Marcin Andreasik
doktorant, Uniwersytet Wrocławski
Daniel Karkut
doktorant, Uniwersytet Wrocławski
Jacek Mazurkiewicz
doktor habilitowany, profesor nadzwyczajny, Uniwersytet Wrocławski
Bartosz Mierzwiński
doktorant, Uniwersytet Wrocławski
Mateusz Popielas
doktorant, Uniwersytet Wrocławski
Karolina Trzeciak-Wach
doktorantka, Uniwersytet Wrocławski
Maria Zaporowska
magister, prawnik, Wrocław
Zofia Zaporowska
magister, prawnik, Wrocław

Orwell w realu, czyli o systemie Echelon z perspektywy polskiego prawa

Wprowadzenie

„Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony" – ta stanowcza i jasna deklaracja, a nie tylko prawna gwarancja, zawarta jest w art. 49 Konstytucji Rzeczypospolitej Polskiej.

Spogląda się na nią z perspektywy, którą stworzył system globalnej inwigilacji komunikacji, nie tylko elektronicznej, zwany Echelonem. Wiadomo było o nim dużo wcześniej zanim z Hongkongu dobiegł głos Edwarda Snowdena. O Echelonie rozmawiano, pisano, dyskutowano, również na poważnych forach, nie tylko w Parlamencie Europejskim. W Polsce jednak zagadnienie to nie budziło wtedy zainteresowania prawników, tak jak w ogóle nie zainteresowało posłów, senatorów, rządu, polityków. W niniejszym tekście

podjęta zostanie przypuszczalnie pierwsza próba oceny konsekwencji Echelonu z perspektywy polskiego prawa. Autorzy z rozmysłem ograniczyli się do tego, co było dla każdego dostępne przed Snowdenem. Taka optyka ma szczególną wymowę: ukazuje bowiem dramatyczną aplikację *in casu* konstytucyjnej zasady demokratycznego państwa prawnego. Uświadamia, gdzie ludzie żyją i co mogą.

* * *

Gdy przed kilkudziesięciu laty kolejne tłumaczenie *Roku 1984* George'a Orwella trafiło do polskich czytelników, kontekst interpretacyjny wydawał się oczywisty. Kontrolujące ludzi państwo utożsamiane było ze Związkiem Radzieckim, z emfazą określanym w propagandzie Stanów Zjednoczonych mianem Imperium Zła.

Nie minęło wiele lat od tytułowego roku, a Związek Radziecki dostał pieriedyszki, zaczął rdzewieć, tracić kontrolę nad samym sobą i w końcu się rozpadł. W tym pozornie jednobiegunowym świecie wydawało się, że na placu boju pozostało już tylko imperium, które zawsze szczyciło się najwyższymi standardami demokracji oraz respektem dla praw człowieka. Jednak właśnie tam zrodził się, choć realizowany jest nie tylko przez to państwo koncept bynajmniej nie pisarski – totalnej kontroli prawie wszystkiego, co ludzie piszą, mówią, czego pragną, co kochają czy nienawidzą. Nie w jednym państwie, ale na całym świecie! To, co wydawało się niegdyś pomysłem *science fiction*, udało się zrealizować!

Dziś obiektem owej kontroli są wszyscy, autorzy i czytelnicy tego artykułu również. Wtedy, gdy rozmawiają przez komórkę, telefon stacjonarny, wysyłają e-mail lub faks, a nawet gdy otwierają link. Jedynym obszarem pozostającym poza kontrolą Echelonu są myśli i marzenia senne. Choć niewykluczone, że tylko do czasu... Genialni technolodzy pracowali, pracują i pracować będą dla imperiów. Oczywiście nie tylko dla Imperium Hipokryzji.

Tajemnica komunikacji pod butem Echelonu

W ramach szeroko pojmowanych wolności obywatelskich i osobistych wyróżnia się wolność komunikowania się, która obejmuje swoim zakresem wszystkie formy i sposoby porozumiewania się między ludźmi. Na tym tle problem tajemnicy korespondencji[1] stanowi wyłącznie fragment, związany jak wskazuje SN „z prawem każdego człowieka do poszanowania jego życia

[1] Zob. także: W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, wyd. 4, Lex nr 8132.

prywatnego, jego prawa do zachowania w tajemnicy przekazu kierowanego do innych osób lub instytucji"[2]. Bezprawne zapoznanie się z treścią cudzej korespondencji stanowi postać naruszenia normy art. 23 k.c. Uwaga ta ma istotne znaczenie w toku dalszych rozważań nad funkcjonowaniem globalnej sieci wywiadu elektronicznego Echelon.

System ten gromadzi i analizuje przekazy elektroniczne z całego świata – faksy, telefaksy, e-maile, transfery plików, a nawet zwykłe rozmowy telefoniczne. Pierwszym źródłem mówiącym o istnieniu takiego systemu były raporty Duncana Campbella przedstawione europejskiej komisji opiniującej zagadnienia naukowe i techniczne w 1997 r. i 1999 r. Dokumenty te dały asumpt do utworzenia przez Parlament Europejski 5 lipca 2000 r. tymczasowej komisji w sprawie systemu Echelon[3]. Rząd USA do tej pory nie potwierdził istnienia takiej cyberstruktury. Podczas prac Parlamentu Europejskiego nad raportem dotyczącym tego zagadnienia również nie została przez rząd Stanów Zjednoczonych Ameryki ujawniona treść porozumienia, zwanego wówczas UKUSA, a pracownicy NSA i CIA, którzy mieli spotkać się z przedstawicielami Parlamentu Europejskiego w tej sprawie, w ostatniej chwili odmówili spotkania[4].

Zjawisko szpiegostwa elektronicznego, którego dopuszczają się państwa-sygnatariusze porozumienia Auscannzukus[5], bezpośrednio godzi w indywidualny interes każdego obywatela. W demokratycznych państwach przestrzeganie praw jednostki stanowi fundament ustroju tych państw. W konsekwencji wszelkie przejawy łamania praw i wolności obywatelskich są wystąpieniem

---

[2] Wyrok SN z 24 września 2010, IV CSK 87/10, Lex nr 622216.

[3] *European Parliament Report on the existence of a global system for the interception of private and commercial communications (ECHELON interceptions system) (2001/2098(INI))*, [w:] www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5--2001-0264+0+DOC+PDF+V0//EN&language=EN, s. 21 [dostęp 29.05.2014, ta sama data dotyczy dostępu do pozostałych publikacji internetowych przywołanych w artykule]. Wspomniana Komisja w opracowanym raporcie nawiązuje do istnienia porozumienia zwanego UKUSA pomiędzy rządem USA i Wielkiej Brytanii, które rozpoczęło proceder przechwytywania informacji i podsłuchu na globalną skalę. 5 marca 1946 r. pomiędzy rządami USA a Wielkiej Brytanii zostało podpisane porozumienie, które jest znane jako „the UKUSA agreement". Początkowo skierowane było przeciwko rządowi ZSRR, w kolejnych latach przystąpiły do niego inne państwa anglojęzyczne, takie jak Kanada, Australia i Nowa Zelandia i od nazw wszystkich państw-sygnatariuszy jest powszechnie nazywane „auscannzukus". Zgodnie z raportem Parlamentu Europejskiego, istnienie porozumienia UKUSA, którego celem jest współpraca wywiadowcza, przechwytywanie oraz wymiana prywatnych i komercyjnych informacji, jest faktem niepodlegającym żadnym wątpliwościom.

[4] Dopiero pod naciskiem opinii publicznej w 2010 r. została oficjalnie odtajniona treść porozumienia UKUSA, którą podano do informacji publicznej i można ją znaleźć na stronach archiwów państwowych oraz amerykańskiego NSA: www.time.com/time/nation/article/0,8599,2000262,00.html.

[5] Zob. więcej: *European Parliament Report…*, s. 11.

przeciwko podwalinom systemu demokratycznego[6]. Jest oczywiste, że prawo do prywatności nie może być prawem bezwzględnym i jak większość praw oraz wolności obywatelskich, podlega pewnym ograniczeniom. Każde państwo musi przecież dbać o swoje bezpieczeństwo. Ograniczenia w tej płaszczyźnie przewiduje m.in. Konstytucja RP[7], a także Europejska Konwencja Praw Człowieka.

Tajemnica korespondencji jest także pojęciem normatywnym, które na gruncie prawa prywatnego występuje m.in. w katalogu dóbr osobistych uregulowanych przepisami art. 23 i 24 k.c., czy w przepisach prawa autorskiego (art. 82 i 83)[8], jak również w sferze prawa *stricte* publicznego. Także akty prawa międzynarodowego w założeniu gwarantować mają nam ochronę życia prywatnego, w tym i ochronę tajemnicy korespondencji[9].

Cechą wspólną krajowej ustawy zasadniczej i aktów prawa międzynarodowego jest przyjęcie generalnego i skądinąd słusznego założenia, że państwo w określonych warunkach musi mieć prawo ingerowania w sferę prywatnych zachowań obywateli, w celu prawidłowego wypełniania swoich funkcji. Jak wskazuje się w literaturze prawniczej, pojawia się tu jednak pytanie o to, jakie funkcje państwa usprawiedliwiają wkroczenie w sferę życia prywatnego oraz

---

[6] Zob. więcej: A. Mednis, *Prawo do prywatności a interes publiczny*, Lex nr 58276.

[7] Ustawodawca w art. 51 Konstytucji RP wprawdzie wskazuje, że każdy może zostać zobowiązany do ujawnienia informacji dotyczących jego osoby, z tym jednak zastrzeżeniem, że „ten sam przepis ogranicza pozyskiwanie informacji o obywatelach do przypadków niezbędnych i uznawanych w demokratycznym państwie. Tak więc władze nie mogą sobie ustalać dowolnie zasobu informacji, jakie pragną uzyskać od obywateli, są w tym względzie ograniczone postanowieniem ustawy. Niezwykle ważne prawo gwarantuje ust. 3 tegoż artykułu, gdyż uprawnia on każdego do uzyskania dostępu do dotyczących go urzędowych dokumentów i zbiorów […]. W ten sposób każdy może wpływać na prawidłowość i kompletność dotyczących go informacji gromadzonych zgodnie z ustawą" (W. Skrzydło, *Konstytucja*…, Lex nr 8132).

[8] W myśl art. 82 PrAut, jeżeli adresat korespondencji nie wyraził innej woli, dla rozpowszechniania korespondencji w okresie dwudziestu lat od jego śmierci, wymagane jest zezwolenie małżonka, a w jego braku kolejno zstępnych, rodziców lub rodzeństwa. Ustawodawca w art. 83 PrAut nakazuje stosować odpowiednio art. 78 ust. 1 PrAut, jeżeli doszło do rozpowszechnienia korespondencji bez zezwolenia osoby, do której została skierowana. Roszczeń przewidzianych w art. 78 ust. 1 nie można dochodzić po upływie dwudziestu lat od śmierci adresata korespondencji.

[9] W art. 12 Powszechnej Deklaracji Praw Człowieka uchwalonej przez Zgromadzenie Ogólne ONZ 10 grudnia 1948 r., można przeczytać, że 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". Z treścią cytowanego przepisu koresponduje 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". Ustawodawca europejski w 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.

o dopuszczalny zakres tej ingerencji? W ustroju demokratycznym działania aparatu państwa są zorientowane na cele publiczne i powinny być realizowane zgodnie z interesem publicznym oraz w jego granicach[10]. W tym miejscu należy również postawić drugie zasadnicze pytanie – jak państwo realizuje swoje zadania w sferze ochrony wszystkich obywateli przed potencjalnym cyberatakiem ze strony obcych systemów wywiadu elektronicznego, chociażby takich jak Echelon?

Przed odpowiedzią na zadane pytania, przedstawić należy pokrótce przywołany wyżej katalog okoliczności uzasadniających ograniczenia w korzystaniu z konstytucyjnych wolności i praw, który został sprecyzowany w ust. 3 art. 31 Konstytucji RP. Katalog ten w mniejszym lub większym stopniu powtarzany jest we wspomnianych już aktach prawa międzynarodowego, m.in. przez art. 52 Karty Praw Podstawowych Unii Europejskiej[11]. Przyjmuje się, że prawnie dozwoloną będzie ingerencja w wolności obywatelskie (w tym i wolność komunikowania się) wtedy, gdy kompetencja ta znajdzie swoje odzwierciedlenie w przepisach ustawy, a także gdy uzasadniona jest z uwagi na zagrożenia dla bezpieczeństwa państwowego, bezpieczeństwa publicznego, dobrobytu gospodarczego kraju, ochrony porządku i zapobieżenia wykroczeniom karnym, ochrony zdrowia i moralności oraz dla ochrony praw i wolności osób trzecich. To powszechnie uznane wartości uzasadniające ingerencję w sferę wolności obywatelskich, co potwierdził ETPC w sprawie Uzun przeciwko Niemcom[12]. Przy tym trudną do przecenienia jest stanowcza opinia, że tam, gdzie może dojść do naruszenia praw i wolności obywatelskich, uznaniowość władzy winna być maksymalnie ograniczona, nie tylko dlatego, że „prawo do prywatności jest warunkiem swobodnej i nieskrępowanej aktywności człowieka w społeczeństwie" [13].

---

[10] A. Mednis, *Prawo do prywatności…*

[11] Dz.Urz. UE 2010, C 83, s. 389.

[12] Wyrok ETPC z 2 września 2010 r., skarga nr 35623/05, [w:] M.A. Nowicki, *Europejski Trybunał Praw Człowieka. Wybór orzeczeń 2010*, Lex 2011, s. 181. W sprawie tej chodziło o posłużenie się systemem GPS w celu inwigilacji podejrzanego o poważne przestępstwo. Wprawdzie Trybunał uznał, że systematyczne „zbieranie danych przez służby bezpieczeństwa o konkretnych osobach i ich przechowywanie, nawet bez posługiwania się tajnymi metodami kontroli, stanowi ingerencję w życie prywatne osób, których one dotyczą", jednak z uwagi na potrzebę ochrony bezpieczeństwa publicznego takie działanie było *in casu* w pełni uzasadnione i nie doszło do naruszenia przepisów konwencji.

[13] A. Mednis, *Prawo do prywatności*…. Zob. także wyrok NSA z 21 czerwca 2001, V SA 3718/00, http://www.orzeczenia-nsa.pl/wyrok/v-sa-3718-00,cudzoziemcy_repatrianci_nabycie_nieruchomosci_przez_pomoc_spoleczna,e37d13.html, w którym sąd ten wyraził zasadę, że w „państwie nie ma miejsca dla mechanicznego i sztywnego pojmowania zasady nadrzędności interesu społecznego nad interesem indywidualnym". Ponadto obowiązkiem organu jest udowodnienie, że wskazany interes jest „tak ważny i znaczący, że bezwzględnie wymaga ograniczenia uprawnień indywidualnych obywatela".

Z perspektywy przedstawionej analizy należy zauważyć, że obecnie nie ma skutecznego instrumentu publicznoprawnego, za pośrednictwem którego można byłoby żądać zaniechania naruszeń sfery życia prywatnego wyłącznie w oparciu o wskazane normy prawa międzynarodowego i konstytucyjnego. Katalog ten nie daje podstaw do skutecznego dochodzenia zaniechania naruszeń prywatności bądź też ochrony przed jej naruszeniem ze strony innych osób, instytucji, systemów. Nie można wyegzekwować od państwa – często działającego w źle pojętym interesie publicznym – aby nie dopuszczało się naruszeń w przestrzeni wymiany informacji między obywatelami, a tym bardziej, aby zabezpieczyło przed zagrożeniami międzynarodowymi, związanymi z działaniem w cyberprzestrzeni obcych systemów szpiegowskich, takich jak Echelon. Skoro komentowane normy transgranicznego i konstytucyjnego prawa nie zapewniają skutecznej ochrony w tej materii, pozostaje przenieść rozważania na grunt prawa prywatnego.

Działalność poszczególnych agencji wywiadowczych współpracujących ze sobą dla realizacji projektu o kryptonimie Echelon stanowi, z punktu widzenia regulacji polskiego kodeksu cywilnego, naruszenie dóbr osobistych, takich jak tajemnica korespondencji – w zakresie przechwytywania wiadomości w formie e-maila, faksu, telefaksu i analizowania transferu innych danych, następującego głównie za pośrednictwem internetu, a także w sferze prywatności człowieka, m.in. w zakresie podsłuchiwania zwykłych rozmów telefonicznych. W szpiegowskich działaniach globalnej sieci wywiadu elektronicznego można doszukiwać się pogwałcania także innych dóbr osobistych – w zależności od obszaru naruszeń czy okoliczności (np. załączenie niektórych zdjęć do wiadomości w formie e-maila i przekazanie ich do analizy materiału w jednostkach Echelonu mogłoby godzić w dobro osobiste wizerunku).

Dla oceny działalności systemu Echelon istotne znaczenie mają regulacje z zakresu prawa ochrony danych osobowych, przede wszystkim dyrektywa 95/46/CE w sprawie ochrony osób fizycznych ze względu na przetwarzanie danych o charakterze osobowym oraz swobodnego przepływu tych danych, Konwencja nr 108 Rady Europy z 28 stycznia 1981 r. o ochronie osób ze względu na automatyczne przetwarzanie danych o charakterze osobowym oraz ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych – mająca na celu ochronę prywatności informacyjnej zarówno w sferze publicznej, jak i prywatnej. Ingerencja w sferę wolności komunikowania się może być postrzegana również w kategoriach naruszania szeregu tajemnic (w szczególności zawodowych)[14].

[14] Do tajemnic tych należy zaliczyć m.in. tajemnicę lekarską, komunikowania się, bankową, zawodową w obrocie instrumentami finansowymi, skarbową, dziennikarską, adwokacką, notarialną i radcowską.

Poniżej zostaną przedstawione jedynie instrumenty ochronne określone przepisami kodeksu cywilnego z perspektywy ich użyteczności w walce z praktykami systemu Echelon.

Polski kodeks cywilny w art. 24 wyposaża każdego, kogo dobro osobiste zostało cudzym działaniem[15] naruszone[16], w instrumenty prawne w postaci roszczeń ochronnych, których charakter przedstawia się różnie. Ustawowy katalog owych roszczeń obejmuje zarówno te o charakterze majątkowym, jak: o zadośćuczynienie pieniężne za doznaną krzywdę wynikającą z naruszenia dobra osobistego lub o zapłatę odpowiedniej sumy pieniężnej na wskazany cel społeczny (w zw. z art. 448 k.c.), o odszkodowanie z tytułu ewentualnej szkody majątkowej powstałej w rezultacie pogwałcenia takiego dobra (art. 361–363, 415 i nast. k.c.), jak i niemajątkowym, tj. o zaniechanie dalszych naruszeń oraz o usunięcie skutków naruszenia, co nastąpić ma w szczególności poprzez złożenie oświadczenia odpowiedniej treści i w odpowiedniej formie. Pomocne w zniwelowaniu stanu zagrożenia dla dobra osobistego ma być wyłącznie roszczenie o zaniechanie działania, jeżeli jest ono bezprawne.

Istnieje także możliwość skorzystania z powództwa o ustalenie w oparciu o przepis art. 189 k.p.c., jako że orzeczenie ustalające, iż określone prawo osobiste przysługuje danej osobie niekiedy wystarczy, aby zapobiec dalszym jego naruszeniom lub uchylić niebezpieczeństwo dokonania naruszeń.

Zaakcentowania wymaga to, że przedstawiony powyżej system wyznacza minimalny standard ochronny, a roszczeń tych nie wyłączają regulacje pozakodeksowe przewidujące ochronę określonych dóbr osobistych. Ze względu na niezaprzeczalną doniosłość społeczną dóbr osobistych zasada *lex specialis derogat legi generali* nie znajduje tu zastosowania.

Dyskusyjna pozostaje kwestia szkody majątkowej oraz niemajątkowej mającej wynikać z naruszania dobra osobistego, przynajmniej w postaci tajemnicy korespondencji, dokonującego się przez działanie systemu szpiegowskiego Echelon. Z powodzeniem można bronić tezy o stratach moralnych, czy ujemnych przeżyciach psychicznych mających swe źródło w świadomości[17] infiltrowania przez specjalne oprogramowania Echelonu treści pisanych i wysyłanych za pośrednictwem poczty elektronicznej wiadomości. Tylko po-

[15] Ochrona przysługuje jedynie przeciwko takiemu zachowaniu, które może być uznane za działanie sprawcy.

[16] Zgodnie z wyr. SN z 26 października 2001, V CKN 195/01, niepubl., należy przyjmować koncepcję obiektywną naruszenia dobra osobistego w kontekście całokształtu okoliczności sprawy.

[17] Pozorny wydaje się problem, co w razie braku świadomości (wiedzy) rzeszy ludzi o istnieniu (przynajmniej hipotezach o istnieniu) Echelonu. Czy uprawnione jest wtedy mówienie o jakiejkolwiek krzywdzie? Naszym zdaniem tak – globalny charakter kontekst krzywdy nie zmienia natury krzywdy.

zornie wątpliwe wydaje się jednak powstanie szkody majątkowej[18] w efekcie pogwałcania tajemnicy korespondencji, skoro sens wywiadu elektronicznego miałby przejawiać się w poszukiwaniu informacji istotnych dla służb wywiadu. A trudno o takie informacje w wiadomościach wymienianych między Markiem a Grzegorzem w sprawie ich planów na piątkową imprezę. Zanegowanie powstawania szkód w rezultacie naruszania tajemnicy korespondencji przez uskutecznianie podsłuchu na globalną skalę prowadziłoby do konkluzji o braku podstaw do występowania z roszczeniami o zadośćuczynienie i odszkodowanie. Jak to jednak w dalszych rozważaniach zostanie podniesione, system Echelon i systemy jemu podobne wyrządzają często olbrzymie szkody majątkowe, przed wszystkim wielkim korporacjom gospodarczym. Ale nawet w sytuacji, gdy hipotetyczny Marek zdaje sobie sprawę z działań systemu Echelon i w jego sferze psychicznej powstaje poczucie krzywdy, uzasadnione wydawałoby się skorzystanie przez niego z roszczenia o zadośćuczynienie. Jednak ze względu na brak jurysdykcji krajowej sądów polskich w tej kwestii, niemożliwe jest skuteczne wytoczenie powództwa przeciwko agencjom NSA czy CIA w Polsce. Ustawodawca nie ustanowił skutecznego narzędzia do obrony praw przed tego typu praktykami.

Warto również pochylić się nad tym, czy istnieją w kontekście „sprawy Echelonu" podstawy do ewentualnego dochodzenia roszczenia o usunięcie skutków naruszenia dobra osobistego. Nasuwa się refleksja, czy przechwytywanie wiadomości mailowych, podsłuchiwanie rozmów telefonicznych itd. wywołuje (przynajmniej dla jednostki) jakiekolwiek skutki, a jeśli tak, to czy na tyle poważne, że wymagałyby ich usunięcia? Wydaje się, że trudno w tej kwestii o jednoznaczne rozstrzygnięcie.

Mając na uwadze powyżej wyrażony sceptycyzm wobec istnienia przesłanek do podniesienia niektórych roszczeń przeciwko Echelonowi, skuteczne wystąpienie na drogę postępowania sądowego wobec tej sieci wydaje się wątpliwe także z innego względu. Jeżeli sprawcą naruszenia dobra osobistego jest osoba prawna lub podmiot bez osobowości prawnej, zachodzi wymaganie spełnienia przesłanek, od których uzależniona jest możliwość przypisania określonego zdarzenia i jego skutków temu podmiotowi. Chodzi tu w szczególności o przesłanki przypisania osobie prawnej lub podmiotowi bez osobowości prawnej skutków zachowania, niekoniecznie będącego oświadczeniem woli, podjętego przez piastuna lub piastunów ich organów. Innymi słowy,

[18] Zob. np. www.wsp.krakow.pl/papers/echelon.html, gdzie informacja, że Komisja Europejska odrzuciła żądania Parlamentu Europejskiego podjęcia działań w sprawie Echelonu, uzasadniając odmowę tym, że nie ma dowodów rzeczywistego poniesienia strat finansowych przez jakąkolwiek firmę europejską na skutek działalności Echelonu.

konieczne jest wykazanie związku pomiędzy działaniem konkretnej osoby fizycznej a działalnością określonego podmiotu charakteryzującego się strukturą organizacyjną tj. zespalającego aktywność grupy jednostek (klasycznym przykładem są spółki prawa handlowego). Łatwo można dostrzec olbrzymie trudności, jakie nastręcza ewentualne dowodzenie owego związku. Może dlatego warto przyjrzeć się temu, w jaki sposób Echelon pozyskuje informacje.

Międzynarodowa społeczność hackerów, skupiona wokół listy dyskusyjnej „Hacktivism", organizator „Dnia zakłócania «Echelonu»" stwierdziła, że rzeczywistą bronią przeciwko Echelonowi i podobnym działaniom jest stosowanie coraz nowocześniejszego oprogramowania szyfrującego. Istotnym zatem aspektem dotyczącym odpowiedzialności za naruszenie dóbr osobistych w Internecie staje się obecność dostawców pośredniczących w procesie komunikowania określonych treści. W specjalistycznej literaturze prawniczej wyróżnia się tutaj dostawców sieci, dostawców dostępu do sieci i dostawców usług. Podmioty te zapewniają samoistne i nieograniczone w czasie przechowywanie treści dostarczonych przez autorów na stronach www, poczcie elektronicznej czy grupach dyskusyjnych. W przypadku naruszenia dóbr osobistych zainteresowanie tą grupą podmiotów jest jak najbardziej zrozumiałe. Regulacje dotyczące konstrukcji tej odpowiedzialności zostały zwarte w dyrektywie 2000/31/EC i stały się podstawą do rozwiązań przyjętych w art. 12––14 u.ś.u.d.e. dotyczących zasad ochrony danych osobowych osób fizycznych korzystających z usług świadczonych drogą elektroniczną. Nie stworzono jednak pełnego modelu odpowiedzialności, lecz wskazano tylko, kiedy odpowiedzialność usługodawcy ulega wyłączeniu. Ma to miejsce między innymi w przypadku, kiedy usługi polegają na prostym przekazie danych; chodzi o automatyczne i krótkotrwałe pośrednie przechowywanie i transmitowanie danych, jeśli działanie to ma wyłącznie na celu przeprowadzenie transmisji danych, a dane nie są przechowywane dłużej niż jest to w zwykłych warunkach konieczne dla przeprowadzenia transmisji lub wówczas, gdy usługodawca transmituje dane i krótkotrwale je przechowuje tylko w celu przyspieszenia ponownego dostępu do nich przez podmiot uprawniony. Warto więc zwrócić uwagę na aspekty dotyczące możliwości przypisania odpowiedzialności za naruszenie dóbr osobistych dostawcom sieci, dostawcom dostępu do sieci czy dostawcom usług oraz rozważyć możliwość dochodzenia wobec nich roszczeń z tego tytułu. Mając na względzie miejsce, jakie zajmuje internet w życiu tzw. społeczeństwa globalnego, trudno nie wyrazić dezaprobaty dla faktu, że do dziś nie istnieje jakikolwiek międzynarodowy akt prawny odnoszący się do ochrony dóbr osobistych w internecie.

Gdy nie wiadomo o co chodzi...

Jak już zauważono, nie mniej doniosłym z punktu widzenia ochrony prawnej jest zagadnienie szkód majątkowych, które mogą być wyrządzone działalnością Echelonu. Przedmiotem niniejszych rozważań nie jest jednak instrumentarium mogące służyć ochronie przed takim konsekwencjami – przede wszystkim dlatego, że ma ono solidne i dobrze poznane podstawy normatywne.

Wskazując na ten obszar skutków istnienia Echelonu warto jednak podjąć próbę ustalenia współczesnych powodów jego dalszego istnienia. U swego zarania uzasadnieniem powstania Echelonu była bowiem, o czym już wspomniano, konfrontacja ze Związkiem Radzieckim i jego sojusznikami. Ale podobnie jak z NATO, które przejawia szczególną aktywność od czasu, gdy zabrakło Układu Warszawskiego, jest z Echelonem. Istnieje do dziś, więc najwyraźniej jest potrzebny i trudne do ustalenia, lecz niewątpliwie olbrzymie koszty tego przedsięwzięcia się opłacają[19].

Najwygodniejszym współcześnie usprawiedliwieniem istnienia tego systemu jest „walka z terroryzmem". Nie z przekory wobec prześmiewczego nakazu Hugona Steinhausa, „nie cudzysłów", termin mówiący o walce z terroryzmem umieszczono w cudzysłowie. Jest bowiem „walka z terroryzmem" przede wszystkim od dawna narzędziem języka propagandy i usprawiedliwieniem dla odwiecznej walki silnych ze słabymi, dla których terroryzm jest najczęściej jedynym orężem, które w nieproporcjonalnej konfrontacji można mniej lub bardziej skutecznie wykorzystać. To osobne, fascynujące badawczo i przecież z natury rzeczy orwellowskie zagadnienie ze sfery nowomowy oraz propagandy współczesnej polityki oraz mediów.

W tym miejscu należy jednak tylko zwrócić uwagę, że ataki terrorystyczne stanowią spektakularną, lecz przecież znikomą część istotnych konfliktów współczesnego świata. I dlatego można mieć zasadnicze wątpliwości, czy „walka z terroryzmem" jest rzeczywistym, a co najmniej głównym powodem dalszej światowej kontroli środków komunikacji. Współcześnie powodem utrzymywania Echelonu nie jest także troska o bezpieczeństwo wojskowe. Ta realizowana jest bowiem przez systemy dużo bardziej wyrafinowane i przede wszystkim wektorowe, nie globalne. Bynajmniej nie oryginalna, wielokrotnie powtarzana w dokumentach i piśmiennictwie poświęconym Echelonowi hipoteza badawcza, która wydaje się tu zasadna, jest nie tylko aplikacją starej,

[19] Zob. np.: A. Bomford, *Echelon spy network revealed*, www.news.bbc.co.uk/2/hi/503224.stm; Q&A, *What you need to know about Echelon*, www.news.bbc.co.uk/2/hi/science/nature/1357513.stm.

ale przecież aktualnej refleksji, że „jak nie wiadomo, o co chodzi, to chodzi o pieniądze".

Zauważyć należy, że olbrzymia, przytłaczająca ilość informacji doniosłych gospodarczo przekazywanych jest w sposób, który umożliwia ich łatwą kontrolę przez Echelon. Nawet wtedy, gdy stosowane są różnorakie zabezpieczenia, nie są one przecież porównywalne z tymi, które wykorzystywane są przy przekazywaniu informacji wojskowych. A dla dysponentów Echelonu bariery stosowane przy przekazywaniu informacji gospodarczych, nie tylko w formie elektronicznej, nie stanowią żadnej istotnej przeszkody.

Bardzo ważną w dyskusji wokół tajemniczych aspektów Echelonu jest prosta konstatacja, że obszernie odniesiono się do jego wykorzystywania dla prowadzenia szpiegostwa przemysłowego w pkt. 10 wspomnianego sprawozdania z 11 lipca 2001 r. komisji tymczasowej Parlamentu Europejskiego[20]. Rozważano tam m.in. szczegółowe cele szpiegowskie, szkody spowodowane taką działalnością prowadzoną przez państwa, przedstawiono znane przypadki takiej działalności, postawę administracji Stanów Zjednoczonych wobec tej działalności oraz jej rolę w promowaniu amerykańskiego eksportu[21]. Niemało miejsca poświęcono w pkt. 11 tego sprawozdania kryptografii jako środka samoobrony także przed szpiegostwem przemysłowych realizowanym przez Echelon[22].

W poważnych przekazach medialnych podkreślano, że sprawozdanie to zawiera bardzo poważne konkretne zarzuty, iż Echelon wielokrotnie pomógł uzyskać amerykańskim przedsiębiorcom przewagę handlową nad przedsiębiorcami europejskimi[23]. Są to ustalenia co do istoty przez nikogo, poza

---

[20] Zob. nadto w szczególności wystąpienie posła G. Schmida w: *Dokumentation: Der offizielle Echelon-Bericht von Gerhard Schmid das Parlament UE*, www.spiegel.de/netzwelt/web/dokumentation-der-offizielle-echelon-bericht-von-gerhard-schmid-an-das-eu-parlament-a-155819.html.

[21] Zob. także: *E-mail users warned over spy Network*, www.news.bbc.co.uk/2/hi/europe/1357264.stm; *EU probes Echelon,* http://news.bbc.co.uk/2/hi/europe/820352.stm.

[22] Zob. np.: www.cryptome.org/echelon-ep-fin.htm; J. Hoenig, *Echelon dient zur Wirtschaftsspionage,* www.handelsblatt.com/archiv/echelon-dient-zur-wirtschaftsspionage/2047436.html.

[23] Warto przytoczyć tu niektóre obserwacje M. Assera z artykułu *Echelon: Big brother without a cause?*, opublikowanego przez serwis BBC: „But a report published by the European Parliament in February alleges that Echelon twice helped US companies gain a commercial advantage over European firms. Duncan Campbell, the British intelligence expert and journalist who wrote the report, raises the prospect that hundreds of US Department of Commerce „success stories", when US companies beat off European and Japanese commercial opposition, could be attributed to the filtering powers of Echelon […]. The journalist, who has spent much of his life investigating Echelon, has offered two alleged instances of US snooping in the 1990s, which he says followed the newly-elected Clinton administration's policy of «aggressive advocacy» for US firms bidding for foreign contracts. The first came from a Baltimore Sun report which said the European consortium Airbus lost a $6bn contract with Saudi Arabia after NSA found Airbus officials were offering kickbacks to a Saudi official. The paper said

władzami państw uczestniczących w systemie Echelon, nie kwestionowane[24]; wyraźnie podkreśla się przy tym udział agend amerykańskiego rządu w wykorzystywaniu Echelonu w interesie amerykańskich korporacji przemysłowych[25]. Wskazywano na konkretne polecenia, np. prezydenta B. Clintona, który nakazał National Security Agency wykorzystać „super-tajny program nadzoru Echelon" do monitorowania osobistych rozmów telefonicznych i prywatnej poczty pracowników, którzy pracowali dla zagranicznych firm, w dążeniu do zwiększenia amerykańskiego handlu[26]. Niektórzy prominentni urzędnicy CIA, w tym także jego byli dyrektorzy, z ostentacją przyznawali wykorzystywanie Echelonu do szpiegostwa przemysłowego „wśród przyjaciół"[27] po to, by amerykańskie korporacje mogły uzyskać przewagę nad europejskimi konkurentami[28].

---

the agency «lifted all the faxes and phone-calls between Airbus, the Saudi national airline and the Saudi Government» to gain this information. Mr Campbell also alleges that the US firm Raytheon used information picked up from NSA snooping to secure a $1.4bn contract to supply a radar system to Brazil instead of France's Thomson-CSF […]. The US strenuously denies passing on commercial information to individual US firms, saying that there are clear laws to prevent it. But former CIA director James Woolsey, in an article in March for the Wall Street Journal, acknowledged that the US did conduct economic espionage against its European allies, though he did not specify if Echelon was involved. However, he poured scorn on the Campbell allegations that the US was using its technological edge to gain unfair advantage in international business. «We have spied on you because you bribe», the ex-CIA boss wrote. «(European) products are often more costly, less technically advanced or both, than (their) American competitors'. As a result (they) bribe a lot». But that is not an argument that will have much influence among concerned European countries, which are currently investigating the threat or otherwise posed by the world's most powerful intelligence-gathering machine"; www.news.bbc.co.uk/2/hi/europe/820758.stm.

[24] Zob. np. www.world-information.org/wio/infostructure/100437611746/100438658866.

[25] Zob. np. www.bibliotecapleyades.net/ciencia/echelon/echelon_2.htm.

[26] *Clinton Used NSA for Economic Espionage*, www.archive.newsmax.com/archives/ic/2005/12/19/114807.shtml ("In 2000, former Clinton CIA director James Woolsey set off a firestorm of protest in Europe when he told the French newspaper Le Figaro that he was ordered by Clinton in 1993 to transform Echelon into a tool for gathering economic intelligence. «We have a triple and limited objective», the former intelligence chief told the French paper. «To look out for companies which are breaking US or UN sanctions; to trace 'dual' technologies, i.e., for civil and military use, and to track corruption in international business»").

[27] Zob. np. *Ex-CIA-Direktor bestätigt Wirtschaftsspionage mittels Echelon*, www.heise.de/newstikker/meldung/Ex-CIA-Direktor-bestaetigt-Wirtschaftsspionage-mittels-Echelon-20861.html.

[28] Zob. F. Patalong, *Große Ohren: Echelon – Spionage unter Freunden*, www.spiegel.de/netzwelt/web/grosse-ohren-echelon-spionage-unter-freunden-a-71135.html (So erregte sich die in Wien herausgegebene konservative österreichische Zeitung „Die Presse" über die US-Abhöraktion gegen europäische Firmen: „Der Affront ist einzigartig. Da munkelt man seit Jahren über ein US-Abhörsystem in Europa, rätselt, warum europäische Firmen Aufträge an US-Firmen verloren haben, lässt Experten monatelang die Möglichkeit der Existenz eines solchen Abhörsystems untersuchen – und dann schreibt der ehemalige CIA-Direktor in einem Gastkommentar frank und frei: 'Ja, liebe Freunde, wir haben euch ausgehorcht'. Die Lauschangriffe

Przed laty w Australii upubliczniony został skandal dotyczący obrotu informacjami gospodarczymi gromadzonymi przez tamtejsze agendy Echelonu. Terrorystyczne zagrożenie Australii jest tak mało znaczące, zaś zasoby pozyskiwane przez Echelon tak wielkie, że zarządcy tych informacji doszli do roztropnego wniosku, że coś trzeba z takim bogactwem danych zrobić[29]. Zwłaszcza, choć nie tylko w Niemczech, podkreślano obawy związane z wykorzystywaniem Echelonu do szpiegostwa przemysłowego na terenie Europy, zważywszy na bezradność wobec niemożliwego do przeciwstawienia się płynącym stąd zagrożeniom wynikającym z poziomu technologii wykorzystywanej przez kolejne rządy Stanów Zjednoczonych[30]. Nawet w polskim ubogim piśmiennictwie o Echelonie zwracano uwagę, że „Tymczasowy Komitet Parlamentu Europejskiego ds. systemu przechwytującego w specjalnym raporcie stwierdzał, że sieć była i jest wykorzystywana do szpiegostwa ekonomiczne-

dienen einzig dazu, US-Firmen einen Vorteil gegenüber ihren europäischen Konkurrenten zu verschaffen. Das hat nichts mit der in den USA so gern strapazierten 'nationalen Sicherheit' zu tun, sondern ist schlicht und einfach Industriespionage – staatlich sanktioniert und finanziert").

[29] Zob. też: G. Kitney, *Australia drawn into spy scandal*, www.converge.org.nz/pma/sisaus.htm ("Australia is being drawn into a row between the United States and its European allies over claims that an American-controlled Cold War electronic spying network is being used for commercial espionage against European governments and companies. The French Government claims the network – which includes a ground station in Australia – is being used by the US, Britain and their «Anglo-Saxon» partners to eavesdrop on the Europeans, picking up commercially sensitive information […]. Allegations in the French and European parliaments this week said Australia, New Zealand, Britain and Canada all helped the US to gather commercial information from their European allies […]. In his report Mr Campbell listed several specific incidents when he alleged Echelon had been used to win contracts for US firms. The French firm Thomson had lost a radar contract in Brazil and the European Airbus consortium missed a $US6 billion ($9.6 billion) contract to the Boeing Corporation. A German conservative MP in the European Parliament claimed the spying activities had already cost European businesses more than $US20 billion in lost contracts […]. After presenting his report to the parliament's Committee for Justice and Home Affairs, Mr Campbell urged the EU to take action to protect members against the unwanted interception of communications, insisting the eavesdropping violated human rights. He also claimed national security agencies were using major US corporations to help with the interception of data, and named Microsoft, IBM and a certain «large American microchip maker». The French Justice Minister warned French businesses to be particularly vigilant to the possibility of eavesdropping on sensitive commercial communications, saying they should never carry vital information"); *ECHELON – MUOS. KOJARENA Spy Base Echelon Station Mobile User Objective System (MUOS) Ground Station Geraldton, West Australia*, www.thelivingmoon.com/45jack_files/03files/ECHELON_Geraldton.html, gdzie niemały zbiór linków dotyczących tego zagadnienia.

[30] Zob. np. S. Schmitt, *Streit um Echelon Wirtschaftsspionage*, www.sueddeutsche.de/digital/streit-um-echelon-wirtschaftsspionage-1.101852; Ch. Radic, *Abhörsystem Echelon Verschlusssache Wirtschaftsspionage Der Fall „Echelon": Betreiben die USA Wirtschaftsspionage zum Schaden Europas?*, http://www.monitor.at/index.cfm/storyid/3842_Abhoersystem_Echelon-Verschlusssache_Wirtschaftsspionage; *US to close Echelon spy stadion*, www.news.bbc.co.uk/2/hi/europe/1365156.stm.

go, faworyzującego firmy krajów członkowskich (głównie z USA i Wielkiej Brytanii)"[31].

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 spowity 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, zaś takie 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. I to także jest znaczącym powodem, dla którego zagrożenia związane z Echelonem nie mogą być bagatelizowane przez Sejm i polski rząd.

Nie tylko cywilny delikt, także przestępstwo

Praktyki Echelonu można również rozpatrywać pod kątem cyberprzestępczości[32] uregulowanej w prawie karnym. W ramach cyberprzestępstwa można wyróżnić między innymi przestępstwa przeciwko poufności, integralności i dostępności danych i systemów informatycznych, tzw. przestępstwa *stricte* komputerowe oraz przestępstwa instrumentalnego wykorzystania elektronicznych sieci informatycznych i systemów informatycznych do naruszania dóbr prawnych chronionych przez prawo karne. Obecnie jedynym aktem prawa międzynarodowego karnego dotyczącym współpracy międzynarodowej w zakresie ścigania cyberprzestępstw jest podpisana 23 listopada 2001 roku w Bukareszcie pod auspicjami Rady Europy konwencja o zwalczaniu cyberprzestępczości (ETS/STE No. 185)[33].

---

[31] *Jak podsłuchuje nas Ameryka – czy legendarna sieć inwigilująca Echelon naprawdę istnieje?*, www.gazetaprawna.pl/wiadomosci/artykuly/515894,jak_podsluchuje_nas_ameryka_czy_legendarna_siec_inwigilujaca_echelon_naprawde_istnieje.html.

[32] Jak zauważa M. Siwicki, ogólnie można stwierdzić, że grupa czynów określana jako cyberprzestępstwa polega na posługiwaniu się systemami lub sieciami informatycznymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne (*Naruszenie tajemnicy informacji*, EP 2012, nr 6, s. 42).

[33] Konwencję przyjęto i weszła ona w życie w 2004 r. Została podpisana przez wiele krajów, m.in. Stany Zjednoczone i inne państwa pozaeuropejskie, a także wszystkie państwa członkowskie UE. Zawiera m.in. wspólne definicje różnych rodzajów przestępstw komputerowych oraz

Na gruncie prawa polskiego założeniom konwencji odpowiada art. 267 § 1–4 k.k. realizujący zarazem konstytucyjną gwarancję ochrony prywatności i tajemnicy komunikowania się, wyrażoną w art. 49 i 51 ust. 1 i 2 Konstytucji RP. „Według stanowiska doktryny przedmiotem ochrony art. 267 k.k. przepisu jest poufność informacji, prawo do dysponowania informacją z wyłączeniem innych osób, a także bezpieczeństwo jej przekazywania. Przepis chroni także sferę prywatności" [34].

Artykuł 267 § 1 k.k. chroni dostęp do informacji nieprzeznaczonej dla sprawcy. Przy czym dotyczy to wszelkich informacji zawartych w zamkniętym piśmie, przekazywanych za pomocą sieci telekomunikacyjnej, zabezpieczonej elektronicznie, magnetycznie, informatycznie lub w inny szczególny sposób. W myśl tego przepisu penalizacji podlega zatem uzyskanie dostępu do informacji nieprzeznaczonej dla sprawcy, nieadresowanej do niego, jeśli nastąpiło to między innymi poprzez uzyskanie bez uprawnienia dostępu do całości lub części systemu informatycznego. Warunkiem koniecznym do dokonania przestępstwa jest naruszenie lub ominięcie zabezpieczeń chroniących informacje oraz uzyskanie dostępu do informacji. Warto zauważyć, że przestępstwem z art. 267 § 1 k.k. jest już samo otwarcie zamkniętego pisma niezależnie od tego, czy sprawca zapoznał się z jego treścią, czy jedynie przejął nad nim władztwo. Sprawcy należy więc udowodnić jedynie zamiar uzyskania dostępu do informacji, a nie zaznajomienie się z jej treścią. Ustawodawca penalizuje przecież uzyskanie informacji, a nie zdobycie władztwa nad nośnikiem. Przestępstwo z art. 267 § 1 ma charakter materialny, jest to również przestępstwo umyślne. Ze względu na istotę czynności wykonawczych przestępstwo to możliwe jest do popełnienia wyłącznie z zamiarem bezpośrednim, trudno bowiem wyobrazić sobie, by sprawca nie miał pełnej świadomości faktu, że uzyskuje informacje dla niego nieprzeznaczone. Zakres penalizacji został również poszerzony o nieuprawnione uzyskanie dostępu do całości lub części systemu informatycznego[35]. Z kolei art. 267 § 3 k.k. poszerza ochronę

ustanawia podstawy funkcjonowania współpracy sądowej między państwami sygnatariuszami Konwencji.

[34] Jak zauważa B. Kunicka-Michalska, bezpośrednim przedmiotem ochrony art. 267 k.k. jest interes, który ma dysponent informacji do zachowania jej w dyskrecji przed osobami nieuprawnionymi (w: *Kodeks karny. Część szczególna*, t. 2, red. A. Wąsek, R. Zawłocki, *Komentarz do artykułów 222–316*, Warszawa 2010, s. 691).

[35] W polskim ustawodawstwie nie znajdzie się jednak definicji pojęcia „system informatyczny". Wyjaśnia je natomiast konwencja o zwalczaniu cyberprzestępczości, według której system ten oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych. Podobnie według art. 1 decyzji ramowej 2005/222/WSiSW w sprawie ataków na systemy informatyczne (Dz.Urz. UE z 2005, L 69, s. 67), „system informatyczny" oznacza wszelkie urządzenia lub grupę połączonych lub powiązanych urządzeń, z których jedno lub więcej,

i sankcjonuje działania polegające na nieuprawnionym uzyskaniu informacji z użyciem urządzeń podsłuchowych, wizualnych czy oprogramowania, co ma na celu ochronę prywatności człowieka przed różnymi formami inwigilacji, przy czym aby zrealizować znamiona strony podmiotowej, niezbędne jest bezprawne działanie w celu uzyskania informacji. Trzeba jednak zauważyć, że sprawstwo i winę według kodeksu karnego można przypisać wyłącznie osobie fizycznej. Tym samym z uwagi na specyfikację działania systemu Echelon w zasadzie niemożliwe okazuje się pociągnięcie określonej osoby do odpowiedzialności karnej z tytułu popełnionych czynów zabronionych stypizowanych w wymienionych wyżej przepisach ustawy. Pozostaje wyłącznie do rozważenia możliwość pociągnięcia do odpowiedzialności aktualnych przedstawicieli państw sygnatariuszy porozumienia UKUSA. Jednak i ta możliwość zdaje się być iluzoryczna. Przytoczone okoliczności prowadzą do wniosku, że również prawo karne nie jest właściwym instrumentem, który mógłby stawić opór przeciwko działaniu systemu Echelon. Założenia polskiego kodeksu karnego nie przystają więc do wciąż zmieniającej się i zaskakującej nas nowymi osiągnięciami techniki rzeczywistości.

Postawa wobec Echelonu skłania do daleko idących refleksji

Wygląda więc na to, że *de lega lata* instrumentarium prawne mogące służyć do obrony przed zagrożeniami wynikającymi z istnienia Echelonu, jakie mają do dyspozycji obywatele polscy, jest żadne. To inspiracja do skądinąd frapującej refleksji nie tylko badawczej. Dobro tajemnicy komunikowania się – chronione przepisami Konstytucji RP i obowiązujących w Polsce innych ustaw przed naruszeniami, które prawie zawsze mają charakter sporadyczny – w ogóle nie może być w Polsce chronione przed naruszeniami globalnymi i totalnymi. W dyskusji o wartości konstytucyjnych gwarancji to chyba znaczący przyczynek o ich możliwej iluzji, nawet nie o połowiczności.

Z perspektywy politycznej Echelon inspiruje do powściągliwej oceny kategorii tak zwanych sojuszy. Otóż, w sferze szpiegostwa przemysłowego nie obowiązują żadne sojusze, szpieguje się i okrada z bezcennych nierzadko informacji także najlepszych przyjaciół. Może kiedyś ci, którzy o tym marzą, doczekają prawa do bezwizowego podróżowania do Stanów Zjednoczonych, prawdopodobieństwo jednak, że Rzeczpospolita zostanie „skreślona" z listy obiektów kontrolowanych przez Echelon jest żadne.

---

zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania.

Mimo minorowego obrazu sytuacji nie można zwolnić Sejmu, ani polskiego rządu z obowiązku troski o ochronę obywateli, w tym także polskich przedsiębiorców przed zagrożeniami i szkodami, które może im w przyszłości wyrządzić Echelon. Nie do końca bowiem się wydaje, że niemożliwe jest podejmowanie prób także zmian legislacyjnych, chociażby takich, które mogłyby być choćby szczątkowym remedium na zagrożenia związane z Echelonem, np. poprzez umożliwienie oskarżania czy pozywania CIA czy pokrewnych agend przed polskim sądem. Tym, którzy nie bez racji stwierdzą, że takie przedsięwzięcia są skazane na niepowodzenia, przede wszystkim nie mogą być skutecznie egzekwowane, można odpowiedzieć, iż możliwa doniosłość wyroków choćby tylko na terytorium państw należących do Unii Europejskiej mogłaby się okazać sankcją w pewien sposób dolegliwą. A jeśliby nawet owe konsekwencje pominąć, to przecież takie werdykty byłyby również doniosłym publicznie ostrzeżeniem przed działaniami nie tylko Echelonu.

Abstract

Orwell in reality i.e. Echelon system from the view of Polish law

„Freedom and privacy of communication is guaranteed. The restrictions may be imposed only in cases specified in the Act and in the manner specified therein." This pronounced and clear declaration, being not only a legal guarantee is included in paragraph 49 of Constitution of the Republic of Poland. We look at it from the hindsight, which was created by a system of global invigilation of communication, not only electronic one, called Echelon. It was widely known before Edward Snowden was heard in Hong Kong. Echelon was talked, written about and discussed not only in European Parliament but also at other formal forum. Yet, in our country this phenomenon did not arouse much interest either of lawyers, ministers, senators, government or politicians. There is probably the first attempt of assessing the consequences of Echelon from the view of Polish law. We limit ourselves intentionally to the point which was reachable for everyone before Snowden. We believe that it has a particular meaning: it illustrates that in our country there is a dramatic implementation of the constitutional right to democratic rule of law. It makes us realize where we live and what we can.

Key words: Constitution of the Republic of Poland, privacy of communication, privacy of correspondence, protection of personal rights, Echelon