mgr Krzysztof Pyka

„Efektywność ochrony prawa do prywatności w świetle stanu prawnego i praktyki dotyczącej poufności komunikacji telefonicznej”.

Spis treści:

1. Prawo do prywatności w systemie praw człowieka.

Prawa człowieka są to powszechne prawa moralne o charakterze podstawowym, przynależne każdej jednostce w jej kontaktach z państwem. Pojęcie praw człowieka opiera się na trzech tezach: po pierwsze, że każda władza jest ograniczona; po drugie, że każda jednostka posiada sferę autonomii, do której nie ma dostępu żadna władza; i po trzecie, że każda jednostka może się domagać od państwa ochrony jej praw (Osiatyński 1998). Według innej definicji: Prawa człowieka - prawa pierwotne w stosunku do państwa, przysługujące każdemu człowiekowi, bez względu na jego przynależność państwową czy pozycję w społeczeństwie. Taki sens tego pojęcia można wyprowadzić z wielu aktów prawnych. Przykładem może być francuska Deklaracja praw człowieka i obywatela z 1789 r., w której stanowi się o "naturalnych, niezbywalnych, świętych prawach człowieka", czy niektóre akty prawa międzynarodowego (...). Sam termin "prawa człowieka" powstał w okresie oświecenia. Po raz pierwszy w akcie prawnym użyty został w Bill of rights Wirginii z 1776 r. i już wówczas obejmował prawa pierwotne w stosunku do państwa i społeczeństwa (Słownik wiedzy o Sejmie 2001). Prawo do prywatności - right to privacy zaliczane jest do podstawowych praw i wolności obywatela, jest to prawo do bycia i pozostawania w spokoju. Jako uprawnienie do wyłączności, odrębności, tajemnicy i samotności zostało ono scharakteryzowane przez amerykańskich profesorów prawa: V. Brandeissa i E. Warrena - właśnie w Stanach Zjednoczonych, pod koniec XIX wieku, w wyniku rozwoju środków masowego przekazu prawo zaistniało po raz pierwszy. Nie sposób podać wyczerpującej listy działań, które mogą być uznane za naruszenie prawa do prywatności, trudno też o takie wyliczenie w zakresie dóbr, które są w ten sposób chronione. Do najczęściej wymienianych można zaliczyć: prawo do poszanowania życia rodzinnego, wolność seksualną (homoseksualizm, transseksualizm), nienaruszalność

mieszkania oraz tajemnicę korespondencji (i innych form przekazywania informacji), z prawem do prywatności związana jest także kwestia ochrony danych osobowych (Brandeis, Warren 1890). Współczesny katalog dziedzin prawa obejmujących poruszana tu tematykę obejmuje m.in.: health privacy laws (prawo do tajemnicy medycznej); financial privacy laws (prawo do ochrony informacji finansowej), online privacy laws (prawo do ochrony prywatności w internecie), communication privacy laws (prawo do ochrony tejemnicy korespondencji, information privacy laws (prawo do ochrony danych osobowych), privacy in one's home (prawo do ochrony miru domowego) (California Office of Privacy Protection 2011).

Podstawowym aktem normatywnym regulującym ochronę prawa do prywatności w stosunkach międzynarodowych jest art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych w brzmieniu:

1. Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię.

2. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami.;

oraz art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, w brzmieniu:

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 innych osób.

Przepis art. 8, ust. 1, Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności należy rozpatrywać w sensie dyspozycji (pozytywnym) i wykluczenia (negatywnym). Władze zobowiązane są zapewnić ochronę prywatności przed naruszeniami (zwłaszcza na płaszczyźnie prawa karnego procesowego i wykonawczego), oraz do powstrzymania się od ingerencji w sferę prywatności, w szczególności jest to zakaz penalizacji zachowań z tej sfery (co ma podstawowe znaczenie w płaszczyźnie prawa karnego materialnego). W przypadku gdy przepisy szczegółowe prawa krajowego dopuszczają naruszenia prawa do prywatności, uznanie takiej ingerencji za dopuszczalną wymaga zgodnie z ust. 2 art. 8 wystąpienia łącznie trzech przesłanek: 1) ingerencja powinna mieć swoje oparcie w ustawie, 2) dopuszczalna jest tylko i wyłącznie w celu ochrony dóbr wymienionych w art. 8 ust. 2, 3) musi być ona konieczna w demokratycznym społeczeństwie ze względu na ochronę tych dóbr. Przyjmując za podstawę wykładnię teleologiczną należy przyjąć, że podlegające ochronie wolności i prawa, aby można było z nich korzystać, muszą podlegać

ograniczeniom. W społeczeństwie funkcjonują nie tylko indywidualne dobra jego członków, ale także dobra wspólne, powszechne, takie jak bezpieczeństwo, porządek, środowisko – na ich straży stoi m. in. prawo karne. Na gruncie prawa krajowego zasadę ogólną poszanowania wolności człowieka wyraża artykuł 31 Konstytucji RP:

1. Wolność człowieka podlega ochronie prawnej.

2. Każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje.

3. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Wyrazem normatywnego ujęcia prawa do prywatności w ścisłym znaczeniu jest natomiast art. 47, w brzmieniu: Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym, artykuł 49 mówi o wolności i tajemnicy komunikowania się, a artykuł 50 ma na celu ochronę nienaruszalności mieszkania. Wszystkie dobra składające się na prawo do prywatności mogą ulec ograniczeniu. Podmiotem uprawnionym do dokonania takiego ograniczenia są organy wykonawcze i sądownicze państwa, może ono nastąpić tylko i wyłącznie na podstawie ustawy i w sposób w niej określony.

2. Wybrane regulacje prawne dotyczące kontroli operacyjnej w kontekście naruszeń prawa do prywatności.

Jako jedno z podstawowych praw człowieka, a w sensie funkcjonalnym także podstawowa gwarancja utrzymania demokratycznego ładu społecznego prawo człowieka do prywatności podlega kontroli instytucjonalnej. Głównym organem Europejskiej Konwencji Praw Człowieka (EKPC) są: Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu i Komisarz Praw Człowieka Rady Europy (jest to niesądowa instytucja, która ma za zadanie wspierać promocję praw człowieka w edukacji, wspomagać ombudsmanów, ustalać braki w prawodawstwie, dostarczać informacji w zakresie praw człowieka). W orzecznictwie organów EKPC przyjęto, że w skład podstawowych praw jednostki podlegających ochronie w ramach prawa do prywatności wchodzi: zapobieganie atakom na integralność fizyczną i psychiczną jednostki oraz jej wolność, zarówno w sferze moralnej, jak i intelektualnej, atakom na jej honor i dobre imię, nadużywaniem nazwiska i tożsamości, szpiegowaniem, obserwacją lub różnymi formami nękania oraz ujawnieniem objętych tajemnicą informacji osobowych. W świetle orzeczeń organów EKPC państwo powinno

powstrzymywać się od ingerencji w sferę wolności zagwarantowanych przez art. 8 EKPC, ma także obowiązek stawać w obronie obywatela, którego prawa naruszono. W obu tych przypadkach ponownie kładzie się nacisk na prawo krajowe i jego regulacje, których celem jest wykonanie zobowiązań międzynarodowych (Czuj 2005). Na poziomie ustawodawstwa krajowego podstawowe znaczenie będzie miał art. 47 Konstytucji RP.

Polskie prawo karne procesowe (art.237-242 k.p.k.) dopuszcza możliwość "kontroli i utrwalania treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa". Przepisy te dotyczą także kontroli "treści przekazów informacji innych niż rozmowy telefoniczne". Oznacza to, że "podgląd" m.in. treści faksu lub danych wysłanych pocztą elektroniczną czy kontrola tradycyjnej korespondencji wymaga także zgody sądu. Postanowienie w tej sprawie wydawane jest przez sąd na wniosek prokuratora (art.237, §.1. k.p.k.). Na postanowienie w tej kwestii przysługuje zażalenie rozpoznawane przez sąd. Ogłoszenie postanowienia osobie, której ono dotyczy, może być odroczone na czas niezbędny ze względu na dobro sprawy. Wyjątkiem jest tu przypadek "nie cierpiący zwłoki" - podsłuch (podgląd) może zarządzić wtedy prokurator; zobowiązany jest on do uzyskania w ciągu 5 dni zatwierdzenia tego środka postanowieniem sądu. Jeśli sąd nie zatwierdzi tego, prawo nakazuje zniszczenie utrwalonych zapisów. Należy zwrócić szczegołną uwagę na fakt, iż obowiązujący od 1997r. Kodeks Postępowania Karnego wprowadził ograniczenia co do procesowej kontroli rozmów telefonicznych. Środek ten może być zastosowany jeśli dotyczy on najpoważniejszych przestępstw (lub obawy ich popełnienia). Art.237, §.3 k.p.k. wylicza 16 kategorii takich przestępstw (od zabójstwa do użycia przemocy lub użycia przemocy lub groźby bezprawnej w związku z postępowaniem karnym). Środki techniczne mogą być wreszcie zastosowane na okres 3 miesięcy z możliwością przedłużenia na okres najwyżej dalszych 3 miesięcy. Stosowanie tych środków ograniczono podmiotowo (choć szeroko) do osoby podejrzanego, oskarżonego, pokrzywdzonego lub innej osoby, z którą może kontaktować się oskarżony albo która może mieć związek ze sprawcą lub z grożącym przestępstwem. Regulacja ta jest postępem w stosunku do poprzednio obowiązującej, poddanie stosowania środków technicznych kontroli sądowej jest podstawowym warunkiem cywilizowanego procesu karnego.

Ustawa o policji przewiduje natomiast możliwość "kontroli korespondencji oraz stosowania środków technicznych umożliwiających uzyskiwanie w sposób tajny informacji oraz utrwalanie dowodów" przy wykonywaniu czynności operacyjno-rozpoznawczych w zakresie nie objętym przepisami k.p.k. Chodzi tu o możliwość zastosowania "środków technicznych" jeszcze przed formalnym wszczęciem postępowania przygotowawczego. Są to tzw. środki techniki operacyjnej, które policja stosuje w celu zapobieżenia lub wykrycia przestępstw umyślnych, ściganych z oskarżenia publicznego, w wypadku powzięcia uzasadnionych poejrzeń co do możliwości

popełnienia czynów karalnych: przeciwko życiu, spowodowania ciężkiego uszkodzenia ciała lub ciężkiego rozstroju zdrowia, pozbawienia człowieka wolności w celu wymuszenia okupu lub zachowania określonego w art. 211 k.k. (wymuszenie rozbójnicze), przeciwko bezpieczeństwu powszechnemu - sprowadzenia zdarzenia powszechnie niebezpiecznego, sprowadzenia pożaru lub jego niebezpieczeństwa, sprowadzenia niebezpieczeństwa powszechnego, nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją materiałami wybuchowymi, środkami odurzającymi lub psychotropowymi oraz materiałami jądrowymi i promieniotwórczymi, gospodarczych, powodujących znaczną szkodę majątkową, przeciwko mieniu znacznej wartości lub skarbowych, polegających na uszczupleniu podatku lub innej należności Skarbu Państwa w znacznej wartości, przyjmowania lub wręczania korzyści majątkowej w wielkich rozmiarach w związku z pełnioną funkcją publiczną lub związaną ze szczególną odpowiedzialnością, podrabiania, przerabiania pieniędzy i papierów wartościowych oraz puszczania ich w obieg, określonych w art. 276 k.k. (udział w zorganizowanej grupie przestępczej i/lub zbrojnej), ściganych na mocy umów i porozumień międzynarodowych (art. 19 ust. 1 ustawy o policji). Zastosowanie tych środków oraz kontrolę korespondencji zarządza na czas określony Minister Spraw Wewnętrznych i Administracji (dalej: Minister SWiA) po uzyskaniu pisemnej zgody Prokuratora Generalnego. W przypadkach nie cierpiących zwłoki, gdy mogłoby to spowodować utratę informacji lub zatarcie dowodów przestępstwa, Minister SWiA może zarządzić stosowanie owych środków i jednocześnie wystąpić do Prokuratora Generalnego o wyrażenie na to zgody. Jeśli ten ostatni w ciągu 24 godzin zgody nie udzieli, Minister SWiA nakazuje natychmiastowe wstrzymanie kontroli korespondencji lub stosowania środków technicznych i zarządza komisyjne, protokolarne zniszczenie uzyskanych w ten sposób materiałów. Prawo nakazuje wreszcie, by kontrolę korespondencji lub środki techniczne stosować tylko wtedy, gdy inne środki okażą się bezskuteczne albo gdy istnieje wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne do wykrycia przestępstwa, ujawnienia jego sprawców i ujawnienia oraz zabezpieczenia dowodów (art. 19 ust. 4 ustawy o policji). Cytowane przepisy nie spełniają standardów art. 8 EKPC. Ustawa zbyt szeroko zakreśla możliwości stosowania podsłuchu. Ustawa o policji używa nieprecyzyjnego określenia "środki techniczne". Wynalezienie nowego, "środka technicznego" nie pociąga za sobą konieczności zmiany ustawy, tylko instrukcji wewnętrznych danej służby. Zgodnie ze standardami państwa demokratycznego podejmowanie decyzji o zastosowaniu "technik operacyjnych" powinno w całości spoczywać w gestii sądów powszechnych. Obecnie o stosowaniu technik operacyjnych decyduje dwóch ministrów (bez kontroli jakiegokolwiek niezależnego od władzy wykonawczej organu). Nie chodzi o to, że mogą oni być kolegami partyjnymi, którzy być może zechcą realizować doraźne partykularne interesy - idzie o wyeliminowanie takiej możliwości. Niezawisły sąd - zwłaszcza przy podejmowaniu decyzji skomplikowanych - jest w Europie standardem

(Kremplewski, Skowron 1998).

Kwestia realności poddania środków techniki operacyjnej faktycznej kontroli sądowej jest osobnym zagadnieniem którym zajmiemy się w dalszej części niniejszego opracowania w kontekście krótkiego omówienia technicznych możliwości niektórych z ich rodzajów, tymczasem poruszyć należy kolejne bezpośrednio związane z tokiem wywodu zagadnienie prawne: w interesie ochrony podstawowych zasad, na których jest oparte, państwo prawa powinno bronić policjantów sprzeciwiających się bezprawiu oraz surowo karać tych, którzy wydają rozkazy sprzeczne z obowiązującym prawem. Wykorzystywanie policji do działań nielegalnych skłoniło organizacje międzynarodowe do opracowania norm regulujących powyższe kwestie (Czapska, Wójcikiewicz 1998). Postanowienia Deklaracji o Policji z 1979r. Nakazują one policjantowi nieposłuszeństwo lub odmowę wykonania bezprawnego rozkazu. "(...) Funkcjonariusz policji jest zobowiązany do nieposłuszeństwa lub niewypełnienia rozkazu czy polecenia, jeśli bezprawność tego rozkazu jest lub powinna być mu znana" (cz. A. pkt 3 Deklaracji). Deklaracja nakazuje "powstrzymać się od wykonania jakiegokolwiek rozkazu, którego bezprawność jest lub powinna być mu znana". Wreszcie pkt 7 cz. A Deklaracji zakazuje podejmowania jakichkolwiek działań karnych bądź dyscyplinarnych wobec funkcjonariusza policji, który odmówi wykonania niezgodnego z prawem rozkazu. Zagadnienia te reguluje art. 58 ust. 1 ustawy o Policji. Nakłada on na policjanta m.in. obowiązek odmowy wykonania rozkazu lub polecenia przełożonego, a także polecenia prokuratora, organu administracji państwowej lub samorządu terytorialnego, jeśli wykonanie rozkazu lub polecenia łączyłoby się z popełnieniem przestępstwa. O odmowie wykonania rozkazu lub polecenia, policjant powinien zameldować Komendantowi Głównemu Policji z pominięciem drogi służbowej. Kodeks Karny z 1997 r. wzmacnia prewencyjne działanie obowiązku odmowy wykonania przestępczego "rozkazu". Przepisy wprowadzające Kodeks Karny wprowadziły do ustawy o policji art. 141a nakazujący odpowiednie stosowanie art. 115 § 18 Kodeksu (definicja rozkazu) oraz art. 318 i art. 344 do funkcjonariuszy policji. Art. 344 K. k. stwierdza, że nie popełnia przestępstwa odmowy wykonania rozkazu żołnierz (w naszym przypadku policjant), który odmawia wykonania rozkazu polecającego popełnienie przestępstwa albo go nie wykonuje. Sąd może zastosować nadzwyczajne złagodzenie kary lub odstąpić od jej wymierzenia jeśli policjant wykonując taki rozkaz, w celu zmniejszenia szkodliwości czynu, wykonał go niezgodnie z jego treścią. Obowiązek nieposłuszeństwa funkcjonariuszy policji wobec nakazanego im bezprawia stanowi jedną z ustawowych gwarancji państwa prawa. Chroni on obywateli przed przestępczymi rozkazami przełożonych. Podporządkowanie się przełożonym, a nie wyłącznie prawu, jest sprzeniewierzeniem się istocie obowiązków zawodowych policjanta. Tak stanowi prawo. Jak jednak wyglądają faktyczne możliwości jego egzekucji, o tym stanowią nie tylko uwarunkowania ustanowione treścią przepisów ale przede wszystkim uwarunkowania instytucjonalne i faktyczne

możliwości kontroli technicznej niektórych środków używanych do prowadzenia działań operacyjno-rozpoznawczych.

3. Niektóre aspekty technicznych możliwości kontroli operacyjnej w sieciach GSM.

Bezpieczeństwo łączności GSM opiera się na tym, że sygnał przesyłany pomiędzy stacją bazową, a telefonem komórkowym jest kodowany. W stacji bazowej jest on rozkodowywany i następnie przesyłany do dalszej części sieci. Kodowanie w części powietrznej zostało złamane już w 1998 roku. Algorytmy wykorzystywane do kodowania to: A5/0, A5/2 oraz A5/1. Klucz na podstawie którego szyfrowana jest rozmowa w niektórych sieciach jest taki sam dla kilku rozmów, co znacznie ułatwia podsłuch. Numer IMSI identyfikujący użytkownika sieci oraz informacja o lokalizacji jest przesyłana w jawnej postaci, co pozwala na zlokalizowanie telefonu komórkowego, model bezpieczeństwa GSM bazuje na tajności klucza identyfikacyjnego Ki (Sutton 2004). Ujawnienie tego klucza oznacza dla konkretnego abonenta złamanie podstawowych zabezpieczeń systemowych (a więc możliwość nieuprawnionego dostępu do przypisanych mu usług, jak również zniesienie poufności informacji). Znajomość klucza Ki daje potencjalnemu włamywaczowi nie tylko pełny dostęp do połączeń (włączając w to deszyfrowanie informacji), ale pozwala też podszywać się pod legalnego abonenta, np. przeprowadzając rozmowy na jego koszt. Podsłuchiwanie rozmów prowadzonych przez telefony GSM jest możliwe w następujących wariantach działań, poza rejestracją w centrali operatora [co wymaga jedynie wydania polecenie kontrolerowi stacji bazowych (BSC)]:

- włączony jest tryb braku szyfrowania transmisji, topologia sieci GSM przewiduje możliwość nadawania części transmisji przy wyłączonym szyfrowaniu, co w praktyce jest realizowane na polecenie kontrolera stacji bazowej (BSC) w momencie w którym obciążenie sieci transmisją wymusza jego zastosowanie z uwagi na konieczność zapewnienia odpowiedniej przepustowości, najczęstszym przypadkiem są momenty w których w danym obszarze sieci jest prowadzonych znacznie więcej rozmów niż przeciętnie, standardowym przykładem jest noc sylwestrowa gdy sieć przeciążają tysiące sms-ów z życzeniami, jak łatwo się jednak domyślić graniczna przepustowość sieci jest projektowana i dostosowywana do przeciętnego ruchu z pobudek ekonomicznych, sytuacja taka występuje więc w praktyce o wiele częściej,
- wykorzystanie IMSI catcher do włączenia w telefonie klienta trybu nieszyfrowanego w sytuacji gdy normalna transmisja przebiegałaby w trybie szyfrowanym, lub do pełnego MITM (ataku typu „man in tehe middle”), w którym atakujący przeszyfrowuje dane otrzymane od klienta i przesyła go do oryginalnego BTS (stacja bazowa nadawczo-

odbiorcza), mając dostęp do treści komunikacji,

- pasywne deszyfrowanie transmisji przy pomocy danych udostępnionych przez operatora lub chwilowego dostępu do karty abonenta,
- pasywne deszyfrowanie transmisji bez wiedzy operatora,

W zakresie interesującym dla niniejszej pracy istotne są przypadki użycia urządzeń klasy IMSI Catcher. Część urządzeń typu IMSI Catcher dostępnych na rynku umożliwia pasywne podsłuchiwanie transmisji GSM w przypadku gdy stosowany jest brak szyfrowania lub algorytm A5/2 - osłabiona wersja szyfru (Daehyun Strobel, Bochum, 2007) lub gdy możliwa jest współpraca z operatorem. Ze względu na brak uwierzytelnienia sieci w stosunku do telefonu w sieci GSM możliwe są ataki man in the middle (MITM), polegające na umieszczeniu w pobliżu docelowego abonenta urządzenia spełniającego rolę fałszywej stacji bazowej (IMSI Catcher). W istocie jest to urządzenie diagnostyczne, służące do symulowania stacji bazowej przy testowaniu telefonów komórkowych. IMSI Catcher (użyty przez włamywacza) może udawać przed telefonem stację bazową, a przed inną stacją bazową może udawać telefon. Za pomocą tego urządzenia możliwe jest wyłączenie szyfrowania (poprzez ustanowienie wersji A5/0) i zastosowanie pasywnego podsłuchiwania rozmów. Pierwsze urządzenie tego typu zostało zaprezentowane publicznie przez firmę Rohde & Schwarz (GA 090) w 1996 roku i obecnie są one dostępne na rynku od wielu producentów (Rhode & Schwarz, Endoacustica, Global Security Solutions, Shoghi). Oferowana przez nie funkcjonalność określana jest jako aktywne przechwytywanie połączeń GSM (GSM interception), zastosowane algorytmy kryptograficzne są słabe - dlatego że miały być słabe (Krysik 2011). Przy ich projektowaniu musiano brać pod uwagę interes służb specjalnych. Zastosowano znany i ogólnie niepochwalany sposób na zachowanie bezpieczeństwa - security through obscurity, klucze sesyjne Kc mają 64 bity, ale algorytmy generujące te klucze zerują 10 ostatnich bitów skracając 1024-krotnie atak brute force, telefon abonenta uwierzytelnia się sieci GSM, ale sieć GSM nie uwierzytelnia się abonentowi. Ta dziura w architekturze bezpieczeństwa otwiera drogę do ataków. IMSI Catchery korzystają właśnie z tej dziury by podszywać się pod stacje bazowe i przechwytywać rozmowy każdego, kto się połączy z takim udawanym BTS-em. W latach osiemdziesiątych był duży rozłam między państwami NATO, dotyczący tego czy używać silnej czy słabej kryptografii do zabezpieczania rozmów w cyfrowej telefonii komórkowej. Według Rossa Andersona wygrał projekt Francuski i pomysł, by silnej kryptografii jednak nie stosować (Anderson 2005). Ujawniono wiele udowodnionych teoretycznie dziur bezpieczeństwa w algorytmach kryptograficznych GSM-u (Krysik 2011). IMSI Catcher widzi wszystkie telefony w swoim zasięgu, należące do sieci, za którą się podaje, a które wykrywają, że jego sygnał jest mocniejszy, niż prawdziwej stacji bazowej, zgłaszają się do niego. W ten sposób - na żądanie - podają swoje dane identyfikacyjne wszystkie włączone aparaty danej sieci w pobliżu. Jeśli zastosujemy antenę

kierunkową, możemy sprawdzić np. jakie w danym budynku są aparaty komórkowe, nie zakłócając pracy sąsiednich. Dostępne są wersje przyrządu "walkman", do sprawdzenia wszystkich sieci komórkowych. Wystarczy skierować antenę na "obiekt" i po chwili mamy numery wszystkich jego telefonów, po włączeniu IMSI-Catcher poznaje wszystkie dane abonenta i może teraz sam zapisać się do sieci z tymi danymi. Jeśli ktoś będzie dzwonił do abonenta, centrala wyśle rozmowę do stacji bazowej, a ta - do inwigilatora, który się za niego podaje. A dlaczego podsłuchiwany tego nie widzi? Stacja wywołuje jego rozmowę: podaje numer IMSI abonenta? Aparat jednak tego nie słucha, bo wyłapuje tylko komunikaty "swojej stacji", czyli w tej chwili IMSI Catcher. Analogicznie w wypadku, kiedy abonent zechce gdzieś zadzwonić. Wybiera numer, IMSI Catcher przekazuje go - wraz z danymi abonenta - do stacji bazowej itd. Jedyną przeszkodą jest szyfrowanie między aparatem, a stacją bazową. Prostsza wersja podsłuchu polega na tym, że aparat zgłasza się do IMSI Catchera i chce wywołać jakiś numer, Catcher - z innej karty - przekazuje tę rozmowę do prawdziwej sieci. Na pierwszym etapie, między aparatem i Catcherem, rozmowa nie jest szyfrowana, dalej przebiega według zwyczajnych reguł. W drugą stronę, kiedy ktoś chce zadzwonić na aparat przejęty przez Catchera, komunikacja jest w tej opcji zablokowana. Stosowanie przyrządów typu IMSI-Catcher jest trudno wykrywalne, a ponadto, co potwierdza praktyka i orzecznictwo w Europie i w Polsce; jeżeli nie ma miejsca podsłuch, a jedynie lokalizacja, to - jak wynika z orzecznictwa - nie można mówić o ochronie tajemnicy korespondencji, dopóki jej sensu stricte nie ma. Samo sprawdzanie technicznej możliwości komunikacji - a tym jest ukryte wywołanie aparatu przez IMSI Catcher - nie stanowi w sensie prawa cywilnego komunikacji. Atak ten, teoretycznie nie jest możliwy w sieciach UMTS, gdzie uwierzytelnienie telefonu i BTS jest dwustronne, jednak od 2005 roku znane są teoretyczne podstawy ataku, umożliwiającego przechwycenie w podobny sposób połączeń UMTS przez wykorzystanie funkcji interoperacyjności UTMS z sieciami GSM. Polega on na przeprowadzeniu pełnego MITM przez IMSI Catcher udający stację bazową GSM działającą w trybie kompatybilności z UMTS (Krawczyk 2010). W istocie nabycie urządzeń przeznaczonych do inwigilacji sieci UMTS nie stanowi problemu, jednym z najbardziej znanych sprzedawców jest np. argentyńska firma MAXX Technology Inc.

4. Podsumowanie.

Pozostając w kontekście rozważań socjologicznych zwrócić należy uwagę na zasadniczy rozziew pomiędzy literalnym brzmieniem przepisów i wykładnią teleologiczną ich brzmienia, a faktycznymi możliwościami sprawowania przez jakiekolwiek instytucje sądownicze kontroli skali i faktycznej liczby przypadków naruszeń prawa do prywatności w związku z prowadzeniem kontroli operacyjnej, zwłaszcza na etapie wykrywczym i prewencyjnym. Zwróćmy uwagę na kilka

wniosków nasuwających się z reasumpcji wyżej omówionego materiału:

Publikowane oficjalnie dokumenty mające obrazować skalę stosowania technik podsłuchu rozmów telefonicznych obejmują jedynie dane przekazywane przez instytucje będące bezpośrednio zainteresowane w poszerzeniu możliwości wykonywania swych funkcji ustawowych, a więc w maksymalnym poszerzaniu dostępu do danych wywiadowczych, a nie w jego zawężeniu, instytucji pozostających w tym zakresie, z mocy prawa, poza jakąkolwiek kontrolą sądową.

Praktyka sądowa uniemożliwia przeprowadzenie dowodu na stosowanie zaawansowanych technik podsłuchu. W omówionym powyżej przykładzie wygląda to tak:

- zastosowanie urządzeń klasy IMSI Catcher może zostać stosunkowo łatwo wykryte przy użyciu urządzeń dostępnych w normalnym obrocie cywilnym, wynika to z prostego faktu, że podstawiona stacja BT musi zagłuszyć transmisje normalnego (cywilnego nadajnika) co powoduje rozmaite perturbacje w obrazie połączeń (wahania mocy, liczne niewytłumaczalne normalną specyfikacja sieci przerwy, przekierowania połączeń na nie występujące w specyfikacjach cywilnych stacje bazowe o nieznanych numerach, itp.);
- stwierdzenie tego faktu w postępowaniu sądowym wymaga jednak powołania biegłego z zakresu „techniki operacyjnej”, takiej specjalności jednak nie ma, w praktyce ekspertyzę wykonują specjaliści z zakresu informatyki, co prowadzi do niemożliwości stwierdzenia przestępstwa, przykładem może być sprawa wykrycia tego typu urządzeń n.t. Firmy Targpiast we Wrocławiu (Prokuratura Rejonowa dla Wrocławia Psiego – Pola; sygn. akt: 1Ds 1910/07).

Techniczne możliwości dostępnych na rynku urządzeń klasy IMSI Catcher umożliwiają równoczesny odsłuch do kilkuset pomieszczeń w których znajdują się zaatakowane telefony komórkowe (przechwycenie kontroli nad aparatem umożliwia po prostu włączenie mikrofonu i nawiązanie połączenie bez potrzeby aktywacji dzwonka czy wyświetlacza), nie tylko samo nagrywanie rozmów czy treści wiadomości SMS. Ponieważ jedną z podstawowych informacji jakie przekazuje sieć GSM jest pozycja aparatu telefonicznego (lokalizacja), to nie nastręcza również trudności propagacja poleceń odsłuchu, np. wg zapytania: „włącz odsłuch na wszystkich numerach IMEI które pozostaną zalogowane w obszarze sieci wspólnym z IMEI kontrolowanym, w odległości mniejszej niż 10 metrów, w czasie dłuższym niż x godzin, w okresie y dni”, lub jakiegokolwiek innego zapytania bazodanowego.

W tej sytuacji jedynym, realnie istniejącym instrumentem prawnym i społecznym który może zapewnić realną ochronę prawa do prywatności są unormowania wewnętrzne regulujące normy etyczno-moralne ale także stricte określone przepisami uprawnienia funkcjonariuszy wykonujących czynności operacyjno-rozpoznawcze do odmowy wykonania rozkazów bezprawnych. Realne wnioski płynące z analizy faktów skłaniają zaś do przekonania, że

wewnętrzna kultura organizacyjna, poziom kompetencji społecznych funkcjonariuszy i wpojenie odpowiednich wartości, zwłaszcza w korpusie oficerskim, jest jedynym czynnikiem który w obecnych realiach prawnych i technicznych (a więc faktycznych) może zagwarantować iż prawo do prywatności nie pozostanie jedynie fikcją prawną. W tym zakresie warto, na zakończenie zacytować fragmenty dokumentu historycznego. Etyka zawodowa policjanta w II Rzeczypospolitej Polskiej: (...) Ojczyzna przyznała Ci wyjątkowe prawa. Tych praw nie nadużywaj, gdyż nie są one przywilejem, lecz obowiązkiem, który sumiennie wypełniasz w służbie Narodu.(...) Przestępstwo jest nieszczęściem. Zachowaj się wobec niego z powagą i ludzkością.(...) Pomóż temu, kto Twojej pomocy potrzebuje i obchodź się ze wszystkimi tak, jakbyś chciał, by się z Tobą obchodzono.(...) Żyj skromnie, zachowasz przez to niezależność. Nie przyjmuj żadnych podarunków, gdyż to zobowiązuje. Jako policjant nie możesz mieć zobowiązań. Życie ponad stan jest hańbą i prowadzi do nieszczęścia. (...) Bądź w życiu i służbie sprawiedliwy. (...) Pamiętaj, że jesteś żołnierzem. Nie zaniedbuj ćwiczyć się w żołnierskiej sprawności i ucz się ciągle, pamiętając o tym, że obywatele widzą w Tobie człowieka, który musi widzieć wszystko.

Bibliografia:

- Daehyun Strobel: IMSI Catcher; Ruhr-Universitat Bochum, 2007;
- Anderson Ross: Inżynieria zabezpieczeń; Wydawnictwo: Wydawnictwa Naukowo-Techniczne 2005;
- Krysik Piotr : Przechwytywanie transmisji GSM w praktyce; http://lwb.elka.pw.edu.pl/trac/lwb/wiki/Przechwytywanie_rozm%C3%B3w_GSM, 10.02.2011;
- Krawczyk Paweł: Jak bezpieczne są telefony GSM; http://ipsec.pl/kryptografia/2010/jak-bezpieczne-sa-telefony-gsm.html 03.06.2010;
- Sutton Roger J.: Bezpieczeństwo Telekomunikacji, Wydawnictwa Komunikacji i Łączności 2004;
- Osiatyński Wiktor, Szkoła Praw Człowieka. Teksty wykładów. Zeszyt 1, Helsińska Fundacja Praw Człowieka, Warszawa 1998;
- Słownik wiedzy o Sejmie, Wydawnictwo Sejmowe, Warszawa 2001;
- Simon A., Walczyk M."Sieci komórkowe GSM/GPRS. Usługi i bezpieczeństwo", Wydawnictwo Xylab, Kraków 2002;
- Kołakowski J., Cichocki J. "UMTS. System telefonii komórkowej trzeciej generacji", WK,, Warszawa, 2003;

- Konstytucja Rzeczypospolitej Polskiej z 02.04.1997;
- Brandeis Louis, Warren Samuel D. "The Right to Privacy", Harvard Law Review 1890;
- California Office of Privacy Protection 2011; http://www.privacy.ca.gov/privacy_laws.htm; 21.02.2011;
- Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 04.11.1950;
- Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966;
- Czuj A. (red.), System ochrony praw człowieka, Zakamycze 2005;
- Kodeks Postępowania Karnego z 06.06.1997;
- Ustawa o Policji z 06.04.1990;
- Kremplewski A., Skowron J. Prawa człowieka a policja, Warszawa: Helsińska Fundacja Praw Człowieka 1998;
- Czapska J., Wójcikiewicz J.: Policja w społeczeństwie obywatelskim. Kraków: Zakamycze 1999;
- Deklaracja o Policji, Rezolucja 690 Zgromadzenia Parlamentarnego Rady Europy.
- Nowicki M.A., Wokół Konwencji Europejskiej. Krótki komentarz do Europejskiej Konwencji Praw Człowieka, Zakamycze, Kraków 2002;
- Sozański J., Prawa człowieka w systemach prawnych Wspólnot i Unii Europejskiej, Polskie Wydawnictwo Prawnicze, Warszawa -Poznań 2005;
- Banaszak B., Bisztyga A., Complak K., Jabłoński M., Wieruszewski R., Wójtowicz K., System ochrony praw człowieka, Kraków 2003;
- Kuźniar R., Prawa człowieka. Prawo, instytucje, stosunki międzynarodowe, Warszawa 2002;
- Abrahamson P. (red.) Welfare States in Crisis: the Crumbling of Scandonavian Model", Kopenhavn 1988;
- Czy Państwo wiedzą... O prawach człowieka. Informacja Heslińskiej Fundacji Praw Człowieka dla prasy, red. zespół, Warszawa 1994;
- Donelly J., Universal Human Rights in Theory and Practice, Ithaca and London 1989;
- Donelly J., The Concept of Human Rights, London 1985;
- Prawa człowieka w społeczeństwie obywatelskim, red. A. Rzepliński, Warszawa 1993;
- Sudre F., Konwencja Europejska o Ochronie Praw Człowieka i Podstawowych Wolności, Warszawa 1993