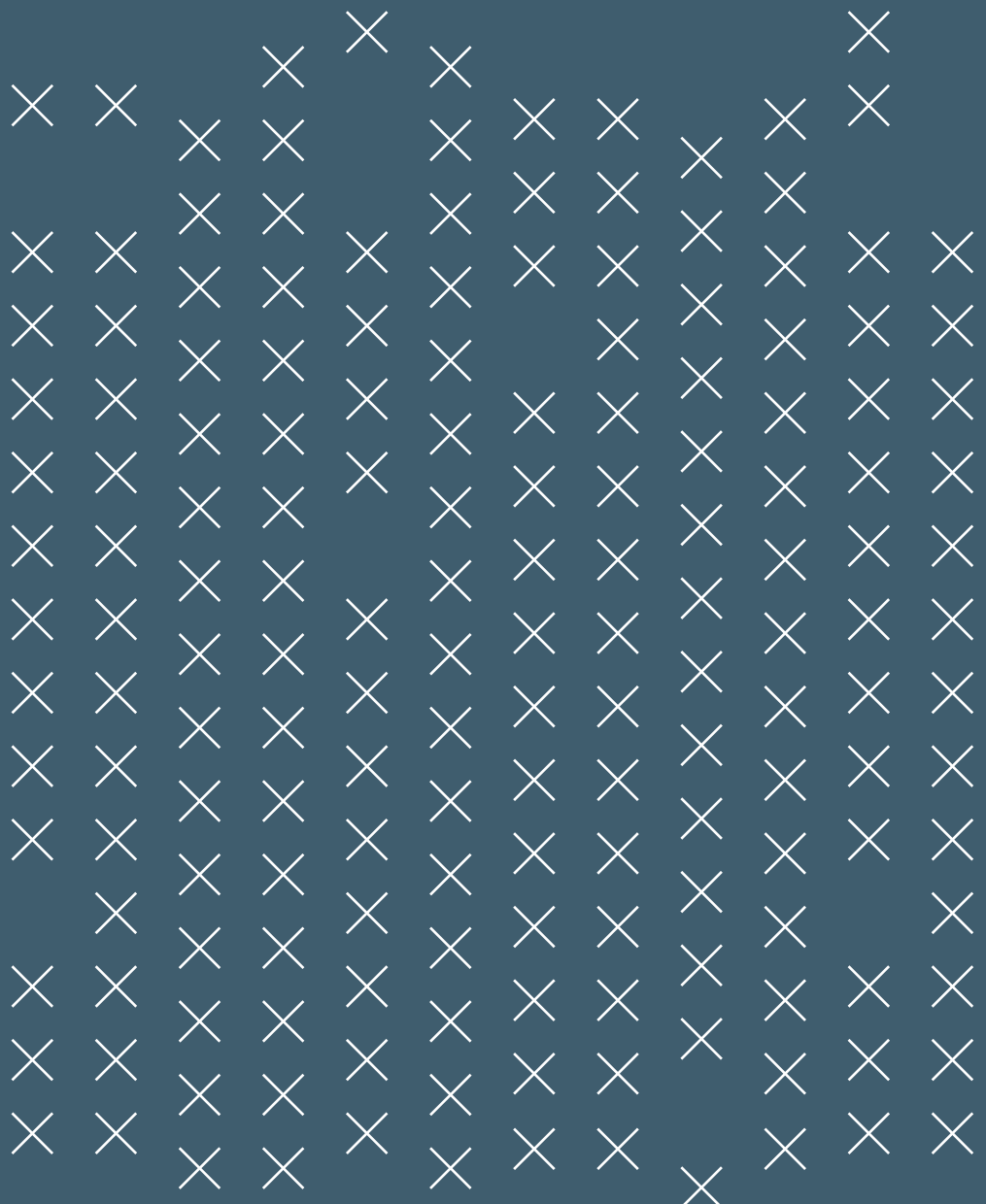
ZABAWKI WIELKIEGO BRATA

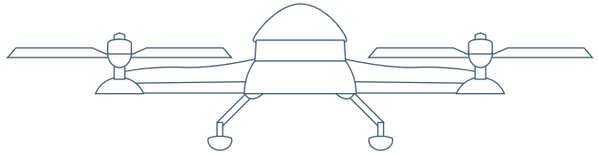


Serdecznie dziękujemy Krzysztofowi Jurusiowi i Radosławowi Stolarczykowi za pomoc pro bono w zebraniu i opracowaniu materiałów, na podstawie których przygotowaliśmy ten przewodnik, a także przedstawicielom instytucji, którzy starali się możliwie wyczerpująco odpowiedzieć na nasze pytania.

Zespół Fundacji Panoptykon

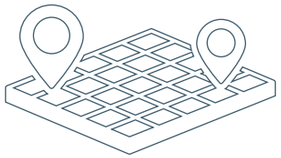
Warszawa 2016

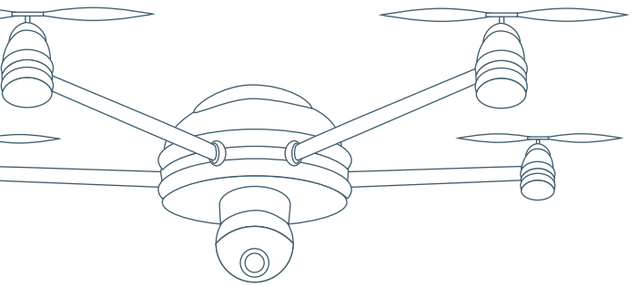
ISBN: 978-83-938554-4-5

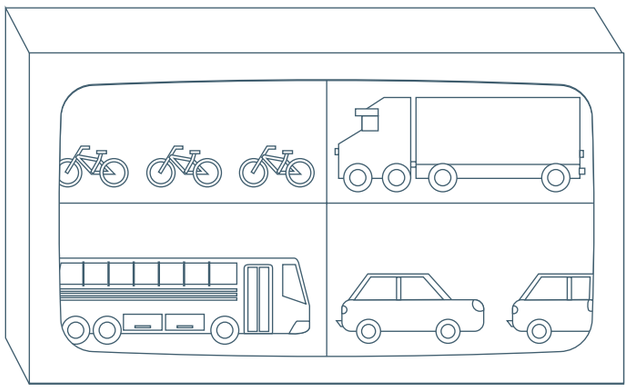


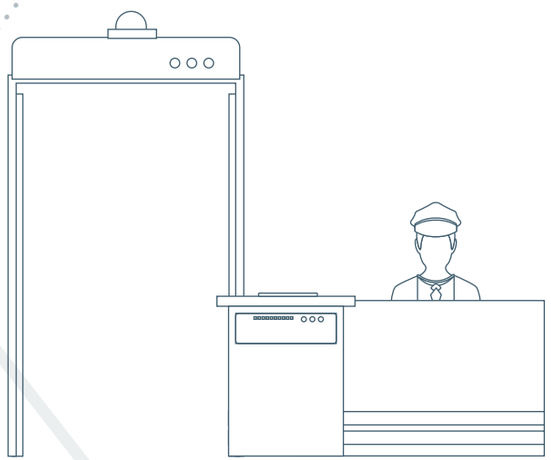
czyli

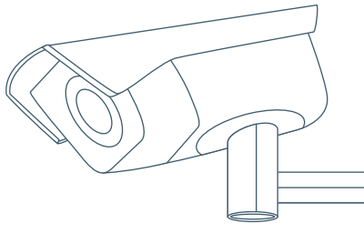
KRÓTKI PRZEWODNIK PO NARZĘDZIACH, KTÓRE POMAGAJĄ PAŃSTWU KONTROLOWAĆ OBYWATELI

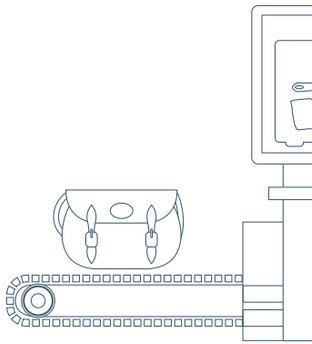


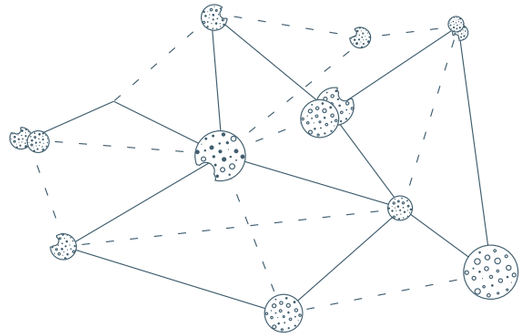


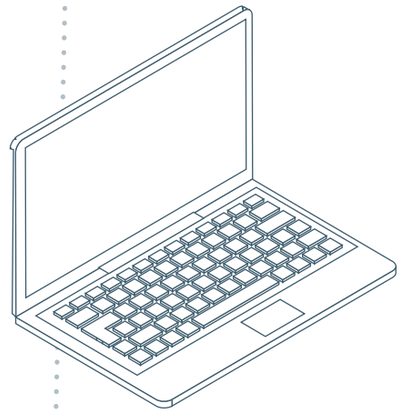


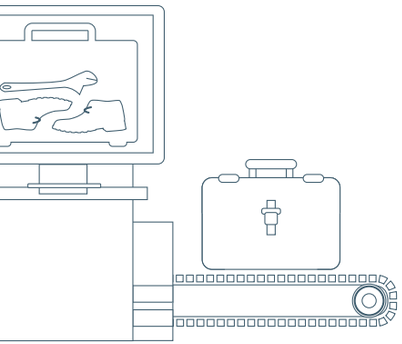


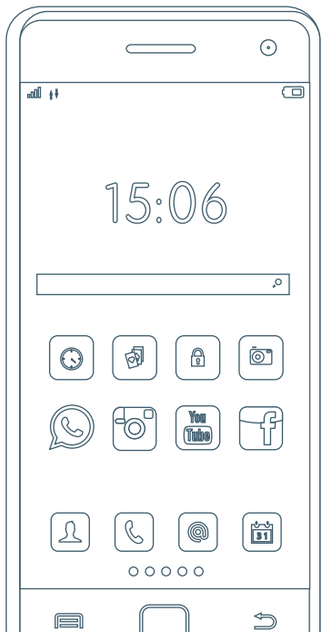


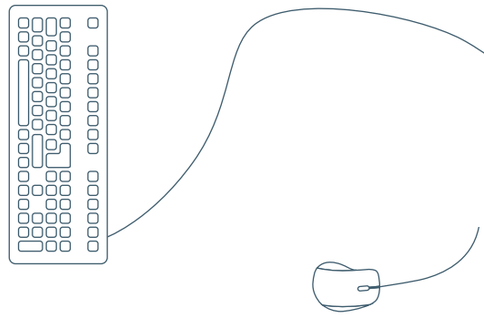












WPROWADZENIE

Które polskie miasto ma największy system miejskiego monitoringu? Jakie instytucje korzystają z dronów? A jakie z systemów rozpoznawania tablic rejestracyjnych? Czego można się o Tobie dowiedzieć dzięki karcie miejskiej? Ile państwo wydaje na rozwój systemów kontroli kierowców? Po co wyższej uczelni odciski palców wykładowców i studentów? W jakim urzędzie mogą być nagrane Twoje rozmowy? Do kogo trafiają informacje o tym, czego szukasz w serwisie swojego urzędu miasta? Czy policja może zdalnie przejąć kontrolę nad Twoim telefonem?

Odpowiedzi na te pytania – i wiele innych – znajdziesz w tym przewodniku.

Przewodnik opisuje różne narzędzia – zarówno sprzęt, jak i oprogramowanie – które są wykorzystywane przez instytucje publiczne do zbierania informacji o obywatelach, zarządzania nimi czy wykrywania rozmaitych nadużyć. Punktem wyjścia nie jest założenie, że wszystkie te narzędzia są z gruntu złe i nie powinny być przez państwo wykorzystywane. Wręcz przeciwnie – niektóre z nich bywają bardzo przydatne. Nie tylko mogą pomóc instytucjom publicznym sprawniej działać, ale też każdemu z nas ułatwić życie.

Kluczowe jest jednak to, kto i w jaki sposób konkretne narzędzie wykorzystuje. Takie spojrzenie na sprawę pozwala dostrzec wiele poważnych wyzwań. W praktyce bowiem często zwycięża ślepa wiara, że technologia pozwala w łatwy i skuteczny sposób rozwiązać każdy, nawet skomplikowany, społeczny problem. Zdarza się, że władze, decydując się na inwestycje w nowe rozwiązania, nawet nie starają się ich rzetelnie uzasadnić, nie analizują, jakie skutki uboczne przyniosą ani czy przypadkiem danego celu nie da się osiągnąć w inny sposób. W konsekwencji wdrażane są rozwiązania, które z jednej strony ograniczają wolność i głęboko ingerują w prawa obywateli, a z drugiej – pochłaniają środki publiczne, które można by znacznie lepiej spożytkować.

Wątek finansowy jest szczególnie istotny. Bo gdy możliwość wydania dużych pieniędzy przez państwo (zasilone środkami z Unii Europejskiej) spotyka się z możliwością zarobienia dużych pieniędzy przez sektor prywatny, dodatkowo rośnie ryzyko ucieczki w rozwiązania kuszące etykietą nowoczesności, ale niekoniecznie rzeczywiście skuteczne czy przyjazne prywatności.

Niestety – jako obywatele – często nie mamy w praktyce dostępu do informacji o tym, jakie narzędzia są używane do zbierania informacji o życiu każdego z nas ani w jaki sposób i przez kogo są wykorzystywane. W Fundacji Panoptykon staramy się to zmienić – wykorzystać dostępną, lecz rozproszoną wiedzę oraz prawo do informacji, aby elementy tej układanki poskładać w całość.

Badając ten temat, analizowaliśmy obowiązujące prawo; korzystaliśmy z zagranicznych raportów, publikacji medialnych oraz materiałów publikowanych przez firmy produkujące narzędzia nadzoru i korzystające z nich insty-

tucje publiczne (na przykład w Biuletynie Informacji Publicznej czy rejestrach zamówień publicznych); braliśmy udział w komercyjnych targach prezentujących dostępne rozwiązania techniczne; rozmawialiśmy z urzędnikami i funkcjonariuszami (również byłymi) policji. Wreszcie – do szeregu instytucji różnego szczebla, w tym centralnych i samorządowych (urzędów miast wojewódzkich oraz największych miast powiatowych w każdym województwie), wystosowaliśmy ponad 200 wniosków o informację publiczną. Do większości z nich dołączyliśmy szczegółowe kwestionariusze z pytaniami.

Przy gromadzeniu informacji nie obyło się bez perypetii. Część instytucji nie wyraziła zgody na przeprowadzenie rozmowy z ich przedstawicielami lub zupełnie zignorowała kierowaną w tej sprawie korespondencję. Przedstawiciele niektórych urzędów miast twierdzili, że musimy złożyć wniosek na specjalnym formularzu (Poznań, Nysa), inni przekonywali, że dostęp do informacji publicznej nie dotyczy stosowanych narzędzi nadzoru (pomorski oddział Narodowego Funduszu Zdrowia). Większość wniosków o informację publiczną doczekała się jednak odpowiedzi, choć nie wszystkie okazały się wyczerpujące. Zdarzały się też przypadki niezrozumienia zadanych pytań, a nawet udzielania odpowiedzi niezgodnych z prawdą. Te z przesyłanych informacji, które wzbudzały nasze wątpliwości, poddawaliśmy weryfikacji.

Zdarzały się również instytucje, które zupełnie zignorowały nasze wnioski o informację publiczną i nie udzieliły odpowiedzi na zadane pytania. Chyba najbardziej przewrotnym uzasadnieniem odmowy popisał się Zakład Ubezpieczeń Społecznych, powołując się na… ochronę danych osobowych. Najbardziej tajemnicze okazały się jednak tradycyjnie policja i inne służby. Żadna z nich na zadane pytania nie odpowiedziała w sposób wyczerpujący, a różnorodność reakcji na bardzo podobne pytania świadczy o stopniu oddalenia od spójnych standardów przejrzystości. Policja, Żandarmeria Wojskowa i Ministerstwo Finansów (pytane o działania kontroli skarbowej i Służby Celnej) udzieliły nam cząstkowych odpowiedzi, Centralne Biuro Antykorupcyjne i Agencja Bezpieczeństwa Wewnętrznego wydały decyzje odmowne, a Straż Graniczna uznała, że po naszej stronie nie ma szczególnego interesu publicznego, który uzasadniałby przekazanie nam przetworzonej informacji. Wszyscy wskazali na konieczność ochrony „form i metod" swoich działań. Służby specjalne wskazały przy tym, że informacje, o które pytamy, są niejawne, a ich upublicznienie zaszkodzi interesom Rzeczpospolitej.

Bezpośrednim efektem naszej pracy jest kilka sporów sądowych o informację publiczną, szereg wystąpień do instytucji, których praktyki wzbudziły wątpliwości co do legalności i poszanowania praw obywateli, oraz zestaw rekomendacji dotyczących wykorzystania narzędzi nadzoru w różnych sferach życia.

A także ten przewodnik. Nie mieliśmy ambicji opisania w nim wszystkich narzędzi nadzoru, jakie ma do dyspozycji państwo. Byłoby to zadanie z gruntu skazane na porażkę – narzędzi jest zbyt wiele, a wciąż tworzone są i wdrażane nowe rozwiązania. Zależało nam natomiast na tym, by pokazać różnorodność zarówno dostępnych narzędzi, jak i sposobów ich wykorzystania w różnych sferach życia (od prostych kamer monitoringu instalowanych w urzędach po szyte na miarę, skomplikowane systemy do analizy informacji). Nie skupialiśmy się przy tym na tych rozwiązaniach, które są używane do inwigilacji podejrzanych, lecz na tych, które są stosowane powszechnie lub mogą być wykorzystane wobec szerokiej grupy ludzi.

Zdajemy sobie sprawę z tego, że przewodnik zostawia wiele znaków zapytania. Mamy jednak nadzieję, że mimo to będzie on dla wszystkich zainteresowanych funkcjonowaniem państwa cennym źródłem wiedzy oraz inspiracją do refleksji nad tym, które z opisywanych narzędzi, rozwiązań prawnych i praktyk mają uzasadnienie, a które mogą okazać się niebezpieczne. Liczymy też, że lektura przewodnika zainteresuje przedstawicieli organizacji społecznych, dziennikarzy i wszystkich aktywnych obywateli tematem i skłoni nie tylko do zadawania własnych pytań i wyrażania opinii, ale też do walki o swoje prawa, w przypadku gdy zostały one naruszone.

Informacja jest pierwszym krokiem do zmiany. Zapraszamy do czytania!

W PRZESTRZENI PUBLICZNEJ

Miasta – niczym ludzie – mają swoje aspiracje. Dzisiaj najczęściej chcą być nowoczesne, inteligentne lub po prostu monitorowane. Ma to swoje konsekwencje. Miejską tkankę coraz częściej przenikają nowe technologie – kamery czy różnego rodzaju czujniki, które zbierają informacje o otaczającym świecie. I nieuchronnie – o ludziach, którzy w tej rzeczywistości żyją. Jednak mało komu przychodzi do głowy krytykować projekty opakowane w obietnicę sprawniejszego, tańszego, szybszego i bezpieczniejszego życia.

Ucieczka za miasto nie uwalnia od rozwiązań nakierowanych na kontrolę codzienności. Spotkamy je na modernizowanych z unijnych funduszy drogach, a nawet w lesie. Pierwsza część przewodnika opowiada o tym, w jaki sposób narzędzia te zadomowiły się w przestrzeni miejskiej i poza nią, jakimi informacjami o sobie dzielimy się, korzystając z komunikacji publicznej, oraz jakie programy pomagają kontrolować nas wtedy, gdy przemieszczamy się własnym samochodem.

PRZESTRZEŃ POD OBSERWACJĄ

Monitoring wizyjny od lat jest jednym z najbardziej popularnych narzędzi kontroli. Możemy go dziś napotkać niemal na każdym kroku: pączkuje w postaci mniejszych lub większych systemów – wykorzystywanych zarówno przez podmioty i osoby prywatne, jak i instytucje publiczne. Monitoring jest najbardziej rozpowszechniony w największych ośrodkach miejskich, jednak moda ta nie omija również mniejszych miejscowości.

W oku miejskiego monitoringu

Kamery monitoringu spotkać można dzisiaj niemal wszędzie – obserwują ulice i chodniki, przystanki, przejścia podziemne, a czasem również osiedla mieszkaniowe. W wielu miastach wyposaża się w nie rutynowo wszystkie kupowane pojazdy komunikacji miejskiej. Są one często instalowane w urzędach (więcej o tym w kolejnym rozdziale), łatwo można się na nie natknąć również w miejscach związanych z odpoczynkiem, rekreacją i kulturą: w parkach, na placach zabaw, na basenach, w ośrodkach sportowych, na stadionach czy w teatrach. Miasta często dokładają również do kamer montowanych w żłobkach, przedszkolach, szkołach czy pogotowiach opiekuńczych. Ich widok nie może dzisiaj dziwić nawet na cmentarzu.

NAJBARDZIEJ INTRYGUJĄCA ODPOWIEDŹ PRZYSZŁA Z KIELC – CELEM DZIAŁANIA TAMTEJSZEGO MIEJSKIEGO SYSTEMU MONITORINGU JEST... MONITOROWANIE PRZESTRZENI PUBLICZNEJ.

Szczegółowe wnioski o informację publiczną dotyczące funkcjonowania miejskich kamer monitoringu Fundacja Panoptykon skierowała do 48 miast wojewódzkich i powiatowych. Okazało się, że prawie w każdym z nich działają scentralizowane miejskie systemy monitoringu. Największe (w Poznaniu i Warszawie) obejmują swoim zasięgiem ponad 400 kamer. Ale są też takie, które ograniczają się do kilkunastu sztuk (na przykład w Słupsku czy Nysie).

Oczywiście kamer finansowanych z budżetów miast jest znacznie więcej – w przypadku większych miast oficjalne szacunki mówią o kilku tysiącach. Trudno tu jednak o ścisłe i porównywalne dane, bo w każdym z miast urzędnicy liczą je na swój sposób. Niektóre na przykład w odpowiedziach na wnioski o informację publiczną wliczyły sprzęt zainstalowany w środkach komunikacji miejskiej i szkołach, inne zaś nie.

W praktyce monitoring może działać w oparciu o różne modele. Rejestracja obrazu jest standardem w większości przypadków, ale stała obserwacja w centrum odbiorczym przez wyszkolonych operatorów jest normą jedynie w przypadku miejskich, scentralizowanych systemów monitoringu. W innych przypadkach zazwyczaj nikt na stałe nie obserwuje obrazu lub robi to jedynie z doskoku (w trakcie wykonywania innych obowiązków). Czasami zdarza się również, że obraz udostępniany jest nieograniczonemu gronu odbiorców (na przykład w przypadku upubliczniania w Internecie podglądu z tego, co dzieje się na basenie czy w przestrzeni miejskiej) bądź wybranym osobom (po zalogowaniu się).

W odpowiedzi na zadane pytania przedstawiciele przeważającej większości miast oświadczyli, że celem działania miejskiego systemu monitoringu jest dbałość o bezpieczeństwo. Było ono jednak definiowane na rozmaite sposoby: od prewencji, poprzez reagowanie na przypadki łamania prawa, po wykrywanie sprawców i dostarczanie dowodów. Pojawiały się również odpowiedzi dotyczące na przykład udzielania pierwszej pomocy, ochrony mienia czy też – w przypadku Łodzi – „wsparcia rozwoju gospodarczego miasta, w tym rozwoju funkcji metropolitalnych". Chyba najbardziej intrygująca odpowiedź przyszła z Kielc – celem działania tamtejszego miejskiego systemu monitoringu jest... monitorowanie przestrzeni publicznej.

W PRAKTYCE MIEJSKI MONITORING SŁUŻY PRZEDE WSZYSTKIM DO WALKI Z NIEPRZEPISOWYM PARKOWANIEM, WZGLĘDNIE – Z OSOBAMI ZAKŁÓCAJĄCYMI PORZĄDEK LUB PIJĄCYMI ALKOHOL W MIEJSCU PUBLICZNYM.

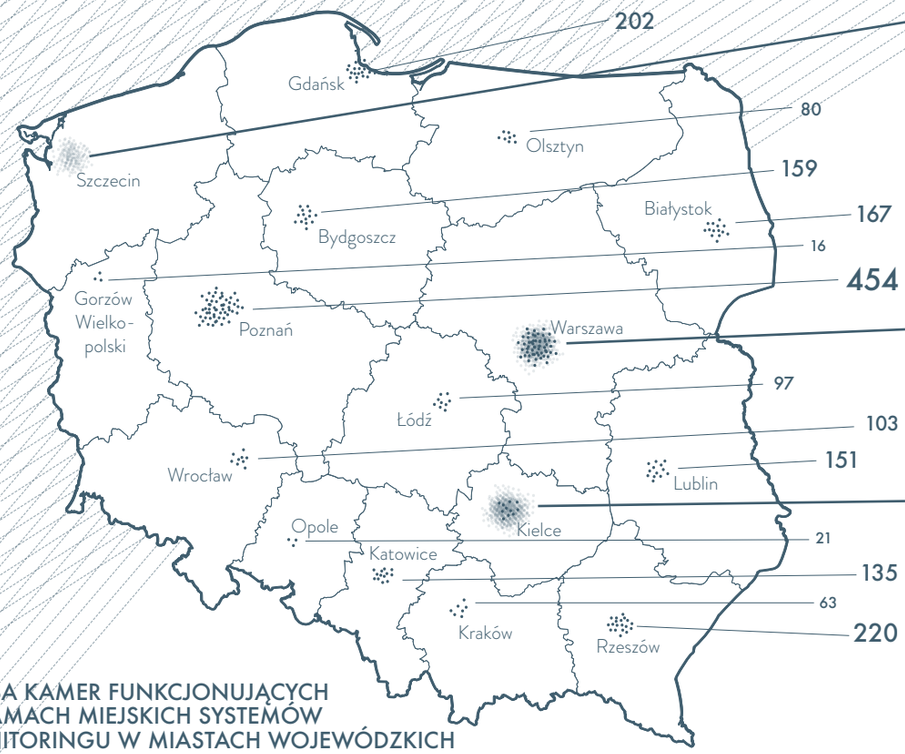
Jak widać, cele te są ogólnikowe i nie do końca spójne. Nie jest to jednak jedyny związany z nimi problem. Kolejny polega na tym, że realizacja tych celów nie jest na poważnie weryfikowana. Jedynie połowa zapytanych miast odpowiedziała, że instytucje odpowiedzialne za działanie miejskiego systemu monitoringu starają się skuteczność jego działania poddawać ewaluacji. Co jeszcze wcale nie oznacza, że robią to w sposób, który pozwala na wyciągnięcie wiarygodnych wniosków. Najczęściej polega to na pytaniu o opinię przedstawicieli policji lub straży miejskiej bądź na analizie statystyk policyjnych. Niedawny raport Najwyższej Izby Kontroli był dla kilkudziesięciu skontrolowanych miejskich systemów monitoringu druzgocący – okazało się, że w przeważającej większości przypadków nikt realnie nie ewaluuje ich działania, a w praktyce monitoring służy przede wszystkim do walki z nieprzepisowym parkowaniem, względnie – z osobami zakłócającymi porządek lub pijącymi alkohol w miejscu publicznym.

Oceniając działanie systemów monitoringu i podejmując decyzje o ich rozbudowie, warto nie tylko sprawdzać ich działanie w praktyce, ale też brać pod uwagę wyniki badań naukowych. A te nie potwierdzają tezy, by monitoring mógł na szerszą skalę odstraszać od popełniania przestępstw czy od innych niepożądanych zachowań. Część przestępców uczy się oszukiwać kamery bądź przenosi się w niemonitorowane miejsca. Pozostali, działający w mniej przemyślany sposób (na przykład osoby nietrzeźwe, działające pod wpływem impulsu), dopuszczają się przestępstw, nie myśląc o obecności kamer.

Korzystanie z monitoringu – jako narzędzia, które wkracza w prywatność obywateli – powinno odbywać się tylko wówczas, gdy przewiduje to ustawa. Odpowiedzi przedstawicieli miast na pytania dotyczące podstawy prawnej do działania miejskich systemów monitoringu wskazują na spory bałagan i dezorientację. Najczęściej powoływali się oni na ustawę o samorządzie gminnym (która nakłada na gminę ogólny obowiązek zapewnienia porządku publicznego i bezpieczeństwa) lub ustawę o strażach gminnych (która przyznaje uprawnienie do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych). Niektóre odpowiedzi mogą jednak budzić większe zdziwienie. Urzędnicy z Piotrkowa Trybunalskiego jako podstawę prawną wskazali ustawę o finansach publicznych, Chełma – ustawę o ochronie osób i mienia, a Nowego Sącza – poza ustawą o strażach gminnych – Konstytucję RP i ustawę o ochronie danych osobowych (która sama w sobie nie daje podstaw do zbierania jakichkolwiek informacji o obywatelach). W odpowiedzi z Przemyśla w ogóle nie wskazano podstawy prawnej, a w piśmie z Rzeszowa – zwrócono uwagę, że choć takiej podstawy brakuje, nie zwalnia to władz miasta z obowiązku dbania o bezpieczeństwo mieszkańców.

Niestety, w Polsce nie doczekaliśmy się wciąż przepisów, które ustalałyby zasady działania monitoringu. Nie wskazuje ich żadna ze wskazanych wyżej ustaw. Oznacza to, że nie jest jasne, kto może korzystać z kamer, gdzie je instalować, do czego wykorzystywać nagrania, jak je zabezpieczać itd. W praktyce co miasto, to inny obyczaj.

Za miejskie systemy monitoringu odpowiadają różne podmioty. Najczęściej administratorem



LICZBA KAMER FUNKCJONUJĄCYCH W RAMACH MIEJSKICH SYSTEMÓW MONITORINGU W MIASTACH WOJEWÓDZKICH

? Szczecin i Katowice w odpowiedzi na wnioski o informację publiczną wskazały, że dysponują kamerami działającymi w miejskich systemach monitoringu, jednak nie podały ich liczby. Wiadomo, że w Szczecinie w jednostkach miejskich pod koniec 2015 r. funkcjonowało 2559 zewnętrznych i wewnętrznych kamer, nie jest jednak jasne, ile z nich włączono w miejski system monitoringu. Z informacji prasowych wynika, że w Katowicach w skład systemu monitoringu wchodziło 130 kamer, miał on być jednak rozbudowany do 265 urządzeń. Niestety, nie udało się ustalić, czy rozbudowa się zakończyła.

410 / ? Kamery funkcjonujące w ramach miejskich systemów monitoringu to jedynie ułamek tego typu urządzeń wykorzystywanych w mieście. Dane na mapie pokazują tylko, ile kamer działa w obrębie takich systemów. Liczba ta nie uwzględnia kamer miejskich działających poza systemem ani kamer monitoringu instalowanych przez urzędy centralne i podmioty prywatne.

5667 Już liczba kamer monitoringu finansowanych z budżetu miasta znacznie przewyższa liczbę tych działających w ramach miejskiego systemu. Zgodnie z szacunkami władz miasta w samych tylko Kielcach w komunikacji miejskiej, w przedszkolach, żłobkach i szkołach, w instytucjach kultury itp. działa co najmniej 5657 kamer.

systemu jest policja lub straż miejska, czasem natomiast urząd miasta lub różne jego jednostki (na przykład biura obsługi informatycznej i telekomunikacyjnej, wydziały bezpieczeństwa czy zarządzania kryzysowego). Każdy z tych podmiotów przechowuje nagrania tak długo, jak uznaje to za stosowne. Nawet jeśli porównamy ze sobą reguły obowiązujące w poszczególnych miejskich systemach, które powinny działać na podobnych zasadach, okaże się, że praktyki są bardzo różne. Przeciętnie nagrania przechowywane są przez 20–30 dni. Ale w Rzeszowie ten okres wynosi 7 dni, a we Włocławku – 60 dni. Władze Olsztyna natomiast odpowiedziały, że przechowują nagrania co najmniej 30 dni i najwyraźniej nie uznały za stosowne wyznaczenia maksymalnej granicy. Czy to oznacza, że zdarza im się nie kasować nagrań?

Brak zasad korzystania z monitoringu dotyczy też publikacji nagrań i udostępniania ich różnym podmiotom. Nawet na poziomie miejskich systemów można się spotkać z rozmaitymi praktykami. W efekcie nikt nie może mieć pewności, że nagranie z jego udziałem nie trafi do telewizji czy Internetu, nawet jeśli nie popełnił żadnego przestępstwa.

Inny problem: choć obywatelom należy się informacja o obecności i sposobie działania kamer, brak wyraźnego obowiązku po stronie podmiotów korzystających z monitoringu przekłada się na to, że o wyczerpującą informację bardzo trudno. Do zupełnej rzadkości należą w Polsce – znane z niektórych krajów – tablice precyzyjnie informujące o tym, kto odpowiada za wykorzystywany w danym miejscu monitoring i do kogo można się zwrócić z pytaniem bądź problemem. Często mamy natomiast do czynienia z dezinformacją, która może polegać na straszeniu kamerami tam, gdzie ich nie ma, bądź instalowaniu atrap.

NIKT NIE MOŻE MIEĆ PEWNOŚCI, ŻE NAGRANIE Z JEGO UDZIAŁEM NIE TRAFI DO TELEWIZJI CZY INTERNETU, NAWET JEŚLI NIE POPEŁNIŁ ŻADNEGO PRZESTĘPSTWA.

Ze względu na popularność monitoringu tworzenie i rozwój systemów jest prawdziwą pożywką dla biznesu. Wybór firm dostarczających monitoringowe rozwiązania techniczne jest bardzo duży. Na rynku funkcjonują zarówno mniejsze przedsiębiorstwa, jak i duże korporacje z siedzibami w różnych państwach (na przykład Pelco, SeeTec).

Utworzenie i utrzymanie miejskiego systemu monitoringu to realny koszt. W mniejszych miastach jego zbudowanie pochłaniało zazwyczaj kilkaset tysięcy złotych, w większych – miliony (w Warszawie – 58 mln złotych, w Poznaniu – 30 mln złotych). Koszty utrzymania systemu są trudniejsze do porównania, bo miasta nie mają spójnego sposobu ich liczenia. Najczęściej szacują je jednak na kilkaset tysięcy złotych rocznie. W przypadku bardziej rozbudowanych systemów są one jednak wyższe. Na przykład w Warszawie koszt utrzymania odpowiadającego za miejski system Zakładu Obsługi Systemu Monitoringu wynosi około 15 mln zł i jest porównywalny z budżetem Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Obraz to nie wszystko

Liczba kamer monitoringu wciąż rośnie, a oczekiwania z nimi wiązane zaczynają wykraczać poza możliwości działania ograniczonej grupy operatorów. Niektórzy uważają, że rozwiązaniem tego problemu jest wsparcie działania ludzi przez rozmaite programy komputerowe. Rozwijane są systemy łączące dane z monitoringu z innymi informacjami. Algorytmy służące rozpoznawaniu twarzy czy automatycznemu wykrywaniu zagrożeń są coraz częściej testowane, również w Polsce, ale jeszcze nie są wykorzystywane na masową skalę. Wciąż również budzą wątpliwości, zarówno pod kątem skuteczności, jak i kontroli nad ich działaniem (na przykład nad tym, kto decyduje, jakie zachowania należy uznać za podejrzane). Niektóre automatyczne funkcjonalności zdążyły już zrobić karierę i są wykorzystywane dość powszechnie. Mowa przede wszystkim o rozpoznawaniu tablic rejestracyjnych (więcej na ten temat w dalszej części rozdziału).

Zdarza się, że sprzęt monitoringowy jest wyposażony w specjalne głośniki, które umożliwiają operatorowi śledzącemu sytuację zwrócenie uwagi osobie naruszającej porządek. W praktyce może chodzić choćby o śmiecenie czy picie alkoholu w miejscu publicznym. Rozwiązanie to nie jest wykorzystywane często (pojawiło się na przykład w Legionowie i Tczewie), jednak zazwyczaj budzi spore poruszenie. Oto bowiem narzędzie, które służy do obserwacji, a samo nie bywa szczególnie widoczne, nagle przemawia ludzkim głosem, i to jeszcze w sytuacjach, które zazwyczaj nie są dla osób dotkniętych interwencją zbyt przyjemne.

W WIELU DUŻYCH MIASTACH W POLSCE STANDARDEM JEST UMIESZCZANIE MIKROFONÓW W KABINIE KIEROWCY AUTOBUSU (MOTORNICZEGO TRAMWAJU) LUB W JEJ POBLIŻU.

Znacznie większe kontrowersje budzi jednak sytuacja, gdy dźwięk przesyłany jest w drugą stronę, czyli wówczas, gdy jest on rejestrowany przez kamery monitoringu lub dołączone do nich mikrofony. Niestety, nie zawsze osoby podsłuchiwane zdają sobie z tego sprawę. Powód jest prozaiczny: nikt ich o tym nie informuje.

W niektórych przypadkach obowiązek rejestracji dźwięku wynika bezpośrednio z prawa. Z taką sytuacją mamy do czynienia na przykład na stadionach czy w większych halach sportowych, które są miejscami szczególnie ściśle nadzorowanymi. Zgodnie z ustawą o bezpieczeństwie imprez masowych w trakcie takich wydarzeń rejestracja obrazu i dźwięku, w sposób umożliwiający wykorzystanie w postępowaniu dowodowym, jest obowiązkowe.

Częściej jednak zdarza się, że nagrywanie dźwięku w miejscach publicznych jest autonomiczną decyzją konkretnego podmiotu. Tak jest na przykład w przypadku mikrofonów montowanych coraz częściej w pojazdach komunikacji miejskiej. Z odpowiedzi na rozesłane przez Fundację Panoptykon ankiety wynika, że w wielu dużych miastach w Polsce standardem jest umieszczanie ich w kabinie kierowcy autobusu (motorniczego tramwaju) lub w jej pobliżu. Rejestratory mają służyć najczęściej kontroli pracy kierowcy i rozstrzyganiu ewentualnych sporów między nim a pasażerami.

Trudno jednak wykluczyć, że taki mikrofon nie zarejestruje rozmów przypadkowych pasażerów. Nigdy też nie wiadomo, jak zostanie to wykorzystane. Problem ten dobrze ilustruje historia wypadku autobusu PKS, do którego doszło w 2013 r. na trasie ze Stegny do Gdańska. Kierowca zasłabł w trakcie jazdy, ale poważniejszych konsekwencji udało się uniknąć dzięki przytomnej reakcji pasażerów. Nagranie z kamery zamontowanej w autobusie trafiło do mediów – każdy mógł nie tylko obejrzeć przebieg wydarzeń, ale też usłyszeć krzyki przerażonych ludzi.

Miejskie zakłady transportu z Łodzi i Opola poszły jeszcze dalej i zamontowały mikrofony w przestrzeni dla pasażerów. Już nagrywanie kierowców można uznać za niepotrzebne i zbyt głęboko ingerujące w ich prywatność, natomiast dla nagrywania dźwięku w przestrzeni pasażerskiej trudno doszukać się jakiegokolwiek przekonującego uzasadnienia. Fundacja Panoptykon zwróciła uwagę na to nadużycie obu zakładom, jednak te – przynajmniej na razie – zignorowały przedstawione argumenty.

Z kamerą wśród zwierząt

Takie narzędzia jak monitoring w przestrzeni miejskiej stały się normą. Ale co z miejscami nieco bardziej dzikimi? Każdy, kto lubi spędzać czas wolny na leśnych szlakach, może trafić na tabliczki z informacją o monitoringu. Czy w lasach rzeczywiście niemal na każdym kroku można zostać nagranym, czy to jedynie strachy na lachy?

Fundacja Panoptykon postanowiła się o tym przekonać, kierując oficjalne pytania do Lasów Państwowych, lasów warszawskich oraz 8 popularnych parków narodowych. Lasy Państwowe potwierdziły, że na ich terenie wykorzystywanych jest co najmniej 419 kamer – co najmniej, bo danymi dotyczącymi tylu kamer dysponuje ich Dyrekcja Generalna. Ale w rzeczywistości może być ich więcej. Lasy warszawskie przyznały się do korzystania tylko z 4 kamer (choć tabliczek-straszaków jest na ich terenie więcej). W parkach narodowych sytuacja wygląda bardzo różnie: są takie, które zadeklarowały, że w ogóle nie wykorzystują monitoringu (Karkonoski), oraz takie, które dysponują ponad 40 kamerami (Słowiński, Tatrzański).

Władze lasów i parków jako monitoring potraktowały również w większości przypadków uruchomiane po wykryciu ruchu fotopułapki, które są montowane w miejscach koncentracji dzikich zwierząt i służą do ich obserwacji. Jeśli trafiają one rzeczywiście do najbardziej odosobnionych miejsc, to trudno mieć zastrzeżenia do takiego wykorzystania nowych technologii. Jednak, zgodnie z deklaracjami, wśród przebadanych instytucji tylko Bieszczadzki Park Narodowy ogranicza się do takiego korzystania z kamer. Inne montują je nie tylko w budynkach i na parkingach, ale również na dostępnych dla odwiedzających ścieżkach i drogach.

Po co w takich miejscach monitoring? Uzasadnienia, które przedstawiły władze lasów i parków są rozmaite i różnią się w zależności od instytucji: od ochrony przeciwpożarowej, przez walkę ze złodziejami drewna, osobami porzucającymi śmieci czy wjeżdżającymi do lasu w miejscach niedozwolonych, po zabezpieczenie mienia i kontrolę pracy ajentów. Przedstawiciele lasów i parków twierdzą, że weryfikują realizację tych celów, w praktyce nie wygląda to jednak tak różowo. Większość podmiotów nie zbiera nawet statystyk wykorzystania kamer, a wszelkie informacje dotyczące metod weryfikacji ich przydatności odnoszą się do monitoringu zachowania zwierząt, a nie ludzi.

KAŻDY LAS I PARK PRZECHOWUJE NAGRANIA WEDLE UZNANIA. NAJCZĘŚCIEJ PRZEZ 14 LUB 30 DNI. ALE KAMPINOSKIEMU PARKOWI NARODOWEMU WYSTARCZA PRZECHOWYWANIE NAGRAŃ PRZEZ 5 DNI, A GORCZYŃSKI I PIENIŃSKI KASUJĄ JE DOPIERO PO 90 DNIACH.

Obraz z kamer rzadko kiedy obserwowany jest na bieżąco, za to w większości przypadków jest on rejestrowany. Ze względu na brak zasad każdy las i park przechowuje nagrania wedle uznania. Najczęściej przez 14 lub 30 dni. Ale na przykład Kampinoskiemu Parkowi Narodowemu wystarcza przechowywanie nagrań przez 5 dni, a Gorczyński i Pieniński kasują je dopiero po 90 dniach. Ciekawe rozwiązanie przyjęto w Bieszczadzkim Parku Narodowym. Ponieważ tam kamery wykorzystywane są do „polowania" na zwierzęta, a nie ludzi, nagrania co do zasady w ogóle nie są usuwane. Jeśli natomiast przypadkiem zostanie zarejestrowany człowiek, pracownicy mają obowiązek od razu skasować odpowiednią część nagrania.

Jeśli jednak celem obserwacji jest kontrolowanie zachowań ludzi, to znów wątpliwości budzi podstawa prawna, w oparciu o którą lasy i parki ingerują w prawa obywateli. Zapytane o to instytucje odpowiadały rozmaicie. Powoływano się na ustawę o lasach lub o ochronie przyrody, ale też na ustawę o ochronie danych osobowych, rozmaite rozporządzenia i zarządzenia. Przedstawiciele części instytucji wprost przyznali, że nie mają podstawy prawnej do korzystania z monitoringu.

Nie udało nam się uzyskać pełnych informacji dotyczących kosztów korzystania z monitoringu w lasach i parkach narodowych. Część z instytucji zignorowała pytania o pieniądze, a na przykład Kampinoski Park Narodowy zasłonił się tajemnicą handlową. W dostępnych danych uwagę przykuwają różnice w deklarowanych kosztach instalacji monitoringu. Bory Tucholskie za swój monitoring obejmujący kilka kamer miały zapłacić kilka tysięcy, a Słowiński Park Narodowy za swój składający się z kilkudziesięciu kamer – ponad milion złotych.

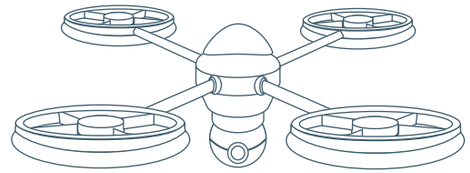
Kamera w ruchu

Obserwować przestrzeń wokół można nie tylko dzięki kamerom przytwierdzonym do ściany czy słupa. Wehikułami, które zapewniają dzisiaj urządzeniom nagrywającym mobilność, mogą być samochody, drony czy wreszcie ludzie. Ci ostatni to na przykład funkcjonariusze nagrywający swoje interwencje. Kamery przymocowane do ciała (*body cameras*) szczególną karierę robią za oceanem, gdzie mają być na przykład odpowiedzią na nadużycia policji. Moda ta dotarła również do Polski – kamery pojawiają się na mundurach strażników miejskich w kolejnych miejscowościach, mimo wątpliwości, czy takie działania można uznać za adekwatne do problemów i zgodne z prawem.

Najbardziej mobilny monitoring możliwy jest dzięki dronom. Tak powszechnie nazywane są bezzałogowe statki powietrzne, których lot jest zaprogramowany albo sterowany zdalnie. Niektóre są duże, inne – naprawdę maleńkie. Różnią się też możliwościami i wyposażeniem, przy czym kamery są montowane w nich standardowo. Dzięki temu drony mogą uzyskać obraz z różnych perspektyw, obserwować trudno dostępne bądź niebezpieczne miejsca, objąć zasięgiem większą przestrzeń czy podążać za interesującym obiektem.

Drony od wielu już lat są wykorzystywane w konfliktach zbrojnych – zarówno do zbierania informacji, jak i zabijania przeciwników (tzw. *targeted killings*) – i ten aspekt ich działania budzi zazwyczaj największe kontrowersje. Jednocześnie stają się one jednak również częścią naszego codziennego życia. Dzisiaj to z jednej strony popularny prezent dla dziecka, a z drugiej – w bardziej zaawansowanej wersji – narzędzie wykorzystywane w codziennej pracy przez różne instytucje. Drony mogą być używane do sprawdzania poziomu wód, reagowania na klęski żywiołowe, w ramach akcji ratunkowych czy do kręcenia filmów promujących dane miasto. Ale też do nadzoru nad obywatelami, choćby w ramach ochrony granic czy kontrolowania przebiegu demonstracji.

DRON TO Z JEDNEJ STRONY POPULARNY PREZENT DLA DZIECKA, A Z DRUGIEJ – W BARDZIEJ ZAAWANSOWANEJ WERSJI – NARZĘDZIE WYKORZYSTYWANE W CODZIENNEJ PRACY PRZEZ RÓŻNE INSTYTUCJE.



Ostatnio głośno było o tym, że PKP Cargo wykorzystuje drony do walki z kradzieżami. Ale nie jest to odosobniony przypadek. Z uzyskanych przez Fundację Panoptykon informacji wynika, że narzędzie to posiadają i w swojej działalności wykorzystują także m.in. policja, Żandarmeria Wojskowa, straż pożarna czy krakowski urząd miasta. Na egzemplarz wydano od kilku do kilkudziesięciu tysięcy złotych. Niestety, część służb nie odpowiedziała na pytania dotyczące wykorzystania dronów, zasłaniając się ochroną informacji niejawnych. Trudno jednak przekonująco uzasadnić, dlaczego obywatele nie mogą wiedzieć, że dana instytucja korzysta z takiego narzędzia.

Drony, choć przydatne w wielu dziedzinach życia, stanowią spore wyzwanie dla prywatności. Niestety, nasze prawo te zagrożenia zupełnie ignoruje, a problem – ze względu na rozwój technologii, jej coraz większą popularność i dostępność – będzie się pogłębiał. W 2015 r. rozpoczęto prace nad rozporządzeniem dotyczącym wykorzystania dronów – dotyczyło ono jednak tylko zagadnień technicznych związanych z bezpieczeństwem lotów. Ochrona prywatności obywateli nie wchodzi bowiem w zakres kompetencji Urzędu Lotnictwa Cywilnego, który był inicjatorem prac nad nową regulacją.

KOMUNIKACJA BARDZO PUBLICZNA

Do pracy, do szkoły, na spotkanie z przyjaciółmi, na wakacje – w wiele miejsc możemy dotrzeć, korzystając autobusów, pociągów i innych środków zbiorowej komunikacji. Każdy, kto się na to zdecyduje, musi się jednak liczyć z kontrolą prowadzoną choćby przez osobę sprawdzającą bilety. Może jednak nie zdawać sobie sprawy z tego, że coraz częściej jest ona uzupełniana o działanie różnych narzędzi technicznych, które w nie zawsze jawny sposób zbierają informacje o pasażerach.

Wszystko wiedzące karty

Przez lata do korzystania z komunikacji miejskiej wystarczał bilet kartonikowy. Dzisiaj bez kart miejskich trudno sobie wyobrazić nowoczesny system komunikacji. W poszczególnych miastach noszą one różne nazwy: URBANCARD – we Wrocławiu, Migawka – w Łodzi, PEKA – w Poznaniu, Śląska Karta Usług Publicznych – w aglomeracji śląskiej, Warszawska Karta Miejska – w Warszawie. W praktyce są to plastikowe elektroniczne karty zbliżeniowe, które nie tylko służą jako nośniki biletów komunikacji miejskiej, ale także umożliwiają korzystanie z innych usług.

Wielofunkcyjność to nie jedyna nowość związana z kartami miejskimi. Druga ważna zmiana polega na tym, że nie są one anonimowe i tym różnią się zarówno od tradycyjnych biletów jednorazowych, jak i wszelkich innych na okaziciela. Co więcej – różnią się one również od tradycyjnych biletów okresowych. Te były zazwyczaj imienne, jednak imienność ta ograniczała się do nośnika, na którym właściciel karty umieszczał swoje imię i nazwisko oraz numer dokumentu tożsamości. W przypadku nowych kart miejskich dane pasażera trafiają nie tylko na noszony przy sobie kawałek plastiku, ale również do bazy danych.

W PRZYPADKU NOWYCH KART MIEJSKICH DANE PASAŻERA TRAFIAJĄ NIE TYLKO NA NOSZONY PRZY SOBIE KAWAŁEK PLASTIKU, ALE RÓWNIEŻ DO BAZY DANYCH.

Każda osoba, która chce korzystać z karty miejskiej, jest zobligowana do podania informacji o sobie. W zależności od miasta mogą to być: imię i nazwisko, numer PESEL (data urodzenia), miejsce zamieszkania (zameldowania), numer telefonu, adres e-mail oraz zdjęcie (to ostatnie jest często kasowane po wydaniu karty).

Karty miejskie są wykorzystywane mniej więcej w połowie z 40 miast wojewódzkich i powiatowych, które odpowiedziały na pytania Fundacji Panoptykon. Podstawą prawną ich funkcjonowania są co do zasady uchwały rady miasta. Ich podejmowanie ma podstawę w ustawie o samorządzie gminnym, zgodnie z którą organizacja transportu miejskiego jest zadaniem gminy.

W każdym z miast podstawową funkcją kart jest kodowanie biletów komunikacji miejskiej. Odbywa się to w różnych formułach, które czasami współwystępują: biletu okresowego (na przykład miesięcznego czy kwartalnego) lub e-portmonetki (która umożliwia opłacanie kolejnych przejazdów z puli środków pieniężnych zakodowanych na karcie).

Korzystanie z kart miejskich to nie tylko wygoda dla pasażerów, ale także możliwość zbierania przez miasto dodatkowych informacji. Wielu przewoźników chwali się, że „rejestracja" kart miejskich w pojazdach pozwala analizować sposób korzystania pasażerów z komunikacji

miejskiej, lepiej zarządzać taborem czy planować rozkład jazdy. Z tego względu mieszkańcy Nowego Sącza są obligowani do zbliżania karty do kasownika przy każdym wejściu do pojazdu, a kaliszanie – zarówno przy wejściu, jak i przy wyjściu. Nie wszystkie miasta jednak decydują się na takie obostrzenia.

MOŻLIWOŚĆ INTEGRACJI DANYCH SPRAWIA, ŻE W JEDNYM MIEJSCU GROMADZONY MOŻE BYĆ SZEROKI ZAKRES INFORMACJI NA TEMAT MIESZKAŃCÓW, ICH ZWYCZAJÓW, UPODOBAŃ, WYDATKÓW.

Dane zbierane na potrzeby wydania karty w trakcie korzystania z niej są uzupełniane o inne informacje. Mogą to być na przykład dane umożliwiające ustalenie tras podróży poszczególnych osób. W przypadku warszawskiego Zarządu Transportu Miejskiego GIODO zakwestionował wprawdzie taką praktykę, nie oznacza to jednak, że takie ograniczenie biorą pod uwagę twórcy systemów w innych miastach. Jeśli dodać do tego informacje związane z korzystaniem z innych funkcji karty miejskiej, otrzymujemy kompleksowy pakiet różnorodnych informacji. Możliwość integracji danych sprawia, że w jednym miejscu gromadzony może być szeroki zakres informacji na temat mieszkańców, ich zwyczajów, upodobań, wydatków.

Bogactwo informacji, jakie można – przynajmniej potencjalnie – zbierać za pomocą kart miejskich, wynika z tego, że do podstawowej funkcjonalności (czyli płacenia za korzystanie z komunikacji miejskiej) wciąż dodawane są kolejne. Dość powszechnie karty miejskie są wykorzystywane jako karta biblioteczna czy bilet do miejskich instytucji rekreacyjno-sportowych i kulturalnych (na przykład na basen, do muzeum czy ogrodu zoologicznego). Umożliwiają też opłacenie wypożyczenia miejskiego roweru czy parkowania. Tarnowska karta miejska może służyć do głosowania w budżecie obywatelskim, Śląska Karta Usług Publicznych pełni funkcję nośnika certyfikatu podpisu elektronicznego, łódzka Migawka daje możliwość zbierania punktów w programie Payback.

A to jeszcze nie koniec. W kolejnych miastach pojawia się również możliwość łączenia kart miejskich z płatniczymi. Takie usługi prowadzi m.in. BZ WBK, PKO BP czy mBank. Możliwe są przy tym różne modele współpracy. Poznań zapłacił BZ WBK za dostawę niespersonalizowanych kart i obsługę aplikacji płatniczej prepaid umieszczonej na karcie PEKA. We Wrocławiu natomiast miasto zgodziło się na wykorzystanie logotypu URBANCARD na karcie płatniczej BZ WBK, a w zamian bank zapewnił możliwość korzystania za jej pomocą z usług miejskich i płaci miastu 30% przychodu uzyskanego za pośrednictwem kart (na przykład opłaty *interchange*). Różnica dotyczy też dostępu do danych osobowych gromadzonych przez miasto: w pierwszym przypadku bank nie może po nie sięgnąć, w drugim – korzysta z informacji podawanych przy wyrobieniu URBANCARD. W obu przypadkach jednak usługi miejskie zostają spięte z ofertą prywatnej firmy.

Banki to nie jedyne podmioty, które mogą uzyskać dostęp do informacji gromadzonych w związku z obsługą kart miejskich. Jeśli instytucje publiczne dysponują odpowiednią podstawą prawną, mogą na potrzeby realizacji swoich zadań sięgać po te dane. Dotyczy to choćby policji czy innych służb. Zdarza się jednak w praktyce, że przepływ danych uruchamia się również poza ramami obowiązującego prawa. Było tak w głośnej niedawno sprawie Karty Warszawiaka. Mogą się o nią ubiegać osoby uiszczające podatki w Warszawie i dzięki niej mniej płacić za komunikację miejską i korzystać z innych zniżek. Takie rozwiązanie samo w sobie budziło wątpliwości, był to jednak dopiero początek problemów. Okazało się, że miasto – dla usprawnienia działania systemu i wygody mieszkańców – postanowiło weryfikować uprawniania do karty, wymieniając się informacjami z Ministerstwem Finansów. Nie miało jednak do tego odpowiedniej podstawy prawnej i przyjęte rozwiązanie zostało zakwestionowane przez GIODO.

Czy ochronę prywatności mieszkańców da się pogodzić z ich wygodą i zyskami miast? Trzy warunki wydają się tutaj absolutnie kluczowe:

- Mieszkańcy, którzy zdecydują się korzystać z karty miejskiej, powinni mieć zagwarantowane prawo do pełnej informacji o celach i zakresie przetwarzania ich danych. Niestety, obecnie rzetelna informacja jest przyćmiewana przez komunikaty reklamowe, które kładą nacisk jedynie na korzyści związane z korzystaniem z kart miejskich. Co więcej – precyzyjnych informacji na temat zakresu zbieranych danych i sposobu ich wykorzystania w wielu przypadkach trudno się doszukać nawet w regulaminach korzystania z kart.

- Mieszkańcy powinni mieć realny wybór, czy chcą korzystać z kart miejskich. Jeśli jakaś usługa nie wymaga podawania danych osobowych, mieszkańcy powinni mieć możliwość skorzystania z niej w sposób anonimowy. Tymczasem zdarza się coraz częściej, że tę możliwość się mocno ogranicza, na przykład przez likwidację biletów na okaziciela, presję cenową (nieproporcjonalnie droższe bilety w wersji niespersonalizowanej) czy utrudnienie lub uniemożliwienie dostępu do usług bez karty miejskiej.

- Zbierane powinny być tylko te informacje, które są absolutnie niezbędne i tylko tak długo, jak jest to rzeczywiście konieczne. Powinny być one również odpowiednio zabezpieczone ze względu na ryzyko ich wycieku bądź wykorzystania niezgodnie z przeznaczeniem. Taki przypadek miał miejsce we Wrocławiu w 2010 r. Użytkownicy systemu URBANCARD otrzymali przed wyborami samorządowymi e-maile zachęcające do głosowania na jednego z kandydatów. Winnym okazał się wówczas asystent prezydenta miasta.

KAŻDY, KTO DECYDUJE SIĘ NA WYPOŻYCZENIE MIEJSKIEGO ROWERU, NIE ROBI TEGO W SPOSÓB ANONIMOWY, TYLKO RÓWNIEŻ W TEJ SYTUACJI DZIELI SIĘ INFORMACJAMI O SOBIE.

Karty miejskie to oczywiście nie tylko plastikowe kartoniki, które wielu z nas trzyma w portfelu, ale również cały system wykorzystywany do przetwarzania gromadzonych informacji. Wśród najpopularniejszych dostawców sprzętu i oprogramowania możemy znaleźć zarówno polskie, jak i zagraniczne firmy (na przykład R&G Plus, Bull Polska).

Koszty wprowadzenia systemów elektronicznych kart miejskich są bardzo zróżnicowane, choć zazwyczaj oscylują w okolicach kilku milionów złotych. Niektóre miasta (Kalisz, Szczecin) nie były w stanie oszacować kosztów ich wdrożenia. Wśród tych, które udzieliły odpowiedzi, najwięcej zapłacił Poznań: PEKA kosztowała niemal 45 mln zł. Na drugim końcu skali znalazła się łódzka karta miejska, której wprowadzenie zamknęło się w kwocie niewiele ponad 1 mln zł. Trudno jednak porównywać te kwoty, ponieważ poszczególne systemy mają zróżnicowane funkcjonalności.

Namierzyć i nagrać

Karty miejskie to oczywiście nie jedyne narzędzie, które można wykorzystać do zbierania informacji o osobach korzystających z komunikacji miejskiej. Coraz częściej obejmuje ono nie tylko autobusy czy tramwaje, ale również system wypożyczania rowerów. Dzisiaj nie działają one w oparciu o monety czy żetony, lecz wymagają rejestracji. Ze względu na potrzebę ochrony sprzętu i nowe możliwości techniczne takie podejście ma swoje uzasadnienie. Ale warto zdawać sobie sprawę z tego, że każdy, kto decyduje się na wypożyczenie roweru, nie robi tego w sposób anonimowy, tylko również w tej sytuacji dzieli się informacjami o sobie. W systemie – poza danymi wymaganymi w ramach rejestracji – zapisywana jest m.in. informacja o tym, skąd i dokąd jedzie, a coraz częściej miejskie rowery wyposażane są również w nadajniki GPS, które pozwalają prześledzić całą

trasę. W przypadku osób korzystających z tego środka transportu regularnie to spory zasób informacji o komunikacyjnych rutynach.

Dzięki takim rozwiązaniom technicznym ze strony stołecznego Zarządu Transportu Miejskiego możemy się na przykład dowiedzieć, kiedy z systemu Veturilo skorzystała stutysięczna użytkowniczka: „Tego dnia, o godz. 14.02, wypożyczyła rower na pl. Wilsona i pokonała na nim dystans ponad 6 kilometrów. Dojechała do Portu Czerniakowskiego".

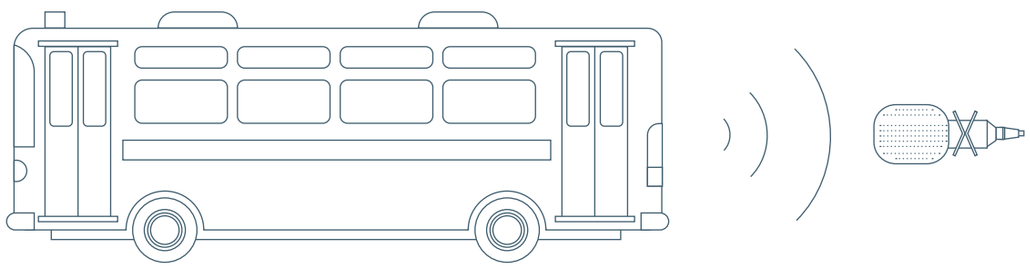
Firma Nextbike Polska, która obsługuje warszawski system, jest obecna również w wielu dużych polskich miastach: Białymstoku, Lublinie, Opolu, Poznaniu, Krakowie, Wrocławiu, Katowicach czy Trójmieście. Jak informuje na swojej stronie, jednorazowa rejestracja w systemie umożliwia korzystanie z floty 21 000 rowerów na całym świecie, m.in. w Niemczech, Austrii, Szwajcarii, Turcji, Cyprze, Emiratach Arabskich, Chorwacji, Azerbejdżanie, Łotwie, Nowej Zelandii i od tego roku w Wielkiej Brytanii, na Węgrzech i w Bułgarii.

PKP SA PODKREŚLA, ŻE KAMERY INSTALOWANE NA DWORCACH KOLEJOWYCH NIE SŁUŻĄ BEZPIECZEŃSTWU, A JEDYNIE INTERESOM GOSPODARCZYM SPÓŁKI.

Niestety, każdy, kto decyduje się na korzystanie z tych usług, wyraża zgodę na kontrowersyjny regulamin. Zakłada on, że wszystkie zgromadzone o użytkowniku informacje przechowywane są w bazie danych firmy aż do czasu złożenia specjalnego wniosku o skasowanie danych. Kto zdaje sobie z tego sprawę i zawraca tym głowę? Pewnie niewiele osób. A zatem większość zgromadzonych danych – przynajmniej w teorii – Nextbike przechowuje w nieskończoność.

Nie można też zapomnieć o monitoringu w pojazdach zbiorowej komunikacji. Była już mowa o kamerach i mikrofonach montowanych w autobusach i tramwajach. Rozbudowany system monitoringu możemy napotkać również w warszawskim metrze (szczególnie spektakularny w drugiej – najnowszej – linii). Monitoring obserwuje też osoby podróżujące na dłuższych trasach. Kamery zainstalowane są w części składów pociągów wykorzystywanych przez Przewozy Regionalne i PKP Intercity. A w tym drugim przypadku – mogą one rejestrować również dźwięk, choć spółka zapewnia, że nie korzysta z tej możliwości w praktyce.

Niewiele wiemy niestety o monitoringu działającym na dworcach kolejowych. PKP SA kilka lat temu odmówiła Fundacji Panoptykon udzielenia informacji na ten temat i sprawa czeka na rozstrzygnięcie w sądzie. Ciekawa jest argumentacja spółki kolejowej: podkreśla ona, że kamery instalowane na dworcach nie służą bezpieczeństwu, a jedynie jej interesom gospodarczym. Dlatego informacja o nich nie ma charakteru informacji publicznej, lecz jest objęta tajemnicą przedsiębiorstwa.



CZTERY KÓŁKA NA RADARZE

Przesiadka z komunikacji miejskiej do samochodu nie gwarantuje wyższego poziomu ochrony prywatności. Zarówno w mieście, jak i poza jego granicami zbiera się wiele informacji o poszczególnych samochodach, a co za tym idzie – o ich właścicielach. Pomagają w tym liczne narzędzia zatopione w otaczającej przestrzeni. Dla przykładu trójmiejski Tristar działa m.in. w oparciu o: 11 855 detektorów pojazdów, 108 kamer, 55 fotorejestratorów wyłapujących przejeżdżających na czerwonym świetle i 43 fotoradary. A to tylko jeden system...

Nadzór w trasie

Nadzorowanie sytuacji na drodze ma dwa główne cele. Z jednej strony – zarządzanie ruchem (na przykład poprzez synchronizację sygnalizacji świetlnej), z drugiej – wyłapywanie różnego rodzaju nadużyć (na przykład jazdy z niedozwoloną prędkością czy przejazdów na czerwonym świetle). Rozwój możliwości technicznych i analitycznych sprawia, że sposób realizacji tych celów bardzo się zmienia: od ogólnego badania natężenia ruchu i wyłapywania piratów drogowych do szczegółowego nadzoru nad każdym kierowcą i jego zachowaniem na drodze.

Niestety, konsekwencje takich procesów nie są łatwe do przewidzenia. Warto się im jednak uważnie przyglądać, ponieważ łączą się one nie tylko z realnym obciążeniem finansowym (dla przykładu wdrożenie wspomnianego wyżej Tristara kosztowało 159 mln zł), ale niosą też konsekwencje istotne z punktu widzenia praw użytkowników dróg.

Szczególnie interesujące są w tym kontekście narzędzia, które pozwalają na automatyzację zbierania i analizowania informacji. Do najpopularniejszych należą te wyposażone w funkcję Automatycznego Rozpoznawania Tablic Rejestracyjnych (ARTR, inaczej: APNR, od ang. *Automatic Plate Number Recognition*). Wykorzystywana jest ona przez różne podmioty, zarówno na ulicach miast, jak i na drogach międzymiastowych.

ODCINKOWY POMIAR PRĘDKOŚCI NIE OGRANICZA SIĘ DO REJESTROWANIA PRZYPADKÓW NARUSZEŃ PRZEPISÓW ORAZ ICH SPRAWCÓW, LECZ OPIERA SIĘ NA ZBIERANIU INFORMACJI O WSZYSTKICH POJAZDACH POJAWIAJĄCYCH SIĘ W KONTROLOWANYM OBSZARZE.

Najbardziej znanym wykorzystaniem technologii ARTR jest CANARD, czyli Centrum Automatycznego Nadzoru nad Ruchem Drogowym, prowadzone przez Inspekcję Transportu Drogowego (ITD). System obejmuje infrastrukturę techniczną (8 zestawów urządzeń do pomiarów statystycznych natężenia ruchu, 400 stacjonarnych i 29 mobilnych fotoradarów, 20 kompletów urządzeń monitorujących przejazd na czerwonym świetle, 29 urządzeń rejestrujących do odcinkowego pomiaru prędkości) oraz oprogramowanie umożliwiające gromadzenie danych i ich zautomatyzowaną analizę. System został stworzony w ramach dofinansowanego przez Unię Europejską projektu o niebagatelnej wartości 188 mln zł.

Z punktu widzenia gromadzenia informacji o podróżujących szczególnie kontrowersyjnym zastosowaniem CANARD-u jest odcinkowy pomiar prędkości. Nie ogranicza się on bowiem do rejestrowania przypadków naruszeń przepisów oraz ich sprawców, lecz opiera się na zbieraniu informacji o wszystkich pojazdach pojawiających się w kontrolowanym obszarze. Każde auto zostaje sfotografowa-

ne i odnotowane w pamięci urządzenia dwa razy – na początku i końcu odcinka pomiarowego. Następnie system oblicza średnią prędkość przejazdu i – jeśli nie doszło do złamania przepisów – zdjęcia zostają od razu automatycznie usunięte z pamięci urządzenia. Natomiast w sytuacji, gdy wynik jest wyższy od dopuszczalnego, zapis wykroczenia trafia do bazy danych CANARD-u.

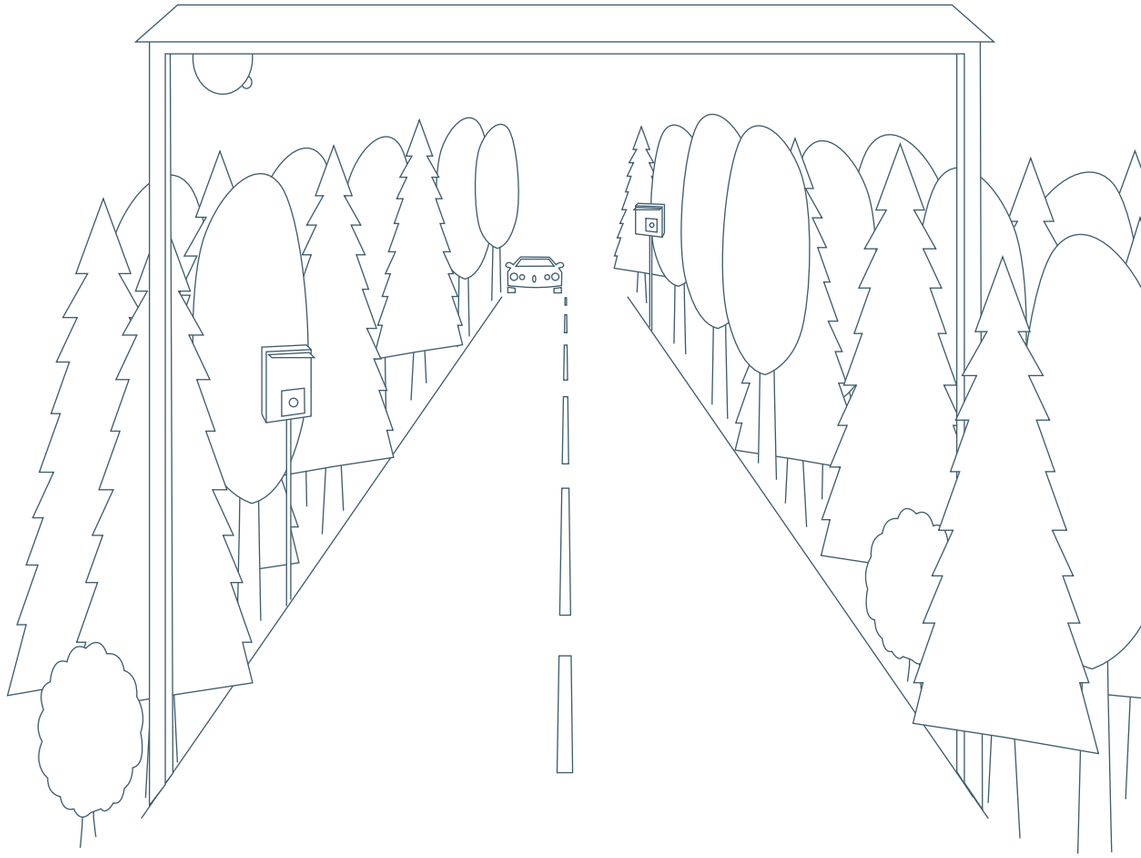
Polskie drogi wciąż nie należą do bezpiecznych. Część kierowców regularnie znacznie przekracza dozwoloną prędkość i zwalnia tylko po dostrzeżeniu na horyzoncie fotoradaru. Dla niektórych to powód do szukania nowych rozwiązań, nawet za cenę jeszcze głębszej ingerencji w prywatność kierowców. Problem jest jednak bardzo złożony, warto więc zadać sobie pytanie, czy stawianie kolejnych fotoradarów i rozwijanie systemu odcinkowego pomiaru prędkości rzeczywiście przybliża nas do jego systemowego rozwiązania.

Funkcjonalność ARTR wykorzystywana jest również przez policję. W odpowiedzi na wniosek Fundacji Panoptykon Komenda Główna potwierdziła, że od kilku lat korzysta z systemu VCOP firmy Telsat (jednego z wiodących producentów systemów monitoringu wyposażonego w automatyczne funkcjonalności). System obejmuje urządzenia działające zarówno w wersji stacjonarnej, jak i mobilnej. Umożliwia zapisanie zdjęcia pojazdu w kolorze i podczerwieni, numeru tablicy rejestracyjnej, daty, godziny i miejsca rejestracji pojazdu. Za ich pomocą policja nadzoruje samochody pojawiające się w punktach pomiarowych oraz może namierzać pojazdy o określonych numerach rejestracyjnych czy innych cechach. System daje też możliwość filtrowania zgłaszanych zapytań i porządkowania uzyskanych odpowiedzi.

Niedawno w mediach głośno było o sprawie zatrzymania na ulicach Warszawy poszukiwanego mężczyzny dzięki wykorzystaniu monitoringu wyposażonego w funkcję ARTR. Cała sprawa wygląda dość zagadkowo. Agencja Bezpieczeństwa Wewnętrznego – która dokonała zatrzymania – odmówiła odpowiedzi na pytania dotyczące wykorzystywania takiej funkcjonalności. Komenda Stołeczna Policji natomiast przyznała, że używała systemu (do czasu jego awarii), którego właścicielem jest m.st. Warszawa. Strona internetowa Telsatu potwierdza, że firma ta wdrożyła system w stolicy. Pytania Fundacji Panoptykon miejscy urzędnicy przekazali jednak do Zakładu Obsługi Systemu Monitoringu. Ten odpowiedział, że system wyposażony w funkcję ARTR został wdrożony przez firmę Sprint, ale Zakład z niego nie korzysta, a administratorem i jedynym użytkownikiem systemu jest... Komenda Stołeczna Policji.

ARTR można spotkać się nie tylko na ulicach Warszawy, ale też w innych większych miastach. Jednym z nich jest Białystok, gdzie funkcjonalność ta wykorzystywana jest do identyfikacji samochodów łamiących zakaz jazdy na czerwonym świetle oraz do zbierania i analizy informacji o ruchu, które są wykorzystywane do prezentowania informacji na elektronicznych tablicach, dzięki którym kierowcy mogą dowiedzieć się, ile czasu zajmie dojazd do centrum miasta różnymi wariantami trasy. Pytanie tylko, czy sprawne działanie takich tablic rzeczywiście wymaga korzystania z funkcjonalności ARTR.

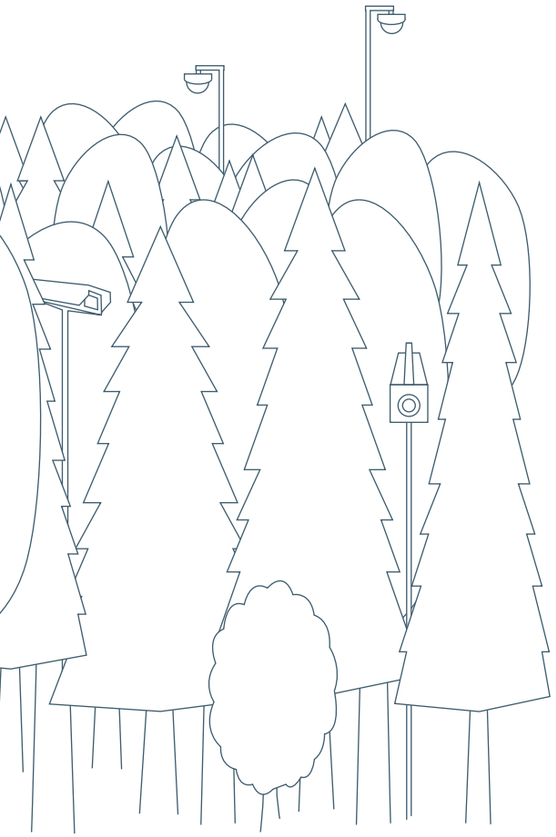
W taki sam zresztą sposób (do zbierania i analizy informacji wyświetlanych kierowcom) ARTR wykorzystuje Generalna Dyrekcja Dróg Krajowych i Autostrad (GDDKiA). Ale to oczywiście nie jedyne zastosowanie tej funkcjonalności. Jest ona również elementem systemu służącego do (pół)automatycznego wykrywania naruszeń polegających na przekroczeniu dopuszczalnej masy całkowitej, nacisku osi bądź wysokości pojazdów ciężarowych. Z punktu widzenia GDDKiA takie praktyki stanowią problem, ponieważ prowadzą do pogorszenia stanu dróg (dlatego na wdrażanie podobnych rozwiązań decydują się również władze niektórych miast).



Wszystkie systemy do wykrywania przeciążonych pojazdów powstały w latach 2010–2014. W ich stworzenie zaangażowanych było kilku ważnych graczy na rynku: Sprint (około 20 instalacji), Mark Elektronics, Zaberd i Telsat (każdy po około 15 instalacji). Pozwalają one na dokonywanie pomiarów w ruchu. Jeśli zarejestrują pojazd podejrzewany o przekroczenie norm, zapisują dla celów dowodowych numer rejestracyjny, zdjęcie pojazdu i wyniki pomiaru. Alarm przekazywany jest ITD, która odpowiada za namierzenie pojazdu i weryfikację podejrzenia. Ma ona dostęp do systemu w czasie rzeczywistym i może na bieżąco obserwować zdjęcia pojazdów podejrzanych o przekroczenie norm.

System nie zapisuje wizerunku kierowcy i według GDDKiA nie zbiera danych osobowych. Tymczasem zarówno ona, jak i ITD mają dostęp do Centralnej Ewidencji Pojazdów i Kierowców, dzięki któremu mogą powiązać numer rejestracyjny z konkretną osobą lub firmą.

Funkcja ARTR to nie jedyny sposób na automatyczną identyfikację samochodu. Inną wykorzystuje viaToll – system elektronicznego poboru opłat za korzystanie z dróg, który obecnie jest obowiązkowy dla TIR-ów i innych dużych pojazdów, ale w przyszłości może objąć również samochody osobowe. Uruchomienie systemu kosztowało – bagatela! – 1,5 mld zł, a jego utrzymanie w 2014 r. – 313 mln zł.



Jednym z kluczowych elementów systemu viaToll jest urządzenie o nazwie viaBox, instalowane w samochodach. Urządzenie komunikuje się z bramownicami, rozmieszczonymi na drogach w całym kraju, które dzięki temu identyfikują użytkownika. Uzupełnieniem systemu viaToll jest kilkaset kamer, które służą do obserwacji i rejestracji obrazu. Część bramownic ma funkcjonalność zbierania informacji na temat wszystkich pojazdów pod nimi przejeżdżających. Wykorzystywana jest ona do walki z kierowcami łamiącymi przepisy, przede wszystkim przekraczającymi dozwoloną prędkość. Zdjęcia ich pojazdów zatrzymywane są dla celów dowodowych, a pozostałe kasowane z pamięci bramownicy.

Informacje zbierane przez systemy nadzoru nad ruchem mogą być wykorzystywane do swoich celów nie tylko przez podmioty, które je obsługują. Dla przykładu: zgodnie z doniesieniami Dziennika Gazety Prawnej od utworzenia w 2011 r. systemu viaToll sukcesywnie rośnie liczba zapytań ze strony służb i innych publicznych instytucji o dane z bramownic, które rejestrują ruch. W 2014 r. pytały one o dane kierowców 1322 razy. Najczęściej robiła to policja i kontrola skarbowa.

Ukryty koszt parkowania

Nie tylko w trasie zbierane są informacje o samochodach i ich właścicielach. Coraz częściej dzieje się tak również przy okazji parkowania. Kolejne miasta decydują się bowiem na wprowadzenie parkometrów, które wymagają od kierowców podania numeru rejestracyjnego pojazdu. Wszystkie parkometry działające w Warszawie (prawie 1700), w Łodzi (około 300) czy we Wrocławiu (ponad 200) funkcjonują na tej zasadzie. Na wymianę części parkometrów zdecydowały się również na przykład władze Krakowa i Katowic, a kolejne przymierzają się do podjęcia takiej decyzji (władze Lublina).

Rok 2012 był przełomowy dla rozwoju systemów pobierania opłat za parkowanie w oparciu o zbieranie numerów tablic rejestracyjnych. Wówczas nowe parkometry pojawiły się w największych miastach. Wdrożenie najbardziej rozbudowanego – warszawskiego – systemu kosztowało ponad 47 mln zł. Wykonawcą (w tym i innych przypadkach) była firma City Parking Group – potentat na krajowym rynku organizacji i obsługi stref płatnego parkowania, która obsługuje aż 36 miast, w tym 7 wojewódzkich, ale także centra handlowe i inne podmioty.

Informacje zbierane przy okazji opłacania parkowania są w poszczególnych miastach przesyłane do baz danych. Poza numerem rejestracyjnym zapisywana jest najczęściej data, czas, na jaki wykupiono możliwość parkowania, wpłacona kwota i sposób dokonania opłaty oraz numer parkometru (który pozwala go zlokalizować). Co istotne, wszystkie te informacje są bardzo długo przechowywane – dla przykładu: w Warszawie – 8 lat, w Łodzi – 7 lat, a we Wrocławiu – 5 lat.

Niestety, nie każdy kierowca zdaje sobie sprawę z tego, gdzie trafiają informacje z parkometrów. Tymczasem powinien zostać o tym poinformowany, bo w gruncie rzeczy zbierane są jego dane osobowe. Ponieważ lokalne Zarządy Dróg Miejskich, które zawiadują systemami parkometrów, mają dostęp do Centralnej Ewidencji Pojazdów i Kierowców, są w stanie łatwo dowiedzieć się, o czyje auto w danym przypadku chodzi. W Warszawie po decyzji GIODO na parkometrach pojawiły się tabliczki informujące o tym, kto jest administratorem danych, w jakim celu dane są zbierane i komu mogą być udostępniane, o prawie dostępu do treści danych oraz ich poprawiania, a także o obowiązku podania danych i jego podstawie prawnej. Niestety, w pozostałych miastach władze nie zadbały o takie tabliczki. Jest jednak szansa, że po interwencji Fundacji Panoptykon sytuacja się zmieni.

KOLEJNE MIASTA DECYDUJĄ SIĘ NA WPROWADZENIE PARKOMETRÓW, KTÓRE WYMAGAJĄ OD KIEROWCÓW PODANIA NUMERU REJESTRACYJNEGO POJAZDU. ZEBRANE INFORMACJE SĄ PRZECHOWYWANE BARDZO DŁUGO: W WARSZAWIE – 8 LAT, W ŁODZI – 7 LAT, A WE WROCŁAWIU – 5 LAT.

Kluczowe pytanie brzmi jednak, czy zapisywanie numerów rejestracyjnych parkujących jest rzeczywiście niezbędne. W mediach pojawiała się informacje, że dodatkowe dane (numer rejestracyjny) mają służyć ograniczeniu przekazywania sobie przez kierowców biletów parkingowych i unikaniu w ten sposób płacenia mandatów (bilet stawał się dowodem na opłacenie miejsca parkingowego). Trudno jednak zakładać, by było to rzeczywiście masowe zjawisko i by dodatkowe zyski rekompensowały nie tylko ograniczenie prywatności kierowców, ale też koszty wdrożenia nowych parkometrów.

Nowe światło na sprawę rzucają wyjaśnienia przesłane przez przedstawicieli Łodzi i Wrocławia, choć nie pozwalają one rozstrzygnąć, czy zbieranie numerów rejestracyjnych jest rzeczywiście jedyną możliwą drogą. Pierwsi przywołali wyrok Sądu Administracyjnego w Łodzi, który unieważnił przepis uchwały nakładający na kierowców obowiązek umieszczania biletu parkingowego za przednią szybą pojazdu. Sąd uznał, że władze miasta nie mają podstaw prawnych do nakładania takiego obowiązku, a tym samym pozbawił je narzędzia do prowadzenia kontroli wnoszonych opłat. Urzędnicy z Wrocławia zwrócili natomiast uwagę na potrzebę rozpatrywania odwołań od nałożonych mandatów. Przedawniają się one po 5 latach, licząc od końca roku, w którym je wystawiono. Mało który kierowca tak długo przechowuje potwierdzenie wniesienia opłaty, a zapisanie informacji w bazie danych pozwala rozstrzygnąć ewentualne wątpliwości.

W URZĘDZIE

Zgłoszenie narodzin dziecka, wyrobienie paszportu czy dowodu, rejestracja samochodu, uzyskanie pozwolenia na budowę domu, otwarcie lub zamknięcie działalności gospodarczej, uzyskanie zasiłku, złożenie rozliczenia podatkowego – jest wiele spraw, które mogą sprowadzić nas do urzędu albo sprawić, że urzędnicy zainteresują się nami i przypomną o obowiązkach wobec państwa. Dla dużej grupy osób instytucja państwowa lub samorządowa jest natomiast miejscem pracy i dlatego ich działania poddane są kontroli.

Instytucje publiczne mają do dyspozycji wiele narzędzi służących usprawnieniu zarządzania, wykrywaniu różnego rodzaju nieprawidłowości, kontroli zachowania przebywających na jej terenie osób, które jednocześnie zbierają wiele szczegółowych informacji zarówno na temat zatrudnionych osób, jak i szerokiej rzeszy obywateli. Jakie są to narzędzia, jakie informacje zbierają, jak są one wykorzystywane oraz jakie może to mieć konsekwencje dla każdego z nas – odpowiedzi na te pytania można znaleźć w drugiej części przewodnika.

BUDYNEK POD KONTROLĄ

Przekraczając próg urzędu, wkraczamy w przestrzeń poddaną ściślejszej kontroli. Do niektórych instytucji osoby z zewnątrz mogą wejść tylko pod ścisłymi warunkami, na przykład na zaproszenie, po wylegitymowaniu się, otrzymaniu przepustki, sprawdzeniu bagażu czy przejściu przez wykrywacz metalu. W urzędach, które przyjmują interesantów, te bariery są siłą rzeczy bardziej ograniczone. Ale w środku z pewnością napotkamy kolejne narzędzia nadzoru, choćby kamery monitoringu.

Dostęp ograniczony

Jednym z popularniejszych elementów instytucjonalnego krajobrazu stały się systemy służące zautomatyzowanej identyfikacji i kontroli wchodzących – czyli różnego rodzaju karty i bramki. Podmioty publiczne starają się na tym polu nie odstawać od prywatnych. Z zebranych przez Fundację Panoptykon dzięki wnioskom o udostępnienie informacji publicznej danych wynika, że na poziomie centralnym korzystanie z takich systemów kontroli dostępu jest właściwie standardem. Bardziej podzielone w swoich praktykach były samorządy i lokalne oddziały instytucji, na przykład Narodowego Funduszu Zdrowia (NFZ).

Działanie systemów kontroli dostępu opiera się na porównaniu danych zapisanych na przykład na karcie z tymi zgromadzonymi w bazie. Zdarza się, że nie wymagają one identyfikacji wchodzących osób – wówczas karty działają podobnie jak zwykłe klucze, tylko w formie elektronicznej. To jednak mało popularne rozwiązanie. Zazwyczaj kontrola wejść polega na weryfikacji tożsamości pracowników (rzadziej gości).

Systemy dostępu na bieżąco gromadzą różne informacje: przede wszystkim godziny wejść i wyjść do budynku lub konkretnego pomieszczenia, ale też na przykład informacje o przypisaniu gościa do osoby odwiedzanej. Z tego względu wykorzystywane są nie tylko do weryfikacji tożsamości wchodzących i ograniczenia możliwości wejścia przez osoby nieuprawnione, ale także do mierzenia czasu pracy. Dzięki temu możliwa jest rezygnacja z podpisywania papierowych list obecności. Do tego na podstawie historii logowań odczytanych z rejestratorów program dokonuje analizy obecności oraz wyliczenia całkowitego przepracowanego czasu wraz z wyszczególnieniem okresów składkowych, nadgodzin, pracy w nocy, delegacji, urlopów itp.

W przypadku instytucji zatrudniających bardzo wiele osób może to być realne ułatwienie. Jednak również mniejsze podmioty decydują się na takie rozwiązania, zwłaszcza że producenci systemów kontroli wejść reklamują je jako narzędzie niosące dodatkowe korzyści. Jak pisze na swoje stronie Unicard – jedna z częściej wybieranych przez badane instytucje firm – „System Rejestracji Czasu Pracy przede wszystkim generuje oszczędności. Dyscyplinując pracowników, pozwala obniżyć koszty pracy i zapobiegać nadużyciom". W podobnym tonie zachwala swoje usługi inna popularna polska firma – Roger.

Na rynku działa bardzo wielu producentów i dystrybutorów systemów kontroli dostępu, trafiających powszechnie zarówno do instytucji publicznych, jak i podmiotów prywatnych. Często są to firmy, które specjalizują się również w produkcji i sprzedaży systemów monitoringu wizyjnego. Koszt nabycia systemu w praktyce waha się zazwyczaj od kilkunastu do kilkuset tysięcy złotych, przy czym rozwiązania wykorzystywane w instytucjach centralnych są zazwyczaj

droższe niż te, z których korzystają samorządy. Ceny najbardziej zaawansowanych systemów sięgały kilku milionów złotych: prawie 1 mln zł za swój system zapłaciło Ministerstwo Sprawiedliwości, a Narodowy Bank Polski (NBP) – ponad 7 mln zł. W części przypadków (na przykład NBP) przyjęcie konkretnych rozwiązań było związane z charakterem instytucji i wymogami prawnymi dotyczącymi ich działania, w innych było autonomiczną decyzją kierownictwa.

Odcisk palca, proszę

Najpopularniejszym identyfikatorem w systemie kontroli dostępu jest karta, zazwyczaj działająca w technologii zbliżeniowej. Coraz częściej zdarza się jednak, że instytucje decydują się na weryfikację tożsamości w oparciu o dane biometryczne, na przykład odcisk palca.

Dane biometryczne to informacje związane z ciałem człowieka, które odróżniają każdego z nas od innych i dlatego mogą być wykorzystywane do identyfikacji. Poza odciskami palców należą do nich na przykład: obraz tęczówki, obraz układu krwionośnego dłoni, geometria twarzy, głos czy sposób poruszania się. Tradycyjnie biometria przywodziła na myśl postępowanie karne: zbieranie odcisków palców przestępców i zabezpieczanie innych śladów, które pozostały na miejscu popełnienia przestępstwa. Dzisiaj firmy rozwijające ten rodzaj technologii dbają o to, by kojarzyła się z czymś nowoczesnym i zaawansowanym technicznie.

KAŻDY, KTO UDOSTĘPNIA SWOJE DANE BIOMETRYCZNE, ODDAJE INNYM INFORMACJE O SOBIE I WŁAŚCIWIE TRACI NAD NIMI KONTROLĘ. JEŚLI TAKIE DANE WYCIEKNĄ, TRUDNO ZASTOSOWAĆ PROSTĄ RECEPTĘ W POSTACI WYMIANY KARTY CZY HASŁA.

Niepowtarzalny charakter danych biometrycznych ma – przynajmniej w teorii – pozwalać na nieomylną identyfikację konkretnej osoby. W praktyce z tą nieomylnością bywa różnie, i to nie ona decyduje o rozwoju biometrycznej technologii. Kluczowym argumentem jest cena i wygoda. Technologia biometryczna nie wymaga zapamiętywania haseł ani wydawania dużej grupie osób kart, które trzeba uzupełniać, a z czasem wymieniać. Nośnikiem informacji jest ludzkie ciało. Wpływa to na wzrastającą popularność biometrii i jej coraz powszechniejsze wykorzystanie – także w codziennym życiu (na przykład w laptopach czy tabletach).

Coraz szersze wykorzystanie technologii biometrycznej ma niestety również swoją ciemną stronę – ingerencję w prywatność. Każdy, kto udostępnia swoje dane biometryczne, oddaje innym informacje o sobie i właściwie traci nad nimi kontrolę. Jeśli takie dane wycieką, trudno zastosować prostą receptę w postaci wymiany karty czy hasła. Właśnie dlatego korzystanie z danych biometrycznych powinno być traktowane jako ostateczność: nie należy po nie sięgać wówczas, kiedy można wykorzystać inne środki. Zgodnie z orzecznictwem sądów administracyjnych zgoda pracowników nie może być wystarczającą podstawą do wdrożenia takich rozwiązań w miejscu pracy, ponieważ – ze względu na zależność od pracodawcy – ich decyzję trudno uznać za w pełni dobrowolną.

Z zebranych przez Fundację Panoptykon informacji wynika, że system dostępu oparty na danych biometrycznych wykorzystują m.in. NBP i śląski NFZ. O ile w przypadku NBP można doszukać się uzasadnienia dla przyjęcia takiego rozwiązania, o tyle decyzja drugiej instytucji budzi wątpliwości, zwłaszcza że inne oddziały NFZ radzą sobie bez takich narzędzi.

Zupełnym kuriozum wydaje się wykorzystanie rozwiązań biometrycznych na Wojskowej Akademii Technicznej. Uczelnia zamówiła taki system do rejestracji wydawanych posiłków na stołówce oraz głosowania w akademickim senacie. Uczelnia techniczna zapewne chce iść z duchem czasu, trudno jednak nie zadać sobie pytania, czy trzeba sięgać aż po takie

środki, żeby ktoś nie pobrał podwójnej porcji zupy.

Nie słychać nic o tym, by pomysły władz Wojskowej Akademii Technicznej spotkały się z negatywnym odzewem. Może dlatego, że – przynajmniej na razie – korzystanie z biometrii nie jest tam obowiązkowe. Zdarza się jednak, że pobieranie danych biometrycznych budzi większe emocje. Przeciwko rozwiązaniom opartym na zbieraniu odcisków palców protestowali na przykład jakiś czas temu lekarze w szpitalach we Wrocławiu i w Jaworznie.

Inne – nieoparte na biometrii – automatyczne systemy kontroli dostępu wrosły już jednak w codzienność wielu instytucji i zazwyczaj nie wzbudzają kontrowersji. Zdarzają się jednak wyjątki. Na przykład wykładowcy Politechniki Opolskiej uznali zautomatyzowany system kontroli wejść wdrażany na ich uczelni za uwłaczający ich godności. I dopięli swego. Władze zrezygnowały z inicjatywy i wróciły do papierowych list obecności.

Ściany mają oczy i uszy

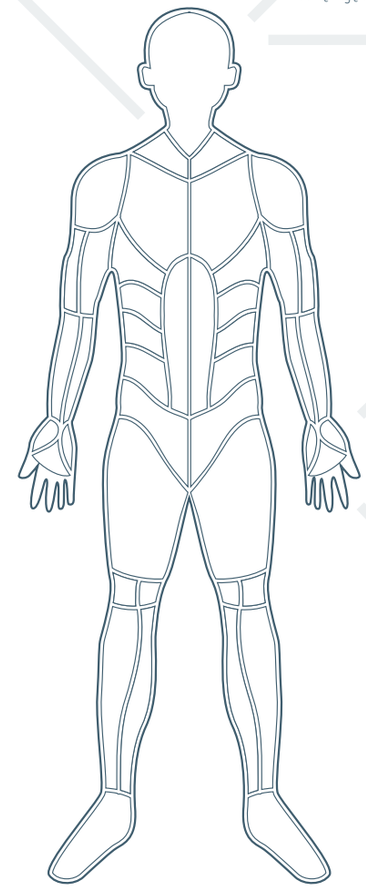
W urzędach, podobnie jak w wielu innych miejscach, trudno nie napotkać szklanego oka obserwującego przebywające w nich osoby. Monitoring jest rozwiązaniem standardowo wykorzystywanym w wielu publicznych instytucjach. Kamery umieszczane są zarówno na zewnątrz, jak i wewnątrz budynków. W części instytucji obejmują swoim zasięgiem przede wszystkim korytarze, w innych przestrzeń, do której mają dostęp głównie pracownicy, w jeszcze innych – miejsca, w których obsługiwani są interesanci.

Brak regulacji prawnej sprawia, że monitoring wymyka się zasadom i jest wykorzystywany w sposób bardzo dowolny. Tymczasem jest to narzędzie, które ingeruje w prywatność obserwowanych osób. Dlatego w teorii każda instytucja publiczna, która chce z niego korzystać, powinna mieć do tego szczegółową podstawę

Biometria głosowa opiera się na wyjątkowości i niepowtarzalności ludzkiego głosu. Wykorzystuje zarówno cechy fizyczne, jak i behawioralne mowy: akcent, szybkość mówienia, sposób wysławiania się, dzięki czemu umożliwia weryfikację tożsamości osoby mimo na przykład chorób gardła czy hałasu z otoczenia. *Voiceprint* – matematyczny model wzorca głosu – tworzy się na podstawie nagrania, odpowiednio opisując jego parametry. Ministerstwo Finansów chciało wykorzystywać tę metodę do potwierdzania tożsamości osób dzwoniących na infolinię podatkową.

Analiza sposobu poruszania się – przykład behawioralnej metody biometrycznej, wykorzystywanej m.in. przez monitoring z funkcją rozpoznawania ruchu do wyszukiwania konkretnych osób na nagraniach i ich identyfikacji na odległość. Opiera się na specyfice indywidualnego sposobu chodzenia każdego z nas (w tym wad chodu) i budowy ciała. Na podstawie nagrań wyodrębnia się postać człowieka w różnych fazach chodu, zaznacza się kluczowe punkty i oblicza różnice w ich położeniu w poszczególnych fazach poruszania się. Tak stworzony model pozwala na stwierdzanie, czy do czynienia mamy z tą samą osobą.

Rozpoznawanie twarzy może wykorzystywać pomiary specyficznych cech twarzy (na przykład odległości między jej poszczególnymi częściami i relację między tymi odległościami) bądź też dopiero rozwijaną metodę tzw. *eigenface* – w tym przypadku kategoryzuje się twarze w oparciu o stopień ich dopasowania do stworzonych modeli. Przypomina to budowanie twarzy z fragmentów cyfrowych fotografii. Geometria twarzy wykorzystywana jest na przykład w biometrycznych paszportach bądź przez monitoring z funkcjonalnością rozpoznawania twarzy (w tym przypadku oprogramowanie porównuje wybrane cechy twarzy nagranych osób z bazą zdjęć poszukiwanych osób).

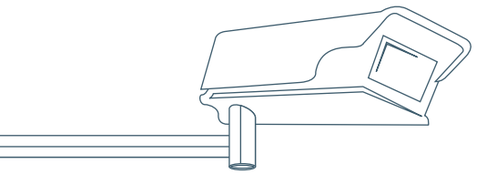


Skanowanie tęczówki oka bazuje na charakterystyce tęczówki, która zgodnie z badaniami jest jedną z najbardziej unikalnych cech człowieka – ma znacznie więcej punktów charakterystycznych niż na przykład odciski palców. Drugą z biometrycznych metod związanych z oczami jest skanowanie siatkówki dna oka – w celu jej wykorzystania tworzy się obraz siatki naczyń krwionośnych w oku, który podlega następnie analizie pod względem charakterystycznych punktów. W obu metodach informacje o tych punktach są zapisywane i wykorzystywane do potwierdzania tożsamości lub identyfikacji. Mogą być one używane na przykład do weryfikacji uprawnień dostępu do ściśle chronionych pomieszczeń.

Identyfikacja w oparciu o geometrię dłoni bazuje na tym, że dłoń każdej osoby jest ukształtowana odmiennie i że po osiągnięciu pewnego wieku nie zmienia się w sposób znaczący. Na podstawie pomiarów dłoni tworzy się jej wzorzec, który następnie porównuje się z dłonią osoby, której tożsamość jest weryfikowana . Metoda ta nie dostarcza jednak wielu danych, dlatego nadaje się jedynie do mniejszych baz – w przypadku bardzo dużej liczby osób ich rozróżnienie może być problemem. By zwiększyć skuteczność weryfikacji, zwiększa się liczbę stosowanych pomiarów, tworząc bardziej skomplikowane wzorce opisu dłoni.

Odciski palców wykorzystywane są w najpopularniejszej metodzie weryfikacji biometrycznej, opierającej się na wyjątkowości linii papilarnych poszczególnych osób. Najczęściej kojarzona jest ona z postępowaniem karnym: pobieraniem odcisków przestępców i zabezpieczaniem dowodów na miejscu przestępstwa. Wykorzystywana jest zarówno do identyfikacji osób, jak i weryfikacji tożsamości. Stosowana jest w biometrycznych paszportach oraz do identyfikacji osób ubiegających się w Unii Europejskiej o ochronę międzynarodową (status uchodźcy).

WYBRANE METODY IDENTYFIKACJI I WERYFIKACJI TOŻSAMOŚCI WYKORZYSTUJĄCE DANE BIOMETRYCZNE



prawną w postaci ustawy. W praktyce taka podstawa nie jest oczywista, a instytucje często w ogóle nie zawracają sobie tym głowy.

Fundacja Panoptykon pod lupę wzięła oddziały Zakładu Ubezpieczeń Społecznych (ZUS) i Narodowego Funduszu Zdrowia. Na pytanie o podstawę prawną korzystania z kamer monitoringu odpowiedziały one rozmaicie. Najwięcej placówek powołało się na ustawę o ochronie osób i mienia, pozostałe – na ustawę o ochronie danych osobowych, rozporządzenie w sprawie środków bezpieczeństwa fizycznego informacji niejawnych, regulacje wewnętrzne, normy techniczne korzystania z monitoringu, a nawet umowę z firmą ochroniarską. Trzy oddziały z rozbrajającą szczerością przyznały, że w ogóle nie mają podstaw prawnych do korzystania z kamer.

Niejednoznacznie prezentowały się też odpowiedzi na pytanie, czy systemy są zgodne z wymogami ustawy o ochronie danych osobowych. Większość badanych instytucji zadeklarowała taką zgodność (niestety, trudno ocenić, czy jest tak w istocie). Wyłamały się z tego jednak trzy oddziały NFZ (warmińsko-mazurski, podlaski i wielkopolski): dwa pierwsze, przyznając, że ich systemy monitoringu wymogów ustawy nie spełniają, a trzeci – przekonując, że nie jest to konieczne.

INSTALACJA KAMER DO OBSERWACJI PROCESU PRZELICZANIA I SORTOWANIA BANKNOTÓW W NBP WYDAJE SIĘ MIEĆ MOCNE UZASADNIENIE. ALE CZY TAKIE NARZĘDZIA SĄ NIEZBĘDNE RÓWNIEŻ W MAŁYM URZĘDZIE?

Podobnie jak w przypadku większości zastosowań monitoringu, również w przypadku jego wykorzystania w urzędach cele nie są jasne i precyzyjnie sformułowane. Może to być szeroko pojęta ochrona mienia przed kradzieżą bądź zniszczeniem czy też kontrola pracowników. Oprócz tego pytane instytucje wskazywały na potrzebę rozstrzygania sporów z interesantami czy tak prozaiczne kwestie jak zniżki na ubezpieczenie. Niestety, nikt właściwie nie bada, jak ten sprzęt wykorzystywany jest w praktyce i czy potencjalne korzyści równoważą koszty: zarówno finansowe, jak i związane z ingerencją w prywatność obserwowanych osób.

Ocena systemów monitoringu montowanych w instytucjach publicznych zależy od sytuacji. Instalacja kamer do obserwacji procesu przeliczania i sortowania banknotów w NBP wydaje się mieć mocne uzasadnienie. Ale czy takie narzędzia są niezbędne również w małym urzędzie? Czy rzeczywiście nie można się już dzisiaj obejść bez obserwowania każdego ruchu pracowników i interesantów?

Ze szczególnie kontrowersyjną praktyką można spotkać się w małopolskim i świętokrzyskim oddziale NFZ. Instytucje te w przestrzeni przeznaczonej do obsługi interesantów rejestrują nie tylko obraz, ale również dźwięk. Stanowi to bardzo głęboką ingerencję w prywatność przebywających tam osób, zwłaszcza że mogą one omawiać wrażliwe kwestie. Inne oddziały NFZ obywają się bez takiego rozwiązania, więc decyzja podjęta przez władze tych dwóch placówek budzi tym poważniejsze wątpliwości.

Co gorsza, nie jest nawet jasne, czy wszyscy interesanci zdają sobie sprawę z tego, że ich rozmowy są nagrywane. Obie instytucje informują wprawdzie o tym za pomocą tablic, ale tylko placówka w Kielcach wyraźnie zwraca uwagę na nagrywanie dźwięku. W budynku w Krakowie można jedynie trafić na napis: „Obiekt monitorowany", choć w odpowiedzi na interwencję Fundacji Panoptykon władze oddziału zapewniły, że zadbają o bardziej wyczerpującą informację.

URZĄD MÓWI: SPRAWDZAM

Od lat polska administracja podążą ścieżką informatyzacji. W założeniu ma ona nie tylko usprawnić pracę urzędników, ale też ułatwić życie interesantom i w dłuższej perspektywie ograniczyć koszty działania instytucji. Ma być szybciej, sprawniej, bez zbędnej „papierologii" i przez Internet. A bywa rozmaicie. Gigantyczne projekty są nie tylko trudne do sprawnego wdrożenia, ale również – ze względu na ogromne pieniądze wchodzące w grę – narażone na korupcję i uwikłanie w różne, nie zawsze jasne interesy.

Informacja w rękach państwa

Szczególne wyzwania są związane z faktem integrowania, często na poziomie centralnym, wielu danych o obywatelach oraz z bezpieczeństwem gromadzonych informacji. Co istotne, impulsem do tworzenia takich systemów i ich ważnym elementem jest potrzeba kontrolowania obywateli – tego, czy wypełniają swoje obowiązki wobec państwa, czy nie próbują go oszukać itp.

Dobrym przykładem jest system Emp@tia, który służy informatyzacji przyznawania i dystrybucji świadczeń przez pomoc społeczną. Jego stworzenie kosztowało około 45 mln zł. W bazie danych przetwarzane są informacje dotyczące kilku milionów osób z niepełnosprawnościami i innych uprawnionych do pobierania zasiłków. Ważną funkcją jest weryfikacja, czy ktoś nie pobiera należnych świadczeń więcej niż raz, w kilku różnych miejscach. Emp@tię będą miały okazję lepiej poznać również osoby niekorzystające na co dzień z pomocy społecznej. System jest bowiem wykorzystywany do dystrybuowania wsparcia dla rodzin objętych programem „Rodzina 500+".

Systemy gromadzenia i przetwarzania informacji coraz częściej opierają się na różnego rodzaju danych biometrycznych (szerzej była o nich mowa wyżej). W Unii Europejskiej są one wykorzystywane na przykład do kontroli granic. Odciski palców osób ubiegających się o wizę albo status uchodźcy i nielegalnie przekraczających granice gromadzone są odpowiednio w systemach VIS oraz Eurodac. Do tego potrzebne są nie tylko określone systemy komputerowe, ale również czytniki linii papilarnych kupowane przez Straż Graniczną i Ministerstwo Spraw Zagranicznych. Wraz z biometrycznym obrazem twarzy odciski palców są również wykorzystywane w paszportach wydawanych przez państwa członkowskie Unii Europejskiej.

Instytucje lokalne nie chcą pozostać w tyle. Jakiś czas temu władze Łomży postanowiły, że miasto to jako pierwsze w Polsce będzie wykorzystywać technologię biometryczną w usługach publicznych. W ramach projektu „Biometryczna Łomża" miała zostać stworzona platforma usług publicznych, dzięki której mieszkańcy mieli uzyskać dostęp – za pomocą skanu układu krwionośnego palców dłoni – do różnych usług publicznych, na przykład komunikacji miejskiej, usług Miejskiego Ośrodka Sportu i Rekreacji czy zasiłków. Ostatecznie jednak ambitna inicjatywa zatrzymała się na ogłoszeniu przez prezydenta enigmatycznego listu intencyjnego oraz na kilku spotkaniach informacyjnych.

Nieco dalej w swoich planach zawędrowało Ministerstwo Finansów, które pracowało nad wdrożeniem głosowej weryfikacji tożsamości jako elementu Systemu Informacji Telefonicznej, który zastąpić miał dotychczasowy system udzielania informacji podatkowej. Przyjęcie takiego rozwiązania miało usprawnić działanie systemu. Dzięki niemu osoby, które dobrowolnie (jak podkreślało Ministerstwo) zdecydują się

na zapisanie w oddzielnej bazie matematycznych macierzy wzorca głosu (tzw. *voiceprint*), nie będą musiały podawać dodatkowych informacji, by uzyskać dostęp do indywidualnych danych umieszczonych na koncie podatnika. Wątpliwości dotyczące braku podstawy prawnej sprawiły jednak, że w 2015 r. Ministerstwo zdecydowało się zawiesić wdrażanie nowego systemu i jedynie testowo wykorzystywać możliwość głosowej weryfikacji tożsamości dzwoniącej osoby względem pracowników administracji podatkowej. Trudno jednak przewidzieć, jakie w rzeczywistości będą dalsze losy projektu.

Wróżenie z danych

Na szczególną uwagę zasługują narzędzia wykorzystujące algorytmy do wyłapywania różnego rodzaju nieprawidłowości, na przykład podejrzanych transakcji czy niezapłaconych podatków. Podstawą funkcjonowania takich programów jest traktowanie wszystkich obywateli jak podejrzanych – po to, by namierzyć nieliczne osoby, które rzeczywiście dopuszczają się nadużyć. Szczegółowa logika działania (co konkretnie decyduje o tym, że dana osoba zostanie uznana za podejrzaną), jak w przypadku większości systemów służących profilowaniu, pozostaje niewiadomą.

Sposób działania jest podobny jak przy analizowaniu przez policję i inne służby informacji publikowanych w Internecie czy pobieranych z sieci telekomunikacyjnej (mowa o tym szerzej w trzecim rozdziale). W tym przypadku jednak źródłem wiedzy są przede wszystkim informacje dostępne w licznych bazach danych, do których mają dostęp instytucje publiczne.

KOMPUTEROWE ALGORYTMY MAJĄ W PRZYSZŁOŚCI POMAGAĆ NAMIERZAĆ OSZUSTÓW PODATKOWYCH.

Systemem śledzenia podejrzanych transakcji dysponuje Generalny Inspektor Informacji Finansowej (GIIF). Otrzymuje on od szerokiej grupy zobowiązanych do tego podmiotów (na przykład banków, domów maklerskich, zakładów ubezpieczeń, innych przedsiębiorstw, adwokatów, radców prawnych i notariuszy, fundacji i stowarzyszeń) informacje o transakcjach przekraczających 15 tys. euro oraz o tzw. transakcjach podejrzanych, czyli takich, które potencjalnie mogą mieć związek z praniem brudnych pieniędzy lub finansowaniem terroryzmu. W 2014 r. GIIF otrzymał zgłoszenia blisko 28 mln transakcji pierwszego rodzaju oraz ponad 3,6 tys. zawiadomień o transakcjach drugiego rodzaju, co oznacza, że został wprost zasypany danymi. Na podstawie informacji namierzonych w tym stogu siana GIIF przekazał 170 zawiadomień o popełnieniu przestępstwa, zablokował 283 rachunki bankowe, skierował 1531 powiadomień do organów kontroli skarbowej oraz kilkaset do innych instytucji i służb.

Komputerowe algorytmy mają w przyszłości pomagać namierzać oszustów podatkowych. Na początku lutego 2016 r. Ministerstwo Finansów przedstawiło projekt ustawy zakładającej powołanie spółki celowej, która ma przygotować rozwiązania informatyczne dla administracji podatkowej. Nowe narzędzia służyć mają analizie prawdopodobieństwa występowania naruszeń prawa podatkowego w oparciu o dane o podatnikach z systemów teleinformatycznych ministra finansów, organów administracji podatkowej i kontroli skarbowej. Skuteczna egzekucja podatków jest ważna, jednak wybrana metoda budzi wątpliwości. Choć algorytm ma tylko typować podejrzanych, a nie rozstrzygać o ich winie, warto mieć świadomość, że już sama decyzja o przeprowadzeniu u danego podatnika kontroli może mieć dla niego poważne konsekwencje.

Wyzwania związane z wykorzystaniem danych o obywatelach przez instytucje publiczne będą się prawdopodobnie pogłębiać. Ma to związek nie tylko z rozwojem nowych technologii, zaplecza informatycznego państwa czy tworzeniem kolejnych baz danych, w których gromadzone

są informacje o obywatelach, ale również ze zmianą w ustawie o ochronie danych osobowych, która została wprowadzona na ostatniej prostej prac nad programem „Rodzina 500+". Zgodnie z nią rozmaite instytucje państwowe – od służb specjalnych, przez organy centralne, po urzędy pomocy społecznej – „uważa się za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu".

ANALIZA DANYCH Z ORTOFOTOMAPY MOŻE BYĆ PIERWSZYM KROKIEM DO WERYFIKACJI, CZY KTOŚ NIE UCHYLA SIĘ OD PŁACENIA PODATKU OD NIERUCHOMOŚCI.

Zgodnie z uzasadnieniem projektu chodzi o to, by instytucje z obszaru rynku pracy i polityki społecznej mogły łatwiej wymieniać się danymi, nieskrępowane przez ustawę o ochronie danych osobowych czy brak odpowiednich uregulowań. Proponowane rozwiązanie dotyczy jednak wszystkich instytucji państwowych i wszystkich obywateli, a pojęcie „tego samego interesu publicznego" jest bardzo pojemne. I rodzi ryzyko, że różne podmioty będą mogły swobodnie wymieniać się informacjami na temat obywateli i wykorzystywać je do swoich celów, a osoby, których to dotyczy, nawet się o tym nie dowiedzą.

Kursorem po mapie

Do kontrolowania obywateli przez instytucje publiczne mogą być wykorzystywane narzędzia stworzone pierwotnie w zupełnie innym celu. Dobrym przykładem są ortofotomapy, czyli popularny dziś rodzaj mapy, z której korzystać można również w Internecie. Składają się one z wielu zdjęć satelitarnych lub lotniczych, przetworzonych i wkomponowanych w układ geodezyjny. Pierwotnie ortofotomapy używane były przede wszystkim do planowania przestrzennego. Z czasem pojawiały się pomysły na ich wykorzystanie w inny sposób.

Spośród urzędów z 42 miast wojewódzkich i powiatowych, które odpowiedziały na zadane przez Fundację Panoptykon pytania, ponad połowa zadeklarowała, że wykorzystuje ortofotomapy do weryfikacji zobowiązań podatkowych (Białystok w analogiczny sposób wykorzystuje również usługę Google: Street View). Najczęściej dotyczy to ściągania podatków od nieruchomości, rzadziej podatku rolnego lub leśnego. Analiza danych z ortofotomapy jest zazwyczaj pierwszym krokiem do weryfikacji, czy ktoś nie uchyla się od płacenia podatku. Zdarza się, że impulsem do jego podjęcia jest donos.

Weryfikacja polega na zestawieniu obrazów z map z deklaracjami podatników i treścią rejestrów. Urzędnicy sprawdzają, czy na mapach nie widać niezgłoszonych budów lub nieścisłości dotyczących powierzchni budynków. W przypadku stwierdzenia rozbieżności organ podatkowy prowadzi postępowanie podatkowe w trybie ordynacji podatkowej, w trakcie którego wzywa podatnika do złożenia wyjaśnień oraz – jeśli to konieczne – przeprowadza u niego oględziny. Może wszcząć również procedurę kontroli podatkowej.

Nie wszystkie urzędy gromadzą informacje o tym, w ilu przypadkach orfofotomapy zadecydowały o wykryciu nieprawidłowości i jakie pieniądze udało się dzięki temu odzyskać. Urzędnicy z Wrocławia twierdzą, że w 2014 r. pomogły one w namierzeniu 30 przypadków nieprawidłowości, a z Łodzi przywołują 100 takich przypadków. Katowice deklarują, że w tymże roku objęto na tej podstawie kontrolą podatkową 19 nieruchomości.

Nie każdy jednak zdaje sobie sprawę z tego, że ortofotomapy są wykorzystywane w różnych częściach Polski do weryfikacji zobowiązań podatkowych. Urzędy nie mają bowiem spójnej praktyki informowania o takich działaniach. Tylko część miast (na przykład Poznań, Białystok, Katowice, Konin) zapewnia, że w wydawanych decyzjach zwraca uwagę na sposób wykrycia

nieprawidłowości. Ale wtedy i tak podatnik dowiaduje się o tym po fakcie.

Przedstawiciele miast dość zgodnie deklarują, że korzystanie z ortofotomap nie generuje dodatkowych kosztów. Mapy są tworzone do innych celów, a ich weryfikacją zajmują się zazwyczaj urzędnicy w ramach swoich codziennych obowiązków. Z doniesień Portalu Samorządowego wynika, że na inną strategię zdecydowały się władze Gliwic: to, co zazwyczaj wyrywkowo robią pracownicy urzędu, zleciła całościowo do wykonania zewnętrznej firmie. Koszt: 300 tys. zł. Władze miasta zapewniają jednak, że zwrócił się on z nawiązką.

PRACA POD SPECJALNYM NADZOREM

Każda instytucja może w praktyce działać dzięki zatrudnionym w niej osobom. Aby działała sprawnie, nie obejdzie się bez kontroli ich pracy. W przypadku instytucji publicznych ma ona dodatkowy – ważny – wymiar: kontrolowania efektywności wydawania środków publicznych. Co więcej – urzędnicy mają dostęp do informacji o obywatelach, również tych wrażliwych, a w wielu przypadkach mogą podejmować decyzje wpływające na życie obywateli. Dlatego bez odpowiedniego poziomu weryfikacji ich działań trudno wyobrazić sobie poszanowania praw każdego z nas. Ta kontrola ma jednak swoje granice, które powinien wyznaczać szacunek dla godności, prywatności i innych praw pracownika.

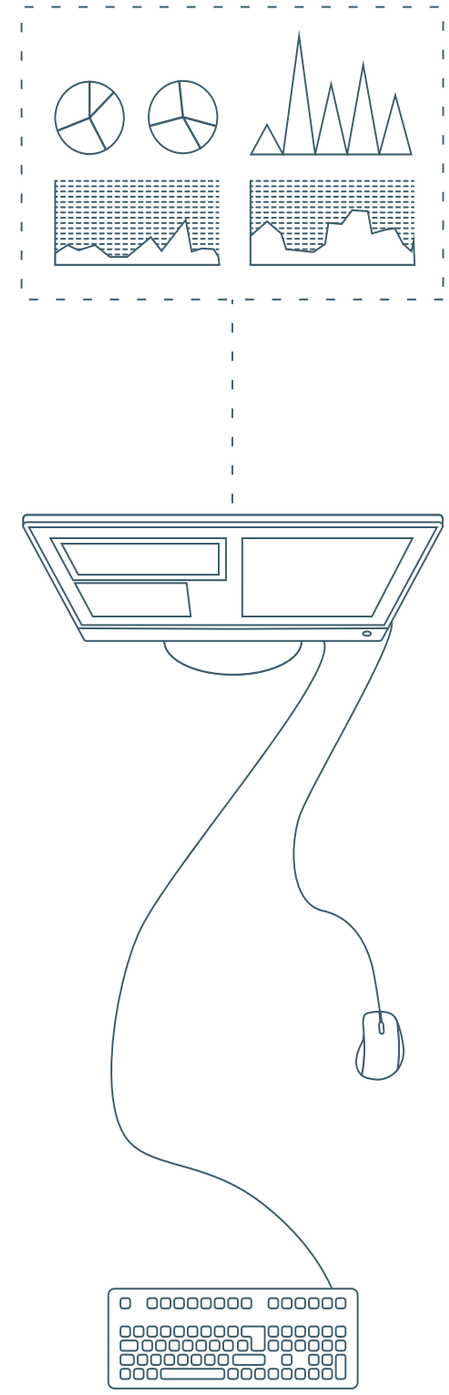
Nowe narzędzia – nowe wyzwania

Wyznaczenie tej granicy w praktyce staje się coraz większym wyzwaniem. Przyczynia się do tego coraz bogatsza oferta narzędzi służących do obserwowania i analizowania działań pracowników, która otwiera przed pracodawcami nowe możliwości i rodzi kolejne pokusy. Przekłada się to na realia funkcjonowania wielu instytucji. Standardem jest dzisiaj (o czym mowa wyżej) korzystanie z monitoringu wizyjnego – a czasem również dźwiękowego – oraz rozliczanie czasu przy pomocy zautomatyzowanego systemu kontroli dostępu. Coraz powszechniejsze jest stosowanie oprogramowania służącego do kontroli korzystania z komputerów i Internetu (o tym można przeczytać niżej) czy nagrywanie rozmów telefonicznych. W niektórych przypadkach wykorzystywane bywają również urządzenia badające zawartość alkoholu lub innych substancji odurzających, a nawet wariografy.

Do kontroli działań pracowników używa się również systemów do zarządzania informacją w organizacji. Przykładem może być baza Audyt wykorzystywana przez ZUS. Działanie wykonane za pomocą systemu zawsze pozostawia po sobie ślad – dzięki temu można powiązać je z loginem konkretnego urzędnika oraz z danymi identyfikującymi ubezpieczonego lub płatnika składek, którego ono dotyczyło. Informacje te są wykorzystywane m.in. do analizy, czy podejmowane działania były uzasadnione z punktu widzenia zadań danej osoby. Zgodnie z biurokratycznymi procedurami przełożeni są zobowiązani do sprawdzenia minimum 10% podległych pracowników, a jednocześnie każdego pracownika co najmniej raz w roku.

Oczywiście nowe narzędzia pozwalają na wyprowadzenie kontroli poza mury urzędu. Szczególnie popularne są w tym przypadku nadajniki GPS montowane w samochodach wykorzystywanych przez pracowników. Na przykład GDDKiA rozpisała niedawno przetarg na usługi monitoringu floty 1610 sztuk służbowych samochodów. Firmy dostarczające tego typu

rozwiązania przekonują, że dzięki ich zastosowaniu można poprawić „wydajność" kierowców. Najczęściej chodzi więc po prostu o większą kontrolę działań zatrudnionych osób, którzy pracują poza biurem. W niektórych jednak przypadkach GPS znajduje dodatkowe zastosowania. Jest tak na przykład w przypadku geolokalizacji autobusów i innych pojazdów komunikacji miejskiej, która pozwala na bieżąco monitorować spóźnienia i informować o nich pasażerów.



Prawo pracy nie formułuje szczegółowych reguł korzystania z narzędzi kontroli, tylko ogólne zasady. Dlatego często trudno ocenić, czy daną praktykę można uznać za legalną, czy też za zbyt głęboko ingerującą w prawa pracowników. Szczególnie w cenie więc są zdrowy rozsądek i poszanowanie godności drugiej osoby. Co istotne: kontrola nie zawsze motywuje do sumienności, może za to utrudniać budowanie wzajemnego zaufania i zaangażowania w wykonywaną pracę oraz sprzyjać postawom „od–do". Znaczenie mają też pieniądze: narzędzia służące do kontroli pracowników kosztują i warto się zastanowić, czy korzystanie z nich wszystkich rzeczywiście się administracji publicznej opłaca.

Niestety, zdarzają się sytuacje, w których narzędzia nadzoru wykorzystywane są do mobbingu, upokarzania czy pokazywania swojej władzy. Jakiś czas temu głośno było o sprawie wójta, który w swoim urzędzie po kryjomu zainstalował kamerę, która obserwowała i podsłuchiwała jedną z urzędniczek. Ostatecznie prokuratura nie dopatrzyła się w jego praktykach przestępstwa, jednak pracownica poczuła się nie tylko poddana „totalnej inwigilacji", ale również oszukana, gdy okazało się, że sprzęt, który miał być czujnikiem ruchu, pełni zupełnie inne funkcje.

Państwowa Inspekcja Pracy w swoich instrukcjach podkreśla, że decyzja o instalacji monitoringu powinna być uzależniona od konkretnej sytuacji, na przykład wielkości instytucji,

rodzaju wykonywanej pracy. Kamery nie powinny być montowane w miejscach, w których nie jest obserwowany proces pracy, ani w sytuacji, w których mogą one ingerować w intymność pracownika. Mowa na przykład o stołówkach, szatniach, gabinetach lekarskich. Pracodawca powinien poinformować pracowników o monitoringu oraz zadbać o to, by nagrania były możliwie szybko kasowane.

Prawo do informacji oraz adekwatność do sytuacji powinny być normą w przypadku wykorzystania wszelkich narzędzi służących do kontrolowania pracowników. I nie tylko ich – również osób zatrudnionych na podstawie umów cywilnoprawnych (co jest coraz częstszą praktyką również w instytucjach publicznych). Sytuacja prawna jest w tym przypadku jeszcze bardziej niejednoznaczna niż u osób mających umowy o pracę. Jednak forma umowy nie powinna determinować poziomu ochrony przed nieuzasadnioną ingerencją w prywatność.

Pracownik w sieci

Komputer z dostępem do Internetu jest dzisiaj jednym z podstawowych narzędzi pracy. Ale pozwala też łatwo oddalić się od obowiązków zawodowych w kierunku sprawdzania prywatnej poczty elektronicznej, zaglądania na portale społecznościowe, korzystania z usług banków, przeglądania różnych stron internetowych, a nawet odwiedzania witryn z zawartością erotyczną. Firmy produkujące oprogramowanie umożliwiające śledzenie aktywności użytkowników sprzętu komputerowego i blokowanie dostępu do treści internetowych przekonują pracodawców, że to właśnie ono stanowi rozwiązanie ich problemów. Czy tak jest w istocie – można mieć wątpliwości. Wielu pracodawców daje się jednak przekonać – według szacunków nawet 80% z nich kontroluje w ten sposób swoich pracowników.

DOSTĘPNE NA RYNKU POGRAMY POZWALAJĄ NA MONITOROWANIE SPOSOBU KORZYSTANIA Z SIECI I APLIKACJI DOSTĘPNYCH NA KOMPUTERZE: REJESTRUJĄ PRZEGLĄDANE STRONY I CZAS ODWIEDZIN, AKTYWNOŚĆ KLAWIATURY I MYSZKI ORAZ DRUKOWANE DOKUMENTY, A TAKŻE ZAPISUJĄ ZRZUTY EKRANU.

Dostępne na rynku pogramy mają różnorodne funkcjonalności. Pozwalają na monitorowanie sposobu korzystania z sieci i aplikacji dostępnych na komputerze: rejestrują przeglądane strony i czas odwiedzin, aktywność klawiatury i myszki oraz drukowane dokumenty, a także zapisują zrzuty ekranu. Rejestrując godziny logowania i wylogowania, mierzą czas pracy użytkowników. Uniemożliwiają dostęp do wybranych stron bądź zasobów internetowych zawierających określone słowa kluczowe. Pozwalają tworzyć raporty dotyczące aktywności poszczególnych pracowników, które mogą być podstawą do oceny ich pracy.

Fundacja Panoptykon przyjrzała się, jak to wygląda w wybranych instytucjach publicznych. Otrzymała odpowiedzi od ponad setki podmiotów: ministerstw i innych instytucji centralnych, oddziałów ZUS i NFZ oraz urzędów miast. Do korzystania z programów komputerowych śledzących aktywność pracowników przyznała się niemal połowa z nich. Zróżnicowanie między instytucjami jest całkiem spore, część w ogóle nie korzysta z takich programów, inne poprzestają na prostych rozwiązaniach, a niektóre zdecydowały się na korzystanie z rozbudowanych systemów. Częściowo można to uzasadnić wielkością czy charakterem instytucji, ale nie w każdym przypadku. Na przykład znaczne różnice można zaobserwować między urzędami miast.

W odpowiedziach instytucji znalazło odbicie bogactwo programów dostępnych na rynku. Wykorzystywane są rozwiązania wielu różnych firm – trudno tu wskazać lidera. Zróżnicowanie w zakresie funkcjonalności przekłada się na dużą rozpiętość cen: od kilku tysięcy do ponad miliona złotych. Programy wykorzystywane w urzędach miast kosztowały zazwyczaj kilkadziesiąt tysięcy złotych, a w urzędach centralnych – zwykle ponad 100 tys. zł. Najdroższe łączą zazwyczaj szereg zaawansowanych funkcji.

Z uzyskanych odpowiedzi wynika, że programy te wykorzystywane są najczęściej do monitorowania sposobu korzystania z Internetu i aplikacji, mierzenia czasu pracy oraz blokowania dostępu do wybranych stron internetowych. Często funkcjonalności związane z kontrolą działań pracowników przenikają się z działaniami nakierowanymi na bezpieczeństwo systemu IT (na przykład ochronę antywirusową czy antyspamową).

Większość instytucji zadeklarowała, że informuje swoich pracowników o tym, że ich komputerowa aktywność jest monitorowana. Odbywa się to na różne sposoby: poprzez nałożenie obowiązku zapoznania się z regulaminem korzystania z zasobów informatycznych; poprzez informację przekazywaną w chwili pierwszego uruchomienia konta pracownika wraz z loginem i hasłem startowym lub wyświetlanie jej na monitorze przy każdym uruchomieniu stanowiska komputerowego; w ramach szkoleń z zakresu bezpieczeństwa informacji; poprzez odebranie specjalnego oświadczenia. Otwarte zostaje pytanie, na ile takie formy przekazywania informacji są przystępne dla pracowników i na ile rzeczywiście rozumieją oni, w jaki sposób ich praca jest obserwowana i analizowana.

Niestety, zdarzają się również niechlubne wyjątki w postaci instytucji, które przyznają się, że w ogóle nie informują zatrudnionych osób o tym, że kontrolują ich pracę za pomocą specjalnych programów komputerowych. Należą do nich urząd warszawskiej dzielnicy Białołęka czy resort pracy. Ten ostatni przypadek szczególnie zwraca uwagę. Ministerstwo w swoich oficjalnych stanowiskach kwestionuje interpretację przepisów promowaną przez Państwową Inspekcję Pracy czy Rzecznika Praw Obywatelskich, zgodnie z którą wszelkie formy kontroli wymagają – przynajmniej co do zasady – poinformowania o tym pracownika. I jak widać – w najbardziej bezpośredni sposób – przenosi tę opinię na swoją praktykę działania.

W SIECI

Sieć stała się częścią codziennego życia. Za jej pomocą kontaktujemy się ze sobą, pracujemy, robimy zakupy, czerpiemy informacje o otaczającym świecie, korzystamy z kultury i rozrywki. A przy okazji zostawiamy całą masę informacji o sobie: część sami – mniej lub bardziej świadomie – upubliczniamy, część przesyłamy innym lub zapisujemy w chmurze, a część wreszcie zostawiamy zupełnie mimowolnie – to tzw. metadane, czyli informacje, z kim się kontaktujemy, na jakie strony wchodzimy, z jakiego sprzętu korzystamy czy gdzie przebywamy. Wbrew pozorom – w sieci prawie nigdy nie jesteśmy anonimowi. Choćby dlatego, że informacje połączone ze sobą pozwalają nas zidentyfikować. A nawet ich ułamek wystarcza, by stworzyć obraz, który nie musi być w pełni zgodny z rzeczywistością, ale z pewnością będzie bardzo bogaty.

Z tego bogactwa korzystają różne publiczne instytucje. Może się ono okazać ważnym źródłem wiedzy dla policji i innych służb, których zadaniem jest stanie na straży szeroko pojętego bezpieczeństwa i porządku. Ale – co już mniej oczywiste, a bardziej prozaiczne – z informacji na temat aktywności użytkowników Internetu mogą korzystać również urzędy prowadzące swoje strony internetowe. Ostatnia część przewodnika opisuje, jakie cyfrowe ślady zostawia każdy z nas oraz jakimi narzędziami dysponują publiczne instytucje, by móc je wykorzystać w swojej działalności.

CIEKAWSKIE SERWISY

Dzisiaj właściwie każda instytucja publiczna dysponuje własną stroną internatową. Dla obywateli to duże ułatwienie – internetowe serwisy pozwalają szybko znaleźć przydatne materiały i informacje: formularze urzędowe, zapowiedzi ważnych wydarzeń, godziny otwarcia urzędów, numery telefonów czy rozkłady jazdy komunikacji miejskiej. Instytucje publiczne – tak jak inni administratorzy, a może nawet bardziej – powinny dbać o ochronę prywatności użytkowników. W przypadku firm często przeważa chęć wykorzystywania informacji w celach komercyjnych. Instytucje publiczne nie kierują się chęcią zysku, a jednak na ich stronach można znaleźć sporo elementów śledzących. Decydująca okazuje się zapewne wygoda lub zwykły brak świadomości, jakie konsekwencje niesie korzystanie z nich.

Ciasteczkowe potworki

Już samo wejście na dowolną stronę internetową uruchamia przepływ danych. Administrator serwisu automatycznie uzyskuje: adres IP użytkownika oraz informacje o przeglądarce, z której korzysta (m.in. jej wersję, system operacyjny, język). Strony internetowe wykorzystują różne mechanizmy służące pozyskaniu informacji. Najpopularniejsze są ciasteczka (ang. *cookies*), czyli specjalne pliki zapisywane na komputerze użytkownika. Służą powiązaniu internetowych aktywności z konkretną osobą. Część z nich jest niezbędna do prawidłowego wyświetlania strony, logowania bądź zapisania wyników ankiety, inne jednak pozwalają zdobyć dodatkowe informacje o aktywności odwiedzających.

Fundacja Panoptykon zbadała, jakie informacje o użytkownikach zbierane są na stronach 70 różnych publicznych instytucji. Za pomocą dodatków do przeglądarki internetowej: Lightbeam (dostępny dla Firefoksa) oraz Disconnect i Ghostery przetestowała strony wszystkich ministerstw, policji i innych służb, wszystkich miast wojewódzkich i wybranych powiatowych (konkretnie strony urzędów miast i lokalnych zakładów komunikacji), ZUS i NFZ – w tym ich oddziałów – oraz GIODO. W przypadku ministerstw dodatkowo przeanalizowane zostały dostępne na stronach internetowych polityki prywatności.

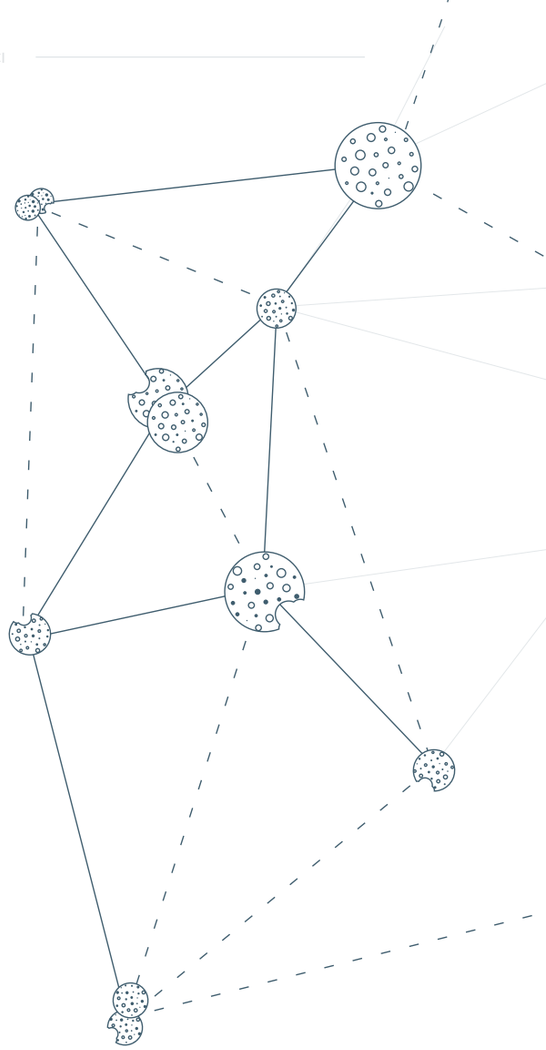
Wnioski? Instytucje publiczne powszechnie korzystają z różnych aplikacji i wtyczek pozwalających na zbieranie informacji o osobach odwiedzających ich serwisy oraz zapisują ciasteczka na wykorzystywanych do tego urządzeniach. Wśród aplikacji zbierających informacje o użytkownikach najczęściej stosowane są programy o charakterze analitycznym, które pomagają dowiedzieć się m.in. tego, jak korzystają oni ze strony, jakie informacje ich interesują i w jaki sposób wyszukują konkretne treści (czy bezpośrednio na stronie, czy poprzez wyszukiwarki internetowe). Statystyki odwiedzin są dla każdego administratora serwisu bardzo przydatne, jednak oprócz nich programy analityczne mogą zbierać o wiele więcej informacji o odwiedzających, niż jest to niezbędne do zarządzania stroną – nawet dane pozwalające na ich identyfikację.

JEŚLI INSTYTUCJE PUBLICZNE SIĘGAJĄ PO NARZĘDZIA ŁĄCZĄCE ICH STRONY Z ZEWNĘTRZNYMI SERWISAMI, TO DZIELĄ SIĘ Z NIMI INFORMACJAMI O SPOSOBIE KORZYSTANIA Z DANEJ STRONY PRZEZ UŻYTKOWNIKÓW.

Zbieranie nadmiernej ilości informacji to nie jedyny problem. Ważną kwestią jest również to, że wykorzystywane programy mogą przekazywać je dalej różnym zewnętrznym podmiotom, w tym zagranicznym firmom. Służą do tego specjalne wtyczki, które zapisują na sprzęcie użytkowników ciasteczka należące do podmiotów zewnętrznych, tzw. *third party cookies*. Jeśli instytucje publiczne sięgają po narzędzia łączące ich strony z zewnętrznymi serwisami, to dzielą się z nimi informacjami o sposobie korzystania z danej strony przez użytkowników, a tych ostatnich (o ile nie włączą oni odpowiednich blokad) zmuszają do akceptowania polityk prywatności komercyjnych podmiotów.

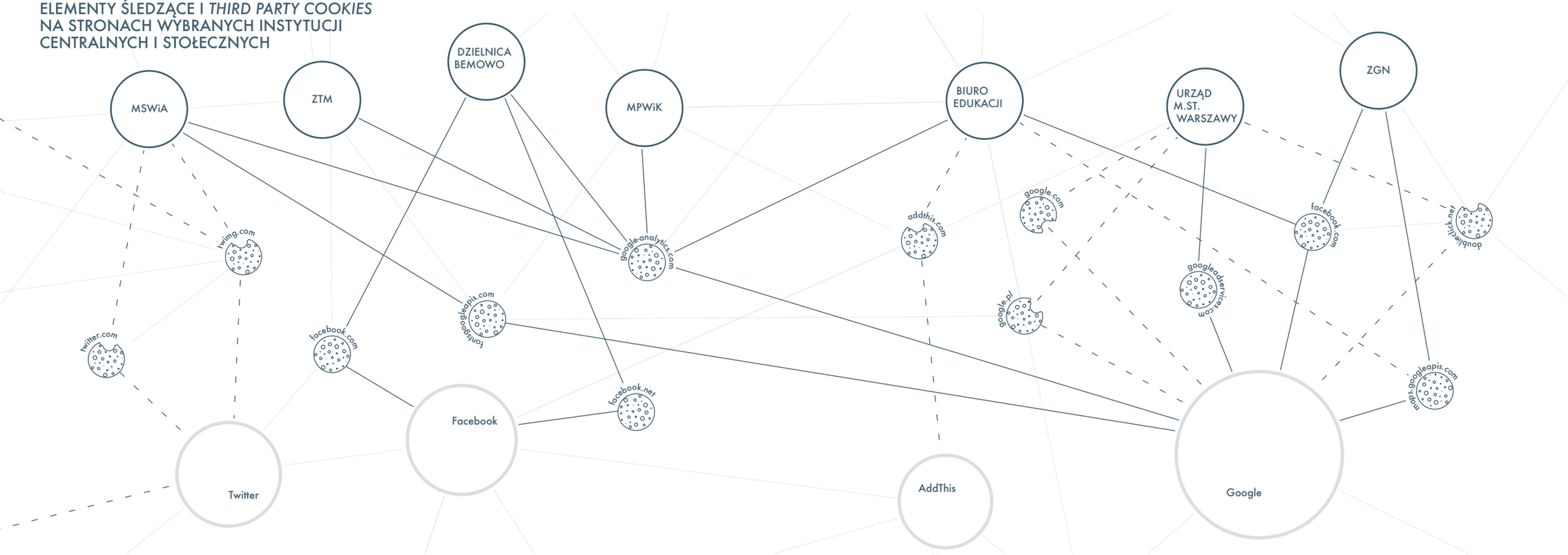
Third party cookies pojawiają się na prawie wszystkich monitorowanych publicznych serwisach. Zdecydowanie najbardziej popularne są wtyczki należące do Google'a (w tym przede wszystkim Google Analytics, wyszukiwarka, mapy, Google+, YouTube), często wykorzystywane są też wtyczki Facebooka czy Twittera. Zdarza się, że nie są one obecne na stronach głównych, ale wystarczy wejść nieco głębiej, by szybko na nie trafić. Google Analytics – najpopularniejszej aplikacji służącej do zbierania i analizy informacji o tym, jak użytkownicy korzystają z danej strony – używa większość ministerstw, znaczna część urzędów miast czy oddziałów NFZ. Decydują się one w ten sposób przekazywać firmie Google nie tylko informacje o popularności swojej strony internetowej, ale też o sposobie korzystania z niej przez poszczególnych użytkowników. Powiększa to zbiór informacji, którym ta firma dysponuje (a jest on bardzo duży, choćby ze względu na popularność jej produktów i fakt, że Google łączy informacje pochodzące ze swoich usług, na przykład z wyszukiwarki, poczty, YouTube'a, Google+, Picasy).

Inne popularne rozwiązanie Google'a to wyszukiwarka zintegrowana z serwisem danej instytucji. W takim przypadku wpisanie zapytania w okno wyszukiwania na stronie w rzeczywistości oznacza skorzystanie z wyszukiwarki Google. Co ciekawe, umożliwiająca taką integrację wtyczka umieszczona jest na przykład na stronie GIODO, czyli instytucji powołanej do stania na straży prywatności.



Spora część administratorów publicznych serwisów korzysta z wtyczek portali społecznościowych, które bezpośrednio na stronie instytucji pozwalają na „polubienie" konkretnego materiału lub nawet wyświetlają treści pojawiające się na profilu danej instytucji na portalu społecznościowym – robi tak na przykład Ministerstwo Spraw Wewnętrznych i Administracji oraz Centralne Biuro Antykorupcyjne (CBA). W tym przypadku informacje, ile czasu użytkownik spędził na stronie czy co czytał, mogą

ELEMENTY ŚLEDZĄCE I *THIRD PARTY COOKIES* NA STRONACH WYBRANYCH INSTYTUCJI CENTRALNYCH I STOŁECZNYCH



○○○ – wybrane serwisy instytucji publicznych:

•• Ministerstwo Spraw Wewnętrznych i Administracji – mswia.gov.pl •• Zarząd Transportu Miejskiego w Warszawie – ztm.waw.pl ••
•• warszawska dzielnica Bemowo – bemowo.waw.pl •• Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w Warszawie – mpwik.pl ••
•• Biuro Edukacji m.st. Warszawy – edukacja.warszawa.pl •• Urząd m.st. Warszawy – um.warszawa.pl ••
•• Zakład Gospodarowania Nieruchomościami w warszawskiej dzielnicy Śródmieście – zgn.waw.pl ••

– *third party cookies*

– inne elementy śledzące

○○○ – wybrane firmy, które otrzymują informacje o użytkownikach serwisów instytucji publicznych

być połączone z bogactwem informacji gromadzonych w portalach społecznościowych. A co ważne, Facebook nie tylko wzbogaca dzięki temu profile osób, które korzystają z jego usług, ale tworzy również profile-cienie tych, których nie uda mu się rozpoznać jako swoich użytkowników.

Niektóre portale samorządowe szczególnie upodobały sobie instalowanie *third party cookies*. Na przykład oficjalna strona urzędu miasta Wrocławia serwuje ciasteczka z 10 innych serwisów (tylko 2 z nich wyglądają na powiązane miejskie strony), a strona Gdańska – z 9 innych portali. Jest to szczególnie ważne, ponieważ lokalne portale cieszą się zazwyczaj popularnością i są odwiedzane przez spore rzesze użytkowników.

Rzadziej, ale jednak, instytucje publiczne wykorzystują wtyczki o charakterze marketingowym, które pozwalają na określenie, jakie treści pokażą się odbiorcom z konkretnego obszaru, czy na dopasowanie reklam do ich statystycznie określonych preferencji – taką wtyczką o nazwie DoubleClick posługuje się choćby Ministerstwo Spraw Zagranicznych. Część komunikatów (na przykład ostrzeżenia o zagrożeniach czy informacje, gdzie szukać pomocy) przygotowywanych przez Ministerstwo zapewne skierowana jest do osób przebywających na określonym terytorium. Możliwość geograficznego sprofilowania komunikacji w niektórych przypadkach może mieć uzasadnienie, ale znowu warto się zastanowić, czy powinno się to odbywać za pośrednictwem aplikacji, które mogą przekazywać dane podmiotom trzecim.

Korzystanie z wtyczek analitycznych czy umożliwiających dzielenie się treściami na portalach społecznościowych oferowane jest za darmo, a przynajmniej tak to wygląda na pierwszy rzut oka. W rzeczywistości często płaci się za to informacjami o użytkownikach stron, co zwiększa potencjał i zyski firm internetowych, które oferują „darmowe" aplikacje. Aspekt finansowy jest ważny – instytucje publiczne powinny w rozsądny sposób dysponować środkami – jednak podmioty te jako administratorzy stron internetowych powinny również uwzględnić potrzebę zachowania prywatności użytkowników i poszukać rozwiązań, które pozwalają na większą kontrolę nad informacjami, na przykład sięgać po mniej znane, ale i mniej śledzące, rozwiązania techniczne.

SŁUŻBY W GĄSZCZU DANYCH

Na początku 2016 r. spore poruszenie wywołała ustawa zwana potocznie inwigilacyjną. Przyznała ona policji i innym służbom szersze możliwości dostępu do danych dotyczących aktywności w Internecie. Społeczny niepokój był uzasadniony. Nie oznacza to jednak, że wcześniej służby nie mogły sięgać po dane internetowe czy podążać tropem innych naszych cyfrowych śladów. Mogły to robić i z tej możliwości korzystały. A teraz mogą to robić na jeszcze szerszą skalę.

Dane w służbie bezpieczeństwa

Im powszechniej korzystamy z telefonu czy rozmaitych urządzeń podłączonych do Internetu, tym więcej danych do analizowania mają policja, ABW, CBA, Służba Celna i inne służby. W ramach prewencji czy ścigania sprawców przestępstw podejmują różnorodne działania, które w mniejszym lub większym stopniu mogą ingerować w naszą prywatność. W przypadku policji może to być na przykład:

- wstępne rozpoznanie zagrożenia, które może się wiązać z pobraniem informacji dotyczących szerokiego kręgu osób;
- analiza zebranych danych, na przykład analiza połączeń telefonicznych czy sieci społecznościowych (w ramach tzw. analizy kryminalnej);
- dalsza, pogłębiona inwigilacja już określonych osób lub urządzeń, która może polegać m.in. na przechwytywaniu komunikatów;
- zabezpieczenie dowodów na potrzeby sprawy karnej, co może się wiązać z koniecznością złamania zabezpieczeń telefonu czy komputera i wydobyciem danych z pamięci urządzenia (w ramach tzw. informatyki śledczej).

Im szerzej zakrojone są działania służb w sieci, tym bardziej warte są uwagi. Bardzo często są one bowiem poza jakąkolwiek kontrolą, a jednocześnie siłą rzeczy dotykają również ludzi, którzy nie mają nic wspólnego z naruszeniami prawa. O ile zastosowanie inwigilacji wobec określonej osoby w wielu przypadkach wymaga zgody sądu, o tyle szeroko zakrojone zbieranie i przetwarzanie metadanych czy analizowanie ruchu w sieci – już nie. W dodatku działania służb w tym obszarze mają co do zasady tajny charakter, więc nawet jeśli ktoś znajdzie się w orbicie ich zainteresowania, może nigdy się o tym nie dowiedzieć.

Ogrom informacji dostępnych w sieci to dla służb jednocześnie Eldorado i stajnia Augiasza. Z jednej strony – znaleźć można tam niemal wszystko, a z drugiej – szalenie łatwo się pogubić. Żeby trafić na coś interesującego, czasami niezbędne okazują się potężne zdolności analityczne – algorytmy, zaawansowane techniki profilowania ludzi i kojarzenia danych. Naprzeciw tym szansom i wyzwaniom wychodzi oczywiście biznes i instytucje badawcze, proponując rozwiązania techniczne, które mają ułatwić służbom życie. Spektrum dostępnych narzędzi jest szerokie. Z czego służby korzystają w praktyce?

Paradoksalnie więcej można powiedzieć o działaniu amerykańskich służb niż ich polskich odpowiedników. Wiedzę tę zawdzięczamy byłym pracownikom agencji wywiadowczych USA, którzy zdecydowali się głośno krytykować system, który wcześniej współtworzyli. Jego założeniem było zasysanie i analizowanie właściwie wszystkiego, co pojawia się w sieci. Takie działanie nie byłoby możliwe bez biznesu – nie tylko tworzącego coraz bardziej zaawansowane narzędzia, ale też przejmującego część zadań należących do służb. Pewne wyobrażenie o skali i znaczeniu tej współpracy dają liczby – amerykańskie media szacują, że w przypadku samej Narodowej Agencji Bezpieczeństwa (NSA, od ang. *National Security Agency*) w grę wchodzą kontrakty na 6 miliardów dolarów rocznie.

Zdaniem Michaela Haydena, człowieka, który nadzorował prywatyzację inwigilacyjnych zadań NSA między 1999 a 2005 r., „największa koncentracja cybermocy na naszej planecie znajduje się na rogu Baltimore Parkway i Maryland Route 32". To aluzja do lokalizacji parku biznesowego zajmowanego przez firmy świadczące usługi na rzecz amerykańskich służb. Jedną z najbardziej wpływowych jest Narus – spółka należąca do Boeinga, która dostarcza agencjom rządowym kluczowe oprogramowanie, pozwalające na monitorowanie i przechwytywanie olbrzymich ilości danych bezpośrednio ze światłowodów. Inna firma – były pracodawca Edwarda Snowdena, czołowego amerykańskiego sygnalisty (ang. *whistleblower*), który ujawnił skalę inwigilacji prowadzoną przez NSA – to Booz Allen Hamilton. Jest ona zaangażowana w zasadzie w każdy aspekt pracy wywiadowczej: od doradzania wysokiej rangi urzędnikom, przez obsługę technicznej infrastruktury, po analizę i integrację pozyskiwanych danych. Lista zleceniobiorców NSA jest o wiele dłuższa, są na niej mniej i bardziej rozpoznawalne firmy, takie jak SAIC, TRW czy Palantir Technologies.

OGROM INFORMACJI DOSTĘPNYCH W SIECI TO DLA SŁUŻB JEDNOCZEŚNIE ELDORADO I STAJNIA AUGIASZA. Z JEDNEJ STRONY – ZNALEŹĆ MOŻNA TAM NIEMAL WSZYSTKO, A Z DRUGIEJ – SZALENIE ŁATWO SIĘ POGUBIĆ.

Zdaniem krytyków taki system, oparty na powszechnej inwigilacji, nie tylko godzi w prawa człowieka i pochłania ogromne pieniądze, ale też generuje liczne błędy i jest w gruncie rzeczy nieskuteczny. William Binney, były analityk amerykańskiej NSA, matematyk specjalizujący się w sieciowej analizie danych, w następujący sposób opisuje w wywiadzie opublikowanym na łamach Gazety Wyborczej „porażkę masowej inwigilacji": „Gromadzenie terabajtów przypadkowych danych sprawia, że NSA nie jest w stanie ich analizować. Codziennie gromadzi dane telekomunikacyjne – lokalizację, połączenia telefoniczne i internetowe, łącznie z treścią rozmów, SMS-ów i e-maili – około czterech miliardów ludzi. Aby to miało sens, jeden pracownik musiałby skontrolować dziennie 200 tys. osób. Przywaleni danymi funkcjonariusze zarzucili analizę kierunkową – jedyną, która może wykryć rzeczywiste zagrożenia – na rzecz prostego przeszukiwania baz danych po słowach kluczowych. To daje mnóstwo nic nieznaczących »trafień« zamiast wiedzy o istotnych powiązaniach między danymi".

Zdaniem samych sygnalistów najprostszym i najtańszym rozwiązaniem tego problemu byłoby zbieranie o wiele mniejszej ilości danych, za to w oparciu o lepsze rozpoznanie siatek przestępczych i uprzednią analizę powiązań między ludźmi komunikującymi się w globalnej sieci. Do podobnych wniosków prowadzą wyniki projektu badawczego SURVEILLE. Po zestawieniu wszystkich badanych aspektów – od oceny prawnej i etycznej po użyteczność w rozumieniu samych praktyków – najlepsze wyniki osiągnęły w ocenie badaczy „tradycyjne" techniki nadzoru.

W ujawnionych informacjach dotyczących działania amerykańskiego systemu inwigilacji można znaleźć rodzime tropy. Polska została zaklasyfikowana przez NSA do grupy 19 państw, z którymi amerykańska służba prowadzi „skupioną współpracę". To jedynie poziom niżej od „wszechstronnej współpracy" z państwami tzw. sojuszu pięciorga oczu, obejmującego poza Stanami Zjednoczonymi również Wielką Brytanię, Kanadę, Australię i Nową Zelandię. Wedle materiałów dołączonych do książki Glenna Greenwalda *Snowden. Nigdzie się nie ukryjesz* polskie służby przekazywały Amerykanom dane w ramach programów ORANGECRUSH i OAKSTAR. A serwis publikujący dokumenty pochodzące od sygnalistów

Cryptome udostępnił jakiś czas temu serię tabel finansowych NSA. Wynika z nich, że Amerykanie prowadzili w Polsce działania, w których partnerem była Agencja Wywiadu.

W 2013 r. w ramach akcji „100 pytań o inwigilację" Fundacja Panoptykon, Amnesty International Polska i Helsińska Fundacja Praw Człowieka skierowały serię wniosków o informację publiczną dotyczących polsko-amerykańskiej współpracy. Jedynie CBA odpowiedziało przecząco. Natomiast inne służby na różne sposoby próbowały wymigać się od odpowiedzi (z częścią z nich trwa walka o te informacje w sądzie).

Amerykański kompleks przemysłowo-inwigilacyjny nie pozwala na wyciąganie wniosków o polskiej rzeczywistości, ale daje pojęcie o zapotrzebowaniu i trendach, jakim niewątpliwie podlegają również nasze służby. Nic nie wskazuje jednak na to, by system przypominający amerykański mógł u nas funkcjonować. Polskie służby nie dysponują środkami porównywalnymi z amerykańskimi (roczny budżet ABW wynosi 500 mln zł), a obowiązujące prawo – przynajmniej na razie – nie pozwala na przykład na masowe zasysanie informacji objętych tajemnicą korespondencji. Jednak służbom pozostawiono dużą elastyczność, jeśli chodzi o dostęp do metadanych oraz wykorzystywane narzędzia. Ustawodawca wyszedł z założenia, że technologia się zmienia, praktyczne środki dostępne również, a więc prawo musi w tym zakresie dawać pewną swobodę.

W UJAWNIONYCH INFORMACJACH DOTYCZĄCYCH DZIAŁANIA AMERYKAŃSKIEGO SYSTEMU INWIGILACJI MOŻNA ZNALEŹĆ RODZIME TROPY. POLSKA ZOSTAŁA ZAKLASYFIKOWANA PRZEZ NSA DO GRUPY 19 PAŃSTW, Z KTÓRYMI AMERYKAŃSKA SŁUŻBA PROWADZI „SKUPIONĄ WSPÓŁPRACĘ".

Obowiązująca w służbach kultura tajności sprawia, że wiedza na temat ich działań jest bardziej niż niepełna. Nie ulega wątpliwości, że niektóre aspekty tej działalności muszą pozostać niejawne, jednak – szczególnie w przypadku narzędzi wykorzystywanych do prewencyjnego zbierania i analizowania informacji o szerokiej grupie obywateli – pewien minimalny poziom transparentności jest niezbędny.

Informacje publicznie dostępne

Informacje dostępne w Internecie to prawdziwa kopalnia wiedzy – również dla różnego rodzaju służb. Zbieranie i analiza informacji z otwartych zasobów internetowych (OSINT od ang. *open source intelligence*) to wbrew pozorom bardzo ważne narzędzie ich pracy. Bez kontrowersji towarzyszących bardziej inwazyjnym formom inwigilacji, przełamywania zabezpieczeń czy uzyskiwania nakazów sądowych mają one dostęp do wielu cennych informacji.

Jak wiele można wyczytać o drugim człowieku z sieci, wie każdy, kto – choćby z ciekawości – analizował profil innej osoby na portalu społecznościowym. Służby są w stanie wyciągnąć z tego jeszcze więcej. Mogą one bowiem wykorzystywać publicznie dostępne zasoby nie tylko do wyłuskiwania informacji o zainteresowaniach czy działaniach poszczególnych osób, ale także o powiązaniach między nimi, zjawiskach, trendach itp. Te możliwości są wykorzystywane choćby do prowadzenia białego wywiadu (na przykład dotyczącego zagrożeń energetycznych), przeciwdziałania „ustawkom" kibiców czy innym niebezpiecznym działaniom, ścigania mowy nienawiści czy naruszeń praw autorskich.

Nie są to jednak działania tak proste, jak mogłoby się wydawać na pierwszy rzut oka. Tak jak każdy z nas może utonąć w morzu informacji dostępnych w Internecie, tak samo toną w nich służby. Dlatego zaczynają sięgać po mniej lub bardziej wyrafinowane algorytmy, sztuczną inteligencję, techniki profilowania ludzi i kojarzenia danych. Rynek narzędzi OSINT, które pomagają poruszać się w tym gąszczu informacji, jest

bardzo bogaty. Dostępne rozwiązania (na przykład Prompt Cloud, Palantir Metropolis) z jednej strony pozwalają automatycznie przeszukiwać dostępne treści (strony internetowe, fora, blogi, portale społecznościowe), a z drugiej – analizować dostępne dane.

Analiza *open source* obejmuje:

- przeszukiwanie dostępnych treści pod kątem zdefiniowanych kryteriów, na przykład słów kluczowych;
- wyłapywanie powiązań między faktami, analizę trendów;
- mapowanie relacji i interakcji między ludźmi, analiza wzorców komunikacji w konkretnych grupach;
- analizę treści stron, nastroju i stylu piszącego;
- wizualizację danych.

Dostępne jest również oprogramowanie (na przykład Baseprotect, Logistep) wyspecjalizowane w monitorowaniu ruchu w sieciach P2P (ang. *peer-to-peer*) pod kątem możliwych naruszeń praw autorskich. Wykorzystuje ono otwarty dostęp do takich sieci i techniczną możliwość analizowania, jakie pliki są aktualnie przesyłane oraz przez kogo. Nie wymaga ona przełamywania jakichkolwiek zabezpieczeń, nie jest się jednak w stanie obejść bez rozbudowanej infrastruktury.

Wiele rozwiązań jest powszechnie dostępnych i korzystają z nich nie tylko służby, ale również podmioty prywatne. Jednak instytucje, które swoje działanie opierają na systemach masowej inwigilacji, inwestują w oprogramowanie „krojone na miarę". Na przykład, zgodnie z informacjami ujawnionymi przez Edwarda Snowdena, amerykańska NSA korzysta m.in. z aplikacji MARINA, która pozwala tworzyć indywidualne profile internautów, a brytyjska GCHQ – z systemu SQUEAKY DOLPHIN pomagającego analizować w czasie rzeczywistym posty publikowane na najpopularniejszych platformach internetowych, na przykład na Facebooku.

SŁUŻBY MOGĄ WYKORZYSTYWAĆ PUBLICZNIE DOSTĘPNE ZASOBY NIE TYLKO DO WYŁUSKIWANIA INFORMACJI O ZAINTERESOWANIACH CZY DZIAŁANIACH POSZCZEGÓLNYCH OSÓB, ALE TAKŻE O POWIĄZANIACH MIĘDZY NIMI, ZJAWISKACH, TRENDACH ITP.

A jak to wygląda w Polsce? Policja przyjmuje, że może zbierać i analizować zasoby powszechnie dostępne w Internecie w ramach czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych bez zgody sądu. Nie jest przy tym w pełni jasne, jaki standard ochrony praw obywateli i kontroli nad działaniami służb obowiązuje w tym przypadku.

Z informacji publikowanych przez Polską Platformę Bezpieczeństwa Wewnętrznego wynika, że polska policja dysponuje na przykład pakietem narzędzi informatycznych wspomagających poszukiwanie nielegalnych materiałów wysyłanych w trybie P2P oraz systemem IBIS służącym do monitorowania publicznie dostępnych usług internetowych. Z odpowiedzi na wnioski o informację publiczną wynika, że Służba Celna korzysta z serii narzędzi służących do monitoringu i analizy takich treści (EMM Osint Suite, WebSite-Watcher, Paterva Maltego).

Co ciekawe, do tej pory największe kontrowersje wzbudziły w Polsce wcale nie narzędzia faktycznie wykorzystywane, a program badawczy. Projekt INDECT (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*) był realizowany przez konsorcjum polskich i zagranicznych uczelni i instytucji, w tym Komendę Główną Policji, formalnie reprezentowaną przez Ministerstwo Spraw Wewnętrznych. Służby o swoich narzędziach wolą milczeć, tymczasem stojąca na czele projektu krakowska Akademia Górniczo-Hutnicza aktywnie promowała projekt i ideę tworzenia narzędzi rozpoznających „podejrzane zachowania", również w sieci. Wywołało to niepokój części opinii publicznej i poważny kryzys komunikacyjny. Ministerstwo

Spraw Wewnętrznych poinformowało nawet o „zawieszeniu udziału w projekcie INDECT ze względu na konieczność poszanowania prawa obywateli do prywatności". Jednocześnie nigdy formalnie nie wycofało się z projektu, stawiając na przeczekanie burzy. A ta z czasem ucichła.

Oczywiście inicjatyw badawczych mających podobne ambicje jest w Polsce i na świecie wiele. Warto wspomnieć choćby o projekcie realizowanym przez Narodowe Centrum Badań i Rozwoju, w ramach którego tworzone jest narzędzie służące do integracji i analizy danych dostępnych powszechnie w sieci pod kątem wyłapywania informacji o zagrożeniach w cyberprzestrzeni.

— Metadane, czyli tropem cyfrowych śladów —

Ślady pozostawiane w sieci nie ograniczają się do tego, co mniej lub bardziej intencjonalnie każdy z nas opublikuje (teksty, zdjęcia, filmy, statusy, polubienia itp.), lecz obejmują także informacje tworzone mimowolnie, niejako przy okazji aktywności w sieci. Każde kliknięcie zostawia po sobie ślad, który niemal zawsze można powiązać z konkretnym użytkownikiem (choćby dzięki opisywanym wyżej ciasteczkom). Wszystko to wygląda niepozornie, jednak na podstawie historii aktywności w danym serwisie czy interakcji z innymi można stworzyć całkiem dokładny profil konkretnej osoby. Administratorzy stron internetowych i reklamodawcy tworzą je najczęściej po to, żeby lepiej dopasować usługę do odbiorcy czy podsunąć mu „skrojoną na miarę" reklamę, ale jednocześnie stanowią one atrakcyjny informacyjny kąsek dla państwa i jego służb.

NAUKOWCY Z MASSACHUSETTS INSTITUTE OF TECHNOLOGY USTALILI, ŻE NA PODSTAWIE DANYCH TELEKOMUNIKACYJNYCH TYLKO Z JEDNEGO MIESIĄCA MOŻNA ODTWORZYĆ SIEĆ KONTAKTÓW I W 90% PRZYPADKÓW USTALIĆ TOŻSAMOŚĆ OSÓB NALEŻĄCYCH DO TEJ SIECI.

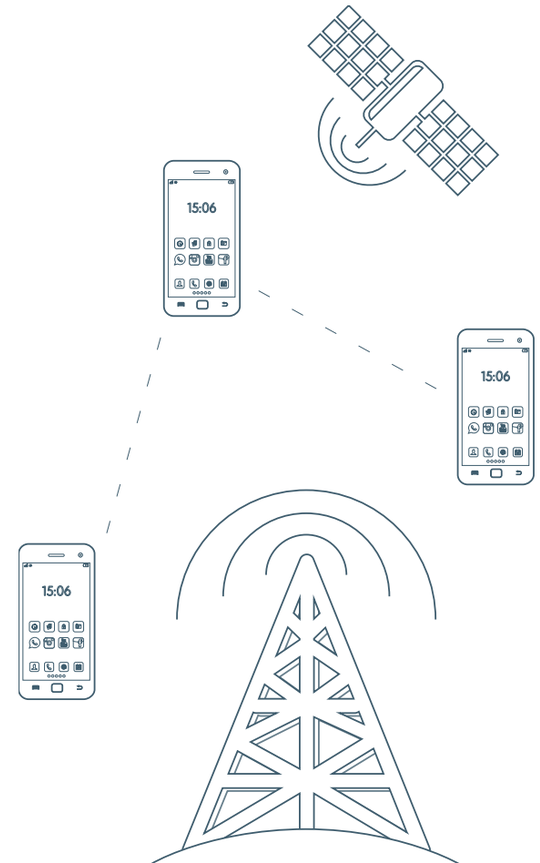
Kolejnych szczegółowych informacji o codziennym życiu dostarcza telefon komórkowy. Nawet jeśli nie jest wykorzystywany do korzystania z Internetu, pozwala on gromadzić informacje o wszystkich nawiązywanych i odbieranych połączeniach czy komunikacji esemesowej oraz jest nadajnikiem, który na bieżąco komunikuje się ze stacjami BTS, informując operatora o lokalizacji swojego właściciela. Naukowcy z Massachusetts Institute of Technology ustalili, że na podstawie danych telekomunikacyjnych tylko z jednego miesiąca można odtworzyć sieć kontaktów i w 90% przypadków ustalić tożsamość osób należących do tej sieci. Co więcej – aż w 95% przypadków na podstawie danych telekomunikacyjnych można przewidzieć, gdzie dana osoba znajdzie się w ciągu kolejnych 12 godzin. Dlatego świetnie nadają się one do analizowania tras poruszania się czy ustalenia sieci kontaktów – zarówno za pomocą telefonu, jak i twarzą w twarz (dzięki geolokalizacji). A stąd już tylko krok od ustalenia charakteru danej relacji.

Dane telekomunikacyjne miały stać się jednym z głównych oręży w walce z terroryzmem. Na fali strachu wywołanego zamachami w Madrycie i Londynie dyrektywą z 2006 r. wprowadzono w Unii Europejskiej obowiązek przechowywania tych danych przez operatorów i udostępniania ich na żądanie służb i innych publicznych instytucji. Polskie władze początkowo zdecydowały się na maksymalny, 2-letni okres zatrzymywania danych. Dopiero w styczniu 2013 r., na skutek społecznej krytyki, został on skrócony do 12 miesięcy.

W teorii dane telekomunikacyjne miały być wykorzystywane przede wszystkim do walki z najpoważniejszą przestępczością: terroryzmem czy handlem ludźmi. W Polsce jednak umożliwiono sięganie po nie m.in. policji i kilku innym służbom również w najdrobniejszych sprawach, a nawet prewencyjnie. I to bez żadnej zewnętrznej kontroli. Choć w 2014 r. Trybunał Sprawiedliwości Unii Europejskiej orzekł, że dyrektywa retencyjna jest nieważna, a polski Trybunał Konstytucyjny zakwestionował zasady dostępu do tych danych, niewiele się od tej pory zmieniło. Nowe przepisy obowiązujące od lutego 2016 r. (wprowadzone tzw. ustawą inwigilacyjną) przewidują jedynie pozorny mechanizm kontrolny: służby co pół roku mają składać do sądu specjalne sprawozdanie.

W Polsce źródłem metadanych telekomunikacyjnych są w tym momencie przede wszystkim bazy danych czterech największych operatorów telekomunikacyjnych. Służby nie muszą ich jednak prosić o udostępnianie danych – same mogą po nie sięgać za pomocą stałych łączy i specjalnych interfejsów, które zostały wprowadzone na koszt operatorów. Oni też płacą (a ostatecznie ich klienci) za cały proces udostępniania danych telekomunikacyjnych.

W TEORII DANE TELEKOMUNIKACYJNE MIAŁY BYĆ WYKORZYSTYWANE PRZEDE WSZYSTKIM DO WALKI Z NAJPOWAŻNIEJSZĄ PRZESTĘPCZOŚCIĄ. W POLSCE JEDNAK UMOŻLIWIONO SIĘGANIE PO NIE RÓWNIEŻ W NAJDROBNIEJSZYCH SPRAWACH, A NAWET PREWENCYJNIE.



Stałe łącza oraz brak konsekwencji finansowych i realnej kontroli przekładają się na skalę korzystania przez służby z tych danych. Dane przekazane przez operatorów do Urzędu Komunikacji Elektronicznej mówią o niespełna 2,4 mln pobrań w 2014 r., natomiast w odpowiedzi na pytania Fundacji Panoptykon sama tylko policja zadeklarowała, że sięgała po nie w tym czasie ponad 1,6 mln razy (i – nieco rzadziej – około 1,2 mln razy w 2015 r.). Dane te są niespójne i nie do końca wiarygodne, brakuje bowiem jednolitej metodologii liczenia zapytań. Jedno jest pewne: dane płyną z telekomów do służb szerokim strumieniem.

Policja tłumaczy, że skala zapytań wynika m.in. z metod, jakie standardowo się stosuje w pracy operacyjnej czy analizie danych. Każda nowa informacja o danym numerze telefonu to kolejne zapytanie, często kierowane osobno do każdego z operatorów. Namierzanie jednej bądź kilku podejrzanych osób odbywa się nieraz dzięki pobraniu i analizie informacji dotyczących wszystkich numerów, które w danym momencie łączyły się z konkretnymi stacjami BTS. W tym gąszczu informacji funkcjonariusze starają się znaleźć jakieś istotne tropy – w ich wyławianiu znowu mają pomagać narzędzia służące do analizy danych. Podobnie jak w przypadku opracowywania informacji z publicznie dostępnych źródeł część z nich to programy do analizy statystycznej wykorzystywane do wielu innych celów, inne są dedykowane działaniom analitycznym służb. W tym drugim przypadku mowa na przykład o środowisku LINK/MAMUT (opracowanym przez Polską Platformę Bezpieczeństwa Wewnętrznego) czy LINK2 (efekcie pracy naukowców z Akademii Górniczo-Hutniczej). Zgodnie z medialnymi doniesieniami policja korzysta również z Analizatora Faktów i Związków (oprogramowania stworzonego na Politechnice Poznańskiej).

Policja i inne służby mają też dostęp do danych przetwarzanych przez dostawców usług internetowych, czyli na przykład administratorów portali informacyjnych, społecznościowych czy sklepów internetowych. Przez lata sięganie po nie odbywało się na zupełnie innych zasadach niż w przypadku danych telekomunikacyjnych. Nie było mowy o bezpośrednim dostępie do tych informacji. Obowiązujące prawo budziło wprawdzie wątpliwości interpretacyjne, jasne było jednak, że aby uzyskać dostęp do danych użytkowników usług internetowych, służby muszą do firmy świadczącej takie usługi zwrócić się z wnioskiem lub postanowieniem wskazującym podstawę prawną. Firmy rozpatrywały je według wewnętrznych procedur, zdarzało się, że kwestionowały żądania i odmawiały udostępniania danych.

Taki stan rzeczy znajdował odbicie w skali sięgania po dane internetowe. Choć dostępne informacje na ten temat są jeszcze bardziej dziurawe niż w przypadku danych telekomunikacyjnych, nie ma wątpliwości, że dane internetowe były udostępniane o wiele rzadziej. Policja w 2014 r. sięgała po nie około 50 tys. razy, ale w 2015 r. – już ponad 200 tys. razy. Dynamika wzrostu zwraca uwagę, choć w porównaniu z liczbą pobrań danych telekomunikacyjnych (sięgającą odpowiednio 1,6 i 1,2 miliona) liczby bezwzględne nie robią już takiego wrażenia.

W 2016 r. sytuacja może wyglądać już zgoła inaczej. Tzw. ustawa inwigilacyjna, która weszła w życie w lutym, ułatwiła służbom dostęp do danych internetowych. Teraz – podobnie jak dane telekomunikacyjne – mogą one być pobierane również poza konkretnym postępowaniem oraz za pomocą stałego łącza i dedykowanego interfejsu. W połączeniu z brakiem realnych mechanizmów kontroli może to sprawić, że dane internetowe popłyną do służb równie szerokim strumieniem, jak dane telekomunikacyjne. Tym samym pojawi się okazja do korzystania z narzędzi analitycznych na szerszą skalę oraz wdrażania nowych rozwiązań.

TZW. USTAWA INWIGILACYJNA UŁATWIŁA SŁUŻBOM DOSTĘP DO DANYCH INTERNETOWYCH. W POŁĄCZENIU Z BRAKIEM REALNYCH MECHANIZMÓW KONTROLI MOŻE TO SPRAWIĆ, ŻE DANE TE POPŁYNĄ DO SŁUŻB RÓWNIE SZEROKIM STRUMIENIEM, JAK DANE TELEKOMUNIKACYJNE.

Policja i inne służby mogą również przechwytywać dane bezpośrednio z Internetu i analizować je. W przypadku metadanych polega to przede wszystkim na bieżącym monitoringu sieci w celu wyłapania konkretnych korzystających z niej adresów IP. Na rynku dostępna jest długa lista narzędzi, które można wykorzystać do tego celu – zarówno rozwiązań komercyjnych (IPCopper, FireEye), jak i wolnego oprogramowania (Wireshark). Takie działania są rutynowo prowadzone przez operatorów w ramach dbania o bezpieczeństwo sieci, zapobiegania cyberatakom, blokowania spamu czy szeroko pojętego zarządzania ruchem. Obowiązuje ich jednak zakaz zaglądania do wnętrza pakietów, czyli monitoringu treści.

Komunikacja i prywatne treści

Interesująca dla służb może być oczywiście również treść komunikacji (SMS-y, e-maile, wiadomości na portalach społecznościowych czy czatach) oraz rozmaite materiały (filmy, zdjęcia, dokumenty), powszechnie zapisywane nie tylko na komputerach czy telefonach, ale też w chmurze (nie zawsze ze świadomością, że trafiają na serwery na drugim końcu świata). Zazwyczaj jednak te informacje są lepiej chronione niż metadane dotyczące aktywności w sieci. Jeśli na przykład policja miałaby uzyskać do nich dostęp bez wiedzy użytkownika, powinno się to odbyć w ramach kontroli operacyjnej, czyli tak jak w przypadku zakładania podsłuchu – za zgodą sądu.

Nie udało się namierzyć żadnych komercyjnych produktów, które umożliwiałyby bezpośredni dostęp do danych przechowywanych na

wirtualnych serwerach, czyli w chmurze. Dostęp ten jest jednak możliwy, z jednej strony dzięki narzędziom stworzonym na zlecenie samych służb (w przypadku amerykańskiej NSA wypracowywanych na przykład przez firmę Booz Allen Hamilton), a z drugiej – dzięki współpracy komercyjnych podmiotów, które sprawują nad nimi kontrolę. Na dostępie do danych gromadzonych na serwerach amerykańskich informatycznych potentatów (Google'a, Yahoo, Microsoftu czy Apple) opierał się jeden z filarów amerykańskiego programu masowej inwigilacji, czyli PRISM.

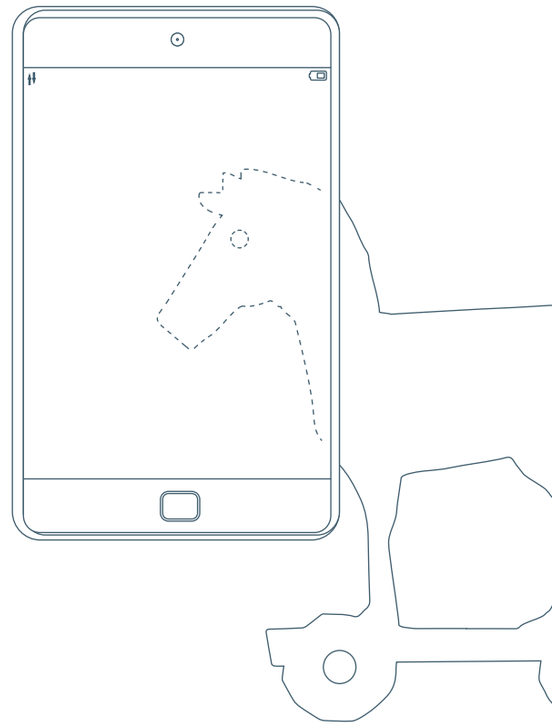
W 2012 R. CBA ZA 178 TYS. EURO KUPIŁO OD WŁOSKIEJ FIRMY HACKING TEAM LICENCJĘ NA OPROGRAMOWANIE REMOTE CONTROL SYSTEM – PLATFORMĘ SŁUŻĄCA DO INFEKOWANIA, A NASTĘPNIE ZDALNEGO I UKRYTEGO KONTROLOWANIA SPRZĘTU ELEKTRONICZNEGO.

Dostępne na rynku jest natomiast oprogramowanie umożliwiające zdalne infekowanie sprzętu – tzw. konie trojańskie. Ani policja, ani inne polskie służby nie chcą udzielać informacji na temat korzystania z tego rodzaju narzędzi. Nowe światło na sprawę rzucił natomiast wyciek danych, z którego wynikało, że w 2012 r. CBA za 178 tys. euro kupiło od włoskiej firmy Hacking Team licencję na oprogramowanie Remote Control System, a w kolejnych latach płaciło ponad 35 tys. euro rocznie za wsparcie techniczne.

Remote Control System to platforma służąca do infekowania, a następnie zdalnego i ukrytego kontrolowania urządzeń takich jakich komputery i telefony komórkowe. Po przejęciu kontroli nad wybranym urządzeniem pozwala utrwalać wszystkie czynności jego użytkownika: oglądać odwiedzane przez niego strony, czytać przesyłaną pocztę, słuchać rozmów wykonywanych przez Skype'a, a nawet przechwytywać wpisywane hasła. Przeprowadzona przez społeczność hakerską analiza kodu Remote Control System daje podstawy, by sądzić, że to narzędzie umożliwiało również modyfikowanie treści na zainfekowanych urządzeniach, co może być – przynajmniej w teorii – wykorzystywane na przykład do podrzucania fałszywych dowodów.

Zakres możliwości technicznych, jakie stwarzała licencja wykupiona przez CBA, nie jest jasny. Wiadomo tylko, że pozwalała na zainfekowanie do 10 komputerów, bez możliwości zarażania urządzeń mobilnych. Zagadką pozostaje również, czy i w jaki sposób była wykorzystywana w praktyce.

Zdaniem krytyków stosowanie takich narzędzi jak konie trojańskie uderza w podstawy bezpieczeństwa w sieci i jako takie powinno być zakazane bez względu na okoliczności. Obecnie jednak ich wykorzystywanie jest na gruncie polskiego prawa dopuszczalne. Przepisy nie precyzują bowiem, z jakich konkretnie narzędzi służby mogą korzystać, sięgając po informacje dotyczące obywateli. To jeden z problemów, na które kilka lat temu w swoim wniosku do Trybu-



nału Konstytucyjnego zwróciła uwagę ówczesna Rzecznik Praw Obywatelskich Irena Lipowicz. Sędziowie uznali jednak, że na poziomie przepisów nie ma potrzeby doprecyzowania uprawnień służb tak długo, jak sądy – wyrażając zgodę na kontrolę operacyjną – jasno wyznaczają jej granice, wskazując rodzaj środka technicznego, jaki może być wykorzystany do pozyskania informacji.

Większe wątpliwości interpretacyjne wiążą się z użyciem narzędzi, które pozwalają na dostęp do treści komunikacji i przesyłanych w sieci informacji, ale nie są wymierzone w konkretne osoby. Rodzaj monitoringu sieci, który umożliwia analizę przesyłanych treści, nazywa się „głęboką inspekcją pakietów" (DPI, od ang. *Deep Packet Inspection*). Technika ta umożliwia służbom kontrolę treści na przykład pod kątem naruszeń praw autorskich lub namierzanie materiałów dotyczących seksualnego wykorzystywania dzieci. Z nieoficjalnych rozmów z funkcjonariuszami policji wynika, że aż do momentu namierzenia konkretnej osoby i przechwytywania jej korespondencji nie traktują oni zbierania ani analizy danych z Internetu jako kontroli operacyjnej i korzystają z tych możliwości bez zgody sądu. Nie udało się jednak potwierdzić tych informacji w drodze oficjalnej korespondencji skierowanej do służb.

SŁUŻBY W DUŻEJ MIERZE WYŁĄCZONE SĄ Z KONTROLI SPRAWOWANEJ PRZEZ GIODO, A ZGODA SĄDU WYMAGANA JEST TYLKO W PRZYPADKU NIEKTÓRYCH DZIAŁAŃ, UWAŻANYCH ZA NAJGŁĘBIEJ INGERUJĄCE W PRYWATNOŚĆ.

Podstawowe techniczne wyzwanie, z którym mierzą się służby chcące na bieżąco monitorować sieć, to „problem prędkości" – dostępne rozwiązania nie są w stanie rejestrować ani analizować danych tak szybko, jak są one przesyłane w Internecie. Dlatego rejestracja i analiza ruchu wymaga bardzo rozbudowanej infrastruktury albo przechwytywania tylko wyselekcjonowanych treści. Z perspektywy służb najprostszym rozwiązaniem jest „wpięcie" się w sieć operatora i zainstalowanie tam odpowiedniego oprogramowania. Żeby masowo przechwytywać lub analizować dane bez współpracy operatora, niezbędne byłoby kopiowanie ruchu sieciowego i przekierowywanie go do odpowiednich urządzeń.

Zgodnie z informacjami ujawnionymi przez sygnalistów takie działania prowadzi na przykład amerykańska NSA. Z nieformalnych rozmów z funkcjonariuszami wynika natomiast, że w Polsce analogiczne praktyki mogą być prowadzone przy współpracy z operatorami. Być może zmieni się to jednak po przyjęciu nowej strategii cyberbezpieczeństwa RP, której założenia przewidują szersze możliwości śledzenia ruchu w Internecie poprzez stworzenie systemu monitorowania w punktach wymiany ruchu internetowego.

Obok narzędzi wykorzystywanych do działań niejawnych służby korzystają z takich, które pomagają im w pracy na dalszym etapie postępowania – gdy w ich ręce trafia sprzęt należący do osób podejrzanych o popełnienie przestępstwa, posługują się narzędziami informatyki śledczej. Chodzi przede wszystkim o oprogramowanie, które pozwala uzyskać dostęp do zabezpieczonych laptopów, dysków zewnętrznych, tabletów i smartfonów, a także pozwala odzyskać skasowane dane. Zgodnie z informacjami medialnymi policja korzysta na przykład z oprogramowania XRY Office, a Żandarmeria Wojskowa w trybie przetargu nabyła EnCase Forensic.

Narzędzia poza kontrolą

Z zebranych informacji wynika, że w codziennej pracy służb wykorzystywane są różnorodne narzędzia – zarówno takie stworzone z myślą o służbach, jak i powszechnie dostępne programy służące na przykład analizie statystycznej. Przy czym nierzadko to samo narzędzie może realizować różne cele – od zbierania informacji, poprzez ich analizę, po odzyskiwanie z pamięci urządzeń i zabezpieczanie. Duża różnorodność dostępnych rozwiązań – od bardzo prostych po skomplikowane – znajduje odbicie w cenach komercyjnych produktów. Można wśród nich znaleźć programy, na które służby przeznaczyły niemal kieszonkowe kwoty (na przykład kilkaset złotych), i takie, które kosztowały miliony.

Osobną kategorią są narzędzia o niekomercyjnym charakterze, rozwijane w ramach projektów badawczych. Zwykle są one koordynowane lub wspierane przez Polską Platformę Bezpieczeństwa Wewnętrznego. Innym istotnym podmiotem jest Akademia Górniczo-Hutnicza, szczególnie Laboratorium Informatyki Śledczej i Intelligent Information Systems Group. Podmioty te chwalą się, że przekazują polskim służbom wypracowane przez siebie narzędzia. Nie potwierdziły tego jednak same służby w odpowiedziach na wnioski o informację publiczną.

JEŚLI SŁUŻBY PRZYGLĄDAŁY SIĘ CZYJEJŚ AKTYWNOŚCI W SIECI, ALE NIE TRAFIŁY NA NIC, CO WSKAZYWAŁOBY, ŻE TA OSOBA POPEŁNIŁA PRZESTĘPSTWO, PRAWDOPODOBNIE NIGDY SIĘ ONA O TYM NIE DOWIE.

Niektórzy twierdzą, że wśród wykorzystywanych przez policję i inne służby narzędzi można znaleźć takie, którymi w ogóle nie powinny się one posługiwać (mowa na przykład o opisanych wyżej koniach trojańskich, które pozwalają zdalnie przejąć kontrolę nad sprzętem komputerowym). W większości przypadków jednak to, czy korzystanie z danego narzędzia jest na miejscu, zależy od sytuacji. Tak jak założenie podsłuchu może być uzasadnione w przypadku podejrzanego o poważne przestępstwo, a niedopuszczalne prewencyjnie, tak pobranie danych o lokalizacji 1000 osób czy analiza całej komunikacji danej osoby na portalu społecznościowym w jednej sytuacji da się zaakceptować, a w innej nie.

Problem polega na tym, że polskie prawo nie nakreśla jasnych ram dla weryfikacji zasadności takich decyzji. Służby w dużej mierze wyłączone są z kontroli sprawowanej przez GIODO, a zgoda sądu wymagana jest tylko w przypadku niektórych działań, uważanych za najgłębiej ingerujące w prywatność. Służby twierdzą, że wystarczające są wewnętrzne mechanizmy kontroli. W CBA takim wewnętrznym hamulcem ma być specjalny pełnomocnik ds. ochrony danych (ustanowiony w odpowiedzi na wyrok Trybunału Konstytucyjnego). Policja podkreśla natomiast, że żaden funkcjonariusz nie może samodzielnie sięgnąć po dane telekomunikacyjne – potrzebuje do tego zgody przełożonego (która może jednak przyjąć formę stałego upoważnienia). Trudno uwierzyć, by te mechanizmy mogły w pełni zastąpić zewnętrzną i niezależną kontrolę.

Na ewentualne nadużycia trudno też reagować obywatelom. Powód jest prosty. O ingerencji służb w prywatność można dowiedzieć się właściwie tylko wówczas, gdy policji uda się potwierdzić związek z jakimś przestępstwem na tyle, że dojdzie do etapu procesowego i o udostępnienie danych wystąpi prokurator. Wówczas postanowienie o sięgnięciu po dane osobowe jest doręczane osobie, której dotyczy. Doręczenie może być odroczone do czasu zakończenia postępowania, jeśli jest to niezbędne ze względu na dobro sprawy. Jednak sam obowiązek poinformowania o tym nie znika. Co więcej – osobie, której postanowienie dotyczy, przysługuje prawo do zażalenia, które rozpoznaje sąd.

Analogicznych bezpieczników nie ma na etapie czynności operacyjnych, które z definicji są tajne. Zatem jeśli służby przyglądały się czyjejś aktywności w sieci, ale nie trafiły na nic, co wskazywałoby, że ta osoba popełniła przestępstwo, prawdopodobnie nigdy się ona o tym nie dowie.

PROBLEMY

PODSUMOWANIE

1. PUNKT WYJŚCIA – USTAWA

Zgodnie z Konstytucją RP organy władzy publicznej działają na podstawie i w granicach prawa (art. 7), a ograniczenia praw i wolności powinny być wprowadzane w drodze ustawy (art. 31 ust. 3). Oznacza to, że korzystanie przez państwo z narzędzi nadzoru, które ingerują w prywatność obywateli, powinno się odbywać jedynie na podstawie aktu prawnego tej rangi. Praktyka odbiega jednak od tego konstytucyjnego ideału. Jednym z najbardziej jaskrawych przykładów jest korzystanie z monitoringu wizyjnego przez różne instytucje, które nie mają do tego właściwej podstawy prawnej. W 2010 r. ówczesny Rzecznik Praw Obywatelskich Janusz Kochanowski zwrócił uwagę, że instalowanie kamer monitoringu w szkołach jest w gruncie rzeczy nielegalne. Problem do tej pory nie został rozwiązany, mimo że wielokrotnie zwracały na niego uwagę instytucje i organizacje społeczne. A dotyczy on nie tylko szkolnych systemów, ale również wielu innych zastosowań monitoringu.

Problem braku odpowiedniej podstawy prawnej może być związany z precyzją ustawy – zdarza się, że stawia ona przed daną instytucją określone cele i przyznaje pewne uprawnienia, ale robi to w sposób na tyle ogólny, że nie jest jasne, czy wpisuje się w to korzystanie z danego narzędzia. Oczywiście, trudno oczekiwać, by tworzący prawo za każdym razem szczegółowo wskazywali rozwiązania, z których dana instytucja może korzystać w ramach realizacji jakiegoś zadania. Dostępne narzędzia zmieniają się zbyt szybko. Można jednak oczekiwać chociaż rodzajowego wskazania dopuszczalnych środków i metod działania.

2. TEST PROPORCJONALNOŚCI

Z Konstytucji (art. 31 ust. 3) wynika, że wszelkie ograniczenia praw człowieka, w tym prawa do prywatności, są dopuszczalne tylko wtedy, gdy przejdą tzw. test proporcjonalności. Jego istotą jest analiza, jak bardzo konkretne rozwiązanie ingeruje w prawa i wolności, czy istotnie przyczynia się do ochrony innej wartości (na przykład bezpieczeństwa publicznego) oraz czy tego samego celu nie można osiągnąć w mniej ingerujący w sferę praw i wolności sposób.

Niestety, w procesie tworzenia prawa takie spojrzenie jest często nieobecne i ewentualnie pojawia się dopiero na etapie badania zakwestionowanej regulacji przed Trybunałem Konstytucyjnym.

Podstawowe wyzwanie związane z zastosowaniem testu proporcjonalności w praktyce polega na tym, że o jego wyniku nie przesądza zazwyczaj sama charakterystyka narzędzia, które jest oceniane, ale sposób i kontekst jego wykorzystania. Można wskazać przypadki, w których używanie narzędzi nawet głęboko ingerujących w prywatność ma swoje uzasadnienie. Niestety, ich wykorzystanie na jednym polu rodzi pokusę przenoszenia na kolejne. W konsekwencji na przykład używanie technologii biometrycznej czy rejestrowanie dźwięku staje się coraz powszechniejsze, choć często jest zupełnie zbędne.

3. ZASADY DZIAŁANIA

Dobre prawo powinno nie tylko dawać podstawę do oceny, czy korzystanie z danych narzędzi jest dopuszczalne, ale też wskazywać, w jaki sposób powinny być one wykorzystywane. Oczywiście, trudno oczekiwać, że przepisy będą szczegółowo opisywać właściwy sposób wykorzystania każdego technicznego rozwiązania. W niektórych przypadkach po prostu nie jest to potrzebne – wystarczające powinno być stosowanie na przykład ogólnych zasad ochrony danych osobowych. Jednak im głębiej konkretne działanie ingeruje w prywatność, tym silniejsza staje się potrzeba precyzyjnego określenia dopuszczalnego sposobu jego wykorzystania w przepisach. Niestety, prawo nie zawsze staje na wysokości zadania. W jaki sposób może się to odbić na praktyce wykorzystania narzędzi, obrazują rozbieżności w sposobie działania miejskich systemów monitoringu.

4. KONTROLOWAĆ KONTROLUJĄCYCH

A co, jeśli praktyka odbiega od prawnych standardów? Problem z brakiem dostatecznej kontroli nad korzystaniem z narzędzi nadzoru dobitnie obrazuje przykład policji i innych służb. Uprawnienia kontrolne GIODO są w tym przypadku ograniczone. A sądy weryfikują legalność i niezbędność podejmowanych przez nie działań tylko w wybranych przypadkach. Sięganie po dane telekomunikacyjne i internetowe odbywa się poza zewnętrzną kontrolą, a rola sądu jest w tym przypadku ograniczona do dostępu do statystyk.

Niestety, problem nie ogranicza się do tej sfery. W wielu dziedzinach funkcjonowania administracji publicznej brakuje sprawnych mechanizmów weryfikacji, czy sięgnięcie po dane narzędzie jest uzasadnione – zarówno na poziomie podejmowania decyzji o nabyciu konkretnego urządzenia czy oprogramowania, jak i o zastosowaniu go w konkretnej sytuacji. W pierwszym przypadku, jeśli mamy do czynienia z kontrolą, to odbywa się to raczej post factum i dotyczy w większym stopniu na przykład gospodarności niż wpływu na prawa człowieka, w drugim – wiele zależy od możliwości i determinacji osoby, która została poddana kontroli.

5. PRAWO DO INFORMACJI

Zgodnie z Konstytucją (art. 61 ust. 1) każdy obywatel ma prawo do uzyskania informacji o działalności organu administracji publicznej. Znajduje to odzwierciedlenie w konkretnych uprawnieniach wynikających z ustawy o dostępie do informacji publicznej. To z nich korzysta Fundacja Panoptykon, kiedy zwraca się do rozmaitych instytucji z wnioskami o informację na temat ich działania i wykorzystywanych narzędzi nadzoru. Prawo do informacji ograniczane jest zarówno przez inne regulacje prawne (na przykład ochronę informacji niejawnych), jak i codzienną praktykę niektórych instytucji (brak odpowiednich standardów przejrzystości, kulturę tajności). Mimo to jest to ogromnie ważne narzędzie w rękach społeczeństwa – kluczowe w przełamywaniu dysproporcji informacyjnej między państwem, które wie o obywatelach bardzo wiele, a obywatelami, którzy niekiedy nie dysponują podstawowymi informacjami na temat działania państwa.

Poza abstrakcyjnym prawem do informacji Konstytucja (art. 51 ust. 3), a za nią ustawa o ochronie danych osobowych, przyznaje każdemu prawo do informacji m.in. o tym, jakie dane, przez kogo czy w jakim celu są wykorzystywane. To absolutnie podstawowe uprawnienie, którego realizacja jest warunkiem skorzystania z innych swoich praw. W praktyce jego realizacja pozostawia jednak wiele do życzenia – wiele osób nie ma pojęcia, jakie narzędzia są na co dzień wykorzystywane do zbierania przez państwo informacji na ich temat ani w jaki sposób ta wiedza jest wykorzystywana.

6. WALKA O SWOJE PRAWA

Teoretycznie obywatel, który chce wpłynąć na praktykę działania instytucji lub dochodzić swoich praw naruszonych przez ich ingerencję w swoją prywatność, ma do wyboru wiele różnych dróg. W zależności od sytuacji może zdecydować się złożyć skargę do GIODO lub Państwowej Inspekcji Pracy, może wystąpić z pozwem cywilnym i zażądać odszkodowania lub zadośćuczynienia, a w najpoważniejszych przypadkach złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa. Może również zaalarmować organ nadzoru (na przykład wojewodę sprawującego nadzór nad organami samorządu terytorialnego), Rzecznika Praw Obywatelskich czy Najwyższą Izbę Kontroli.

W praktyce pojawia się jednak wiele ograniczeń. Wyzwaniem są nie tylko ewentualne wydatki i fakt, że skorzystanie z tych procedur może zająć lata – już zmierzenie się z nimi wymaga nie lada determinacji. Najbardziej podstawowy, choć prozaiczny, problem polega na tym, że bez wiedzy o naruszeniach trudno sobie wyobrazić podjęcie jakichkolwiek działań.

7. SPRAWDZIĆ, JAK TO DZIAŁA

W praktyce korzystanie z różnych narzędzi nadzoru wymyka się zarówno ramom prawnym, jak i zdrowemu rozsądkowi. Często korzystanie z kolejnych możliwości, jakie stwarza rozwój nowych technologii, odbywa się zupełnie bezrefleksyjnie. Tymczasem dobrą praktyką jest poświęcenie na wstępie czasu na jasne wyznaczenie celów, jakim dane narzędzie ma służyć, na zastanowienie się, czy nie można ich zrealizować w inny sposób, oraz nad przewidywanymi skutkami wdrożenia danego rozwiązania. Równie ważne jest, by po określonym czasie wykorzystywania narzędzia dokonać jego ewaluacji – i to nie tylko pod kątem skuteczności (oceny, czy pozwala ono na realizację założonych celów), ale również ewentualnych negatywnych efektów ubocznych.

Wiele wskazuje na to, że takie ewaluacje nie są regularnie przeprowadzane, a nawet jeśli, to w sposób pozostawiający wiele do życzenia. Na przykład cele stawiane przed miejskimi systemami monitoringu są bardzo ogólnikowe, a weryfikacja ich osiągnięcia ma miejsce tylko w części miast, i to często w sposób, który nie gwarantuje wiarygodnych wniosków.

8. PUŁAPKA AUTOMATYZACJI

Bezpośredni wpływ na działanie narzędzi wykorzystywanych do nadzoru nad obywatelami ma coraz częściej nie tylko człowiek, lecz również algorytm. Mowa na przykład o rozwiązaniach technicznych, które pomagają w informacyjnym szumie wyłapać podejrzane zachowania. Ponieważ działanie takich systemów zawsze opiera się na zależnościach statystycznych, nie da się uniknąć błędów – fałszywych trafień. Właśnie dlatego ustawa o ochronie danych osobowych zakazuje podejmowania ostatecznych rozstrzygnięć dotyczących danej osoby wyłącznie na podstawie operacji w systemie informatycznym. Decyzja powinna zawsze należeć do człowieka, który może wszechstronnie ocenić daną sytuację. To ważne ograniczenie, lecz wiele wskazuje na to, że niewystarczające. Rozwój automatycznych funkcjonalności prędzej lub później postawi nas przed koniecznością odpowiedzi na pytanie, kto realnie decyduje o tym, w jaki sposób te systemy działają i ile do powiedzenia ma w tej sprawie społeczeństwo.

9. DRUGIE ŻYCIE DANYCH

Zaangażowanie biznesu w tworzenie rozwiązań służących do zbierania i analizowania informacji o obywatelach ma swoje daleko idące konsekwencje. Wiele informacji o codziennym życiu każdego z nas trafia nie tylko w ręce państwowych instytucji, ale również prywatnych podmiotów. Dobrze ilustruje ten problem popularna praktyka korzystania przez administratorów serwisów internetowych instytucji publicznych z rozwiązań technicznych, które przekazują informacje o odwiedzających je osobach zewnętrznym firmom.

Problem jest jednak w istocie dużo szerszy i głębszy, bo dotyczy wielu zadań państwa przekazywanych do realizacji prywatnym firmom oraz narzędzi tworzonych przez zewnętrzne podmioty, które mogą sprawować nad nimi kontrolę i mieć dostęp do zbieranych za ich pomocą informacji o obywatelach. W praktyce może to dotyczyć zarówno miejskich systemów wypożyczania rowerów, jak i zaawansowanych narzędzi technicznych wykorzystywanych przez służby. Czy państwo ma rzeczywistą kontrolę nad tym, jakie informacje trafiają do prywatnych firm i w jaki sposób są wykorzystywane? Niestety, wiele wskazuje na to, że świadomość problemu jest niewystarczająca, co przekłada się zarówno na brak dostatecznej przejrzystości, jak i wypracowanych standardów działania.

10. W PAJĘCZYNIE INFORMACJI

Coraz częściej informacje zebrane dzięki różnym narzędziom są ze sobą łączone. Prowadzi to do sytuacji, w których ingerencje w prywatność – akceptowalne pojedynczo – mogą przekraczać dopuszczalne granice. Z przypadkami łączenia danych z różnych źródeł każdy może zetknąć się na co dzień, często w bardzo prozaicznych sytuacjach. Dzięki dostępowi do Centralnej Ewidencji Pojazdów i Kierowców podmioty odpowiedzialne za miejskie strefy parkowania tam, gdzie funkcjonują parkometry wymagające podania numerów rejestracyjnych pojazdów, mogą dowiedzieć się, gdzie dana osoba najczęściej parkuje, a instytucje mające dostęp do systemów wyposażonych w funkcję ARTR – gdzie i kiedy przejeżdża swoim samochodem. Kolejnym przykładem są karty miejskie łączące różne funkcjonalności (i informacje o użytkownikach).

Problem mogą pogłębiać niedawne zmiany w ustawie o ochronie danych osobowych, zgodnie z którymi wszystkie instytucje państwowe uważa się za jednego administratora, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu. Ryzyko, że różne podmioty będą mogły swobodnie wymieniać się informacjami o obywatelach i wykorzystywać je wedle uznania, stało się w związku z tym bardzo realne.

INSTYTUCJE, KTÓRE OTRZYMAŁY WNIOSKI O INFORMACJĘ PUBLICZNĄ

Agencja Bezpieczeństwa Wewnętrznego
Agencja Nieruchomości Rolnych
Agencja Rozwoju Przemysłu
Agencja Rynku Rolnego
Babiogórski Park Narodowy
Białowieski Park Narodowy
Bieszczadzki Park Narodowy
Biuro Bezpieczeństwa i Zarządzania Kryzysowego m.st. Warszawy
Biuro Pomocy i Projektów Społecznych m.st. Warszawy
Centralne Biuro Antykorupcyjne
Centralny Ośrodek Sportu
Dolnośląski Oddział Wojewódzki NFZ
Dyrekcja Generalna Lasów Państwowych
Generalna Dyrekcja Dróg Krajowych i Autostrad
Główny Urząd Statystyczny
Gorczański Park Narodowy
Górnośląskie Towarzystwo Lotnicze SA w Katowicach
Inspekcja Transportu Drogowego
Instytut Adama Mickiewicza
Kampinoski Park Narodowy
Karkonoski Park Narodowy
Komenda Główna Państwowej Straży Pożarnej
Komenda Główna Policji
Komenda Główna Straży Granicznej
Komenda Główna Żandarmerii Wojskowej
Komenda Stołeczna Policji
Kujawsko-Pomorski Oddział Wojewódzki NFZ
Lasy Miejskie – Warszawa
Lotnisko Zielona Góra/Babimost Spółka z o.o.
Lubelski Oddział Wojewódzki NFZ
Lubuski Oddział Wojewódzki NFZ
Łódzki Oddział Wojewódzki NFZ
Małopolski Oddział Wojewódzki NFZ
Mazowiecki Oddział Wojewódzki NFZ
Mazowiecki Port Lotniczy Warszawa Modlin Sp. z o.o.
Miejski Zarząd Dróg w Opolu
Miejski Zarząd Dróg w Kielcach
Miejski Zarząd Dróg w Toruniu
Miejski Zarząd Ulic i Mostów Katowice
Międzynarodowy Port Lotniczy im. Jana Pawła II Kraków-Balice sp. z o.o.
Ministerstwo Administracji i Cyfryzacji
Ministerstwo Edukacji Narodowej
Ministerstwo Finansów
Ministerstwo Infrastruktury i Rozwoju
Ministerstwo Kultury i Dziedzictwa Narodowego
Ministerstwo Nauki i Szkolnictwa Wyższego
Ministerstwo Obrony Narodowej
Ministerstwo Rodziny Pracy i Polityki Społecznej
Ministerstwo Rolnictwa i Rozwoju Wsi
Ministerstwo Skarbu Państwa
Ministerstwo Sportu i Turystyki Rzeczypospolitej Polskiej
Ministerstwo Spraw Wewnętrznych
Ministerstwo Spraw Zagranicznych
Ministerstwo Sprawiedliwości
Ministerstwo Środowiska
Ministerstwo Zdrowia
Najwyższa Izba Kontroli
Narodowy Bank Polski
Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej
Narodowy Fundusz Zdrowia
Opolski Oddział Wojewódzki NFZ
Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych
Park Narodowy „Bory Tucholskie”
Park Narodowy Gór Stołowych
Pieniński Park Narodowy
Podkarpacki Oddział Wojewódzki NFZ
Podlaski Oddział Wojewódzki NFZ
Poleski Park Narodowy
Polska Wytwórnia Papierów Wartościowych
Polskie Radio SA
Pomorski Oddział Wojewódzki NFZ
Port Lotniczy Bydgoszcz SA
Port Lotniczy Gdańsk Sp. z o.o.
Port Lotniczy Lublin SA
Port Lotniczy Łódź im. Władysława Reymonta Sp. z o.o.
Port Lotniczy Poznań-Ławica Sp. z o.o.
Port Lotniczy Rzeszów-Jasionka Sp. z o.o.
Port Lotniczy Szczecin-Goleniów im. NSZZ Solidarność
Port Lotniczy Wrocław SA
Prokuratoria Generalna Skarbu Państwa
Przedsiębiorstwo Państwowe „Porty Lotnicze”
Urząd Pracy m.st. Warszawy
Słowiński Park Narodowy
Śląski Oddział Wojewódzki NFZ
Świętokrzyski Oddział Wojewódzki NFZ
Tatrzański Park Narodowy
Telewizja Polska SA
Totalizator Sportowy
Urząd Komunikacji Elektronicznej
Urząd m.st. Warszawy
Urząd Miasta Kędzierzyn-Koźle
Urząd Miasta Łodzi
Urząd Miasta Nowego Sącza
Urząd Miasta Olsztyna
Urząd Miasta Opola
Urząd Miasta Piotrkowa Trybunalskiego
Urząd Miasta Płocka
Urząd Miasta Poznania
Urząd Miasta Rzeszowa
Urząd Miasta Skierniewice
Urząd Miasta Szczecin
Urząd Miasta Świnoujście
Urząd Miasta Tarnobrzega
Urząd Miasta Tarnowa
Urząd Miasta Torunia
Urząd Miasta w Białymstoku
Urząd Miasta w Bydgoszczy
Urząd Miasta w Chełmie
Urząd Miasta w Częstochowie
Urząd Miasta w Elblągu
Urząd Miasta w Ełku
Urząd Miasta w Gdańsku
Urząd Miasta w Gdyni
Urząd Miasta w Gorzowie Wielkopolskim
Urząd Miasta w Kaliszu
Urząd Miasta w Katowicach
Urząd Miasta w Kielcach
Urząd Miasta w Koninie
Urząd Miasta w Koszalinie
Urząd Miasta w Krakowie
Urząd Miasta w Legnicy
Urząd Miasta w Lublinie
Urząd Miasta w Ostrowcu Świętokrzyskim
Urząd Miasta w Przemyślu
Urząd Miasta Włocławek
Urząd Miasta Zamość
Urząd Miasta Zielona Góra
Urząd Miejski w Łomży
Urząd Miejski w Nowej Soli
Urząd Miejski w Nysie
Urząd Miejski w Radomiu
Urząd Miejski w Słupsku
Urząd Miejski w Sosnowcu
Urząd Miejski w Starachowicach
Urząd Miejski w Suwałkach
Urząd Miejski w Wałbrzychu
Urząd Miejski Wrocławia
Warmińsko-Mazurski Oddział Wojewódzki NFZ
Wielkopolski Oddział Wojewódzki NFZ
Wojskowa Akademia Techniczna
Zachodniopomorski Oddział Wojewódzki NFZ
Zakład Gospodarki Komunalnej i Mieszkaniowej w Zielonej Górze
Zakład Obsługi Systemu Monitoringu m.st. Warszawy
Zakład Ubezpieczeń Społecznych
Zarząd Dróg i Mostów w Lublinie
Zarząd Dróg i Transportu w Łodzi
Zarząd Dróg i Utrzymania Miasta Wrocław
Zarząd Dróg i Zieleni w Gdańsku
Zarząd Dróg Miejskich i Komunikacji Publicznej w Bydgoszczy
Zarząd Dróg Miejskich w Poznaniu
Zarząd Dróg Miejskich w Warszawie
Zarząd Dróg Zieleni i Transportu w Olsztynie
Zarząd Transportu Miejskiego w Warszawie
ZUS I Oddział w Łodzi
ZUS I Oddział w Poznaniu
ZUS I Oddział w Warszawie
ZUS II Oddział w Łodzi
ZUS II Oddział w Poznaniu
ZUS II Oddział w Warszawie
ZUS III Oddział w Warszawie
ZUS Oddział w Białymstoku
ZUS Oddział w Bielsku-Białej
ZUS Oddział w Biłgoraju
ZUS Oddział w Bydgoszczy
ZUS Oddział w Chorzowie
ZUS Oddział w Chrzanowie
ZUS Oddział w Częstochowie
ZUS Oddział w Elblągu
ZUS Oddział w Gdańsku
ZUS Oddział w Gorzowie Wielkopolskim
ZUS Oddział w Jaśle
ZUS Oddział w Kielcach
ZUS Oddział w Koszalinie
ZUS Oddział w Krakowie
ZUS Oddział w Legnicy
ZUS Oddział w Lublinie
ZUS Oddział w Nowym Sączu
ZUS Oddział w Olsztynie
ZUS Oddział w Opolu
ZUS Oddział w Ostrowie Wielkopolskim
ZUS Oddział w Pile
ZUS Oddział w Płocku
ZUS Oddział w Radomiu
ZUS Oddział w Rybniku
ZUS Oddział w Rzeszowie
ZUS Oddział w Siedlcach
ZUS Oddział w Słupsku
ZUS Oddział w Sosnowcu
ZUS Oddział w Szczecinie
ZUS Oddział w Tarnowie
ZUS Oddział w Tomaszowie Mazowieckim
ZUS Oddział w Toruniu
ZUS Oddział w Wałbrzychu
ZUS Oddział w Zabrzu
ZUS Oddział w Zielonej Górze
ZUS Oddział we Wrocławiu

OPRACOWANIE I REDAKCJA

Małgorzata Szumańska

WSPÓŁAUTORZY

Wojciech Klicki
Jędrzej Niklas
Katarzyna Szymielewicz
Anna Walkowiak

WSPÓŁPRACA

Michał „czesiek" Czyżewski
Krzysztof Juruś
Anna Obem
Radosław Stolarczyk

KOREKTA

Urszula Dobrzańska

PROJEKT GRAFICZNY I SKŁAD

Kasia Iwańska

DRUK

Drukarnia ARKA

WYDAWCA

Fundacja Panoptykon | panoptykon.org

Warszawa 2016

ISBN: 978-83-938554-4-5

Publikacja została sfinansowana z Funduszy EOG w ramach programu „Obywatele dla demokracji" i stanowi podsumowanie projektu „Państwo a biznes nadzoru. Monitoring praktyk instytucji publicznych".

O FUNDACJI PANOPTYKON

Na każdym kroku jesteśmy obserwowani przez kamery, śledzeni w sieci, a nasze dane są zbierane przez państwo i firmy, które na tym zarabiają. Fundacja Panoptykon jest jedyną organizacją w Polsce, która odpowiada na związane z tym zagrożenia i udowadnia, że nie jesteśmy wobec nich bezsilni. Nie walczymy z nowymi technologiami, sami z nich korzystamy. Ale jesteśmy przekonani, że współczesny nadzór powinien mieć swoje granice – wyznaczone przez prawo i świadomych obywateli. Dlatego patrzymy kontrolującym na ręce i nagłaśniamy nadużycia; uczymy, jak zabezpieczyć swoje dane, komputer, portfel czy telefon przed wykorzystaniem; walczymy o to, by tworzone prawo chroniło wolność i prywatność. Po prostu: kontrolujemy kontrolujących.

Jeśli uważasz, że nasza misja jest ważna, wspieraj Panoptykon darowiznami i 1% swojego podatku (KRS: 0000327613). Serdecznie dziękujemy za każde wsparcie!

Które polskie miasto ma największy system miejskiego monitoringu? Jakie instytucje korzystają z dronów? A jakie z systemów rozpoznawania tablic rejestracyjnych? Czego można się o Tobie dowiedzieć dzięki karcie miejskiej? Ile państwo wydaje na rozwój systemów kontroli kierowców? Po co wyższej uczelni odciski palców wykładowców i studentów? W jakim urzędzie mogą być nagrane Twoje rozmowy? Do kogo trafiają informacje o tym, czego szukasz w serwisie swojego urzędu miasta? Czy policja może zdalnie przejąć kontrolę nad Twoim telefonem?

Odpowiedzi na te pytania – i wiele innych – znajdziesz w tym przewodniku.

FUNDACJA PANOPTYKON

ISBN: 978-83-938554-4-5