

Policyjna rzeczywistość, filmowe bajeczki i tworzone prawo. Jak to jest od strony policjanta?

24 września 2015

Polskie prawo w zakresie dostępu służb do billingów nie jest doskonałe, ale czy funkcjonariusze naprawdę masowo go nadużywają? Jak naprawdę wygląda dostęp do tych danych i jakie ma znaczenie dla śledztw? Czy namierzanie telefonu wygląda jak na filmach i w serialach? Czy łatwo wyznaczyć katalog przestępstw, przy których powinno się zajrzeć do billingów? Co może dziwić przy tworzeniu prawa dotyczącego inwigilacji? „Dziennik Internautów” rozmawiał o tym z byłym policjantem.

Często pisałem o problemie, jakim jest dostęp służb do danych o naszych danych telekomunikacyjnych. Skupiałem się na tym jakie mamy prawo w tym zakresie, albo jakie wyroki zapadły w ważnych Trybunałach. Opisywałem jak przebiegają prace nad nowym projektem ustawy w tym zakresie. Często krytykowałem istniejące prawo. Narzekałem, że prawo nie daje wystarczających zabezpieczeń. Moje osobiste poglądy są bliskie poglądom tzw. obrońców prywatności. Dlatego nieco się zdziwiłem, gdy jakiś czas temu zgłosił się do mnie były policjant. Człowiek ten stwierdził, że sam przez wiele lat „inwigilował społeczeństwo” (takich słów użył). Chciał mi opowiedzieć o tym jak wygląda dostęp do billingów od strony policjanta. Nie namawiał mnie na publikowanie czegokolwiek. Po prostu uznał, że jestem dziennikarzem, który być może zechce go wysłuchać i czegoś się nauczyć. Rzeczywiście dużo się dowiedziałem, ale nie chciałem tego zachowywać dla siebie. Namówiłem byłego stróża prawa na opublikowanie wywiadu. Wyszedł z tego bardzo ciekawy i dość obszerny materiał o tym, jak wygląda od strony policjanta to, co nazywamy „dostępem

służb do billingów”.

– Czy dostęp do billingów ma duże znaczenie dla organów ścigania? To znaczy... czy naprawdę bardzo pomaga on w namierzaniu przestępców?

– Mam taką dewizę – „Cyfra nie kłamie”. Nie przekupi się jej, nie zastraszy, nie jest interesowna, nie załtoni się brakiem pamięci czy chorobą psychiczną. Trzeba ją tylko chcieć zrozumieć. Zarówno prokuratorzy, jak i sędziowie traktują materiały oparte na danych pochodzących od operatorów jedynie, jako poszlaki (przynajmniej ja nie znam, nie słyszałem o sprawach, które generalnie opierają się tylko o analizy danych telekomunikacyjnych). Najchętniej widzą materiał dowodowy w postaci zeznań świadków, dokumentów, wyników ekspertyz biologicznych, mechanoskopijnych, balistycznych itp. – to co znają od lat i rozumieją. Ponadto sytuacja taka wynika ze stanowiska operatorów, które prezentowali przed sądami oraz w oficjalnej korespondencji, kierowanej do uprawnionych jednostek Policji. Podkreślają iż nie przypisują sobie prawa do oceny dowodów, która należy do sądów, a jedynie oceniają na sali sądowej techniczną wartość informacji. Akcentują to w opinii, że na obecnym etapie rozwoju techniki telekomunikacyjnej dane lokalizacyjne są w wysokim stopniu niewiarygodne. Są prokuratorzy potrafiący skorzystać z materiałów uzyskanych od operatorów telekomunikacyjnych, lecz jest to niewielka grupa. Kilka lat temu tłumaczyłem sędziemu, że karta pre-paid nie zapewnia anonimowości, że mimo iż nie jest zarejestrowana można ustalić jej użytkownika – był lekko zaskoczony. W innej sprawie tłumaczyłem zawiłości związane z logowaniami telefonów komórkowych, konstrukcją anten kierunkowych i kilkoma innymi aspektami technicznymi. Po godzinie moich wyjaśnień wszyscy na sali rozumieli o co chodzi, ławnicy ironicznie się uśmiechali, a sędzia nie rozumiał. Skrajnym przypadkiem takich zachowań było działanie prokuratora, który co prawda skorzystał z ustaleń dokonanych w oparciu o analizy bilingów wykonane przez policję tj. skład

grupy przestępczej, role członków w grupie, ustalenie świadków, jednak doszedł do wniosku, że wystarczą mu wyjaśnienia podejrzanych. Nie zamówił potrzebnych bilingów u operatora ani nie wystąpił do policji o udostępnienie materiałów pozyskanych na podstawie art. 20c Ustawy o Policji (do sprawy zamawiano ogromną ilość danych). Bywało często, że odpowiedź od operatora zawierała np. kilka bilingów w jednym pliku, a po analizie okazywało się, że nie wszystkie były przydatne w sprawie. Dlatego konieczne było ponowne zamówienie danych ale już tylko tych wyselekcjonowanych). W efekcie prokurator zamieścił w sprawie analizę bez materiału źródłowego, a oskarżeni wycofali się ze złożonych wcześniej wyjaśnień. Na sali sądowej spędziłem wówczas 7 godzin. Gdy okazało się, że nie ma materiału źródłowego obrońcy oskarżonych wyczuli okazję. Chcieli powołać niezależnych biegłych, którzy zweryfikowaliby moją analizę. Zarówno sędzia jak i obrońcy byli zaskoczeni, że jest to nie możliwe, bo policja zgodnie z przepisami zniszczyła materiały od operatorów telefonii komórkowych sprawa trafiła do sądu po trzech latach czyli przekroczono ówczesny 24 miesięczny okres retencji danych telekomunikacyjnych. W ten sposób prokurator pozwolił obronie na wystąpienie do sądu o odrzucenie materiału zawartego w analizie. Na szczęście to co zrobiłem pozwoliło uzyskać inne dowody a i prowadzący sędzia był mądry. Zapadły wyroki skazujące. Tak więc dane telekomunikacyjne są doskonałym narzędziem, w działaniach operacyjnych Policji. Zgromadzona w oparciu o analizy wiedza pozwala znaleźć inne źródła dowodowe powszechnie akceptowane przez prokuratury i sądy. Do tego zwykle się dąży, aby nie utracić efektów pracy. Niestety bywa, że efekty wielu godzin pracy policjantów idą do kosza. Po prostu w każdej sprawie przychodzi taki moment, że aby ją zakończyć potrzeba prokuratorskiej decyzji. Zwykle jest to nakaz zatrzymania, przeszukania niekiedy powołanie biegłego. – Ale ja tu nie widzę podstaw. To zbyt mało. Na podstawie czego pan tak sądzi. Tak to wygląda w realu.

– A policjanci? Jak oni sobie radzą z danymi

telekomunikacyjnymi?

– Policjantom nie zawsze chce się uczyć. Mogą mieć nawet problem z otwarciem pliku *.csv albo *.ack. Niekiedy mówiłem „chodź na chwilę ja ci pokażę jak to zrobić, to proste”. Odpowiedź: nieee, może innym razem, ty zrobisz to szybciej. No dobrze ale ktoś mógłby powiedzieć przecież są wydziały zajmujące się analizą zatrudniające analityków oni to robią. Tak! Oczywiście! Ale materiał do analizy musi zgromadzić policjant prowadzący sprawę. Tu zaczynają się „schody”. Policjanci generalnie nie lubią pisać, a zlecenie zadania dla analityków to duuużo pisanie.

Jaka jest rola analityków i na czym polega ich współpraca z policjantami?

– Komendant decyduje o włączeniu analityka do grupy pracującej nad nową sprawą lub akceptuje wniosek o wsparcie analityczne od naczelnika wydziału prowadzącego sprawę operacyjną lub procesową. Zwykle w przypadku sprawy procesowej analityk porządkuje materiały związane z ustaleniami telekomunikacyjnymi zgromadzone w toku prowadzonego postępowania i opisuje to z zachowaniem właściwej terminologii. Przed sądem występuje w charakterze biegłego. W przypadku sprawy operacyjnej analityk pomaga znaleźć potrzebne informacje zawarte w danych telekomunikacyjnych. Policjant prowadzący sprawę opracowuje wniosek o wsparcie analityka, przekazuje wszystkie niezbędne dane/okoliczności sprawy i materiały uzyskane od operatorów. Podaje też jakich informacji poszukuje. Bywa, że gdy do spełnienia celu analizy niezbędne są dodatkowe dane (np. dane abonentów) analityk we własnym zakresie pozyskuje takie dane od operatorów. Po prostu jeden nie wie jak i o co pytać, a drugi zachowuje się, jak urzędnik zamiast pomóc „klientowi” odsyła go z kwitkiem. Wiem, że założenia dotyczące pracy analityków były piękne ale tylko w teorii. Niestety ale patologia statystyki tam też się objawiła mając zły wpływ na efektywność pracy analityków. Nie wiem, jak to wygląda na dzień dzisiejszy, ale nie przypuszczam, aby dużo

zmieniło się na lepsze.

– Można się spotkać z argumentem, że dostęp do billingów da się zastąpić innymi metodami. Zgodzi się Pan z tym?

– Fundacja Panoptikon i podobne organizacje posługują się nieokreślonym pojęciem „mniej inwazyjnych metod”. Czytałem dość dużo na ten temat i nigdzie nie znalazłem wyjaśnienia co to jest. Mogę jedynie domyślać się „co autor miał na myśli”. Prawdopodobnie chodzi tu o typowe metody pracy policyjnej takie jak obserwacja, rozmowy z ludźmi, pozyskiwanie dokumentów w formie papierowej itp. Jednak gdyby to dawało efekty to policjanci nie sięgali by po dane telekomunikacyjne. Z moich doświadczeń wynika, że bardzo często są one „ostatnią deską ratunku”.

– Jak często – Pana zdaniem – może się zdarzyć niepotrzebne sięganie do billingów?

– Moim zdaniem około 2-3% zapytań kierowanych do operatorów mógłbym określić jako „niepotrzebne”. Te niepotrzebne pytania to efekt: źle sformułowanego zakresu pytania, błędów w przetwarzaniu informacji („literówki” przy zapisywaniu i przepisywaniu numerów) lub błędy systemów operatorów. Zdarza się też zamawianie takich samych danych do tej samej sprawy przez kilka uprawnionych podmiotów np. terenowa jednostka policji (KPP/KMP), nadzorująca jednostka policji (KWP) i prokuratura. Może dochodzić do zamawiania bilingów z bts-ów w sytuacji gdy nie mamy ich z czym porównać lub nie znamy schematu połączeń jaki mamy odnaleźć na tych bilingach. To jedyny przypadek gdzie jestem zdecydowanie przeciwny pobieraniu danych. Sam nie jestem bez winy, ale nie czuję skruchy. Zdarzało mi się „nadużywać”. Kiedyś jesienią znalazłem na ulicy smartfona. Upadł na liście więc się nie potłukł. Sprzęt ze średniej półki cenowej, zadbane. Ekran zablokowany hasłem, karta zabezpieczona pin-em. Dzięki danym od operatora telekomunikacyjnego ustaliłem kontakt do członka rodziny właściciela telefonu. Podziękowano mi za zwrot

telefonu, nie zastanawiając się jak do nich dotarłem. Dla nich najważniejsze było, że odzyskali telefon w którym były zapisane jakieś super ważne informacje. Jakoś nie wstyd mi, że jako policjant nadużyłem prawa.

– Czy zgadza się Pan z tym, że działalność służb przy zaglądaniu do billingów naprawdę można określać jako „niekontrolowaną”?

– W artykule Panoptikonu pt. „Dlaczego walczymy z retencją danych telekomunikacyjnych” pani Szymielewicz (prezeska Fundacji Panoptikon – red.) napisała „Nie ma ustawowych procedur udostępniania danych, a prawdopodobnie istniejące reguły operacyjne są niejawne i realizowane bez kontroli demokratycznej.” To mogłoby wystarczyć za cały komentarz, ale... To, że nie ma ustawowych procedur nie oznacza, że istniejące (bo one istnieją) operacyjne są złe. Nie wiem, jak to wygląda w przypadku służb, ale Policja mając dostęp do różnych baz danych zarówno policyjnych jak i zewnętrznych rejestruje każde sprawdzenie. Dostęp jest reglamentowany i można zawsze odpytać policjanta w jakim celu otwierał daną bazę i dany rekord. Tak samo jest w przypadku danych telekomunikacyjnych. Ba. Przewidując przyszłe zmiany, jak chociażby obowiązek sprawozdań statystycznych już w 2014 rozpoczęto przygotowania w tym zakresie. Niedogodność stanowi to, że w tym celu kilkudziesięciu policjantów w kraju codziennie wypełnia po kilkanaście kolumn do każdego zapytania kierowanego do operatorów. Rozumiem, że pod pojęciem demokratycznej kontroli Panoptikon widziałaby zupełnie nową cywilną instytucję. Z pełnym dostępem do danych operacyjnych w sprawie. Obawiam się, że to nie przejdzie. Nie wiem jakie wyobrażenie o tej pracy ma pani Szymielewicz. Podam przykład. W sprawie zabójstwa na zlecenie zlecający w okresie 17 miesięcy posługiwał się 36 kartami pre-paid polskich operatorów, 1 kartą operatora zagranicznego 1 numerem abonamentowym i 1 kartą do automatów telefonicznych. Karty SIM współpracowały z 6 telefonami. Z kolei pośrednik w tym czasie korzystał z 5 telefonów i 8 kart

pre-paid i abonamentowych. Wykonawcy zlecenia to kolejne karty SIM i telefony. W sprawie łącznie ustalano dane prawie tysiąca abonentów ponadto do operatorów skierowano kilkaset zapytań o bilingi. Czterech ludzi zostało skazanych tylko dlatego, że dostęp do tych danych był względnie nie utrudniony. Fizycznie nie widzę możliwości aby niekiedy kilka razy dziennie biegać ze stertą dokumentów i tłumaczyć urzędnikowi do czego mi to potrzebne. Z całą pewnością nie jest tak, jak niektórzy to komentują – „Nie będzie mi jakiś „krawężnik” grzebał po bilingach”. Nie ma takiej możliwości. Policja wbrew obiegowym opiniom ma jednak sporo ograniczeń. W dobie Wielkiego Brata i powszechnej inwigilacji pięć lat temu prowadząc pewną sprawę potrzebowaliśmy ustalić, jakimi liniami lotniczymi polski obywatel udał się do jednego z krajów na Bliskim Wschodzie. Wydawało się, że znając termin i przybliżoną godzinę wylotu z Polski, port lotniczy, numer paszportu Polaka i kraj docelowy nie będzie z tym problemu szczególnie, że był to wyjazd poza strefę Schengen. Przez rok nie udało się nic ustalić ponadto, że tak naprawdę kontroli podlega tylko 40 procent odlatujących pasażerów. W akcie desperacji zwrócono się do kraju docelowego (takie kontakty też są w policji reglamentowane). Uzyskano informację kto, kiedy i jakimi liniami lotniczymi. Niestety okazało się, że było już zbyt późno, aby tą odpowiedź wykorzystać w prowadzonej sprawie. Służby nie są też tak wszechmocne jak się powszechnie sądzi. Kilka lat temu miałem kontakt ze sprawą, w której jedna ze służb interesowała się człowiekiem, który prowadził dużą część korespondencji przez Internet. Okazało się, że ten człowiek jest dobrym znajomym lokalnego dostawcy Internetu. Fakt ten okazał się barierą nie do pokonania. Mimo iż wszystkie okoliczności wskazywały, że należy zastosować kontrolę korespondencji internetowej nie zrobiono tego w obawie, że sprawa wyda się przedwcześnie.

– Z tego co Pan mówi wynika, że wykorzystanie danych telekomunikacyjnych nie jest całkiem łatwe. To ciekawe, bo wielu ludzi wyobraża sobie, że policja dostaje niemal gotowe informacje o tym co, kto i gdzie. Filmy kształtują w nas

wyobrażenie, że policja tylko pyta i dostaje gotową odpowiedź.

– Często koledzy prosili mnie, żebym dał im program do analizy lub powiedział gdzie można go kupić. Tymczasem... nie ma programu do analizy, wystarczy zwykły Excel. Programy komputerowe stosowane przez analityków pozwalają jedynie na usystematyzowanie wiedzy, przedstawienie w czytelnej – skompresowanej postaci pewnego zbioru danych, odnalezienie w dużej bazie danych interesujących nas elementów. Program komputerowy „analizuje” tylko te dane, których my dostarczymy. Sam z siebie nie zamówi bilingu, nie ustali abonenta, nie sporządzi czytelnej – zrozumiałej dla prokuratora notatki. Wnioski wyciągamy sami. Informacje dostępne po analizie bilingów, czy też wynikające z zastosowania aplikacji śledzących lokalizację nie są „lekiem na całe zło” i niedostatki policyjnej pracy. Bardzo często spotykałem się z wręcz paniczną reakcją, gdy na początku okazywało się, że w sprawie brak jest telefonu. Nawet ci, którzy korzystają w pracy z usług lokalizacyjnych oferowanych przez operatorów często wierzą w bajki np. w ubiegłym roku jeden z kolegów przekonywał mnie, że istnieje „cudowna” aplikacja na smartfona, która DOKŁADNIE pokazuje lokalizację telefonu. Słyszałem też opowieści o „cudotwórcach” potrafiących tylko w oparciu o Cell-ID podać lokalizację z dokładnością do jednej klatki w bloku. Mogę powiedzieć, że zęby na tym zjadłem. Rzadko i w bardzo szczególnych warunkach mogę określić lokalizację z dokładnością do 1-2 budynków w mieście, ewentualnie z dokładnością do 3-4 gospodarstw w terenie wiejskim. Dwa razy spotkałem się z sytuacją gdy mogłem określić lokalizację z dokładnością do kilku metrów – ale to były naprawdę wyjątkowe sytuacje. Prawdopodobnie w żadnym kraju na świecie nie ma prostej możliwości dokładnej lokalizacji telefonu GSM. Wszystkie opracowania poświęcone temu zagadnieniu, które znalazłem w internecie wykorzystują dość skomplikowane metody matematyczne pozwalające na określenie pozycji w dużym przybliżeniu. Bazują one na wykorzystaniu infrastruktury operatora co staje się dodatkowym

problemem. Operatorzy protestują wobec ingerencji w ich systemy obawiając się zakłóceń transmisji, a co za tym idzie spadku zaufania użytkowników sieci i spadku dochodów.

– Więc jest duża rozbieżność pomiędzy tym filmowym i prawdziwym obrazem namierzania ludzi?

– W naszej siermiężnej rzeczywistości frustrację mogą rodzić filmy sensacyjne, gdzie wszystko jest w przysłowiowym zasięgu ręki, telefony komórkowe lokalizowane są z dokładnością do centymetrów niezależnie od tego czy znajdują się w szczerym polu czy na czterdziestym piętrze wieżowca. Są jednak produkcje, gdzie pokazano bardziej realne sytuacje. W niemieckim serialu „Kobra 11” poświęconym pracy policjantów z komisariatu autostradowego, w jednym z odcinków lokalizowano telefon komórkowy na terenie miasta. Policyjny operator korzystał z komputerowej mapy miasta pokrytej siatką regularnych sześciokątów (plaster miodu). Lokalizację telefonu wskazywał podświetlony sześciokąt. Odpowiada to rzeczywistym założeniom budowy sieci BTS-ów telefonii komórkowych – telefon powinien być „widziany” przez 6 najbliższych przekaźników. Implementacja takiego rozwiązania w polskich warunkach byłaby możliwa. Opracowano wiele map elektronicznych dostępnych dla służb ratowniczych w tym policji. Wystarczyłoby nałożyć na te mapy siatki obrazujące zasięg przekaźników i powiązać z aplikacją pobierającą niezbędne dane od operatorów telefonii komórkowych. W duńskim serialu „Orzeł” pokazano pracę specjalnej duńskiej komórki policji powołanej do zwalczania zorganizowanej przestępczości na terenie Danii i UE. W tym serialu też w pewnym momencie jest lokalizowany telefon komórkowy i ci super gliniarze nie mówią o dokładnej lokalizacji. Pada stwierdzenie „...ustaliłem, że jego telefon jest w zasięgu przekaźnika...”. W filmie sprawa jest prosta. Przekaźnik jest w Norwegii, swoim zasięgiem pokrywa fragment drogi prowadzącej wzdłuż skalistego wybrzeża, a na jej końcu jest osada złożona z kilku domów. Wniosek – przestępca jedzie samochodem do osady. Ja też uwierzyłem magii X-muzy i czułem

się przez długi czas, jak ubogi krewny. W końcu znalazłem opracowanie „Cell-ID technika lokalizacji, ograniczenia i korzyści: badanie eksperymentalne” autorstwa Emiliano Trevisani i Andrea Vitaletti z Zakładu Systemów Komputerowych Uniwersytetu Sapienza w Rzymie. We wstępie do tego opracowania autorzy wyjaśniają w czym rzecz. Obecny nacisk na usługi oparte na lokalizacji w Ameryce Północnej rozpoczął się w 1996 roku, gdy Federalna Komisja Komunikacji USA zatwierdziła standard Enhanced 911 (E911), zmieniony w 1999 roku. Wymaga on od operatorów bezprzewodowych zdolności lokalizacji z dokładnością 50 do 100 metrów, każdego telefonu komórkowego dzwoniącego na numer 911, na terenie całego kraju. Operatorzy komórkowi, motywowani wymogami E911, eksperymentują z nowymi i skutecznymi technikami lokalizacji. Większość z nich wymaga jednak znacznych nakładów technologicznych i inwestycji finansowych. Na przykład, Assisted GPS wymaga serwera i odbiornika GPS w każdym telefonie (koszt około 2.000 US \$). Z kolei metoda ToA (Time of Arrival) nie wymaga od abonentów zakupu nowych słuchawek, jednak moduł lokalizacyjny (LMUs, kosztujący ok. 10.000 US \$) musi być zainstalowany w każdej stacji bazowej. Standard E112, europejski odpowiednik amerykańskiego E911, nie nakłada na operatorów żadnych wymogów dokładności lokalizacji lub stosowanej technologii. Istnieje jedynie obowiązek aby udostępnić te możliwości lokalizacji, którymi aktualnie dysponuje operator (Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady o usłudze powszechnej). Z tego powodu większość europejskich operatorów telekomunikacyjnych w celu spełnienia wymogów E112 kieruje się niskimi kosztami pozycjonowania w oparciu o Cell-ID. Ta bardzo podstawowa forma technologii lokalizacji wykorzystuje szerokość i długość geograficzną z obsługi komunikacji, jako przybliżenie faktycznej pozycji telefonu w stosunku do anteny. Rozmieszczenie Cell-ID jest proste i ekonomiczne, nie wymaga modernizacji słuchawek lub urządzeń sieciowych, ale ponieważ telefon może być w dowolnym miejscu w obrębie komórki, dokładność zależy od wielkości komórek.

– Czy można się ukryć przed nadzorem służb?

– Ludzie zachowują się niczym dzicy, którzy sprzedają swoje bogactwo za garść świecidełek. Sprzedają swoją prywatność za to, że telefon ma jedną funkcję więcej, że coś będą mogli łatwiej osiągnąć, że podadzą w formularzu więcej prywatnych danych (nie zastanawiając się po co to komuś), a potem publiczny lament bo jesteśmy okradani z prywatności. Oczywiście są i tacy, którzy dbają o ten swój skarb np. przestępcy. Potrafią być bardzo kreatywni w tej dziedzinie. Świadomie chronią swoją prywatność. Bez specjalnych umiejętności, nakładów finansowych korzystając z normalnych telefonów, bez szyfrowania komunikacji potrafią komunikować się w sposób praktycznie uniemożliwiający kontrolę – teoretycznie możliwość kontroli istnieje, jednak jest ona tylko teoretyczna. Oczywiście są pewne ograniczenia, jednak jeżeli służby czy policja nie będą wcześniej wiedziały, że dwóch ludzi się kontaktuje to nie będą szukać dowodów takich znajomości. Nie podam szczegółów, bo nie zamierzam instruować przeciwnika, ale w ciągu ostatnich czterech lat dwukrotnie miałem do czynienia z tego typu komunikacją pozwalającą zachować anonimowość.

– Jak z Pana punktu widzenia można ocenić działania polskich obrońców prywatności. Co Pan sądzi o argumentach np. organizacji pozarządowych, które walczą o ograniczenie dostępu do billingów.

– Kilka lat temu poszukując rozwiązania niektórych problemów trafiłem na strony EFF – Electronic Frontier Foundation – amerykańskiej fundacji broniącej praw w cyfrowym świecie. Później ucieszyłem się trafiając na jej polski odpowiednik Panoptikon. Z upływem czasu mój entuzjazm zmniejszył się. O ile można pochwalić fundację Panoptikon za podjęcie prób ustanowienia regulacji prawnych dla wielu istotnych we współczesnym świecie dziedzin techniki cyfrowej oraz nagłośnie problemu, jaki stanowi inwigilacja ludzi, to już argumenty za jej ograniczeniem są często nietrafne. Od kilku

lat niezmiennie słyszę, że tylko poważne przestępstwa powinny uprawniać do sięgania po dane telekomunikacyjne. Mimo iż staram się być na bieżąco z publikacjami na ten temat, nigdzie nie znalazłem jasnej definicji czym jest poważne przestępstwo. Nigdy nie wiemy czy sprawa, którą początkowo można by zakwalifikować jako „błahą” nie okaże się sprawą poważną. Kilka lat temu zwrócono się do mnie o pomoc w wyjaśnieniu zdarzenia drogowego. Stosując różne proponowane kryteria tego przypadku nie można zakwalifikować, jako sprawy „poważnej” – godnej do sięgania po dane telekomunikacyjne. W sprawie chodziło o to, że kierowca auta osobowego zajechał drogę ciężarówce. Kierowca ciężarówki chcąc uniknąć kolizji gwałtownie skręcił i ciężarówka z ładunkiem zjechała do rowu. Przybyły na miejsce patrol policji sporządził stosowną dokumentację, po kilku dniach właściciel firmy transportowej złożył wniosek do ubezpieczyciela o wypłatę odszkodowania. Sprawa, jakich wiele każdego dnia. Jednak dzięki analizie danych telekomunikacyjnych ta sprawa miała swój finał w sądzie. Oskarżono kierowcę ciężarówki, jego pracodawcę – właściciela firmy transportowej, właściciela samochodu osobowego, jego znajomego, który kierował tym samochodem oraz policjanta sporządzającego dokumentację. To analiza danych telekomunikacyjnych wykazała, że najprawdopodobniej przemęczony kierowca ciężarówki wjechał do rowu. Powiadomił o tym telefonicznie właściciela. Ten próbując ratować sytuację zwrócił się o pomoc do znajomego X. Ponieważ ów znajomy przebywał kilkadziesiąt kilometrów od domu zadzwonił do swojego kolegi Y. Kolega Y udał się do domu X wziął jego samochód, pojechał na miejsce zdarzenia oddalone o ok. 70 kilometrów. Tam od kilku godzin cierpliwie czekał patrol policji, aby w dokumentach potwierdzić, że to Y zajechał drogę ciężarówce. Pani Szymielewicz powołuje się na badania przeprowadzone przez niemiecki Instytut Maxa Plancka. Badania miały wykazać niewielką użyteczność danych retencyjnych w rozwiązywaniu spraw kryminalnych. Według przytoczonych liczb wynosiła ona poniżej jednego promila. Ja widzę to inaczej. Zamachy terrorystyczne z 11 września 2001 roku wymogły zmiany

w prawie poszczególnych krajów np. w Niemczech zmian takich dokonano w sierpniu 2002 roku. Do tego czasu identyfikacja numerów IMSI i IMEI za pomocą środków technicznych była w Niemczech nielegalna (użycie urządzeń typu IMSI-catcher). Tymczasem w Polsce już od kilku lat używano tego typu urządzeń. Co prawda w ograniczonym zakresie z uwagi na bardzo wysoką cenę urządzenia, jednak z powodzeniem. W 2003 roku prowadzono czynności w związku z działaniami zorganizowanej grupy przestępczej dokonującej włamań metodą „na śpiocha” na terenie całej Polski. W pewnym momencie policjanci prowadzący sprawę zorientowali się, że aktywność grupy znacząco spadła. Okazało się, że zaczęli oni dokonywać przestępstw na terenie Niemiec. Nawiązano kontakt z policją niemiecką. W wyniku wymiany informacji ustalono, że Polacy są sprawcami serii kradzieży samochodów. W ciągu dwóch miesięcy ukradli w jednym rejonie ok. 40 samochodów jednej marki. Niemcy nie mogli sobie poradzić z tym problemem. Gdy wyjaśniono im szczegółowo, jak rozpracowano grupę dzięki zastosowaniu analizy danych telekomunikacyjnych byli zaskoczeni. Nie znali tych metod. Jeżeli nie pracowali posługując się tymi metodami to nie mieli w tym doświadczenia, jak skutecznie i efektywnie je wykorzystywać. Stąd moim zdaniem taka śladowa przydatność tego instrumentu w tropieniu przestępstw.

– Czy Pana zdaniem w dyskusji na temat dostępu do billingów zdarza się, że obrońcy prywatności przywołują jakieś argumenty, z którymi Pan by dyskutował?

– Czasem rodzą się mity. Przykładowo samobójcza próba wojskowego prokuratora, jaka miała miejsce w styczniu 2012 roku na konferencji prasowej wywołała falę dyskusji. Próba ta była m.in. efektem medialnej krytyki po ujawnieniu, że prokuratura żądała ujawnienia bilingów i treści SMS-ów z telefonów należących do dziennikarzy. Uwaga autorytetów prawnych skoncentrowała się na pytaniu czy prokurator miał do tego prawo. Ogromna ilość wywiadów i komentarzy z tamtego okresu pomija jeden aspekt tej sprawy – czy było to w ogóle

możliwe? Media praktycznie zbyły milczeniem stanowisko operatorów telefonii komórkowych. Tymczasem, jak opisała jedna z gazet, wszyscy operatorzy zgodnie odmówili ujawnienia treści SMS-ów tłumacząc, że nie mają do tego prawa bez uprzedniego postanowienia sądu, że nie posiadają rozwiązań technicznych umożliwiających rejestrowanie treści korespondencji w innych przypadkach niż przewidziane prawem. Operatorzy nie gromadzą treści SMS-ów oprócz jednej sytuacji, kiedy to treść SMS-a pozostaje na serwerach operatora do czasu dostarczenia go do odbiorcy. Nie wiem skąd bierze się to przekonanie, że treści SMS-ów są gromadzone przez operatorów. Z jednej strony przez cały czas utyskują oni, że ponoszą nie małe koszty retencji danych, a z drugiej strony mieli by tak sobie gromadzić treść korespondencji? Być może w początkach rozwoju telefonii komórkowych byłoby to możliwe, jednak przy obecnej intensywności korespondencji koszty utrzymania takich baz byłyby ogromne.

– Są jeszcze jakieś inne, Pana zdaniem błędne argumenty obrońców prywatności?

– W artykule Panoptikonu pt. „Dlaczego walczymy z retencją danych telekomunikacyjnych” przywołany jest aspekt wykorzystywania danych retencyjnych nie tylko do wykrywania przestępstw, ale także w działaniach prewencyjnych stosownie zapisany w ustawach o poszczególnych służbach. Wydaje mi się, że problem polega na terminologii. Prewencja to ogólnie zapobieganie. Termin „prewencja” może kojarzyć się ludziom z policjantami mundurowymi z którymi najczęściej mają kontakt na ulicy. Tymczasem nie o to chodzi. W przypadku realnych przesłanek zagrożenia czyjegoś życia lub zdrowia służby kryminalne podejmują działania mające zapobiec temu. Bywa, że nie wiemy kto może być ofiarą, a kto sprawcą. Działania mają zapobiec popełnieniu przestępstwa – taki jest cel. Celem prowadzonych czynności nie jest wszczęcie śledztwa. Tak rozumiana prewencja to dyskretna ochrona lub nadzór realizowane przy wykorzystaniu danych telekomunikacyjnych. We

wspomnianym artykule pani Szymielewicz odnosząc się m.in. do użyteczności i wiarygodności danych retencyjnych napisała „Pytanie ilu niewinnych ludzi zostało oskarżonych nie jest pytaniem akademickim.” Pytanie jest co najmniej demagogiczne. Znam słownie jeden taki przypadek kiedy niewinnemu człowiekowi postawiono zarzut popełnienia przestępstwa w oparciu o dane telekomunikacyjne. Błąd nie wynikał jednak z wątpliwej wiarygodności danych, a z nieumiejętnej ich interpretacji. W toczącej się dyskusji zarzuca się uprawnionym w tym głównie służbom specjalnym oraz policji nadmierne i nieuzasadnione korzystanie z danych telekomunikacyjnych. W opiniach wypowiedzianych na ten temat, jako przykład podawane są bilingi w sprawach rozwodowych. Rozumiem, że argument w postaci sprawy rozwodowej jest zrozumiały dla odbiorców, tylko co to ma wspólnego ze służbami specjalnymi i policją? W tych sprawach o bilingi występowali do operatorów sędziowie na wniosek adwokatów. Jako przykład „błahej sprawy” pani Szymielewicz podaje też wycięcie drzewa w lesie. Ten argument moim zdaniem też nie jest zbyt trafny, bo inaczej ocenimy wycięcie choinki na święta, a inaczej na przykład ścięcie drzewa uznanego za pomnik przyrody (np. dąb Bartek). Dodam, że zabawy z masową inwigilacją to bardzo kosztowny biznes. Polskich służb i policji nigdy nie będzie stać na takie fanaberie, jak służby amerykańskie czy brytyjskie. Dynamiczny rozwój technologii cyfrowych sprawia, że sprzęt do inwigilacji jest bardzo specjalistyczny i cholernie drogi. Mówię o kwotach rzędu setek tysięcy, a nawet miliona euro. Gdyby nie to że ludzie wierzą w różne brednie wypisywane w Internecie na przykład, że każda Komenda Powiatowa dysponuje IMSI-catcherem, to bym się z tego śmiał. To czym dysponujemy zwykle jest opóźnione o jedną dwie generacje w stosunku do aktualnych możliwości technologicznych dostępnych na rynku. Tworzenie psychozy powszechnej inwigilacji nie jest dobre szczególnie, że niektóre osoby jej ulegają i dokładają tylko niepotrzebnej pracy organom ścigania, ale to już temat na inną opowieść.

– Czy Pana zdaniem prawo zaglądania w bilingi jest naprawdę

dużym zagrożenie dla prywatności? Obserwuje Pan prace nad tym prawem?

– Moim zdaniem dopóki bazy danych nie są zagregowane, obowiązują różne procedury dostępu nie ma niebezpieczeństwa dla prywatności ludzi. Powstanie ono gdy jednym kliknięciem wywołamy całą wiedzę o człowieku. Mam świadomość, że moje poglądy i spojrzenie na problem są wypaczone przez lata pracy w policji, ale tu nie chodzi o inwigilację tych milionów szarych obywateli, bo nimi służby specjalne się nie zajmują. Gdy kogoś dotknie nieszczęście to może mi Pan wierzyć, nie interesuje go jakimi metodami pracuje policja. Nie wiem czy zwrócił Pan uwagę, że w prawie zaczyna się coś dziać z chwilą, gdy dotyka to ludzi z immunitetem. Gdy doszło do afery starachowickiej, a potem do podsłuchiwanie środowiska sędziowskiego na Wybrzeżu, zaczęło się limitowanie kontroli operacyjnych. Sporo zamieszało pojęcie wniosków następnych, bardzo różnie interpretowane. Gdy już utarły się zwyczaje związane z wnioskami następczymi, wprowadzono kolejne zmiany, aby nie było zbyt łatwo. Afera hazardowa i spotkanie ministra Kaczmarka w hotelu Marriott dostarczyły argumentów przeciwko bilingom – „ubogim krewnym” kontroli operacyjnej. Historia sięgania po bilingi i SMS-y dziennikarzy była tylko przyczynkiem do tego, aby rozprawić się z problemem. Nie jestem pewien czy aktualne ożywienie w temacie nie jest efektem afery podsłuchowej i wpadki byłego ministra sprawiedliwości Grabarczyka. Uwaga mediów skoncentrowana jest na tym, że senacki projekt ma się nijak do wyroku TK i wytycznych unijnych. Projekt ewidentnie jest przygotowany niestaranie, ale zawiera nowe uregulowania chroniące parlamentarzystów. To czysta polityka. Ja nie mam takich możliwości, ale Pan tak. Niech Pan spróbuje zgłębić ten temat. Kto zgłosił do projektu w art. 19 Ustawy o Policji dodanie ust. 15k i czym się kierował, jakie były przesłanki bo wcześniej nikt o to nie zabiegał, a dyskusja toczy się od lat. W Polsce zamiast tworzyć prawo jasne i przejrzyste budowę próbuje się rozpoczynać od wyjątków. I tak w odniesieniu do

danych telekomunikacyjnych mamy propozycje zamkniętego katalogu plus samobójcy, plus osoby zaginione, plus przestępstwa popełnione za pośrednictwem lub przy użyciu telefonu i internetu, w których inne działania są niemożliwe i będą nieskuteczne. Może się wydawać, że ten szeroki zestaw jest wystarczający, ale w dalszym ciągu nie obejmuje np. bilingów z telefonu osoby pokrzywdzonej. To nie jest jakiś ewenement, że pobiera się taki biling w sytuacji gdy pokrzywdzony w wyniku traumatycznego przeżycia nie jest w stanie umiejscowić zdarzenia w czasie i przestrzeni. Szczególnej ochronie (czytaj dużo utrudnień) mają podlegać dziennikarze, adwokaci, parlamentarzyści – zawody publicznego zaufania. Nota bene jak pokazuje afera podsłuchowa, z tym zaufaniem do polityków to gruba przesada. Jest szansa, że powstanie kolejny potworek prawny, a jedyne osoby, które na tym skorzystają to ci z różnych względów uprzywilejowani. Prosty człowiek usłyszy jedynie, że prawo nie pozwala. Dla lepszego zrozumienia przytoczę przykłady. Dwa lub trzy lata temu do jednego z komisariatów policji zgłosiła się starsza pani, która poinformowała, że jej 70-letni przyjaciel wyjechał do innego miasta i od dwóch dni nie ma z nim kontaktu. Przyjaciel nie odbiera telefonów od niej, a ona się niepokoi czy coś mu się nie stało. Chciała podać numer telefonu przyjaciela, aby policja pomogła go odnaleźć. Policjant, z którym rozmawiała powiedział jej, że on nic nie może, bo potrzebna jest zgoda prokuratora (sic!). Zdesperowana pani chciała szukać pomocy u prywatnego detektywa na szczęście przyjaciel po kilku dniach odnalazł się. Zasłabł na ulicy i karetka zabrała go do szpitala. Kilkanaście lat temu jeden z lokalnych przedsiębiorców prowadzący stosunkowo dużą firmę odebrał dziwny telefon od nieznanego mężczyzny. Trochę zaniepokojony zwrócił się o pomoc/poradę do znajomego oficera policji. Właściwie to przedsiębiorcy zależało jedynie na ustaleniu kto go niepokoi. Jako, że nie było specjalnych podstaw do działań policyjnych więc wymyślono, że nieznanym rozmówcą groził przedsiębiorcy. Dzięki danym telekomunikacyjnym szybko ustalono kto dzwonił. Ponieważ

dzwoniący sensownie się tłumaczył (co potwierdził też biling z jego numeru) sprawę szybko zamknęto. Przedsiębiorca był usatysfakcjonowany – cel osiągnął.

AKTUALIZACJA

Po wywiadzie były policjant udzielający wywiadu przedstawił następujące dodatkowe wyjaśnienia.

– Każdy operator infrastrukturalny (MNO) tj. przedsiębiorca telekomunikacyjny działający na bazie własnej infrastruktury telekomunikacyjnej upoważniony jest do udzielania informacji dotyczących jedynie swoich abonentów oraz informacji dot. abonentów operatorów wirtualnych (MVNO) korzystających z jego infrastruktury.

– Informacje o lokalizacji BTS zawiera wykaz publikowany przez UKE pozostałe, dotyczące parametrów technicznych (w tym zasięg) stanowią Tajemnicę Przedsiębiorstwa zgodnie z Ustawą o zwalczaniu nieuczciwej konkurencji (Dz.U. 478/93 poz. 211) i nie są publikowane.

– Dane o lokalizacji abonenta przekazywane uprawnionym podmiotom podlegają też pewnym ograniczeniom. Lokalizacja ograniczona jest do Cell-ID (oznaczenie obszaru znajdującego się w zasięgu konkretnej anteny) i związanych z tym niektórych parametrów technicznych. Dlaczego tak jest – to będzie wyjaśnione w dalszej części wywiadu.

Z byłym policjantem rozmawiał Marcin Maj

Źródło: DI.com.pl