Zbigniew Nowak*

Polska w sieci Echelon

Streszczenie

Aktualne dążenia społeczności światowych, państw, koncernów do uzyskiwania jak najszerszej gamy informacji nie byłyby niczym dziwnym, gdyby działania te nie pozostawały poza obowiązującymi regulacjami prawnymi. Informacja to siła. Przyjmuje się tu każdą wygodną dla odbiorców argumentację. Może to być wszechobecne zagrożenie terrorystyczne, mogą to być przestępstwa korupcyjne, ale najczęściej cel ekonomiczny, szpiegostwo przemysłowe. Działania takie godzą w przepisy prawa międzynarodowego czy krajowego, a mimo to organy państwowe udają, że nie wiedzą i nie uczestniczą w procesie inwigilacji własnych społeczeństw. Czy zwykły obywatel, który nie ma nic wspólnego z terroryzmem czy kontraktami na dostawy sprzętu wojskowego, może mieć dziś zagwarantowane jakiekolwiek prawa, prawo do prywatności, jakiejkolwiek tajemnicy korespondencji? Do kogo ma się zwrócić, jeżeli będzie podejrzewał, że zostały naruszone jego swobody konstytucyjne? Przedmiotem artykułu jest działalność budzącej kontrowersje globalnej sieci inwigilacji komunikacji Echelon, widziana z punktu widzenia polskich regulacji prawnych.

Słowa kluczowe: Echelon, inwigilacja, tajemnica, komunikacja, korespondencja, wywiad, terroryzm, cyberbezpieczeństwo, ochrona dóbr, szpiegostwo

* Ppłk dr Zbigniew Nowak, Dowództwo Generalne Rodzajów Sił Zbrojnych, Oddział Prawny, e-mail: zb.nowak@ron.mil.pl.

Wstęp

„Informacja to potęga, nigdy nie sprawiaj wrażenia kogoś, komu potrzeba więcej informacji”[1].

Nieco ponad 400 lat temu angielski filozof Francis Bacon spopularyzował wśród ludzi łacińską sentencję: „scientia potentia est” (wiedza to potęga)[2]. Paremia ta jest niewątpliwie nadal wyjątkowo istotna i prawdziwa. Jednakże dziś światem w pierwszej kolejności rządzi informacja.

Informacja to potęga – to wiedza, władza i pieniądze. Klienci specjalnych serwisów giełdowych płacą najwięcej za wiadomości otrzymywane w czasie rzeczywistym. Bazy danych są cenne, ponieważ oferują dostęp do informacji przefiltrowanych. Wydawcy encyklopedii elektronicznych zarabiają na eliminacji nośnika papierowego. To tylko nieliczne z wielu sposobów zarabiania pieniędzy na handlu informacją[3]. Szeroko pojęta informacja to domena transsektorowego bezpieczeństwa informacyjnego, jednego z podstawowych wyznaczników bezpieczeństwa narodowego oraz międzynarodowego[4].

Dziś chyba już niewielu, poza konstytucjonalistami[5] i osobami skupionymi wokół organizacji zajmujących się ochroną praw obywatelskich, dziwią coraz bardziej wymyślne metody kolejnych państw prowadzące do uzyskiwania powszechnego, pełnego dostępu do wszelkich informacji. Proces pozyskiwania informacji nie dotyczy już nawet pojedynczych państw. Państwa łączą się umowami, żeby jeszcze pełniej zapewniać sobie dostęp do tego, co je interesuje.

W myśl powszechnie rozumianego bezpieczeństwa, jak się wydaje, nic nie powinno stać temu procesowi na przeszkodzie, nawet obostrzenia konstytucyjne w zakresie tajemnicy komunikowania się, korespondencji czy utrzymania innych praw i wolności obywatelskich, np. prawa do ochrony własnych danych osobowych. Dążenia te dotyczą coraz większej grupy państw, nie tylko Polski, dla której chociażby w myśl artykułu 49 Konstytucji RP z 1997 roku:

1 C. Brayfield, *Boski Andy i przyjaciele*, Warszawa 2006.
2 F. Bacon, *Meditationes sacrae*, https://link.springer.com/article/10.1023.
3 C. Shapiro, H.R. Varian, *Potęga informacji. Strategiczny przewodnik po gospodarce sieciowej*, Warszawa 2008.
4 K. Derlatka, *Potęga informacji*, „Interdyscyplinarne Studia Społeczne” 2016, nr 1.
5 Między innymi w 2001 r. Echelon był przedmiotem dochodzenia Unii Europejskiej – *Raport European Parliament Report on the existence of a global system for the interception of private and commercial communications (ECHELON interceptions system) (2001/2098(INI))*, www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5--2001-0264+0+DOC+PDF+V0//EN&language=EN.

„Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony”[6].

Dziś ta konstytucyjna gwarancja przestaje mieć fundamentalne znaczenie. W świecie globalnej inwigilacji, w tym inwigilacji komunikacji[7], nie ma możliwości ukrycia się przed kamerami lub systemami podsłuchu. W społeczeństwie budzi to niepewność wynikającą z nadmiernej kontroli życia osobistego przez służby bezpieczeństwa i porządku publicznego. Argumentacją przeważającą, argumentacją na „tak” są różnego rodzaju strategiczne działania ochronne czy działania społeczne w sferze bezpieczeństwa[8], przeciwdziałające zagrożeniom narodowym czy planowanym zamachom terrorystycznym.

Jeszcze w 2015 roku amerykańska administracja (zresztą tak w praktyce jest do dziś), nawet wbrew stanowisku innych państwa, sygnatariuszy tej samej umowy – Australii czy Nowej Zelandii[9], zaprzeczała istnieniu ogólnoświatowej sieci inwigilacyjnej Echelon, pomimo że Narodowa Agencja Bezpieczeństwa Stanów Zjednoczonych (NSA; zwana przekornie „No Such Agency”), budując swoją pozycję, co najmniej od kilkunastu lat czerpała z dobrodziejstw otrzymywanych ogólnoświatowych, wybranych informacji, które pozyskane w krótkim czasie zyskiwały status informacji niedostępnych, prawnie chronionych.

To Echelon namierzył telefon satelitarny Osamy bin Ladena podczas operacji „Tora Bora” pod koniec 2001 roku, zmuszając lidera Al-Kaidy do przejścia na tradycyjne systemy łączności. To on wychwycił rozmowy osobistego kuriera bin Ladena, dzięki czemu CIA udało się ustalić kryjówkę terrorysty, a prezydent Obama mógł wydać rozkaz fizycznego wyeliminowani szefa Al-Kaidy.

To Echelon jeszcze pod koniec lat 90. ubiegłego wieku podsłuchiwał księżną Dianę tylko dlatego, że w toczonych przez nią rozmowach telefonicznych z członkami rodziny królewskiej w sprawie pomocy humanitarnej dla ludności państw byłej Jugosławii używano słów „miny”, „pola minowe” czy „bomby”[10].

W ostatnich latach stało się również jasne, że amerykańsko-brytyjski wytwór – Echelon – działa i podsłuchuje nawet najważniejszych polityków,

6 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483, z późn. zm.

7 Inwigilacja – tajna obserwacja kogoś lub tajny nadzór nad kimś. *Inwigilacja*, [w:] *Słownik języka polskiego*, https://sjp.pwn.pl/sjp/inwigilacja;2561945.html.

8 Por. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2014.

9 S.M. Scholl, *How to detect infiltrators and observe covert police misconduct: The crimes of cellular on patrol*, 2010.

10 Por. https://www.gazetaprawna.pl/wiadomosci/artykuly/515894.

wystarczy tu przypomnieć ujawnienie podsłuchiwania rozmów Angeli Merkel[11].

Działania takie są zauważalne przez społeczeństwa, są pojmowane w kontekście łamania praw obywatelskich. Intrygującym wydarzeniem był protest 21 października 1999 roku – „Jam Echelon Day", kiedy to przeciwnicy systemu Echelon z całego świata starali się zablokować jego działanie poprzez wysyłanie e-mail z co najmniej 50 słowami kluczowymi. Nie było ważne, jaki był kontekst pisemnej treści, ważne było, żeby były to słowa klucza, które wyłapie system Echelon: „bunt", „bomba" czy „zamach"[12].

Przedmiotem badań tego artykułu jest zwięzła analiza funkcjonowania międzynarodowego projektu – sieci inwigilacyjnej, wywiadowczej Echelon, przedstawienie historii jej powstania i zasad działania, tj. technologii sieci. Wskazanie roli, jaką w procesie pozyskiwania określonych kategorii informacji odgrywają – potencjalnie, gdyż oficjalnie nikt tego nie przyzna – organy Rzeczypospolitej Polskiej.

To także pytanie o współczesne, realne cele działania Echelon – czy są nimi bezpieczeństwo narodowe lub międzynarodowe czy też dostęp do informacji ma tu inny – może ekonomiczny, a może stricte polityczny mianownik. Funkcjonowanie Echelon można rozpatrywać w kategoriach bliżej niezidentyfikowanych czynności operacyjno-rozpoznawczych prowadzonych bez widocznych podstaw prawnych przez organy nieposiadające jakichkolwiek uprawnień ustawowych do działania w myśl polskiego prawa. Czy Rzeczpospolita Polska – o ile w Echelon funkcjonuje – czerpie przy tym skutecznie i efektywnie z dobrodziejstwa systemu czy też jest jedynie narzędziem amerykańskiego NSA?

Powstanie i zasady działania sieci Echelon

„W końcu w życiu jest tak, że nie zawsze właściwe jest to, co właściwe, tylko to, co jest właściwe według tego, kto decyduje"[13].

Powstanie Echelon, pierwotnie tzw. niejawnej – militarnej – nazwy kodowej rządu[14], zdecydowanie wyprzedza oficjalne i jawne standardy Organizacji

11 Por. https://www.gaia.com/article/oldest-conspiracies-proven-true-project-echelon. Por także http://www.psz.pl/95-unia-europejska/parlament-europejski-broni-snowdena-przed-ekstradycja-wycofac-zarzuty-wobec-niego.

12 Por. http://www.echelon.wiretapped.net.

13 J. Jonason, *Stulatek, który wyskoczył przez okno i zniknął*, Warszawa 2011.

14 G. Webster, *History of the British Inter-Services Security Board and the Allocation of Code-Names in the Second World War*, https://www.tandfonline.com/doi/abs.

Traktatu Północnoatlantyckiego w zakresie ogólnego jej funkcjonowania w środowisku informacyjnym. Echelon i NATO to oczywiście dwa odrębne światy, choć jako sojusze budowane generalnie w oparciu o podobne założenia – walkę z terroryzmem, kreowanie właściwego przekazu w mediach, cyberobronę czy przeciwdziałanie dezinformacji.

Uznaje się, że u podstaw powstania sieci Echelon w 1971 roku[15] stały dwa wcześniejsze porozumienia – BRUSA (British–U.S. Communication Intelligence Agreement; zawarty w 1943 roku między rządami brytyjskim i amerykańskim w celu ułatwienia współpracy w wymianie informacji wywiadowczych), sformalizowane następnie w treści porozumienia UKUSA (United Kingdom–United States of America Agreement) z marca 1946 roku[16].

To właśnie to drugie porozumienie, rozszerzane o udział kolejnych państw (w latach 1952–1955 przystąpiły: Norwegia, Dania oraz Niemiecka Republika Demokratyczna) przekształcono finalnie w porozumienie krajów anglojęzycznych – tzw. AUS/CAN/NZ/ UK/US Eyes Only, czyli porozumienie Five Eyes[17].

Pierwotnym celem powstałej stricte wojskowej sieci było monitorowanie telemetrii radzieckiej broni, obrony przeciwlotniczej i innych radarów z lat 70. ubiegłego wieku[18], transmisji naziemnych satelitów i naziemnej komunikacji mikrofalowej. Położenie państw członkowskich zapewniało wtedy i zapewnia teraz pokrycie praktycznie całej kuli ziemskiej.

W pewnym – zadaniowym, wojskowym – sensie pojęciu Echelon odpowiada militarne wyjaśnienie terminologiczne zaczerpnięte z *Cambrige Dictionary* (https://dictionary.cambridge.org/pl/dictionary/english/echelon): „Echelon – a special arrangement of soldiers, aircraft, or ships".

15 Por. http://news.bbc.co.uk 29.01.2001. „W 1966 r. pierwsze satelity Intelsat pojawiły się na orbicie, a zaraz po tym Agencja Bezpieczeństwa Narodowego (NSA) i Centrala Łączności Rządowej (GCHQ) postanowiły rozbudować swoje naziemne stacje wywiadowcze. W 1971 r. GCHQ rozpoczął działalność w tajnej nowej stacji w Morwenstow, niedaleko Bude w Kornwalii, w Anglii. Przechwycił komunikację satelitarną nad Oceanem Atlantyckim i Indyjskim. Aby przechwycić komunikację regionalną Pacyfiku, NSA zbudowała drugą stację w Yakima, niedaleko Seattle, w północno-zachodniej części Stanów Zjednoczonych".

16 Por. http://www.nationalarchives.gov.uk/ukusa/. Podpisane przez przedstawicieli The London Signals Intelligence Board i amerykańskiego odpowiednika.
W 2010 r. została oficjalnie odtajniona treść porozumienia UKUSA, którą podano do informacji publicznej i można ją znaleźć na stronach archiwów państwowych oraz NSA. Por. www.time.com/time/nation/artic-le/0,8599,2000262,00.html.

17 W ramach porozumienia ustalono zasady współpracy marynarek wojennych tych państw na poziomie dowodzenia, kontroli, komunikacji i komputerów (z ang. C4 – Command, Control, Communications and Computers).

18 W 1966 r. pierwsze satelity Intelsat pojawiły się na orbicie, a zaraz po tym NSA i GCHQ postanowiły rozbudować swoje naziemne stacje wywiadowcze.

Dziś Echelon jest globalną siecią wywiadu elektronicznego, programem nadzoru – programem inwigilacji komunikacji, siecią gromadzenia, przechwytywania komunikacji satelitarnej oraz analizowania danych wywiadowczych. To system, który analizuje rozmowy telefoniczne, wiadomości tekstowe, komunikację przez Internet, e-maile, dane z urządzeń telekomunikacyjnych, informatycznych (np. radarów, satelitów rozpoznawczych, satelitów telekomunikacyjnych), faksy, telefaksy, transfery plików, dane gromadzone w prywatnych komputerach.

W praktyce są to wszystkie niezaszyfrowane kanały komunikacji dostępne dziś na świecie. Potężne centra komputerowe analizują pozyskane dane i na podstawie wyłapanych słów kluczowych oraz ich powiązań kontekstowych wskazują na te, które potencjalnie mogą zawierać informacje o zagrożeniu narodowym, planowanych zamachach, akcjach terrorystycznych, morderstwach[19]. To system globalny, który de facto może zbierać informacje o każdym, o kim chce[20]. Echelon analizuje około 3 mld komunikatów na dobę, co oznacza, że może kontrolować 90% światowego ruchu internetowego.

W skład Echelonu ma wchodzić około 10 stacji nasłuchowych rozsianych po całym świecie. Do tego dochodzi sześć satelitów telekomunikacyjnych i kilka satelitów szpiegowskich[21]. Sygnały telefoniczne wychodzące z Europy i Bliskiego Wschodu odbijają się od satelity i trafiają do zbiorczej anteny kompanii telefonicznej AT&T w Etam (Zachodnia Virginia) na wschodnim wybrzeżu Stanów Zjednoczonych. Podobną funkcję spełnia stacja RAF w Menwith Hill w północnej Anglii. Z kolei region Pacyfiku obsługuje stacja w Waihopai w Nowej Zelandii[22]. Rejonów Azji nasłuchuje skupisko anten satelitarnych należących do kompanii Verestar Inc. Największa stacja nasłuchowa znajduje

19 Zebrane lokalnie informacje z całego świata przesyłane są do centrali w Fort Meade, głównej siedziby NSA. Superkomputery dokonują analizy materiału dostosowanej do regionu, językowej, tworzą słownik haseł i stanu materiału, ustalają rodzaj kompresji, algorytm szyfrowania.

20 Por. https://tech.wp.pl/echelon-system-ktory-czyta-twoje-maile-sms-y-i-slucha-twoich-rozmow. „Kiedy komputery wskażą wiadomość/rozmowę, która zawierała połączenie odpowiednich słów, ta trafia na biurko analityka, który dokonuje ostatecznej klasyfikacji. Cały problem polega na tym, że system nie jest przeznaczony do inwigilowania i podsłuchiwania jedynie grup przestępczych lub też osób w jakikolwiek sposób podejrzanych o złe intencje i zamiary".

21 Obecnie globalna komunikacja satelitarna jest świadczona przez satelity obsługiwane przez INTELSAT, INMARSAT i INTERSPUTNIK. Podzielono ziemię na trzy strefy (obszar Oceanu Indyjskiego, Pacyfiku i Atlantyku), wprowadzone w momencie wysłania pierwszych generacji satelitów.

22 Por. https://tech.wp.pl/echelon-system-ktory-czyta-twoje-maile-sms-y-i-slucha-twoich-rozmow.

się w północnej Anglii, niedaleko miejscowości Harrogate. Oficjalnie leży na terenie bazy wojskowej Wielkiej Brytanii, ale część terenu jest dzierżawiona stronie amerykańskiej. Dzięki niej można podobno szpiegować wszystkich w UE[23].

Większość raportów na temat Echelon koncentruje się na przechwytywaniu satelitów. W tym celu wykorzystuje naziemne anteny radiowe, które przechwytują transmisje satelitarne, a także ma własną flotę satelitów, które przenikają do transmisji między miastami[24].

Sieć wywiadowcza sięga również do kabli podmorskich. Przykładami mogą być: Azja Południowo-Wschodnia, Bliski Wschód, Europa Zachodnia – łączy je morski optyczny kabel telekomunikacyjny, ukończony pod koniec 2000 roku. Jest on prowadzony przez France Telecom oraz China Telecom i jest zarządzany przez Singtel, operatora telekomunikacyjnego będącego własnością rządu Singapuru. Jest jednym z najważniejszych kabli podmorskich, do których dostęp ma Five Eyes[25].

23 Por. https://www.tygodnikprzeglad.pl/szpieg-ktory-podsluchuje-kazdego-nas/.

24 „W 2006 r. 99% światowego ruchu głosowego i transmisji danych zostało przeniesione na światłowód". Por. https://www.cnet.com/news/nsa-eavesdropping-how-it-might-work/. „Kable zastąpiły satelity jako główny sposób przesyłania danych pomiędzy kontynentami. Jeden kabel może przenosić dziesiątki tysięcy rozmów telefonicznych jednocześnie. Echelon ma również wiele witryn na całym świecie, które korzystają z komunikacji prowadzonej za pośrednictwem przewodów. Dane przesyłane w sieciach światłowodowych nie są bezpieczne. Istnieją podejrzenia, że NSA opracowała urządzenia, które mogą wykorzystać optyczne kable podwodne".

25 D. Philip, *Australian spies in global deal to tap undersea cables*, The Sydney Morning Herald, Retrieved, 29.08.2013 Por.: https://www.smh.com.au/technology/. „TAT-14 to kabel telekomunikacyjny łączący Europę ze Stanami Zjednoczonymi. Dzięki kablom telekomunikacyjnym uzyskano dostęp do większości Internetu i połączeń telefonicznych w Europie, Stanach Zjednoczonych i innych częściach świata".

Por. też https://www.gazetaprawna.pl/wiadomosci/artykuly/515894,jak-podsluchuje-nas-ameryka-czy-legendarna-siec-inwigilujaca-echelon-naprawde-istnieje.htm. „Od czasu zastosowania światłowodów większość rozmów telefonicznych obiega świat tą właśnie drogą – kable ułożone na dnach oceanów łączą wszystkie kontynenty. Te obsługiwane przez obce państwa są rutynowo podsłuchiwane metodą indukcji elektromagnetycznej. Do tego rodzaju inwigilacji przystosowany jest m.in. okręt podwodny USS „Jimmy Carter", mogący przymocować urządzenie podsłuchowe wielkości pontonu do podwodnego kabla. Tę metodę Rosjanie odkryli w 1981 r. na Morzu Ochockim – przez dekadę NSA podsłuchiwało komunikację sowieckiej Floty Pacyfiku przy pomocy 6-metrowego ucha przyssanego do kabla biegnącego po dnie morza wzdłuż Wysp Kurylskich. Urządzenie, zainstalowane tam przez specjalnie przerobioną amerykańską łódź podwodną USS „Halibut", wymagało zmiany baterii i wymiany taśmy z nagraniem co cztery tygodnie. Zebrane informacje trafiały do centrali NSA w Fort Meade w stanie Maryland […]".

Echelon oprócz sieci anten radiowych, flot satelitów i podsłuchów wykorzystuje rozległą sieć komputerową do przeglądania ogromnej puli danych, które nieustannie gromadzi. System ten wyszukuje kluczowe słowa, frazy, adresy i nazwiska. Twierdzi się również, że system obejmuje rozpoznawanie głosu, a nawet tłumaczenia językowe.

Systemem Echelon zarządza powstała w 1952 roku amerykańska służba wywiadu National Security Agency[26]. Stany Zjednoczone mają również inne, pochodne organy ścigania, ale o zdecydowanie mniejszym budżecie i przyjmowanej liczbie personelu (NSA to ok. 40 tys. zatrudnionych osób; takim przykładem jest Central Intelligence Agency – CIA, Centralna Agencja Wywiadowcza, prowadząca działalność wywiadowczą)[27].

Każde państwo członkowskie Five Eyes posiada powiązaną z siecią Echelon instytucję bądź jednostkę wywiadowczą. W Wielkiej Brytanii od 1946 roku jest to Government Communications Headquarters (GCHQ)[28], w Kanadzie funkcjonuje Communications Security Establishment (CSEC)[29], w Australii – Australian Signals Directorate (ASD)[30], a w Nowej Zelandii – Government Communications Security Bureau (GCSB)[31].

Najważniejszym państwem oprócz Stanów Zjednoczonych jest Wielka Brytania, gdzie zadania monitoringu wykonuje agencja Government Communications Headquarters. Nadzór nad łącznością elektroniczną w Wielkiej Brytanii jest kontrolowany przepisami prawnymi wydanymi w brytyjskim parlamencie, w szczególności dostęp do treści prywatnych wiadomości, tj. przechwytywanie wiadomości takich, jak e-mail lub telefon, musi być autoryzowany przez nakaz podpisany przez sekretarza stanu[32].

Na współpracę z NSA zdecydowała się również Communications Security Establishment, rządowa agencja wywiadowcza Kanady. Oferuje ona NSA

26 Por. https://www.nsa.gov.

27 G.M. Gellman Barton, *US spy network's successes, failures and objectives detailed in black budget summary*, „The Washington Post". Por. https://cyber-peace.org/wpcontent/uploads/2013/06/%E2%80%98Black-budget%-summary-details-U.S.pdf. „Według założeń amerykańskiego budżetu z 2013 roku CIA posiadało środki na realizację pięciu zadań, gdzie największym priorytetem były inicjatywy zwalczające terroryzm, ale także ochrona przed rozprzestrzenianiem się broni jądrowej i broni masowego rażenia, ostrzeganie, informowanie przywódców amerykańskich, kontrwywiad i cyberprzestępczość".

28 Por. https://www.gchq.gov.uk/.

29 Por. https://www.cse-cst.gc.ca/en.

30 Por. https://www.asd.gov.au/.

31 Por. https://www.gcsb.govt.nz/.

32 *Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme*, 17.07.2013, s. 1–3.

zaawansowane gromadzenie, przetwarzanie i analizy. W imieniu NSA, CSEC otworzył tajne obiekty nadzoru w 20 krajach na całym świecie.

Z innymi członkami społeczności ściśle współpracuje też Australian Signals Directorate. Australijskie ambasady są potajemnie wykorzystywane do przechwytywania połączeń telefonicznych i danych w całej Azji. Government Communications Security Bureau to departament bezpieczeństwa Nowej Zelandii, którego zadaniem jest wywiad zagraniczny, zapewnienie bezpieczeństwa cybernetycznego i pomoc innym agencjom rządowym Nowej Zelandii[33]. Witryna The Intercept i The New Zealand Herald 5 marca 2015 roku ujawniły, że GCSB szpiegowało południowo-wschodnich sąsiadów Nowej Zelandii. Program masowej inwigilacji GCSB został skrytykowany przez partie opozycyjne[34].

To wycinek działalności głównych instytucji zarządzających siecią wywiadowczą. Sieć organizacyjna Echelon jest zdecydowanie bardziej rozległa, gdyż oprócz państw założycielskich, także wiele innych krajów angażuje się w gromadzenie danych wywiadowczych niezbędnych do jej funkcjonowania. Pomiędzy państwami ramowymi a Danią, Izraelem, Japonią, Libią, Holandią, Francją[35], Norwegią, Singapurem, Hiszpanią, Szwajcarią czy Szwecją następuje wymiana informacji, która np. umożliwiła dostęp do telekomunikacyjnych kabli podwodnych w Bałtyku.

W ramach globalnej sieci monitoringu Echelon największy punkt odsłuchowy poza Wielką Brytanią i Stanami Zjednoczonymi znajduje się w Bawarii[36]. Niemcy uzyskali dostęp do systemu wywiadowczego NSA po podpisaniu porozumienia P6, obsługiwanego wspólnie przez CIA, BfV (Bundesamt für Verfassungsschutz) i BND (Bundesnachrichtendienst). To ogromna baza zawierająca dane takie, jak: zdjęcia, numery tablic rejestracyjnych, historie wyszukiwania w Internecie i telefony, została opracowana w celu lepszego zrozumienia relacji społecznych dżihadystów, terrorystów[37]. W Niemczech istnieje również baza wojskowa Dagger Complex obsługiwana przez amerykańską armię. W bazie można przetwarzać, przechowywać i deszyfrować miliony danych.

33 Por. https://www.gcsb.govt.nz/our-work/.

34 Por. https://www.nzherald.co.nz/nz/news.

35 Directorate General for External Security (DGSE, Dyrekcja Generalna ds. Bezpieczeństwa Zewnętrznego) w 2001 r. podpisała z NSA memorandum dotyczące wymiany danych, które ułatwiło przekazywanie NSA danych dotyczących milionów danych z DGSE. Por. http://www.lemonde.fr/international/article/2013.

36 R. Wobst, *Cryptology unlocked*, Wiley 2007, s. 5.

37 Por. https://www.spiegel.de/international/germany/cia-worked-with-bnd-and-bfv-in-neuss-on-secret-project-a-921254.html.

W zakresie funkcjonowania Echelon istnieje również współpraca handlowa – współpracuje z Orange S.A czy Vodafone, która przyznała brytyjskiej agencji wywiadowczej GCHQ nieograniczony dostęp do swojej sieci podmorskich kabli. Istotny udział w przetwarzaniu danych miała udział firma Microsoft, która pomogła NSA w obchodzeniu zabezpieczeń szyfrowania oprogramowania. Pozwoliło to rządowi federalnemu np. monitorować czaty internetowe w portalu Outlook.com. W 2013 roku również Skype współpracował z agencjami wywiadowczymi, żeby umożliwić zbieranie rozmów wideo i audio[38].

Szczególną rolę w gromadzeniu danych odgrywa największa amerykańska sieć telefonii komórkowej AT&T[39]. Swego czasu „The New York Times" ujawnił, że CIA wypłaca AT&T ponad 10 mln dolarów rocznie za pomoc w działaniach antyterrorystycznych, wykorzystując jej ogromną bazę danych telefonicznych, która obejmuje rozmowy międzynarodowe Amerykanów (Verizon i AT&T to dwie największe kompanie telekomunikacyjne w Ameryce i jedne z największych na świecie – łącznie obsługujące niemal 0,5 mld abonentów)[40].

Obecnie zasięg sieci Echelon jest – jak się powszechnie wydaje – już nieograniczony i jest niemożliwe, żeby jakakolwiek potrzebna informacja nie została zarejestrowana[41].

Niejawność systemu – przypadek Edwarda Snowdena

„Celem władzy jest władza"[42].

Istnienie porozumienia Five Eyes i samego systemu Echelon przez lata było informacją chronioną. Jak wskazano, pierwotnym uzasadnieniem powstania Echelonu była konfrontacja ze Związkiem Radzieckim i jego sojusznikami

38 Por. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.
Por. także https://www.svd.se/sverige-deltog-i-nsa-overvakning.
39 S. Kleinfield, *The biggest company on earth a profile of AT&T*, New York 1981, s. 84, 135, 174.
40 Por. http://www.zdnet.com/zdtv/cybercrime/chaostheory/story/.
41 Por. https://tech.wp.pl/echelon-system-ktory-czyta-twoje-maile-sms-y-i-slucha-twoich-rozmow. Sygnały telefoniczne wychodzące z Europy i Bliskiego Wschodu odbijają się od satelity i trafiają do zbiorczej anteny kompanii telefonicznej AT&T w Etam (Zachodnia Virginia) na wschodnim wybrzeżu Stanów Zjednoczonych. Podobną funkcję spełnia stacja RAF w Menwith Hill w północnej Anglii. Z kolei region Pacyfiku obsługuje stacja w Waihopai w Nowej Zelandii. Rejonów Azji nasłuchuje skupisko anten satelitarnych należących do kompanii Verestar Inc.
42 G. Orwell, *Rok 1984*, Warszawa 1988.

w czasach zimnej wojny ubiegłego wieku. W 1991 roku amerykańskie służby wywiadowcze miały przedłożyć nowy program działania po rozpadzie bloku wschodniego, który uwzględniał zmienioną sytuację geopolityczną. Głównym zadaniem amerykańskich służb specjalnych miał być odtąd wywiad gospodarczy[43].

Pierwszym źródłem mówiącym o istnieniu systemu Echelon były raporty Duncana Campbella przedstawione europejskiej komisji opiniującej zagadnienia naukowe i techniczne w 1997 i 1999 roku (Science and Technology Option Assessment – STOA, komisja, w której skład wchodzą członkowie Parlamentu Europejskiego zajmujący się wszelkimi sprawami związanymi z nauką i oceną technologii). Dokumenty te dały asumpt do utworzenia przez Parlament Europejski 5 lipca 2000 roku wspomnianej Tymczasowej Komisji w sprawie Systemu Echelon (The European Parliament's Temporary Committee on the Echelon Interception System), której raport stwierdzał, że zadania sieci wykraczają poza utrzymanie właściwego poziomu bezpieczeństwa narodowego państw członkowskich, będąc wykorzystywana do szpiegostwa ekonomicznego, faworyzującego firmy krajów członkowskich (głównie ze Stanów Zjednoczonych i Wielkiej Brytanii).

Mimo niekorzystnego stanowiska Unii Europejskiej z 2001 roku (5 września 2001 r. ukazał się specjalny raport, który zawierał m.in. sugestie, że część działań Echelonu powinno się zakwalifikować jako szpiegostwo przemysłowe) i miażdżącego, przygotowywanego raportu Parlamentu Europejskiego[44], w maju 2011 roku prezydent Obama w związku z działaniami terrorystycznymi

43 Potwierdziły to zarówno badania Unii Europejskiej, jak i wypowiedzi byłego dyrektora centrali wywiadu (DCI), tym samym szefa CIA, Roberta Jamesa Woolseya, w artykule z 17 marca 2000 r. w „Wall Street Journal".

44 Por. Rezolucja Parlamentu Europejskiego z dnia 4 lipca 2013 r. w sprawie programu inwigilacji amerykańskiej Agencji Bezpieczeństwa Narodowego, służb wywiadowczych w różnych państwach członkowskich i wpływu na prywatność obywateli UE (2013/2682(RSP)), Dz. Urz. UE 2016, C 075/14 (w zakresie działalności sieci, głównie systemu PRISM ukierunkowanego na pozyskiwanie danych z baz danych największych firm internetowych), w którym Parlament Europejski – mając na uwadze, że „[…] partnerstwo transatlantyckie między UE i USA musi opierać się na wzajemnym zaufaniu i szacunku, lojalnej i wzajemnej współpracy, poszanowaniu podstawowych praw i praworządności: 1) stanowczo potępia szpiegowanie przedstawicielstw UE, ponieważ – o ile dotychczas dostępne informacje potwierdzą się – oznaczałoby to poważne naruszenie Konwencji wiedeńskiej o stosunkach dyplomatycznych i mogłoby wpłynąć na stosunki transatlantyckie; 2) domaga się od władz USA natychmiastowych wyjaśnień w tej sprawie, czy wyraża poważne zaniepokojenie ujawnionymi informacjami dotyczącymi domniemanych programów inwigilacji realizowanych przez państwa członkowskie – zarówno z pomocą Agencji Bezpieczeństwa Narodowego USA, jak i jednostronnie; wzywa wszystkie państwa członkowskie do zbadania zgodności takich programów z prawem pierwotnym i wtórnym UE".

postanowił rozszerzyć ustawę Patriot Act, podpisaną przez George W. Bush'a po zamachach z 11 września 2001 roku. Ustawa zwiększyła od teraz możliwości globalnego nadzoru służbom bezpieczeństwa Stanów Zjednoczonych. W ten sposób do współpracy z ogólną siecią wywiadu elektronicznego przyczynił się Biały Dom w Stanach Zjednoczonych[45].

Zakres szpiegowania NSA, zagranicznego i krajowego, został ujawniony w czerwcu 2013 roku w brytyjskim dzienniku „Guardian"[46] przez byłego pracownika NSA Edwarda Snowdena. Stacja BBC poinformowała wtedy o „globalnej sieci szpiegowskiej" z wykorzystaniem Echelon jako jednego z elementów systemu. Przy okazji na NSA spadła krytyka państw sojuszu UKUSA, ponieważ na jaw wyszły informacje, że w ostatnich latach system Echelon był wykorzystywany przez Amerykanów już praktycznie na stałe w celach innych niż zapewnianie bezpieczeństwa, mając na myśli szpiegostwo przemysłowe oraz polityczne[47].

Dokumenty NSA uzyskane przez Snowdena potwierdziły oficjalnie istnienie omawianej tu tajnej sieci nadzoru szpiegującej komunikację satelitarną Echelon[48]. Snowden wskazał, że w praktyce NSA mogła inwigilować każdego człowieka – od zwykłych, przeciętnych ludzi na ulicy po urząd prezydenta. Teoretycznie szpiegowska agencja miała przeprowadzać wyłącznie rozpoznanie elektromagnetyczne dotyczące zagranicznych celów, zwane SIGINT, ale faktycznie wyglądało to tak, że zbierała metadane na temat milionów Amerykanów. Bez ich wiedzy oraz zgody rejestrowano rozmowy telefoniczne i e-maile. NSA oraz GCHQ robiły to, montując podsłuchy na podmorskich światłowodach obiegających świat. Dzięki temu Stany Zjednoczone i Wielka Brytania uzyskały dostęp do ogromnej ilości komunikacji międzyludzkiej.

Snowden ujawnił wiele tajnych spraw dotyczących pośrednio działalności Echelon, np. treść dyrektywy prezydenckiej z października 2012 roku[49]. Według dokumentu, prezydent Barack Obama nakazał urzędnikom sporządzić

45 George W. Bush skomentował ustawę: „To nowe prawo, które dziś podpisałem, umożliwi nadzór nad wszelką komunikacją używaną przez terrorystów, w tym przez maile, Internet i telefony komórkowe". Barack Obama do tej ustawy dodał zapis o niedozwolonym posłuchu, który śledzi cel nadzoru. Por. https://www.pbs.org/newshour/world/terrorism-july-dec01-bush_terrorismbill.

46 Por. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

47 *Globalny nasłuch*, „PC Format" 2008, nr 5, s. 4–5.

48 Por. https://www.rt.com/usa/311489-snowden-files-confirm-echelon/.

49 L. Harding, *Polowanie na Snowdena*, Warszawa 2014, s. 48 i nast.

listę zagranicznych obiektów, które mogą stać się celami potencjalnych cyberataków Stanów Zjednoczonych (OCEO – Offensive Cyber Effects Operations)[50].

Snowden ujawnił również informacje odnoszące się do szczegółów umów technicznych firm technologicznych z Doliny Krzemowej (Microsoft, Apple, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL), za pomocą których te zostały oficjalnymi partnerami NSA w działalności Echelon w ramach programu PRISM, zapewniającemu środowisku wywiadowczemu Stanów Zjednoczonych dostęp do ogromnych ilości danych cyfrowych uzyskanych z e-maili, postów na Facebooku i wiadomości z komunikatorów internetowych. Racjonalnym uzasadnieniem tego typu współpracy było to, że program jest potrzebnym narzędziem do głównie internetowego tropienia zagranicznych terrorystów zamieszkałych poza Stanami Zjednoczonymi. Do czasu, kiedy Snowden ujawnił istnienie programu PRISM, związało się z nim co najmniej dziewięć wymienionych firm – gigantów w dziedzinie technologii komputerowych[51].

Dalsze, istotne wskazania Snowdena – w kontekście Echelon – dotyczyły funkcjonowania tajnych programów pozyskiwania informacji również na bazie współpracy NSA z podmiotami gospodarczymi, jak TEMPORA czy BULLRUN[52].

50 Dyrektywa określała „[...] unikalne i niekonwencjonalne możliwości forsowania narodowych interesów Stanów Zjednoczonych na całym świecie z nieznacznym ostrzeżeniem lub bez ostrzeżenia wroga lub celu". Tematem Echelonu zainteresował się dziennikarz Mariusz Max Kolonko. W Internecie możemy znaleźć kilka filmów nakręconych przez niego, gdzie wypowiada się na temat sieci Echelon. W 2013 r. pojawiły się dwa nagrania z serii „Max Kolonko – Mówi jak jest" zatytułowane: „Tajemnice największej szpiegowskiej sieci świata" oraz „16.08.2013", w 2015 r. kolejne dostępne online nagranie „Życie na podsłuchu".

51 Oprócz Echelon funkcjonuje, będący przedmiotem raportu Parlamentu Europejskiej z 2013 r., system PRISM, który jest właśnie nastawiony na pozyskiwanie danych z baz danych największych firm internetowych.

52 L. Harding, op. cit., s. 88.

TEMPORA – program miał jeden szczególnie wrażliwy aspekt, a mianowicie sekretną rolę firm telekomunikacyjnych, które są właścicielami podmorskich przewodów światłowodowych lub nimi zarządzają. GCHQ nazwało te firmy partnerami przechwytującymi, a relacje z nimi utrzymują specjalnie powołane w tym celu zespoły do spraw dyskretnej współpracy. Wśród nich pojawiły się firmy przodujące na rynku światowym, które łącznie pomagały w przechwytywaniu większości kablowych łącz telefonicznych wychodzących na brzeg w Wielkiej Brytanii.

BULLRUN – fundusze przeznaczone na ten program wyniosły 254,9 mln dolarów w 2013 r., a agencja wydała ponad 800 mln dolarów na „uruchomienie programu SIGINT" od 2009 r. Raport donosił, że program BULLRUN aktywnie włączał amerykańskie i obce firmy IT w potajemne wprowadzanie zmian i pozyskiwanie wzorów ich produktów na rynki komercyjne. Z tych doniesień wynikało, że NSA wie, że zwyczajni obywatele nie mają pojęcia, że do ich codziennej, zaszyfrowanej korespondencji można się teraz włamywać, co oczywiście robili.

Rząd Stanów Zjednoczonych jednoznacznie uznał, że Snowden ukradł informacje niejawne, a jego decyzja miała poważne i niebezpieczne konsekwencje dla bezpieczeństwa Waszyngtonu[53]. Informatyk bronił się, że nie chciał zniszczyć podstawy amerykańskiej obrony narodowej, ale pokazać ich nadużycia i zapobiec zanikowi prywatności. Miał na celu zdemaskowanie pięciookiego potwora[54].

Dopóki Snowden nie pokazał pełnego potencjału NSA i innych rządowych agencji szpiegowskich, dopóty Echelon był w dużej mierze kolejnym kryptonimem w notatniku teoretyków światowego spisku[55].

Echelon a polskie prawo

„Balansujcie dopóki się da, a gdy się już nie da, podpalcie świat!"[56].

Zarówno nikłe prawdopodobieństwo funkcjonowania sieci powiązań terrorystycznych na terytorium RP, jak i relatywnie niewielkie znaczenie Rzeczpospolitej Polskiej dla gospodarki światowej nie są i tak kontrargumentami za wycofaniem się naszego kraju z wielce prawdopodobnej współpracy w ramach Echelon.

Oficjalnie – mimo wielu mniej lub bardziej sensacyjnych domniemań medialnych – nie udało się potwierdzić obecności elementów sieci Echelon w Polsce. Mówiono w tym kontekście i o bazie w Kiejkutach, i o terenach Jednostki Wojskowej 2305 GROM w Rembertowie czy przykabackich Pyrach[57].

Z danych ujawnionych przez Edwarda Snowdena wynika, że w 2012 roku podczas tylko jednego dnia system analizował od 2 do 4 mln komunikatów płynących z Polski[58]. Z innej partii ujawnionych dokumentów, a szczególnie z raportu „Dzielenie się zaszyfrowanymi informacjami z zagranicznymi partnerami

53 Por. https://www.rt.com/usa/311489-snowden-files-confirm-echelon/.

54 Por. https://www.theguardian.com/comment/snowden-spyware-five-eyed-monster-50000-networks-five-eyes-privacy.

55 Por. https://www.telegraph.co.uk/news/worldnews/europe/cyprus/British-military-base-inCyprus-used-to -spy-on-Middle-East.html.

56 Por. https://www.tvp.info/30576824/balansujcie-dopoki-sie-da-a-gdy-sie-juz-nie-da-podpalcie-swiat. Piłsudski mawiała: „Balansujcie dopóki się da, a gdy się już nie da, podpalcie świat!".

57 Por. https://gazetabaltycka.pl/promowane/sensacyjne-odkrycie-tajny-szpiegowski-system-echelon-dziala-na-terenie-polski.

58 Por. https://tech.wp.pl/echelon-system-ktory-czyta-twoje-maile-sms-y-i-slucha-twoich-rozmow.

o operacjach przeprowadzanych w sieciach komputerowych" wynika, że Polska należy do 20 krajów, które pozwoliły szpiegować swoich obywateli amerykańskim służbom specjalnym.

Amerykanie są praktyczni, dlatego ułatwili sobie robotę w branży szpiegowskiej i podzielili kraje, z którymi współpracują, na trzy kategorie.

W pierwszej tzw. kategorii A znalazły się: Australia, Kanada, Nowa Zelandia i Wielka Brytania. To właśnie w tych krajach funkcjonują największe centra nasłuchowe i anteny do globalnego przesyłania danych. Te kraje należą do najbardziej zaufanych.

Polska razem z Hiszpanami jest w grupie B. Łącznie znalazło się w niej 20 państw. Współpraca z tymi krajami miała być rozważana pod kątem utrzymania stałych korzyści dla Stanów Zjednoczonych – ujawnił Snowden[59].

W jakim celu Polska partycypuje w systemie Echelon, jakie realnie korzyści takie uczestnictwo przynosi Polsce czy sygnatariuszom porozumienia Five Eyes, w szczególności Stanom Zjednoczonym? W demokratycznych państwach przestrzeganie praw jednostki stanowi przecież fundament ustroju państw.

Oczywiście realnym argumentem jest jakaś forma współpracy międzynarodowej, funkcjonowania w sieci powiązań, mimo oczywistego naruszania podstawowych praw i obowiązków obywatela poprzez dorozumianą zgodę samego państwa na szpiegostwo elektroniczne (naruszenie tajemnicy korespondencji, innych wolności i swobód obywatelskich) dokonywane na jego obywatelach.

Na gruncie polskiego prawa praktyki Echelonu można rozpatrywać pod kątem deliktu cywilnego, ale także cyberprzestępczości regulowanej w konkretnych przepisach prawa karnego. Przyjmuje się, że w ramach cyberprzestępstwa można wyróżnić m.in. przestępstwa przeciwko poufności, integralności i dostępności danych i systemów informatycznych, tzw. przestępstwa stricte komputerowe oraz przestępstwa instrumentalnego wykorzystania elektronicznych sieci i systemów informatycznych do naruszania dóbr prawnych chronionych przez prawo karne[60].

Nawet bez zbyt dogłębnej analizy prawnokarnej wydaje się, że działalność sieci Echelon może godzić w rodzajowy przedmiot ochrony, jakim jest ochrona

59 Por. https://innpoland.pl/globalny-system-podsluchow-echelon-w-polsce-kto-i-jak-nas-sledzi.

60 M. Andreasik i in., *Orwell w realu, czyli o systemie Echelon z perspektywy polskiego prawa*, „Studia Prawnicze. Rozprawy i Materiały" 2014, nr 2, s. 68.

informacji, choćby na podstawie treści art. 267 k.k. z 1997 roku[61]. Może również dotyczyć innych czynów zabronionych typizowanych w kodeksie karnym, gdzie przedmiotem ochrony jest np. państwo jako podmiot prawa publicznego czy przestępstwa szpiegostwa z art. 130 k.k., w szczególności art. 130 par. 3[62].

W kontekście potencjalnych przykładów naruszeń obowiązującego polskiego prawa należy wymienić, oczywiście poza Konstytucją RP (oprócz wspominanego art. 49, również art. 51 – prawo do ochrony danych osobowych[63], oraz art. 31 – prawo do wolności osobistej[64]):

1) na gruncie prawa międzynarodowego:

a) art. 12 Powszechnej Deklaracji Praw Człowieka uchwalonej przez Zgromadzenie Ogólne ONZ 10 grudnia 1948 r. „[…] nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu",

b) art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych, który stanowi w ust. 1, że nikt „[...] nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję"[65],

c) art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności również opowiedział się za bezwzględnym obowiązkiem poszanowania życia prywatnego i rodzinnego, w tym także tajemnicy korespondencji[66],

d) art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej (Zakres i wykładnia praw i zasad) o treści: „Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne

61 Por. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j., Dz.U. 2019, poz. 1950, z późn. zm., art. 267, par. 1–5.

62 Ibidem, art. 130.

63 Konstytucji RP…, art. 51, ust. 1–5.

64 Ibidem, art. 31, ust. 1–3.

65 Dz.U. 1977, nr 38, poz. 177.

66 „Art. 8 ust. 1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. 2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób".

i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób”[67];

2) na gruncie prawa cywilnego:

a) art. 23 kodeksu cywilnego[68] oraz art. 24 par. 1 kc: „Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach”,

b) art. 82 prawa autorskiego[69]: „Jeżeli osoba, do której korespondencja jest skierowana, nie wyraziła innej woli, rozpowszechnianie korespondencji, w okresie dwudziestu lat od jej śmierci, wymaga zezwolenia małżonka, a w jego braku kolejno zstępnych, rodziców lub rodzeństwa”. Ponadto w art. 83 ustawodawca nakazuje stosować odpowiednio art. 78 ust. 1 prawa autorskiego, jeżeli doszło do rozpowszechnienia korespondencji bez zezwolenia osoby, do której została skierowana;

3) na gruncie prawa karnego:

a) wspominany art. 267 par. 1–4 k.k.,

b) art. 130 par. 1–4 k.k. (potencjalne szpiegostwo – „branie udziału w działaniach wywiadowczych” na rzecz innych państw).

Oczywiście funkcjonowanie Echelon stoi w absolutnej sprzeczności z prawnymi możliwościami podsłuchu i wykorzystania jakiejkolwiek tajemnicy prawnie chronionej – zawodowej – tajemnicy adwokackiej, dziennikarskiej czy innej, do której zobowiązane są określone kręgi zawodowe, osobowe.

Powszechnym wytłumaczeniem funkcjonowania w ramach systemu Echelon jest walka z terroryzmem. Szczęśliwie problem ten nie dotyka Polski. Wobec tego należałoby postawić znak zapytania przy takiej argumentacji. Pamiętać tu także należy, że polski system prawny dopuszcza własne metody badań

67 Dz. Urz. UE 2010, C 83.

68 Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, t.j., Dz.U. 2019, poz. 1145, z późn. zm., art. 24, par. 1: „Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny”.

69 Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j., ibidem, poz. 1231, z późn. zm..

– procesowe[70] i pozaprocesowe (operacyjno-rozpoznawcze[71]) pomagające zwalczać tego typu tendencje – zagrożenia terrorystyczne. Istnieje co najmniej kilka służb państwowych mających ustawowe prerogatywy do stosowania tego typu metod, form i środków pracy[72].

W tym kontekście przewijają się również hasła szpiegostwa przemysłowego czy wywiadu gospodarczego, których zwalczaniem zajmują się te same lub inne służby państwowe mające uprawnienia operacyjne, w tym głównie wynikające z możliwości stosowania kontroli operacyjnej[73].

70 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, t.j. ibidem, 2020, poz. 30, z późn. zm., art. 237, par. 1: „Po wszczęciu postępowania sąd na wniosek prokuratora może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa". Takimi przestępstwami mogą być przykładowo: uprowadzenie statku powietrznego lub wodnego, zamach na niepodległość lub integralność państwa, zamach na konstytucyjny ustrój państwa lub jego naczelne organy albo na jednostkę Sił Zbrojnych Rzeczypospolitej Polskiej, szpiegostwao lub ujawnienie informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne", gromadzenie broni, materiałów wybuchowych lub radioaktywnych.

71 L. Schaff, *Zakres i formy postępowania przygotowawczego*, Warszawa 1961, s. 77. „Jedną z pierwszych definicji czynności operacyjno-rozpoznawczych sformułował Leon Schaff jako: »pozaprocesowe techniczne i taktyczne czynności wykształcone przez praktykę organów ścigania karnego, służące profilaktycznej walce z przestępczością«". Por. również: D. Czerwińska, *Pojęcie czynności operacyjno-rozpoznawczych*, https://prawo.uni.wroc.pl/sites/default/files/students-resources/czynności%20operacyjno-rozpoznawcze.pdf. „Dzisiaj nazywamy je ogółem niejawnych działań upoważnionych ustawowo wyspecjalizowanych służb i organów państwowych, których celem jest sprawne wykrywanie negatywnych zjawisk godzących w porządek publiczny i bezpieczeństwo powszechne, rozpoznawanie środowisk przestępczych, ustalanie źródeł dowodowych, zabezpieczanie środków dowodowych, które mogą zostać wykorzystane w procesie karnym oraz ujawnienie okoliczności sprzyjających popełnieniu zachowań nieakceptowanych społecznie".

72 Policja (Ustawa z dnia 6 kwietnia 1990 r. o Policji, t.j., Dz.U. 2020, poz. 360, z późn. zm.), Straż Graniczna (Ustawa z dnia 12 października 1990 r. o Straży Granicznej, t.j., ibidem, poz. 305), CBA (Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, t.j., ibidem 2019, poz. 1921, z późn. zm.), ABW i AW (Ustawa z 25 listopada 2016 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiad, t.j., ibidem 2020, poz. 27), KAS (Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej, t.j., ibidem, poz. 505, z późn. zm.), SKW i SWW (Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, t.j., ibidem 2019, poz. 687), Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, t.j., ibidem, poz. 796, SOP (Ustawa z dnia 8 grudnia 2007 r. o Służbie Ochrony Państwa, t.j., ibidem, poz. 828), ŻW (Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, t.j., ibidem 2020, poz. 431, z późn zm.).

73 J. Sałek, *Nielegalność czynności operacyjno-rozpoznawczych a możliwość ich procesowego wykorzystania w postępowaniu dowodowym*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 289. Kontrola operacyjna, zaliczana do czynności operacyjno-rozpoznawczych, zgodnie z art. 19 ust. 6 ustawy o Policji jest prowadzona niejawnie i polega na

W literaturze wskazuje się, że: „[…] Poza tymi powszechnie dostępnymi informacjami, istnieją dwie okoliczności, które racjonalizują obserwację, że Echelon wykorzystywany jest dzisiaj przede wszystkim w wywiadzie gospodarczym. Otóż, gospodarka z natury rzeczy ma charakter globalny. I takim też jest Echelon. To zaś, że Echelon owiany jest tajemnicą, nie utrudnia konstatacji, że koszty związane z jego utrzymywaniem są horrendalne. Z tej, również ekonomicznej perspektywy, system globalnej kontroli informacji nie może być zracjonalizowany wyłapywaniem incydentalnych informacji o zagrożeniach terrorystycznych, co oczywiście nie znaczy, że i w tym celu może być on wykorzystywany, takie zaś jego wykorzystywanie może stanowić usprawiedliwienie jego istnienia. Dlatego wydaje się, że głównym ekonomicznym uzasadnieniem nakładów na Echelon mogą być tylko korzyści związane z polowaniem na pokaźną ilość informacji doniosłych gospodarczo”[74].

Jak wskazano, gospodarka Polski, choć z pewnością rozwijająca się, nie pozwala państwu polskiemu na wejście do ścisłej elity państw utrzymujących najwyższe światowe PKB, a tym samym jako nabywca, nie producent dóbr, nie może liczyć na zbytnie zainteresowanie służb wywiadowczych Stanów Zjednoczonych.

Pytania, które niewątpliwie rodzą się przy analizie zjawiska elektronicznej inwigilacji komunikacji polskiego społeczeństwa, za zgodą organów państwowych, to m.in.:

1) kto jest gwarantem ochrony polskiego obywatela w sytuacji, gdy samo państwo godzi się na ujawnianie wszelkich danych obcym państwom, a może służbom wywiadowczym;

2) kto jest gwarantem praw polskiego obywatela w sytuacji, gdy to ustawowe prerogatywy przyznające określonym polskim służbom uprawnienia operacyjno-rozpoznawcze stanowią tak naprawdę zdecydowanie mniejszy katalog pozyskanych informacji aniżeli totalny podsłuch własnego społeczeństwa przez – głównie – amerykański system;

3) w jaki sposób – prawnokarny – ocenić odpowiedzialność – czyją i jakiego typu, w sytuacji pozyskania/ujawnienia informacji objętych tajemnicą

uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, rozmów telefonicznych, ale także obrazów lub dźwięków osób z pomieszczeń, środków transportu i innych miejsc niż publiczne, zawartości przesyłek, treści korespondencji, w tym także elektronicznej oraz różnych danych informatycznych z nośników, systemów itd.

74 M. Andreasik i in., op. cit., 2, s. 68.

zawodową (adwokacką, lekarską) czy szczególnie prawnie chronioną, obcym państwom;

4) w jaki sposób realizować konstytucyjne prawo każdego obywatela (art. 51 ust. 3 ustawy zasadniczej) do uzyskania dostępu do dotyczących go urzędowych dokumentów i zbiorów;

5) kto poniesie odpowiedzialność, który organ państwowy, funkcjonariusz państwowy, a może – indywidualnie – osoba fizyczna, w razie uzyskania podejrzeń odnośnie do „przestępstwa szpiegostwa", zgodnie z kodeksową regułą art. 240 par. 1 k.k. „nie zawiadamiają odpowiedniego organu, za co grozi nam za to kara pozbawienia wolności do 3 lat"[75].

Zakończenie

„It's the economy, stupid"[76].

Takich pytań retorycznych można dziś postawić zdecydowanie więcej. Odpowiedź na nie nie leży w interesie państwa. Od inwigilacji własnych społeczeństw, mimo obwarowań i konstytucyjnych, i ustawowych niezależnie od przeciwnych stanowisk, opinii i protestów społeczeństwa, nie ma odwrotu, a państwa z pewnością będą sięgały po te atrybuty coraz częściej.

W ostatnich dniach, przed powstaniem niniejszego artykułu, ujawniono, że dzięki posiadanym wewnętrznym systemom podsłuchu – Pegasus – Agencja Bezpieczeństwa Wewnętrznego wraz z Centralnym Biurem Antykorupcyjnym mogły doprowadzić do wielu aresztowań osób znanych w kręgach businessowych, wojskowych i politycznych, w tym byłego ministra transportu, budownictwa i gospodarki morskiej. A jeszcze do niedawna media powszechnie

75 Art. 240 par. 1 k.k.: „Kto, mając wiarygodną wiadomość o karalnym przygotowaniu albo usiłowaniu lub dokonaniu czynu zabronionego określonego w art. 118, art. 118a, art. 120–124, art. 127, art. 128, art. 130, art. 134, art. 140, art. 148, art.156, art.163, art.166, art. 189, art. 197 § 3 lub 4, art. 198, art. 200, art. 252 lub przestępstwa o charakterze terrorystycznym, nie zawiadamia niezwłocznie organu powołanego do ścigania przestępstw, podlega karze pozbawienia wolności do lat 3".

76 Zob. https://wiadomosci.wp.pl/najslynniejsze-hasla-6038688162636929g/18. „Hasło »Ekonomia, głupcze« (»It's the economy, stupid«) przyniosło Billowi Clintonowi zwycięstwo w wyborach prezydenckich w USA w 1992 r.". Por. również M. Andreasik i in., op. cit., s. 66. „Wskazywano konkretne polecenia, np. prezydenta Clintona, który nakazał National Security Agency wykorzystać »super-tajny program nadzoru Echelon« do monitorowania osobistych rozmów telefonicznych, a także prywatnej poczty pracowników, którzy pracowali dla zagranicznych firm, w dążeniu do zwiększenia amerykańskiego handlu".

krytykowały koszty posiadania i użytkowania systemu przez wskazane służby państwowe[77]. To we wrześniu 2019 roku pisano: „Cyberbezpieczeństwo stało się dziś tematem numer jeden kampanii wyborczej. […] Wszystko za sprawą Pegasusa, czyli stworzonego w Izraelu systemu. Obsługujący go ludzie są w stanie włamać się na dowolny smartfon, w dowolnej sieci i z dowolnymi zabezpieczeniami. Kłopotem jednak nie jest wykorzystywanie Pegasusa, lecz brak realnej kontroli nad tym narzędziem"[78].

Pegasus to ani pierwszy, ani ostatni system tego typu. W 2016 roku służby pobrały 1,15 mln danych telekomunikacyjnych, w 2017 – 1,23 mln , a w 2019 – 1,356 mln. Zakładając nawet, że polskie sądy bezrefleksyjnie wydają zgody na stosowanie podsłuchów, to uzyskane dane podlegają bądź podlegać mogą jakiejkolwiek kontroli polskich organów państwowych, czego w przypadku Echelon nikt nie jest w stanie zagwarantować.

Nawet w przypadku systemu użytkowanego przez polskie służby istnieje jeden delikatny wątek. Przecież to firma, która sprzedała system, gwarantuje sobie do niego wgląd i kontrolę nad nim. „Polska służba specjalna, jeśli to kupiła i używa w Polsce, jednocześnie informuje obce służby specjalne o swoich zainteresowaniach operacyjnych. Można by to określić nawet kodeksowo, że wystąpił casus artykułu 130 paragraf 2 Kodeksu karnego, czyli udzielenie informacji obcemu wywiadowi" – stwierdzał były szef Agencji Bezpieczeństwa Wewnętrznego Krzysztof Bondaryk[79].

Wszystko to prowadzi do jedynej możliwej konstatacji – procesu podsłuchiwania każdego, kogo chce się podsłuchiwać, nie da się już zatrzymać. Państwo polskie nie posiada przy tym żadnych ani praktycznych, ani technicznych czy prawnych środków przeciwdziałania tej światowej tendencji, tendencji do wszechwiedzy w myśl interesu, nawet bliżej niezidentyfikowanego interesu godzącego w dobra prawne każdego z nas.

77 Por. https://crowdmedia.pl/pegasus-jeszcze-bardziej-niebezpieczny-niz-sie-wydawalo-zobaczcie-kto-ma-dostep-do-systemu/. „Pod koniec wakacji TVN24 ujawnił, że Centralne Biuro Antykorupcyjne za 25 milionów kupiło system do inwigilacji o nazwie Pegasus, który służy do śledzenia osób za pośrednictwem smartfonów. Wszystkie koszty związane z wdrożeniem sytemu zamykają się w kwocie 34 mln zł. Cała sprawa zaczęła się od kontroli, jaką przeprowadziła w CBA Najwyższa Izba Kontroli, odkrywając fakturę na kwotę odpowiadającą cenie za Pegasusa".

78 Por. https://prawo.gazetaprawna.pl/artykuly/1428575,pegasus-ceberbezpieczenstwo-podsluch-inwigilacja-opinia.html.

79 Por. https://tvn24.pl/polska/system-pegasus-i-walizki-imsi-catcher-do-podsluchiwania-i-inwigilacji-odpowiedz-cba-ra972059-2285741.

Bibliografia

Literatura

Andreasik M. i in., *Orwell w realu, czyli o systemie Echelon z perspektywy polskiego prawa*, „Studia Prawnicze. Rozprawy i Materiały" 2014, nr 2.
Brayfield C., *Boski Andy i przyjaciele*, Warszawa 2006.
Derlatka K., *Potęga informacji*, „Interdyscyplinarne Studia Społeczne" 2016, nr 1.
Harding L., *Polowanie na Snowdena*, Warszawa 2014.
Jonason J., *Stulatek, który wyskoczył przez okno i zniknął*, Warszawa 2011.
Kleinfield S., *The biggest company on earth a profile of AT&T*, New York 1981.
Orwell G., *Rok 1984*, Warszawa 1988.
Sałek J., *Nielegalność czynności operacyjno-rozpoznawczych a możliwość ich procesowego wykorzystania w postępowaniu dowodowym*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16.
Schaff L., *Zakres i formy postępowania przygotowawczego*, Warszawa 1961.
Shapiro C., Varian H.R., *Potęga informacji. Strategiczny przewodnik po gospodarce sieciowej*, Warszawa 2008.
Wobst R., *Cryptology unlocked*, Wiley 2007.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483, z późn. zm.
Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, t.j., Dz.U. 2019, poz. 796.
Ustawa z dnia 12 października 1990 r. o Straży Granicznej, t.j., Dz.U. 2020, poz. 305.
Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej, t.j., Dz.U. 2020, poz. 505, z późn. zm.
Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, t.j., Dz.U. 2019, poz. 1145, z późn. zm.
Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, t.j., Dz.U. 2020, poz. 431, z późn. zm.
Ustawa z dnia 25 listopada 2016 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiad, t.j., Dz.U. 2020, poz. 27.
Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j., Dz.U. 2019, poz. 1231, z późn. zm.
Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, t.j., Dz.U. 2020, poz. 30, z późn. zm.
Ustawa z dnia 6 kwietnia 1990 r. o Policji, t.j., Dz.U. 2020, poz. 360, z późn. zm.
Ustawa z dnia 8 grudnia 2007 r. o Służbie Ochrony Państwa, t.j., Dz.U. 2019, poz. 828.
Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, t.j., Dz.U. 2019, poz. 1921, z późn. zm.
Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, t.j., Dz.U. 2019, poz. 687.

Poland as the part of Echelon system

Abstract

The overarching aim of this article is to present the legal framework for the potential use of the Echelon system in the Republic of Poland. Echelon, known as worldwide surveillance program, was created by the American and British specialist in the late 1960s to observe and monitor military and diplomatic communications of the former Soviet Union and the Eastern Block. Nowadays, the role of Echelon seems to be completely different, as

recently revealed by e.g. European Parliament. It's the tool evolved into „a global system for the interception of private and commercial communications" (mass surveillance and industrial espionage). Numerous press reports as well as 2013 Snowden accusations suggest Poland plays quite an effective role as the part of the European Echelon Network. The question this article answers is whether our national presence and involvement in gaining information is based on the legal, constitutional grounds or whether, like some other nations, Polish authorities become indifferent to any kind of legal obstacles when need an information for their purposes.

Key words: Echelon, surveillance, communications, correspondence, intelligence, terrorism, cybersecurity, infringement of civil rights, national interests, espionage