FUNDACJA PANOPTYKON

Warszawa, 14 kwietnia 2016 r.

Stanowisko Fundacji Panoptykon w sprawie stosowania narzędzi nadzoru elektronicznego przez organy powołane do walki z przestępczością

Na rynku rozwiązań technologicznych pojawia się coraz więcej narzędzi, które służą zbieraniu i analizowaniu danych użytkowników sieci telekomunikacyjnych. Ich wykorzystanie nie zawsze wymaga niejawnego dostępu do danych osobowych – coraz lepsze efekty analityczne można osiągnąć w oparciu o tzw. Open Source Intelligence (dalej: OSINT), czyli gromadzenie, łączenie i analizę powszechnie dostępnych danych w oparciu o odpowiednio zaprojektowane algorytmy. Z monitoringu przeprowadzonego przez Fundację Panoptykon wynika, że Policja i służby specjalne dostrzegają użyteczność tego typu narzędzi i decydują się na inwestowanie środków publicznych w komercyjne rozwiązania, oferowane przez polskie i zagraniczne firmy lub instytucje badawcze.

Nie budzi wątpliwości, że w uzasadnionych wypadkach Policja i służby specjalne powinny mieć dostęp do danych osobowych obywateli na potrzeby prowadzonych postępowań, a zarazem dostęp do technicznych narzędzi, które umożliwiają zbieranie takich danych. Z drugiej strony, w związku z rozwojem możliwości technicznych i analitycznych, które pozwalają na budowanie szczegółowych profili użytkowników sieci telekomunikacyjnych również na masową skalę, prawo powinno precyzyjnie regulować okoliczności uzasadniające ich gromadzenie i narzędzia, które można wykorzystywać w celu ich pozyskiwania. W naszej opinii obowiązujące przepisy nie odpowiadają na wszystkie wyzwania, jakie na tym polu stwarza technologia, co może stwarzać praktyczne i prawne problemy, również z perspektywy ochrony prawa do prywatności.

W niniejszym stanowisku podsumowujemy informacje, jakie w 2015 r. udało nam się zebrać na temat narzędzi nadzoru elektronicznego – programów, których pierwotnym przeznaczeniem jest ukierunkowane lub systematyczne zbieranie informacji o ludziach oraz ich zachowaniach w sieciach telekomunikacyjnych – wykorzystywanych w celu zapewnienia bezpieczeństwa publicznego i walki z przestępczością.

1. Cele i założenia monitoringu narzędzi nadzoru elektronicznego

W 2015 r. Fundacja Panoptykon, w ramach projektu „Państwo a biznes nadzoru. Monitoring praktyk instytucji publicznych”[1], poświęconego komercyjnym narzędziom nadzoru, nabywanym i wykorzystywanym przez instytucje publiczne, zbierała informacje na temat narzędzi służących do pozyskiwania i analizowania danych w sieciach telekomunikacyjnych. Opieraliśmy się na doniesieniach medialnych, publikacjach naukowych, raportach niezależnych ekspertów i organizacji, odpowiedziach, jakich monitorowane instytucje udzieliły nam na wnioski o dostęp do informacji publicznej oraz informacjach publikowanych na ich stronach internetowych. Listę instytucji, którym zadaliśmy pytania o narzędzia nadzoru, oparliśmy na analizie ich uprawnień,

[1] Realizacja projektu współfinansowana była ze środków Europejskiego Obszaru Gospodarczego w ramach programu „Obywatele dla demokracji” oraz dzięki wsparciu Open Society Foundations.

w szczególności istotne było dla nas to, czy mogą one zbierać informacje o obywatelach na dużą skalę w ramach czynności operacyjno-rozpoznawczych lub dochodzeniowo-śledczych.

Za istotne czynniki, determinujące zakres naszego monitoringu, uznaliśmy cel, jakiemu służy zbieranie informacji (czy w grę wchodzi ściganie konkretnych przestępstw, czy szeroko zakrojone działania prewencyjne lub rozpoznawcze) oraz skalę przetwarzania danych (czy dotyczy to konkretnych osób, podejrzanych w danej sprawie, czy – przynajmniej potencjalnie – wszystkich lub dużej grupy użytkowników sieci telekomunikacyjnych). Z uwagi na te czynniki, na potrzeby prowadzonego monitoringu, podzieliliśmy narzędzia nadzoru elektronicznego na następujące kategorie: (i) narzędzia do zbierania lub analizy danych o szerokiej grupie osób (w tym OSINT); (ii) narzędzia do przechwytywania komunikacji konkretnych osób; (iii) narzędzia wykorzystywane do analizy i zabezpieczenia dowodów.

W prowadzonym badaniu wychodziliśmy z założenia, że uprawnione organy powinny mieć możliwość zbierania i analizowania danych o obywatelach, kiedy jest to niezbędne dla realizowanych przez nie zadań, jak również, że przebieg i wynik czynności o charakterze operacyjno-rozpoznawczym lub dochodzeniowo-śledczym powinien być objęty klauzulą tajności. Dlatego nie pytaliśmy o narzędzia do przechwytywania komunikacji konkretnych osób (tj. podejrzanych), a skoncentrowaliśmy się na dwóch pozostałych kategoriach narzędzi nadzoru elektronicznego.

Podstawowym problemem, który w naszej opinii wymagał zbadania, było to, czy Policja i inne służby powinny mieć pełną dowolność w gromadzeniu i przetwarzaniu informacji o obywatelach na masową skalę (lub przynajmniej znacznie wykraczającą poza krąg osób podejrzanych) oraz w doborze służących temu narzędzi. Wychodziliśmy przy tym z założenia, że fakt zbierania informacji o obywatelach, wobec których nie toczą się żadne postępowania (np. w ramach zapobiegania przestępczości lub wstępnego rozpoznania zagrożeń) powinien być jawny.

Opierając się na powyższych założeniach, we wnioskach o udostępnienie informacji publicznej skierowanych do Policji i innych służb pytaliśmy o wykorzystywanie komercyjnych narzędzi służących do automatycznej analizy danych przesyłanych przez sieci telekomunikacyjne, analizy bilingów lub innych zbiorów danych, monitorowania sieci peer-to-peer, semantycznego monitoringu sieci i analizy danych pochodzących z otwartych źródeł (OSINT).

2. Wyniki przeprowadzonego monitoringu

Żaden z zapytanych przez nas organów nie udzielił pełnej odpowiedzi na pytania postawione we wnioskach o dostęp do informacji publicznej. Częściowych odpowiedzi udzieliły Policja, Żandarmeria Wojskowa, kontrola skarbowa i Służba Celna (w imieniu dwóch ostatnich organów odpowiedzi udzieliło Ministerstwo Finansów). Centralne Biuro Antykorupcyjne i Agencja Bezpieczeństwa Wewnętrznego opierając się na przepisach o ochronie informacji niejawnych wydały decyzje odmowne, powołując się na potencjalne zagrożenie dla bezpieczeństwa państwa w przypadku ujawnienia informacji o wykorzystywanych „środkach technicznych".

Dodatkowe informacje na temat narzędzi nadzoru elektronicznego wykorzystywanych przez wspomniane organy pozyskaliśmy na podstawie informacji publikowanych na ich stronach internetowych i w Biuletynach Informacji Publicznych (zamówienia publiczne) oraz w mediach.

Bezpośrednio od monitorowanych instytucji nie udało nam się uzyskać informacji potwierdzających wykorzystywanie komercyjnych narzędzi do przechwytywania informacji o konkretnych osobach w sposób niejawny. Jedyna poszlaka w tym zakresie dotyczy faktu zakupienia przez CBA licencji od firmy Hacking Team na korzystanie z oprogramowania Remote

Control System w 2012 roku (178 tys. euro za samą licencję, ponad 35 tys. euro rocznie za wsparcie techniczne). Natomiast udało nam się ustalić, że różne komercyjne rozwiązania lub efekty finansowanych ze środków UE projektów badawczych są wykorzystywane do zbierania lub analizy danych o szerokiej grupie osób (w szczególności pochodzących z otwartych źródeł) lub zabezpieczenia dowodów. W tej kategorii pojawiały się m.in.:

- oprogramowanie do analizy połączeń telefonicznych (billingów) o nazwie LINK 2, udostępnione nieodpłatnie policji przez AGH (Laboratorium Informatyki Śledczej);
- narzędzia firmy IBM do analizy informacji, w tym billingów o nazwach IBM i2 Analyst's Notebook i IBM i2 Base, wykorzystywane przez Policję, Służbę Celną i kontrolę skarbową;
- oprogramowanie Paterva Maltego oraz oprogramowanie EMM Osint Suite (opracowane przez Joint Research Centre – Institute for the Protection and Security of the Citizen) do analizy powiązań między publicznie dostępnymi informacjami w sieci Internet, wykorzystywane przez Służbę Celną;
- oprogramowanie ENCASE FORENSIC (Guidance Software), wykorzystywane przez Żandarmerię Wojskową, kontrolę skarbową i niektóre komendy Policji do analiz kryminalistycznych danych znajdujących się w telefonach komórkowych oraz innych urządzeniach mobilnych.

To jedynie przykłady rozwiązań, ponieważ spektrum narzędzi, jakie są dostępne na rynku i mogą być wykorzystywane na różnych etapach przeciwdziałania, rozpoznawania i ścigania przestępczości, jest ogromne. Co istotne, z analizowanych przez nas technicznych specyfikacji wynika, że większość dostępnych narzędzi może realizować różne cele i w różny sposób ingerować w prywatność obywateli – od zbierania informacji z sieci telekomunikacyjnych (także w czasie rzeczywistym), poprzez ich łączenie i analizę, po proste odzyskiwanie danych z pamięci urządzeń i ich zabezpieczanie.

Na podstawie publicznie dostępnych lub udostępnionych nam informacji nie stwierdziliśmy faktu wykorzystywania przez żaden z monitorowanych organów narzędzia, którego sposób działania byłby naszym zdaniem niezgodny z prawem. Na tej podstawie nie możemy jednak wyciągać daleko idących wniosków, ponieważ wiele z naszych pytań pozostało bez odpowiedzi. Ponadto, nie byliśmy w stanie ustalić, na ile faktyczny sposób korzystania z narzędzi nadzoru elektronicznego pozostaje zgodny z prawem i celami realizowanymi przez dany organ. Ten fakt utrudnia ocenę zasadności nabycia i sposobu wykorzystania konkretnych narzędzi, która była jednym z celów prowadzonego monitoringu.

3. Zdiagnozowane problemy i postulaty zmian

a. „Domniemanie tajności" ograniczające dostęp do informacji publicznej

Organy państwa dysponują zaawansowanymi środkami technicznymi, których odpowiednie wykorzystanie umożliwia gromadzenie informacji nie tylko o osobach podejrzanych, ale również przesiewową analizę informacji publikowanych lub przesyłanych przez przypadkowe osoby. Tak jak podkreślamy w punkcie 1, przeprowadzony monitoring nie dotyczył technik kontroli operacyjnej, a jedynie narzędzi nadzoru elektronicznego, które służą prewencyjnemu zbieraniu informacji o obywatelach, wobec których nie toczy się żadne postępowanie. W naszej opinii zarówno fakt zbierania tego typu informacji przez Policję lub inne służby, jak i rodzaje wykorzystywanych do tego celu narzędzi powinny być jawne. W praktyce napotkaliśmy jednak

na barierę w postaci „domniemania tajności": każda z monitorowanych instytucji w swoich odpowiedziach przyznała prymat ochronie informacji niejawnych stwierdzając, że obywatele i ich organizacje (jak np. Fundacja Panoptykon) – nie mają prawa do informacji o tym, jakie narzędzia są wykorzystywane przez organy powołane do walki z przestępczością.

W naszej opinii takie podejście – zrównujące informacje na temat technik kontroli operacyjnej stosowanych względem konkretnych osób, w przypadku których utajnienie ma wyraźne oparcie w przepisach prawa, z informacjami na temat wszelkich narzędzi wykorzystywanych do gromadzenia i analizowania danych o obywatelach – idzie za daleko i jest sprzeczne z zasadami, jakie wynikają z Konstytucji RP.

Odmowa udostępnienia informacji publicznej ze względu na ochronę informacji niejawnych jest wyjątkiem od ogólnej zasady wynikającej z art. 61 Konstytucji. Jak podkreślił Naczelny Sąd Administracyjny (wyrok z 2 lipca 2003 r., sygn. II SA 837/03) „ogólną zasadą wynikającą z art. 61 Konstytucji RP jest dostęp do informacji. Wszelkie wyjątki od tej zasady powinny być formułowane w sposób wyraźny, a wątpliwości powinny przemawiać na rzecz dostępu". Również Trybunał Konstytucyjny w wyroku z 15 października 2009 r. (sygn. K 26/08) traktuje wartości wymienione w art. 61 ust. 3 Konstytucji RP z 1997 r. jako ograniczenia zasady dostępu. Wskazuje przy tym, że „ograniczenia dostępności informacji publicznej i kryteria ważenia kolidujących ze sobą wartości podlegają ocenie z punktu widzenia mechanizmu proporcjonalności".

Oznacza to, że organ wydający decyzję o odmowie udostępnienia informacji publicznej powinien w swoim uzasadnieniu wykazać konieczność, adekwatność i proporcjonalność sensu stricto wprowadzanych ograniczeń, także gdy czyni to w imię innych wartości wymienionych w Konstytucji. Przeprowadzony przez nas monitoring wykazał natomiast, że organy powołane do walki z przestępczością i uprawnione do prowadzenia działań w sposób niejawny zwykle nie podejmują takiego wysiłku argumentacyjnego, przyjmując ochronę informacji niejawnych za wartość, która nie wymaga szczegółowego uzasadnienia.

Ponadto, niektóre organy – np. ABW i CBA – odmowę udzielenia odpowiedzi na pytania dotyczące stosowanych narzędzi lub technik uzasadniały tym, że niewiedza co do możliwości, jakimi rzeczywiście dysponuje organ, ma charakter „prewencyjny" czy „odstraszający". Trudno nam się zgodzić z taką argumentacją, a wręcz można przeprowadzić dokładnie odwrotne rozumowanie: świadomość , że organy powołane do walki z przestępczością dysponują zaawansowanymi narzędziami technicznymi, które wspomagają ich działanie, może skutecznie odstraszać osoby o przestępczych zamiarach. Odwrotny skutek mogłoby odnieść informowanie obywateli o sposobie wykorzystania tego typu narzędzi czy konkretnych działaniach podejmowanych przez uprawniony organ – np. o tym, na jakie cechy, słowa kluczowe czy zachowania komunikacyjne są wychwytywane dzięki oprogramowaniu do automatycznej analizy treści publikowanych w Internecie. Rozumiejąc to zagrożenie, postulujemy przejrzystość ograniczoną do informowania o samym fakcie nabywania i wykorzystywania narzędzi nadzoru elektronicznego, które mogą służyć do zbierania i przetwarzania informacji o obywatelach na szeroką skalę.

Warto przy tym zwrócić uwagę, że zdaniem Naczelnego Sądu Administracyjnego (wyrok z 1 października 2010 r., sygn. I OSK 1149/10) „prawo dostępu do informacji publicznej jest jednym z najważniejszych praw w katalogu praw obywatelskich i politycznych. Ma służyć tworzeniu społeczeństwa obywatelskiego, poprzez zwiększanie transparentności w działaniach władzy publicznej, chronić i umacniać zasady obowiązujące w demokratycznym państwie

prawa, wreszcie zapewniać społeczną kontrolę nad działaniami organów władzy publicznej. (…) Zagrożenie terroryzmem i rozwój przestępczości zorganizowanej powodują, że coraz częściej musimy godzić się na takie działania służb chroniących porządek prawny i nasze bezpieczeństwo, które ograniczają swobody obywatelskie, w tym sferę prywatności. Do opinii publicznej docierają przy tym informacje o nadużywaniu uprawnień dotyczących działań operacyjnych, w tym m.in. nagrywania i podsłuchiwania rozmów telefonicznych. Tym ważniejsze jest, aby działalność służb specjalnych podlegała społecznej kontroli w obszarach, które nie ograniczają możliwości ich skutecznego działania".

Problem braku informacji na temat stosowanych przez Policję i inne służby narzędzi pogłębia nieprzejrzysty sposób publikowania informacji o nabywanych narzędziach w Biuletynach Informacji Publicznej. Przeprowadzony monitoring pokazał, że publikowane w BIP-ach informacje o zamówieniach publicznych na oprogramowanie pomijają istotne szczegóły dotyczące funkcjonalności i celów, jakie takie oprogramowanie ma realizować, lub posługują się trudnym żargonem technicznym. Jeśli publikacja tego typu informacji ma rzeczywiście służyć przejrzystości, sposób ich opracowania i wykorzystywany język powinien być dopasowany do potrzeb i poziomu kompetencji przeciętnego obywatela. W szczególności, publikowane informacje powinny w jasny sposób odnosić się do tego, czy i jakie dane o obywatelach będą gromadzone lub analizowane za pomocą nabywanych narzędzi.

b. Brak adekwatnych gwarancji prawnych i niezależnych mechanizmów kontroli

Relacja pomiędzy organami stosującymi narzędzia nadzoru elektronicznego a osobami, których dane mogą być pozyskiwane i wykorzystywane, zakłada nierównowagę zarówno pod względem wiedzy, jak i możliwości kontrolnych. Obywatel nie tylko nie posiada wiedzy na temat podejmowanych wobec niego czynności i gromadzonych w ten sposób informacji, ale nie ma też żadnej możliwości skontrolowania, czy w tej sferze nie dochodzi do nadużyć. Z kolei organy uprawnione do walki z przestępczością dysponują bardzo szerokimi uprawnieniami, w tym do podejmowania czynności w sposób niejawny.

Jest zrozumiałe, że nie w każdej sytuacji obywatel powinien mieć dostęp do wiedzy na temat takich czynności (np. ze względu na dobro prowadzonego postępowania), jak również trudno sobie wyobrazić bezpośrednie mechanizmy kontrolowania organów uprawnionych do walki z przestępczością przez obywateli. Tym bardziej jednak powinny istnieć mechanizmy pośrednie, gwarantujące – z jednej strony – niezależność i ochronę informacji niejawnych, z drugiej – ochronę praw osób, których prywatność może być naruszana. Obecnie nie istnieje mechanizm, który umożliwiałby obywatelowi zweryfikowanie, czy – mimo braku prowadzonych wobec niego postępowań – dane na jego temat nie były zbierane lub analizowane (w tym przy wykorzystaniu narzędzi nadzoru elektronicznego). Nie chodzi tylko o możliwość wyłapania błędów lub działań niezgodnych z prawem, ale także o realizację konstytucyjnego prawa do prywatności, którego elementem jest dostęp do danych, jakie na nasz temat gromadzi państwo, o ile nie stoi to w sprzeczności z innymi wartościami chronionymi przez Konstytucję RP.

W naszej opinii wzrost technicznych możliwości gromadzenia, łączenia i analizy danych – także pochodzących z otwartych źródeł – powinien iść w parze ze wzmocnieniem gwarancji chroniących obywateli przed możliwymi nadużyciami w tej sferze oraz umożliwiających im pełną realizację prawa do prywatności. Takie gwarancje powinny być realizowane z jednej strony przez sądy – kontrolujące udostępnianie danych w konkretnych sprawach oraz przez niezależny, wyspecjalizowany organ kontrolujący działania policji i innych służb pod kątem ich

zasadności i skuteczności, a także rozpatrujący wnioski obywateli o dostęp do ich własnych danych.

Korzystanie z konkretnych narzędzi nadzoru i zbieranie określonych typów informacji powinno podlegać kontroli nie tylko ze względu na ochronę praw człowieka, ale także faktyczną skuteczność tych działań w walce z przestępczością. Jak pokazują choćby doświadczenia amerykańskich służb, tego typu kontroli nie jest w stanie realizować komisja parlamentarna, opierająca się przede wszystkim na oświadczeniach kontrolowanych organów i przygotowywanych dla nich dokumentach.

c. Wielofunkcyjność narzędzi i nowe możliwości analityczne

W toku prowadzonego monitoringu nie natknęliśmy się na doniesienia ani tym bardziej na potwierdzone informacje o zakupie lub wykorzystywaniu narzędzi nadzoru elektronicznego, których funkcjonalności wykraczałyby poza to, co dopuszcza polskie prawo. Z drugiej strony, jako obywatele nie mieliśmy możliwości zweryfikowania, w jaki konkretnie sposób tego typu narzędzia są wykorzystywane i czy np. nie prowadzi to do gromadzenia danych w sposób nieproporcjonalny lub nieuzasadniony w kontekście konkretnego postępowania. Problem, jaki zdiagnozowaliśmy w toku prowadzonego monitoringu, polega właśnie na tym, że to samo narzędzie może być wykorzystywane w różnych celach i z różnym skutkiem (jeśli chodzi o ingerencję w prawa i wolności obywateli), a decyduje o tym jedynie dysponujący tym narzędziem organ.

Ta sama czynność – np. zabranie i analiza danych o lokalizacji 1000 osób, analiza porównawcza kilkudziesięciu billingów czy analiza wszystkich komunikatów publikowanych na portalu społecznościowym pod kątem wybranych słów kluczowych – może być w danych okolicznościach uzasadniona, a w innych nie. Z tego względu nie ma sensu ocena samego faktu nabycia narzędzia, które taką czynność umożliwia. Potrzebna jest natomiast kontekstowa ocena sposobu i celów, w jakich jest ono faktycznie wykorzystywane. W naszej opinii takiej oceny również powinien dokonywać niezależny organ (vide powyższy punkt).

W tym kontekście zwracamy również uwagę na potrzebę precyzyjnego uregulowania zasad korzystania z narzędzi nadzoru elektronicznego, w szczególności określenie, jakie czynności stanowią kontrolę operacyjną (obecnie podlegającą nadzorowi sądów), a jakie kwalifikują się jako szeroko pojęte czynności operacyjno-rozpoznawcze, które mogą być realizowane bez kontroli sądów. W tym zakresie przepisy regulujące zasady działania policji i innych służb nie są precyzyjne i nie uwzględniają specyfiki nadzoru elektronicznego. Zwiększające się możliwości analizy i kojarzenia danych (również w czasie rzeczywistym oraz na masową skalę) powodują, iż nawet informacje pozyskiwane z otwartych źródeł po odpowiednim przetworzeniu mogą stanowić istotną ingerencję w prywatność obywateli. Ta zmiana w sferze technologii przemawia za zrewidowaniem katalogu czynności, jakie funkcjonariusze policji i innych służb mogą dokonywać bez zewnętrznej kontroli.