowe regulacje, podkreślając konieczność istnienia nadzoru sądowego oraz zawiadomienia osoby podejrzanej o prowadzonej inwigilacji po jej zakończeniu w celu zapoznania się z materiałami i ustosunkowania się do nich[23].

Zróżnicowanie przepisów stanowych i federalnych oraz stosowanych w nich niejednolitych kryteriów zmusiło Kongres do przyjęcia rozwiązań prawnych obowiązujących we wszystkich przypadkach prowadzenia elektronicznej inwigilacji w sprawach kryminalnych[24]. Tytuł III tej ustawy po jej nowelizacji w 1986 r.[25] obejmuje zasady prowadzenia monitorowania na terenie Stanów Zjednoczonych elektronicznej komunikacji, w tym poczty elektronicznej, oraz ich rejestracji dla celów dowodowych w późniejszych postępowaniach karnych. Podstawowym warunkiem jest jej prowadzenie przez

---

[19] Zob. *Konstytucja oraz inne podstawowe dokumenty i symbole amerykańskiej kultury patriotycznej*, red. K. Michałek, Warszawa 2005, s. 77.

[20] *Communication Act of 1934*, PL73-416, 48 stat. 1103 (1934).

[21] *Nardonne* v. *United States*, 302 U.S. 379 (1937) i *Nardonne* v. *United States*, 308 U.S. 338 (1939) ( *Nardonne II*).

[22] 389 U.S. 347 (1967).

[23] *Berger* v. *New York*, 388 U.S. 41 (1967).

[24] *Omnibus Crime Control and Safety Streets Act of 1968*, PL 90-351, 82 Stat. 211-225 (1968).

[25] *The Electronic Communications Privacy Act of 1986* (ECPA), PL 99-508, 100 Stat. 1848 (1986).

organy ścigania pod nadzorem sądowym. Nakaz sądowy może być wydany tylko w przypadku zaistnienia uzasadnionego powodu i zakłada obowiązek poinformowania osoby po zakończeniu inwigilacji. Jednocześnie w trakcie jej prowadzenia muszą być zastosowane metody minimalizujące pozyskiwanie informacji niezwiązanych z celem monitorowania.

Z oczywistych powodów te warunki nie mogły być spełnione w odniesieniu do monitorowania aktywności obcych służb specjalnych na terenie USA celem zabezpieczenia interesów państwa. Tego typu działania wymagają nieraz wieloletnich obserwacji, zanim dojdzie do powstania uzasadnionego podejrzenia, że popełniono przestępstwo. Trudno sobie wyobrazić realizację obowiązku poinformowania o prowadzonej inwigilacji, zwłaszcza, że mogłoby to doprowadzić do skandalu dyplomatycznego, gdyby wchodziła w grę aktywność służb państwa sojuszniczego. Podobnie w przypadku zastosowania procedur minimalizacyjnych.

Te znaczne odmienności zdecydowały, iż początkowo tego typu działania były prowadzone w oparciu o konstytucyjne prerogatywy prezydenta jako naczelnego dowódcy oraz egzekutora prawa, podkreślone dodatkowo w orzeczeniu Sądu Najwyższego w sprawie *United States* v. *Curtiss-Wright Export Company*[26], w którym został on określony jako wyłączny organ władz federalnych w dziedzinie stosunków zagranicznych.

Prezydenci za pośrednictwem Prokuratorów Generalnych zarządzali podejmowanie inwigilacji obcych służb, zarówno na terenie kraju, jak i za granicą, w szczególności w trakcie drugiej wojny światowej i „zimnej wojny"[27]. Przez kilkadziesiąt lat temat nie był podejmowany przez Sąd Najwyższy. O ile w orzeczeniu *Katz* SN nie odniósł się w ogóle do tej kwestii, to w wyroku *United States* v. *United States District Court* (Keith) marginalnie ją poruszył, uznając, iż prezydent nie posiada uprawnień do zarządzania inwigilacji elektronicznej osób, które nie mają znaczących kontaktów z obcymi państwami lub ich służbami wywiadowczymi na terenie Stanów Zjednoczonych[28]. Sędzia Powell stwierdził, że „informacje dotyczące bezpieczeństwa narodowego oraz ustawy nie ograniczają konstytucyjnych uprawnień prezydenta do podejmowania działań koniecznych dla ochrony Stanów Zjednoczonych przed działaniami wywrotowymi, stąd nie można do nich zastosować przepisów tytułu III". Co ciekawe, SN zwrócił uwagę na związki inwigilacji z I poprawką do Konstytucji gwarantującą wolność słowa, zrzeszania się i religii w kontekście monitorowania dysydentów, w sytuacji braku jasnych regulacji ustawowych. Wstrzemięźliwość SN niższe instancje odczytały jako odmowę objęcia gwarancjami z IV poprawki inwigilacji obcych służb specjalnych, która pozostała w związku z tym w wyłącznej gestii władzy wykonawczej[29].

Władze sądownicze dostrzegały jednak odmienny charakter monitorowania aktywności obcych służb wynikający między innymi z pozyskiwania informacji z różnorodnych źródeł, trudności w identyfikacji obiektu oraz prewencyjnego celu podejmowanych działań i ich dłuższej perspektywy czasowej[30]. Z tej perspektywy zmienia się

[26] 299 U.S. 304 (1936).

[27] Zob. A.A. Bradley, *Comment*: *Extremism in the Defense of Liberty?*; *The Foreign Intelligence Surveillance Act and the Significance of the USA Patriot Act*, „Tulsa Law Review" 2002, t. 77, s. 465 i nast.

[28] 407 U.S. 297 (1972).

[29] *United States* v. *Brown*, 484 F.2d 418 (5th Cir. 1973); *United States* v. *Butenko*, 494 F.2d 593 (3rd Cir. 1974).

[30] Zob. P. Swire, *The System of Foreign Intelligence Surveillance,* „George Washington Law Review" 2004, t. 72, s. 1306 i nast.

również rozumienie przesłanki „uzasadnionego podejrzenia" w odniesieniu do spraw związanych z inwigilacją obcych służb i koniecznością uregulowania przez Kongres w warunkach szybkich zmian, głównie w płaszczyźnie aplikacji coraz nowocześniejszych technologii informatycznych[31].

## Nowe technologie informatyczne

W przeciwieństwie do technologii stosowanych nawet kilkanaście lat temu, współczesne sposoby cyfrowego komunikowania się za sprawą Internetu koncentrują się bardziej na przesyłanych informacjach niż na uczestnikach tego procesu[32]. Przesyłanie zwykłych danych, informacji wideo i audio odbywa się obecnie z wykorzystaniem metod cyfrowych, które polegają rozczłonkowaniu ogółu przekazywanych informacji na drobne pakiety (*packets*). Pakiety są ciągami zer i jedynek, które odpowiadają stronie zapisanej informacji. Taka wiązka danych zaczyna się od nagłówka (*header*) i odpowiada adresowi nadawcy i adresata na zwykłych listach. Nagłówek wyjaśnia zatem, skąd przychodzi komunikat, na jaki adres IP (*Internet Provider*) ma trafić, do jakiego programu się odnosi i jaka jest jego długość. Po nim pojawia się treść pakietu (*payload*), czyli dane zawarte w komunikacie, które mogą być odpowiednio kształtowane przez nadawcę poprzez stosowanie na przykład szyfrów lub różnej ich objętości.

Z chwilą wysłania informacji, czyli wpuszczenia jej w sieć połączeń internetowych nadawca praktycznie traci kontrolę nad sposobami i szybkością dotarcia komunikatu do komputera odbiorcy. Wędrują one po niezależnych trasach i nie ma – jak 30 lat temu – przydzielonej linii przesyłania, co więcej, komunikacja od nadawcy do odbiorcy może być każdorazowo przesyłana innymi drogami, zwłaszcza z wykorzystaniem szybkich połączeń networkowych i techniki bezprzewodowej[33]. Komputerowe przekaźniki (*switches* lub *routers*) określają w danym momencie i na całej trasie przekazu najbardziej wydajne drogi przesyłania pakietów uwzględniające przede wszystkim natężenie ruchu w sieci, a nie tylko najkrótszy dystans pomiędzy nadawcą a odbiorcą. Pakiety często wędrują przez cały kraj, a nierzadko przez kontynenty dzięki kanałom zwanym podporami internetowymi (*backbones*). Na przykład, gdy ktoś z Warszawy chce wejść na stronę serwera w Chicago, to pakiet najpierw może trafić do Kalifornii, a dopiero potem do wietrznego miasta. Wysyłając komunikaty, np. z Iraku do Afganistanu, pakiet może przechodzić przez serwer w Stanach Zjednoczonych, zanim trafi do afgańskiego odbiorcy. Gdy komunikat trafia do komputera odbiorcy, następuje automatyczna agregacja pakietów i odtworzenie oryginału.

Warto dodać, iż amerykańska przewaga technologiczna, globalizacja i koncentracja w sektorze telekomunikacyjnym powodują, że bardzo duża ilość pakietów przepływa tranzytem przez routery w Stanach Zjednoczonych, gdzie znajduje się też najwięcej serwerów obsługujących światową sieć internetową. Nie pozostaje to bez

[31] Zob. B. Mucha, *op. cit.*

[32] Zob. O.S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, „University of Chicago Law Review" 2008, t. 75, s. 233–235.

[33] Zob. K. A. Taipale, *The Ear of Dionysus*: *Rethinking Foreign Intelligence Surveillance*s, „Yale Journal of Law and Technology" 2007, t. 9, s. 147 i nast.

wpływu na zmiany obowiązujących regulacji prawnych mających zapewnić większe bezpieczeństwo Stanów Zjednoczonych.

Technika przekazu ma we współczesnych warunkach ogromne znaczenie i jest równolegle wykorzystywana, zarówno przez odpowiednie państwowe służby bezpieczeństwa, jak i przez organizacje terrorystyczne, które stosują trudne do wykrycia zastępcze adresy (*proxy* IP), stąd nawet przechwycenie komputera takiej organizacji może nie wskazać na osoby, które go używały. Używanie specjalnych telefonów internetowych stosujących technikę przesyłania głosu za pośrednictwem sieci (*Voice over Internet Provider* – VoIP) powoduje dodatkowe trudności z wykryciem użytkowników, albowiem telefon ma przydzielony amerykański lokalny numer, co wskazuje na komunikację krajową chronioną konstytucyjnie, podczas gdy w rzeczywistości ma ona charakter międzynarodowy.

Monitorowanie w sieci przez agencje wywiadowcze komunikacji przeciwnika polega głównie na podłączeniu do niej automatycznych analizatorów sieciowych lub inaczej „programów węszących" (*packet sniffers*)[34]. Są to programy *software* lub *hardware*, których zadaniem jest przechwytywanie strumieni pakietów w całej sieci lub jej części. Gdy pakiety płyną w sieci monitorowanej przez te programy, dochodzi do przechwycenia ich wszystkich lub tylko niektórych w zależności od stosowanych przez operatora filtrów, czyli algorytmów, które realizują cele będące przedmiotem jego zainteresowania. Są one potem dekodowane, analizowane i składane w spójną i logiczną całość. Automatyczne analizatory pracują bez udziału czynnika ludzkiego. Tylko w razie wykrycia na przykład podejrzanych połączeń lub kanałów przepływu informacji włącza się operator obsługujący system monitorowania.

W piśmiennictwie wyróżnia się trzy rodzaje automatycznego monitorowania[35]. Pierwszy typ polega na monitorowaniu treści komunikacji (*content filtering*). Program poszukuje poszczególnych słów lub zwrotów zawartych w przesyłanych informacjach, których pojawienie się oznacza konieczność bliższej analizy. Na przykład program *Echelon* realizowany przez NSA we współpracy z odpowiednimi służbami z Australii, Kanady, Nowej Zelandii i Wielkiej Brytanii stosuje specjalne słowniki składające się z kluczowych słów i zwrotów, nazwisk, adresów, w tym internetowych IP oraz numerów telefonów (*signal of interest*). Pojawienie się ich w treści komunikacji powoduje przechwycenie jej i poddanie analizie, natomiast inne informacje przepływają bez żadnej kontroli. Istnienie tego typu programów nie zostało potwierdzone przez żadną ze służb, chociaż wiadomo, iż używają one specjalnych algorytmów zbudowanych w oparciu o sztuczną inteligencję oraz zaawansowane metody statystyczne sygnalizujące operatorowi konieczność zainteresowania się danym komunikatem[36].

Drugi rodzaj automatycznego monitorowania polega na analizie ruchu w sieci (*traffic analysis*). Obserwowana jest częstotliwość przesyłanych informacji, ich długość oraz trasy bez analizy treści. Analiza ruchu wskazuje na typowe wzory postępowań organizacji terrorystycznych i ich członków, na przerwy w przesyłaniu poczty elektronicznej pomiędzy poszczególnymi odległymi od siebie komórkami. W połą-

[34] Takim narzędziem diagnostycznym FBI jest *Narus STA 6400* monitorujący komunikację sieciową, zob. D. McCullagh, *FBI Turns to Brand New Wiretap Method*, CnetNews.com z 30.01.2007.

[35] Zob. K. A. Taipale, *Whispering Wires and Warrantless Wiretaps*: *Data Mining and Foreign Intelligence Surveillance*, „New York University Law and Security" Spring 2006, No. VII Supp.

[36] *Ibidem*, s. 157.

czeniu z analizą treści oraz z wykorzystaniem teorii socjologii sieciowej programy tego rodzaju są w stanie zidentyfikować organizacje, ich wewnętrzne komórki i członków. Dobrą ilustracją tego zjawiska były typowe zachowania grupy Al-Kaidy przygotowującej atak na Nowy Jork, mimo że część przesyłanych informacji była szyfrowana[37].

Trzecią kategorię stanowią programy analizujące typowe formy zachowań, aktywności, po których można ewentualnie rozpoznać przeciwnika (*pattern analysis*). Ten rodzaj monitorowania ma na celu obserwację i szukanie hipotetycznych związków, dzięki czemu można ujawnić nieznane i ukrywane powiązania. Raport Komisji 9/11 ujawnił, że liderzy 19-osobowej grupy zamachowców przeprowadzili 206 rozmów międzynarodowych z osobami w Arabii Saudyjskiej, Syrii i Niemczech. Rozmowy międzynarodowe były więc typowym wzorem zachowania się, a w związku z tym ich inwigilacja przy pomocy firm telekomunikacyjnych może doprowadzić do wykrycia „uśpionego" agenta lub całej grupy przebywającego na terenie Stanów Zjednoczonych.

*Data mining* z punktu widzenia celu ich stosowania można podzielić na programy ukierunkowane na podmiot zainteresowania, czyli wyszukiwania wszelkich informacji z różnorodnych baz na temat określonej osoby (*target driven*)[38]. Mogą one dokonywać porównania posiadanych informacji z osobą, co do której może zachodzić podejrzenie o prowadzenie działalności terrorystycznej (*match driven*). Takim programem był na przykład *Secure Flight* porównujący nazwiska na liście podejrzanych z listą pasażerów linii lotniczych. W obu powyższych przypadkach obiektem zainteresowania są osoby i od nich zaczyna się przeszukiwanie baz danych.

Natomiast szukanie typowych zachowań, które zarejestrowano w przeszłości i były skojarzone z podejrzaną aktywnością, jest zadaniem programu *event driven*. Temu celowi służył zarzucony program TIA, w ramach którego zbierano informacje dotyczące metod działania terrorystów w przeszłości, kreując pewne modele zachowań. Dzięki temu pozyskiwano materiał dla analityków, którzy budowali pewne teorie, w jaki sposób może ewentualnie dojść do kolejnego ataku i jaką strategię należy przyjąć, by mu zapobiec.

Krytycy tych programów twierdzą, iż są wprawdzie przydatne, ale nie dla celów zapobiegania atakom, ponieważ w przypadku braku informacji o typowych zachowaniach członków różnorodnych grup terrorystycznych i sposobach ich postępowania niezwykle trudno zbudować użyteczne algorytmy, zastosowane później do wykrywania nieznanych zachowań w celu przewidywania, jakie skutki mogą wystąpić w przyszłości[39]. W rezultacie następuje marnowanie pieniędzy podatnika, albowiem zbyt dużo występuje błędnych wniosków w odniesieniu do wskazania potencjalnych sprawców, a przy tym dochodzi do zbyt dużej ingerencji w prawa i wolności człowieka.

---

[37] Zob. Raport Komisji w sprawie ataku z 9 września 2001.

[38] Zob. Ch. Slobogin, *Government Data Mining and the Fourth Amendment*, „University of Chicago Law Review" 2008, t. 75, s. 322–323.

[39] Zob. J. Jonas, J. Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, Cato Institute, Washington, December 11, 2006, s. 7.

## Ustawodawcze formy kontroli inwigilacji

Ustawa FISA została przyjęta przez Kongres w następstwie afery Watergate i raportu senackiej komisji pod przewodnictwem F. Churcha[40]. Wynika z niego, że FBI, CIA, służby specjalne armii i IRS były odpowiedzialne za otworzenie i skopiowanie w latach 1953–1973 250 tys. listów, a informacje z nich posłużyły do zbudowania bazy danych zawierających przeszło 1,5 mln nazwisk. FBI w latach 1940–1966 otworzyła 130 tys. listów, które nadeszły do 8 głównych urzędów pocztowych w miastach amerykańskich. Do bazy danych CIA w latach 1967–1973 wprowadzono przeszło 300 tys. nazwisk, otworzono teczki dla 7,2 tys. obywateli USA i 100 różnych organizacji w czasie akcji pod kryptonimem *Chaos*. Miliony telegramów było czytanych przez pracowników NSA w latach 1947–1975 na mocy tajnego porozumienia z firmami telekomunikacyjnymi. Służby specjalne armii założyły teczki przeszło 100 tys. osób w latach 1965–1971, zaś FBI posiadała listę 26 tys. osób, które miały być aresztowane w wypadku ogłoszenia stanu nadzwyczajnego. Dla swoich celów podsycała ona na przykład atmosferę zagrożenia komunistycznego.

Wymienione wyżej dane wskazują na skalę szpiegowania społeczeństwa amerykańskiego i ignorowanie obowiązujących regulacji prawnych, podczas gdy ofiary były nieświadome podejmowanych względem nich działań. Informacje pozyskane w ten sposób stanowiły instrument używany w walce politycznej z przeciwnikami, do których należeli między innymi członkowie Kongresu, sędziowie, aktywiści Partii Demokratycznej, obrońcy praw obywatelskich, nowa lewica itp. Trudno się dziwić, iż w tych warunkach narastało poparcie społeczne i polityczne do uregulowania zagadnienia.

Ustawa FISA stanowiła w tym czasie swoisty kompromis pomiędzy środowiskiem służb specjalnych, których podstawowym zadaniem jest ochrona bezpieczeństwa narodowego a koniecznością wprowadzenia kontroli sądowej akcentowaną przez obrońców wolności i praw człowieka oraz ukrócenia praktyk szeroko opisanych w raporcie senatora F. Churcha[41]. Ustawa stworzyła system prowadzenia na terenie Stanów Zjednoczonych legalnej inwigilacji służb specjalnych obcych państw, ich agentów, w tym członków międzynarodowych organizacji terrorystycznych. W celu odróżnienia ich od podmiotów amerykańskich ustawodawca posłużył się kryterium obywatelstwa lub siedziby firmy. Podmiotami amerykańskimi są obywatele Stanów Zjednoczonych, stali rezydenci oraz osoby prawne zarejestrowane w USA. Podmioty amerykańskie mogą być potraktowane jako agenci państw obcych pod warunkiem, że świadomie brali udział w enumeratywnie wymienionych czynnościach, w tym w tajnych operacjach wywiadowczych na rzecz obcego mocarstwa, które mogą stanowić naruszenie przepisów karnych.

Kontrolę nad działaniami służb specjalnych sprawuje specjalnie utworzony na podstawie przepisów ustawy sąd FISA złożony obecnie z 11 sędziów wytypowanych na 7-letnią kadencję przez Prezesa Sądu Najwyższego. Sędziowie wyrażają zgodę na elektroniczną inwigilację, kierując się szeregiem przesłanek. Podstawową przesłanką jest istnienie uzasadnionego podejrzenia, iż obiektem obserwacji jest funkcjonariusz

[40] S Rep. No. 94-755, 1978 USCCAN 3909. Nielegalną inwigilację upublicznili w swojej książce m.in. M. Halperin, J. Berman, R. Borosage, Ch. Marwick, *The Lawless State*: *The Crimes of the U. S. Intelligence Agencies*, New York 1976.

[41] Przeciwnicy bezskutecznie próbowali podważyć jej konstytucyjność na gruncie I poprawki – *United States* v. *Falvey*, 540 F.Supp. 1306 (E.D.N.Y. 1982); V i VI poprawki – *United States* v. *Belfield*, 692 F.2d 141 (D.C. Cir. 1982); IV poprawki – *United States* v. *Duggan*, 743 F.2d 59 (2d Cor. 1984).

obcego państwa lub jego agent albo członek organizacji terrorystycznej lub osoba z nią powiązana.

Procedura uzyskania nakazu sądowego w świetle przepisów ustawy FISA najbardziej wyróżnia ją od podobnej procedury w sprawach kryminalnych. Została ona ukształtowana wyłącznie pod kątem umożliwienia służbom specjalnym zgromadzenia obcych informacji wywiadowczych, a nie w celu zdobycia dowodów niezbędnych w postępowaniu karnym[42]. Ponadto ma charakter podkreślający konieczność zachowania w tajemnicy podejmowanych działań. Stąd przebiega przed niezależnym organem sądowym, sądem FISA, niekiedy nazywanym tajnym sądem, który jest powołany wyłącznie w tym celu i nie rozstrzyga innych spraw. Narzędzia inwigilacji, na których stosowanie zezwalał sąd, ulegały stopniowemu poszerzaniu, głównie w odpowiedzi na bieżące zagrożenia i zachodzące zmiany technologiczne.

Sąd FISA wydaje nakazy lub odrzuca wnioski dotyczące elektronicznej inwigilacji, przeszukania pomieszczeń[43], zakładania podsłuchów linii telefonicznych, konfiskaty przedmiotów, zakładania urządzeń rejestrujących komunikację przychodzącą i wychodzącą oraz wydania wskazanych rzeczy[44].

Procedura uzyskania zezwoleń sądowych na podsłuchiwanie rozmów telefonicznych, elektronicznej inwigilacji i przeszukania pomieszczeń wykorzystywanych przez agentów obcych państw, w którym to pojęciu mieszczą się członkowie organizacji terrorystycznych, jest identyczna[45]. Nakazy wydaje sąd FISA w składzie jednoosobowym po rozpatrzeniu wniosku zatwierdzonego przez Prokuratora Generalnego lub inną osobę upoważnioną przez prezydenta. W dotychczasowej praktyce wnioski składali samodzielnie wysocy funkcjonariusze FBI. Zatwierdzanie wniosków przez specjalną komórkę Departamentu Sprawiedliwości ma stanowić zabezpieczenie przed powtórzeniem się nagannych praktyk z czasów J. E. Hoovera.

Dodatkowe gwarancje ustawowe wprowadził Kongres nieco wcześniej, przyjmując regulacje dotyczące zamknięcia dostępu do teczek obywateli[46], rozszerzenia dostępu opinii publicznej do dokumentów urzędowych[47] oraz upublicznienia własnej aktywności[48]. Jednocześnie Departament Sprawiedliwości wydał wytyczne, podkreślając, iż wszelkie śledztwa w sprawach związanych z bezpieczeństwem wewnętrznym muszą być prowadzone tak, aby nie naruszać postanowień Konstytucji i zwykłego ustawodawstwa. Nadzór nad FBI i innymi służbami specjalnymi powierzono w ramach tego departamentu Urzędowi ds. Służb Specjalnych i Nadzoru (*Office of Intelligence Policy and Review* – dalej OIPR). Stanowił on jedyny kanał, przez który przechodziły pozyskane informacje wywiadowcze do organów ścigania. Do 2001 r. istniał rodzaj muru (*wall*) oddzielającego te działania, co – zdaniem Komisji 9/11– było jedną z przyczyn

---

[42] W oryginalnym brzmieniu ustawy ten cel miał charakter wyłączny. Po nowelizacji w ustawie *USA Patriot Act of 2001* złagodzono wymogi, określając, iż gromadzenie obcych informacji wywiadowczych musi być „znaczącym" celem starania się o zgodę sądu FISA – 50 U.S.C. 1804(a)(7)(B) (1982 ed.); *In re Sealed Case*, 310 F.3d 717 (F.I.S.Ct.Rev.2002); *United States* v. *Ning Wen,* 477 F.3d 896, 897 (7th Cir. 2007).

[43] W następstwie afery szpiegowskiej z 1995 r. A. Ames'a nowela ustawy FISA [PL103-359, 108 Stat. 3444 (1995)] przyznała uprawnienie do prowadzenia rewizji.

[44] Nowelizacja z 1998 r. w odpowiedzi na zamachy bombowe w Oklahoma City i WTC – PL105-272, 112 Stat. 2396 (1998).

[45] 50 U.S.C. 1801-1829.

[46] *The Privacy Act of 1974*, PL 93-579, 88 Stat. 1896 (1974).

[47] *The Freedom of Information Act of 1974*, PL 93-502, 88 Stat. 1561 (1974).

[48] *The Government in the Sunshine Act of 1976*, PL 94-409, 90 Stat. 1241 (1976).

uniemożliwiających wcześniejsze wykrycie zamiarów terrorystów Al-Kaidy[49], albowiem zabrakło koordynacji działań między służbami a pionem kryminalnym Departamentu Sprawiedliwości. Nastąpiło to w rezultacie wydania w 1995 r. nowych wytycznych, które usztywniły ten rozdział przez wprowadzenie całkowitego zakazu kontaktu personelu wywiadu FBI z przedstawicielami wydziału karnego bez zgody OIPR[50].

Wniosek o wydanie nakazu przez sąd FISA musi zawierać obecnie następujące informacje:

- wskazanie wnioskodawcy,
- określenie podmiotu, którego komunikacja będzie przedmiotem inwigilacji, w tym fakty przemawiające za tym, że ten podmiot jest agentem obcego państwa lub że używa określonych pomieszczeń dla celów działalności wywiadowczej,
- określenie przedmiotu monitorowania, w tym rodzaj pozyskiwanej komunikacji i poszukiwanych informacji[51],
- opis stosowanych procedur minimalizujących pozyskiwanie zbędnych informacji, w szczególności odnoszących się do podmiotów amerykańskich,
- poświadczenie przez wysokiego funkcjonariusza służb specjalnych lub inną upoważnioną osobę, że znaczącym celem jest pozyskanie informacji obcych wywiadów i że w inny sposób nie można ich zgromadzić,
- opis stosowanych technik monitorowania, w tym fizycznego przeszukania pomieszczeń[52],
- historia monitorowania tego samego podmiotu lub obiektu,
- wskazanie okresu, na jaki ma obowiązywać zgoda sądu i czy monitorowanie zostanie zakończone z chwilą pozyskania poszukiwanych informacji[53].

Sąd FISA rozpatruje, czy wszystkie wymogi prawa zostały spełnione, a w szczególności, czy jest uzasadnione podejrzenie, że obiekt inwigilacji jest agentem obcego mocarstwa. W przypadku wyrażenia zgody nakaz wydany przez sąd zawiera wszystkie elementy wskazane we wniosku oraz dodatkowo polecenie współpracy ze służbami specjalnymi prowadzącymi inwigilację firm telekomunikacyjnych, kurierskich oraz osób fizycznych opiekujących się pomieszczeniami stanowiącymi przedmiot obserwacji. W odniesieniu do współpracujących osób prawnych i fizycznych nakazy sądowe zawierają zakazy przekazywania przez nich jakichkolwiek informacji na temat podejmowanych działań (*gag rule*), rodzaj rekompensaty ze strony władz za ich pomoc oraz zwolnienie od wszelkiej odpowiedzialności prawnej[54].

---

[49] Zob. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, Norton Publishers, New York 2004, s. 362 i nast. Zdaniem W. Funka było to niezgodne z pierwotnymi zamierzeniami federalnego ustawodawcy – zob. W. Funk, *op. cit.*, s. 1099.

[50] Zob. P. Swire, *op. cit.*, s. 1306 i nast.

[51] Na podstawie noweli *FISA Amedment Act of 2008*, PL 110-261, złagodzono wymóg szczegółowego opisu rodzaju poszukiwanych wiadomości, obecnie wystarczy wskazanie, jakie informacje spodziewa się pozyskać wnioskodawca.

[52] Nowelizacja ustawy FISA z 2008 r. złagodziła wymagania w odniesieniu do określenia technik. Obecnie wystarczy tylko ogólny opis, bez podawania szczegółów, w celu zwiększenia elastyczności działania służb i metod, którymi się posługują. Na tle oryginalnych regulacji zastosowanie innych niż wnioskowanych instrumentów inwigilacji wymagało ponownego zwrócenia się do sądu FISA o wyrażenie na nie zgody.

[53] Nowela z 2008 r. zniosła wymóg wskazania we wniosku, że zyskał on aprobatę Prokuratora Generalnego lub prezydenta.

[54] Dotyczy to także retroaktywnego immunitetu, czyli za udzielaną pomoc w latach 2001-2007 w świetle zmian do ustawy FISA z 2008 r.

W przypadku gdy konieczne okaże się w trakcie inwigilacji obserwowanie innych obiektów wnioskodawca ma obowiązek zawiadomić niezwłocznie sąd. Podobnie w przypadku osiągnięcia celu i pozyskania informacji, jednakże nie później niż po 90 dniach. Przedłużenie nakazu w sytuacji, gdy podmiotami są agenci obcego państwa jest ograniczone do 120 dni lub jednego roku, w przypadku obcych rządów, ich organów lub przedstawicielstw.

W sytuacjach niecierpiących zwłoki inwigilacja może być obecnie początkowo prowadzona bez nakazu sądowego przez okres do 7 dni (oryginalnie było to 24 godziny, później 3 dni). W przypadku ogłoszenia wojny przez Kongres termin ten wynosi 15 dni.

W świetle najnowszych regulacji rozszerzono zakres monitorowania, które nie wymaga zgody sądu i obejmuje oprócz inwigilacji prowadzonej poza terytorium Stanów Zjednoczonych także prowadzenie monitorowania komunikacji pomiędzy obcymi państwami lub komunikacji niesłownej prowadzonej z miejsc znajdujących się pod kontrolą obcych państw. W tych przypadkach władze są zobowiązane składać sprawozdania Kongresowi i sądowi FISA[55], co ma na celu pokazanie skali prowadzonej pozasądowej inwigilacji, w szczególności jeśli obejmowała ona podmioty amerykańskie. W tym ostatnim przypadku może powstać zarzut, iż narusza to prawo obywateli do ochrony z IV poprawki. Sądy federalne w większości odmawiały zasadności tego typu skarg[56].

Ustawa FISA zawiera szczegółowe rozwiązania dotyczące wykorzystania informacji zebranych w trakcie inwigilacji. Przede wszystkim mogą one trafić tylko do osób posiadających akces do tajnych źródeł. W przypadku chęci ujawnienia informacji musi być zgoda Prokuratora Generalnego, zaś w przypadku użycia ich jako dowodu w sprawie osoba monitorowana musi otrzymać stosowne zawiadomienie, chyba że zachodzi możliwość ujawnienia informacji narażających na szkodę bezpieczeństwo państwowe (*suppression procedure*)[57]. W takich sytuacjach sąd zapoznaje się na niejawnym posiedzeniu (*in camera*) z treścią zebranych informacji bez udziału pełnomocników podejrzanego (*ex parte*)[58].

Stosowanie urządzeń rejestrujących rozmowy wychodzące i przychodzące (*pen register and trap and trace devices*) do podmiotu monitorowanego odbywa się na podobnych zasadach jak w sprawach kryminalnych z pewnymi odmiennościami wynikającymi z charakteru pozyskiwanych informacji. Nakaz może wydać członek sądu FISA lub sędzia administracyjny (*magistrate*) na wniosek federalnego funkcjonariusza, który zaświadcza, iż poszukiwane informacje są relewantne do prowadzonego śledztwa w sprawie międzynarodowego terroryzmu lub aktywności obcych służb wy-

---

[55] 50 U.S.C. 1802(a)(2),(3); 1822 (a)(2),(3) (text is appended). W latach 1981–1990 sąd FISA wydawał średnio pomiędzy 433 a 600 nakazów rocznie. W latach 1995–2000 odpowiednio 697–1012. Ich liczba wzrosła po 2001 r. Np. w 2003 r. wyniosła 1727 nakazów, podczas gdy w latach 2006 i 2007 odpowiednio 2176 i 2370 – ww.epic.org/privacy/wiretap/stats .

[56] *United States* v. *Mubayyid,* 521 F. Supp.2d. 125 (D. Mass.2007); *Mayfield* v. *United States*, 504 F.Supp.2d 1023 (D. Ore. 2007). Instancja odwoławcza sądu FISA odrzuciła skargę firmy telekomunikacyjnej na podważającą konstytucyjność nowelizacji ustawy z 2008 r. – zob. E. Lichtblau, *Intelligence Court Rules Wiretapping Power Legal*, „New York Times" 16.11.2009, s. A16.

[57] 50 U.S.C. 1806(e),(f),(g),(h).

[58] *United States* v. *Campa*, 529 F.3d 980 (11th Cir. 2008); *United States* v. *Amawi*, 531 F.2d 832 (N.D. Ohio 2008).

wiadowczych[59]. W nakazie może być zawarte polecenie ujawnienia informacji dotyczących określonej osoby znajdujących się w zasobach firm telekomunikacyjnych, czyli wykaz numerów telefonów, pod które dany podmiot dzwonił lub z których się z nim kontaktowano. Prokurator Generalny posiada uprawnienia do zarządzenia natychmiastowego zainstalowania takich urządzeń pod warunkiem, że w ciągu następnych 48 godzin przedstawi sądowi FISA odpowiedni wniosek. Gdyby sąd odmówił wydania nakazu, nie można użyć w przyszłości pozyskanych informacji przeciwko monitorowanej osobie.

Zagadnienie dostępu do dokumentów biznesowych kurierów pocztowych, wypożyczalni samochodów lub firm wynajmujących pomieszczenia magazynowe stanowi odrębnie regulowaną kwestię przez ustawę FISA. Do czasu nowelizacji z 2001 r. sąd FISA mógł wydać odpowiedni nakaz na wniosek wysokiego funkcjonariusza FBI, w którym poświadczał zasadność podejrzenia, iż dane tych firm mają związek z obcym państwem lub jego agentem. Po wejściu w życie ustawy *USA Patriot Act* i przedłużeniu jej obowiązywania wystarczy, że dokumenty są relewantne do toczącego się śledztwa. Jednocześnie rozszerzono ich definicję, obejmując nią wszelkie dokumenty prywatne i służbowe osób fizycznych i prawnych, o ile mogą przydać się w inwigilacji obcych służb albo w działaniach kontrwywiadowczych służb amerykańskich[60]. Podmioty, do których zwrócono się o ich przekazanie, mają zakazane ujawnianie samego faktu istnienia takiego nakazu, mogą jednak zwrócić się o pomoc prawną w odniesieniu do ich praw i obowiązków. Objęte są immunitetem federalnym z tytułu udzielania pomocy władzom.

Z uwagi na liczne obiekcje i skargi libertarian, które dotyczyły na przykład przekazywania informacji bibliotecznych lub księgarń, Kongres wprowadził regulacje minimalizujące pozyskiwanie zbędnych informacji oraz ograniczył sposób ich wykorzystania[61]. Jednocześnie uruchomił wnikliwą kontrolę sposobów wykorzystania nakazów przez Departament Sprawiedliwości z obowiązkiem przedkładania co pół roku sprawozdań odpowiednim komisjom Izby i Senatu, włączając w to krajowe polecenia w sprawach bezpieczeństwa (*National Security Letters*).

W dniu 10 lipca 2008 r. prezydent podpisał najnowszą nowelizację ustawy FISA[62]. Reguluje ona cztery grupy zagadnień i z jednej strony łagodzi niektóre poprzednio istniejące wymagania, zapewniając większą elastyczność operacji służb specjalnych, z drugiej zaś zawiera nowe instrumenty kontrolne ich działań. Przede wszystkim wprowadza tymczasowe zezwolenie na pozyskiwanie obcych informacji wywiadowczych od podmiotów przebywających poza granicami Stanów Zjednoczonych. Potwierdza jednocześnie, że elektroniczna inwigilacja może być prowadzona wyłącznie na podstawie przepisów tytułu III/ECPA lub ustawy FISA. W celu kontroli prowadzenia programów TSP generalni kontrolerzy w poszczególnych agencjach rządowych mają obowiązek przygotowywać okresowe sprawozdania przedkładane następnie Kongresowi.

---

[59] 50 U.S.C. 1842.

[60] 50 U.S.C. 1861 (a).

[61] 50 U.S.C. 1861 (g), (h).

[62] *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, PL110-261. Szerzej na temat dyskusji w związku z ustawą pisze E. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of Selected Issues*, CRS Report for Congress, Order Code RL 34279, Washington, July 7, 2008.

Udzielanie pomocy władzom przez osoby prywatne i prawne objęte jest nadal immunitetem sądowym.

Nowela wprowadza trzy procedury tymczasowe obowiązujące do końca 2012 r., które regulują sprawy autoryzacji pozyskiwania obcych informacji wywiadowczych od podmiotów, co do których jest przekonanie, że przebywają za granicą[63]. Pierwsza dotyczy informacji uzyskiwanych od osób niebędących podmiotami amerykańskimi. Druga i trzecia odnosi się do sytuacji, gdy obiektem elektronicznej inwigilacji jest podmiot amerykański przebywający za granicą, i obejmuje również zagraniczne bazy danych i dokonywanie fizycznego przeszukania pomieszczeń zajmowanych za granicą przez obywatela amerykańskiego.

W pierwszym przypadku, gdy obiektem są osoby niebędące podmiotami amerykańskimi, procedurę rozpoczyna przedłożenie przez Prokuratora Generalnego lub Dyrektora Krajowej Służby Wywiadu wniosku do zatwierdzenia przez sąd FISA lub wydania przez niego wstępnej zgody w sprawach niecierpiących zwłoki. We wniosku muszą oni poświadczyć, iż znaczącym celem podejmowanych działań jest zamiar pozyskania informacji obcych służb i do tego konieczna jest pomoc firm telekomunikacyjnych, które z tego tytułu mogą uzyskać rekompensatę i być zwolnione ze wszelkiej odpowiedzialności prawnej. Muszą oni zapewnić, że obiektem jest osoba przebywająca za granicą i w związku z tym będą podejmowane działania zapobiegające pozyskiwaniu informacji od podmiotów znajdujących się na terenie Stanów Zjednoczonych, łącznie ze stosowaniem procedur minimalizujących oraz spełniających wymogi IV poprawki do Konstytucji. Warto dodać, iż metody używane przez odpowiednie służby nie muszą być sprecyzowane w celu zwiększenia elastyczności podejmowanych działań. Nie muszą być zatem określone miejsca prowadzenia inwigilacji. Jeśli chodzi o czas, to inwigilacja może być prowadzona przez okres do 12 miesięcy. W sytuacji gdy firmy nie chcą kooperować, sąd FISA może wydać zarządzenie i zmusić je do wydania posiadanych informacji. Przysługuje im prawo do złożenia apelacji do instancji odwoławczej FISA lub Sądu Najwyższego[64].

Ostrzejsze wymagania są stosowane, gdy obiektem monitorowania jest podmiot amerykański za granicą lub gdy pozyskiwanie informacji ma miejsce na terenie USA. W tym wypadku nie wystarcza tylko poświadczenie Prokuratora Generalnego. Konieczne jest złożenie oświadczenia pod przysięgą przy składaniu wniosku do sądu FISA o prawdziwości zawartych w nim danych. Obejmują one ujawnienie tożsamości obiektu monitorowania, faktów wskazujących na zasadność, iż ta osoba przebywa za granicą lub jest agentem obcego państwa. Warto w tym miejscu podkreślić, że podejrzenia o agenturalne powiązania nie mogą być oparte na zarzutach związanych z I poprawką, czyli na głoszeniu na przykład poglądów sprzecznych z oficjalnymi, krytyce polityki USA itp.

Oprócz standardowych informacji przedkładanych sądowi wnioskodawcy w przypadku podmiotów amerykańskich muszą sprecyzować rodzaj monitorowanej aktywności i pozyskiwanych informacji oraz ich związek na przykład z działalnością terrorystyczną, sabotażową lub polityką zagraniczną USA. Są zobowiązani określić stosowane techniki, w tym konieczność przeszukania konkretnych pomieszczeń, bu-

[63] PL110-261, §403(b)(1), 122 Stat. 2474 (2008).

[64] 50 U.S.C. 1881a(h)(6), (i).

dynków lub budowli, a także wskazać na poprzednio wydane nakazy dotyczące danej osoby. W przypadku podmiotów amerykańskich nakaz monitorowania ich komunikacji nie może przekroczyć 90 dni. Władze w uzasadnionych przypadkach mogą występować o jego przedłużenie na kolejny okres. Natomiast w sytuacjach niecierpiących zwłoki mogą natychmiast uruchomić system inwigilacji i w ciągu 7 dni przedłożyć stosowne wnioski do sądu FISA o zatwierdzenie podjętych działań. Gdyby sąd odmówił zatwierdzenia wniosku – podobnie jak poprzednio – żadne informacje pozyskane w tym czasie nie mogą służyć jako dowód w postępowaniu sądowym lub innym oficjalnym, chyba że okaże się, iż obiekt nie był podmiotem amerykańskim.

Odrębnym zagadnieniem jest instytucja krajowych listów bezpieczeństwa (*National Security Letters*, dalej NSL), czyli urzędowych poleceń przekazania informacji, których znaczenie w ostatnich latach ogromnie wzrosło[65]. Pierwowzór tych poleceń znalazł się w ustawie *Right to Financial Privacy Act of 1978*[66]. Był to rodzaj wyjątku od zasady ochrony tajemnicy finansowej obywateli. Początkowo dotyczył więc instytucji finansowych, które po otrzymaniu poleceń miały obowiązek ujawnienia informacji o swoich klientach. Wiele z nich odmawiało, korzystając z prawnych możliwości, stąd Kongres pod naciskiem FBI znowelizował tę ustawę i wprowadził NSL, dzięki którym FBI mogło zażądać przekazania informacji, jeśli były one niezbędne w sprawach dotyczących bezpieczeństwa narodowego, nie tylko finansowych, ale również znajdujących się w posiadaniu firm telekomunikacyjnych oraz świadczących usługi elektroniczne, które jednocześnie miały zakazane ujawnienie tego faktu swoim klientom[67]. W ten sposób FBI mogła otrzymać informacje dotyczące obcych państw, ich przedstawicieli lub agentów. Warto zaznaczyć, iż początkowo nie było regulacji karnych w przypadku niezastosowania się do poleceń zawartych w NSL. W latach 90. XX w. Kongres rozszerzył możliwość korzystania przez FBI z tych poleceń w przypadku prowadzenia dochodzeń związanych z ujawnieniem tajemnic państwowych[68] oraz gdy niezbędne były informacje kredytowe[69].

Ustawa *USA Patriot Act of 2001* zmieniła zasady stosowania NSL, a w szczególności wprowadziła możliwość wystawiania ich nie tylko przez centralę FBI, jak to było dotychczas, ale także przez szefów 56 regionalnych biur (*special agent-in-charge*) i inne agencje federalne. Mogą oni je wydawać nie tylko w sprawach związanych z wywiadem, a więc obejmującymi obce państwa lub ich agentów. Obecnie wystarczy, ażeby żądanie ujawnienia informacji miało charakter relewantny do prowadzonego dochodzenia w sprawach związanych z terroryzmem lub szpiegostwem. Rozszerzono zakres podmiotów, od których można żądać ujawnienia informacji i włączono do nich szereg drobnych instytucji finansowych, jak np. kantory wymiany walut, biura udzielania szybkich pożyczek, komisy, sklepy złotnicze, a także dilerów samochodowych, kasyna gry i biura podróży.

---

[65] O ile w 2000 r. wydano ich 8500, to w 2005 r. aż 47 tys. – zob. Ch. Doyle, *National Security Letters in Foreign Intelligence Investigations*: *A Glimpse of the Legal Background and Recent Amendments*, CRS Report for Congress, Order Code RS 22406, Washington March 28, 2008, s. 7 i nast.

[66] PL 95-630, 92 Stat. 3697 (1978).

[67] *Electronic Communication Privacy Act of 1986* (ECPA), PL 99-508, 100 Stat. 1848 (1986).

[68] *National Security Act of 1947*, PL 80-235, 61 Stat. 496 (1947).

[69] *Fair Credit Reporting Act of 1970*, 15 U.S.C. 1681 et seq.

W celu przeciwdziałania ewentualnym nadużyciom na płaszczyźnie swobód obywatelskich Kongres wprowadził przepis, że NSL nie mogą być wydawane, gdy dochodzenia dotyczą wyłącznie spraw związanych z dobrami chronionymi przez I poprawkę, a więc wolnością słowa, zrzeszania się i religii.

Nadmierne stosowanie NSL po 2001 r.[70] spotkało się z krytyką opinii publicznej, która podnosiła, że proces ich wydawania nie podlega żadnej kontroli sądowej[71]. W podobny sposób wypowiedziały się sądy federalne, które rozstrzygały skargi na naruszenie postanowień IV i I poprawki do Konstytucji przez przepisy regulujące ich stosowanie[72]. W orzeczeniu *Doe* v. *Ashcroft* nowojorski sąd federalny uznał, że procedury wydawania NSL stanowią naruszenie postanowień IV poprawki, albowiem upoważniają do stosowania przeszukania bez nadzoru sądowego. W kwestii I poprawki ten sam sąd orzekł, iż wymogi zachowania bezwzględnej tajemnicy związane ze stosowaniem NSL naruszają dobra chronione tą poprawką oraz konstytucyjną zasadę podziału władz. Wprawdzie interes władz w walce z terroryzmem w celu zapewnienia bezpieczeństwa państwa jest przekonywający, ale procedury wystawiania tych poleceń były niewystarczające w świetle przepisów I poprawki.

W związku z tym Kongres nieco zmodyfikował zasady wydawania krajowych listów bezpieczeństwa NSL, wprowadzając przede wszystkim nadzór sądowy, który polega na przyznaniu podmiotowi zobowiązanemu do ujawnienia informacji prawa do dokonania przez sąd federalny oceny niezbędności ich zakresu oraz granic nakazu milczenia[73]. Ponadto wprowadzono kontrolę Kongresu, zobowiązując Inspektora Generalnego Departamentu Sprawiedliwości do corocznego przedkładania sprawozdań co do liczby wydawanych NSL.

Z jego pierwszych dwóch raportów wynika nie tylko ogromny wzrost ich ilości, z czego 75% dotyczy aktywności kontrwywiadowczej, ale także wzrastający odsetek podmiotów amerykańskich, o których informacji żądano[74]. Dzięki wzmożonej kontroli wykryto 739 przypadków omijania przez FBI wymagań narzuconych przez przepisy, zwłaszcza w odniesieniu do niezwłocznych poleceń (*exigent letters*)[75]. Dzięki temu skorygowano procedury w ramach FBI, eliminując zaobserwowane naruszenia[76].

Podsumowując, trzeba stwierdzić, iż system kontroli inwigilacji dla celów ochrony bezpieczeństwa narodowego Stanów Zjednoczonych podlega nieustannej ewolucji. Zaobserwowane tendencje wskazują z jednej strony na uwzględnianie w zmienianych regulacjach potrzeb służb specjalnych, zwłaszcza w płaszczyźnie uelastycznienia ich działalności w celu zapewnienia jak największej skuteczności w walce z zagrożeniami,

---

[70] O ile w 2000 r. wydano 8,5 tys., to w 2005 r. odnotowano pięciokrotny wzrost. Wydano przeszło 47 tys. NSL.

[71] Zob. D. Stout, *FBI Admits Mistakes in Use of Security Act*, „New York Times" 10.03.2007, s. A10. Administracja prezydenta G. W. Busha starała się otrzymać zgodę na wystawianie NSL przez CIA i Departament Obrony na terenie USA bez pośrednictwa FBI lub Departmanetu Sprawiedliwości, zob. E. Lichtblau, J. Risen, *Broad Domestic Role Asked for CIA and the Pentagon,* „New York Times" 23.03.2003, s. A1.

[72] *Doe v. Ashcroft*, 334 F.Supp.2d. 471 (S.D.N.Y. 2004), *vac'd and remanded,* 449 F.3d 415 (2d Cir. 2006), *after remanded,* 500 Supp.2d 379 (S.D.N.Y. 2007); *Doe v. Gonzales*, 386 F.Supp.2d 66 (D.Conn.2005), *dis'd as moot* 449 F.3d 415 (2d Cir. 2006).

[73] *USA Patriot Reauthorization Act of 2006,* PL 109-177 i 178 (2006).

[74] W 2003 r. wynosił on 39%, zaś w 2006 r. wzrósł do ponad 57%.

[75] Zob. Ch. Doyle, *National Security Letters in Foreign Intelligence Investigations*: *Legal Backgrounds and Recent Amendments*, CRS Report for Congress, Order Code 33320, Washington, March 8, 2008, s. 17 i nast.

[76] *Ibidem,* s. 19.

głównie o charakterze terrorystycznym. Z drugiej strony obserwuje się rozszerzający zakres kontroli nad służbami nie tylko ze strony odpowiednich branżowych komisji Kongresu, lecz również sądownictwa, i to nie tylko tego specjalistycznego w postaci sądu FISA, ale zwykłych sądów federalnych.