BIULETYN FUNDACJI PANOPTYKON

REC

PODSŁUCH JAK SIĘ PATRZY

Klicki o:
WALCE O KONTROLĘ NAD SŁUŻBAMI

Haertle o:
CENIE PRYWATNOŚCI

HISTORIE INWIGILOWANYCH

POLITYKA STRACHU
OD WTC DO USNARZA GÓRNEGO

FUNDACJA PANOPTYKON

W BIULETYNIE:

REDAKCJA: **Małgorzata Szumańska**

WYWIADY: **Krzysztof Story**

PROJEKT GRAFICZNY, ILUSTRACJE I SKŁAD: **Jakub Sudra [sudragrafika.com]**

KOREKTA: **Urszula Dobrzańska**

WSPÓŁPRACA: **Justyna Dywańska, Anna Obem**

ISBN: 978-83-938554-8-3

Fundacja Panoptykon
Warszawa 2021

NIKT CI NIE POWIE, KIEDY BĘDĄ CIĘ PODGLĄDAĆ

Co może zrobić policjant, czekając dwie minuty na zaparzenie herbaty? Może zjeść pączka albo zamówić obiad. Albo skorzystać z toalety. Albo zadzwonić do córki i spytać, jak poszedł jej sprawdzian z chemii.

Może też sprawdzić każdego i każdą z nas. Na przykład gdzie byliśmy pół roku temu i z kim. Prosta sprawa: kilka kliknięć.

Sama możliwość kontrolowania aktywności obywateli i obywatelek przez służby powołane do dbania o nasze wspólne bezpieczeństwo nie jest problemem. Szkopuł w tym, że nikt z zewnątrz nie weryfikuje, czy ściągnięcie twojego billingu lub sprawdzenie mojego IP było w danej sprawie uzasadnione. A żadne z nas nigdy nie dowie się, że było przedmiotem kontroli. W takich sytuacjach łatwo o nadużycia.

Codziennie przedstawiciele Policji i innych polskich służb zakładają średnio kilkadziesiąt podsłuchów, sprawdzają kilka tysięcy billingów i danych o lokalizacji. Czy wszystkie te działania dotyczą przestępców? A może po prostu ludzi, którzy wydali się podejrzani – z powodu wyglądu, przekonań, społecznego lub politycznego zaangażowania? Wiemy, że takie przypadki się zdarzają. Niestety bez zewnętrznej kontroli nad służbami nie ma możliwości sprawdzenia, czy to tylko wypadki przy pracy, czy systemowe nadużycia.

Problem nie tylko nie rozwiąże się sam, ale będzie narastał. Wraz z przenoszeniem się do sieci kolejnych sfer życia rośnie liczba naszych cyfrowych śladów i zapotrzebowanie służb na cyfrową inwigilację. Sektor technologiczny odpowiada na to tworzeniem takich narzędzi, jak słynny Pegasus. To, co jeszcze kilkanaście lat temu należało do sfery science fiction, nie tylko istnieje, ale wkrótce stanie się tańsze i będzie coraz powszechniej dostępne.

Aby pokazać skalę problemu i jego konsekwencje, Fundacja Panoptykon w 2021 roku wystartowała z kampanią „Podsłuch jak się patrzy", w której domaga się kontroli nad służbami. Zdajemy sobie sprawę z tego, że zmiana prawa nie wydarzy się z dnia na dzień. Jednak nie możemy bezczynnie na nią czekać. Bez przewrotu w głowach polityków i społeczeństwa nie możemy liczyć na lepsze prawo.

MAŁGORZATA SZUMAŃSKA

MIERZĄC SIĘ Z GOLIATEM
HISTORIA ZMAGAŃ O KONTROLĘ NAD SŁUŻBAMI

WYWIAD Z WOJCIECHEM KLICKIM,
PRAWNIKIEM I AKTYWISTĄ Z FUNDACJI PANOPTYKON

„Pewne ograniczenia w jawności działania służb są bezdyskusyjnie konieczne, ale muszą mieć one swoje granice. Bez nich nie powinniśmy spodziewać się skuteczności, tylko samowoli. Służby są tajnym, zbrojnym ramieniem państwa i ja to akceptuję, ale dopóki działają wyłącznie w cieniu, bez naszej kontroli, jesteśmy bardzo narażeni na manipulację z ich strony".

Krzysztof Story: Jestem dziennikarzem. Zdarza mi się krytykować władzę, relacjonować protesty, rozmawiać z aktywistami. Czy mam się bać, że jestem obserwowany przez służby?
Wojciech Klicki: Nie wiem. Ty też nie masz możliwości, by się tego dowiedzieć. Nie mamy pojęcia, kto i dlaczego jest dziś w Polsce inwigilowany – to zrozumiałe i konieczne, by służby mogły skutecznie działać. Problem w tym, że o działaniach służb nie dowiemy się nawet po fakcie. Nie mamy nad nimi jako społeczeństwo żadnej kontroli. Ale tak, masz sporą szansę na bycie w grupie inwigilowanych, ja zresztą też. A rozmawiając ze sobą, zwiększamy tę szansę.

Nawet jeśli moim największym konfliktem z prawem było przejście przez ulicę na czerwonym świetle?
Podobnych historii wcale nie trzeba szukać na Węgrzech, gdzie system Pegasus został wykorzystany przeciwko ponad setce dziennikarzy. W Polsce także co jakiś czas słyszymy o inwigilacji dziennikarzy przez ABW, CBA czy Policję. A niewykluczone, że to tylko czubek góry lodowej. W kampanii „Podsłuch jak się patrzy" opisujemy historię Mariusza Gierszewskiego – służby obserwowały nie tylko jego, ale też ponad 30 osób z jego kontaktów: adwokatów, polityków, rzeczników służb, a nawet znajomego lutnika. Dzieje się to nie tylko w świecie mediów – w 2018 roku aktywiści Greenpeace'u przed szczytem klimatycznym w Katowicach, a także w jego trakcie, byli śledzeni, znajdowali lokalizatory GPS w samochodach, choć przecież działali zupełnie legalnie. Wychodzi na to, że aktywizm ekologiczny to

w Polsce działalność podwyższonego ryzyka.

Chyba nie czuję się na tyle ważny, by służbom opłacało się mną zajmować.
Pozyskanie bardzo wielu Twoich danych to dziś dla służb kwestia kilku kliknięć. Do kogo dzwoniłeś, z kim się regularnie kontaktujesz, gdzie logowałeś się do sieci – to wszystko jest na wyciągnięcie ręki. Wystarczy jeden zirytowany Twoim artykułem polityk, który ma jakiś wpływ na służby i delikatnie zasugeruje, że warto Cię obserwować. Szansa, że poniesie jakiekolwiek konsekwencje, jest bliska zeru. Ten zakazany owoc wisi bardzo nisko.

Jak nisko?
Na tyle, że w 2020 roku służby sięgnęły po nasze billingi i dane lokalizacyjne 1,53 miliona razy. W Polsce jest dziewięć instytucji uprawnionych do prowadzenia tzw. czynności operacyjno-rozpoznawczych: Agencja Bezpieczeństwa Wewnętrznego, Biuro Nadzoru Wewnętrznego MSWiA, Centralne Biuro Antykorupcyjne, Krajowa Administracja Skarbowa, Policja, Służba Kontrwywiadu Wojskowego, Służba Ochrony Państwa, Straż Graniczna i Żandarmeria Wojskowa. Zdecydowanie najczęściej z danych retencyjnych korzysta Policja, na drugim miejscu jest Straż Graniczna. By uzyskać do nich dostęp, służby nie muszą nikogo pytać o zgodę, wszystko dzieje się w ramach ich wewnętrznych procedur.

Upoważniony do tego funkcjonariusz siada przed komputerem, wpisuje mój numer PESEL i już?
Ale po co PESEL, kiedy wystarczy numer telefonu? Operatorzy komunikacyjni specjalnie dla służb stworzyli łącza bezpośrednio z bazami danych, więc ta procedura jest błyskawiczna. Policjant lub funkcjonariusz innej służby ma dostęp do tych danych, zanim zdąży zaparzyć herbatę.

To dotyczy jedynie danych retencyjnych, które operatorzy muszą przechowywać przez 12 miesięcy. Przy dzisiejszym cyfrowym stylu naszego życia z tych metadanych można wyczytać bardzo dużo. Na podstawie np. tego, czy często dzwonimy do adwokata specjalizującego się w sprawach rozwodowych, można wyciągnąć różne wnioski nawet bez wnikania w treść komunikacji. Jeśli służby chcą jednak tę treść poznać i założyć nam podsłuch, procedura nie jest już tak łatwa.
Teoretycznie podsłuchy są dużo lepiej kontrolowane, każde takie działanie wymaga zgody sądu i prokuratury. W praktyce ta kontrola jest fikcją. Sądy akceptują ponad 99 proc. wszystkich wniosków, prokuratura – 97 proc.

Sądy nie wywiązują się ze swoich zadań?
Można tak powiedzieć, ale system bardzo je do tego zachęca. By wyrazić zgodę na podsłuch, sędzia musi jedynie podpisać wniosek i przystawić pieczątkę. By odmówić, musi napisać uzasadnienie. W większości przypadków nie ma czasu, by każdy przypadek rozpatrzyć indywidualnie, zgody wyraża się taśmowo. Dodatkowo taki wniosek nie musi wcale zawierać wszystkich informacji o sprawie, a jedynie te, które uzasadnią konieczność założenia podsłuchu. W aktach nie musi być nawet nazwiska podsłuchiwanej osoby, wystarczy tylko numer telefonu albo numer IMEI. Gdyby na wniosku było napisane „Donald Tusk", sędzia potraktowałby to ze szczególną uwagą. W obecnym systemie na podstawie okrojonych danych sędzia może nawet nieświadomie zaakceptować podsłuchiwanie samego czy samej siebie.

Podałeś przykład Donalda Tuska, wcześniej rozmawialiśmy o dziennikarzach i aktywistach. To szczególne przypadki. Co to wszystko obchodzi zwykłego człowieka?
Po pierwsze efekt mrożący inwigilacji, przez który na przykład dziennikarz porzuci dane śledztwo lub straci informatora, nie służy nam jako społeczeństwu. Po

drugie wcale nie musisz być Donaldem Tuskiem, żeby być narażonym na inwigilację. Nic nie stoi na przeszkodzie, żeby powiatowa komenda Policji podsłuchiwała właściciela firmy, która konkuruje z firmą szwagra komendanta. Brak kontroli zwykle prowadzi do nadużyć, zwłaszcza w czasach, gdy służby mają coraz większe możliwości. Przecież nie jest już tak, że Policja czy ABW masowo wysyłają funkcjonariuszy, by ci śledzili pojedyncze osoby. Mają coraz więcej technologii, które robią to za nich. Przykładem narzędzia, które bardzo rozwinęło się w ostatnich latach, jest oprogramowanie do rozpoznawania twarzy.

tak naprawdę nie mamy żadnego katalogu narzędzi, którymi dysponują służby. Mogą robić wszystko, na co pozwala im technologia: uzyskiwać dostęp do baz danych albo żądać stałego dostępu do obrazu z kamer w warszawskich tramwajach (co pod koniec 2020 roku uczyniło ABW). Trudno mi wymienić zbiór danych, do którego służby nie miałyby dostępu, może poza zaszyfrowanym dyskiem na komputerze odłączonym od Internetu. Drugą kwestią jest to, z jaką łatwością po te dane sięgają. Na przykład informacje o naszych wydatkach są chronione tajemnicą bankową, dostęp do nich jest przyznawany na takich

I pewne ograniczenia w jawności są bezdyskusyjnie konieczne, ale muszą mieć one swoje granice. Bez nich nie powinniśmy spodziewać się od służb skuteczności, tylko samowoli. To nie jest tylko kwestia ochrony naszej prywatności, ale też swobody decyzji. Służby są tajnym, zbrojnym ramieniem państwa i ja to akceptuję, ale dopóki działają wyłącznie w cieniu, bez naszej kontroli, jesteśmy bardzo narażeni na manipulację z ich strony. Im mniej o nich wiemy, tym bardziej obracają się przeciwko nam. Zobaczmy, że dwa zamachy terrorystyczne w Polsce wydarzyły się akurat w trakcie prac nad nową ustawą antyterrory-

Wcale nie musisz być Donaldem Tuskiem, żeby być narażonym na inwigilację. Nic nie stoi na przeszkodzie, żeby powiatowa komenda Policji podsłuchiwała właściciela firmy, która konkuruje z firmą szwagra komendanta. Brak kontroli zwykle prowadzi do nadużyć, zwłaszcza w czasach, gdy służby mają coraz większe możliwości.

Takie rozmowy zawsze brzmią trochę jak scenariusz science fiction.
Ale my naprawdę nie musimy sobie tego wyobrażać, wystarczy spojrzeć na protesty w Hongkongu, gdzie demonstranci niszczyli kamery monitoringu, by zapewnić sobie bezpieczeństwo. W Polsce nie potwierdziliśmy wykorzystania podobnej technologii. Często posługujemy się przykładem podsłuchów i danych retencyjnych, bo są obrazowe i znamy konkretne liczby, ale

samych zasadach jak zgoda na podsłuch. Z tą różnicą, że tutaj sądy akceptują 100 proc. wniosków służb. Dostęp do bazy danych z parkometrów czy nagrań z monitoringu to często kwestia jednego pisma lub wręcz skorzystania z tzw. stałego łącza. Często tym, co nas ratuje, jest chaos i rozproszenie danych.

Potrzebujemy służb, które działają skutecznie. Skuteczność często wyklucza jawność.

styczną, przyznającą służbom dodatkowe przywileje. Mówię o podłożeniu bomby w autobusie wrocławskiego MPK oraz nieudanej próbie podpalenia radiowozów przy komisariacie Warszawa-Włochy. Ja oczekuję, że w takiej sytuacji ktoś z zewnątrz zweryfikuje, czy mamy do czynienia z zagrożeniem, czy z manipulacją. Inaczej pozostają nam tylko domysły. To jest zagrożenie nie tylko dla naszej prywatności, ale też dla podstawowych wolności:

manifestowania, wyrażania swoich poglądów.

Naszej wolności i prywatności bardziej zagrażają służby czy wielkie korporacje internetowe?
Ja wątek służb traktuję szczególnie. Mimo wszystko to, czy wrzucę zdjęcie mojego nowo narodzonego syna na Facebooka, jest moją decyzją. To, czy na moim telefonie jest zainstalowany Pegasus – nie. Oczywiście, problem śledzenia i profilowania przez internetowych gigantów jest jak najbardziej realny, bo Google czy Facebook mogą równie dobrze sprzedać nam buty, książkę, jak i nowy rząd. Ale tylko państwo ma za sobą przymus. Może działać absolutnie wbrew mnie. Niedawno minęło 20 lat od zamachów na World Trade Center. Dla mnie to był kluczowy moment, w którym rozkręciła się machina rządzenia za pomocą strachu. Machina, która doprowadziła do tego, że służby w wielu krajach mają bezprecedensowe możliwości śledzenia wszystkich obywateli i są niemal państwem w państwie.

Przecież wcześniej mieliśmy zimną wojnę.
Po 11 września rozpoczęliśmy wojnę nie z konkretnym mocarstwem, a z bliżej nieokreślonym wrogiem, terrorystą, Innym, którym może w łatwy sposób stać się każdy z nas. I to dało podstawę do inwigilacji całych społeczeństw.

Co możemy zrobić, by się przed tym chronić?
Nie będę wymieniał bezpiecznych komunikatorów, sposobów szyfrowania e-maili i zasad cyberbezpieczeństwa. Co ja mam zrobić, żeby wygrać ze służbami? To jest źle postawione pytanie, jakbyśmy brali udział w jakimś wyścigu zbrojeń. Przecież służby powinny nam służyć.
Ja wcale nie chcę zabierać im natychmiastowego dostępu do naszych danych, bo wyobrażam sobie wiele sytuacji, w których jest to niezbędne. Tylko musimy mieć pewność, że mechanizm zaprojektowany przeciwko przestępcom nie zostanie użyty przeciwko niewinnym obywatelom. Najważniejsze jest przełamanie wdrukowanego założenia, że służby muszą działać poza wszelką kontrolą, by działać skutecznie. Za tym dopiero mogą iść regulacje i zmiana polityczna.

Panoptykon proponuje kilka rozwiązań wzorowanych na tym, jak służby funkcjonują w innych krajach europejskich.
Wcześniej wspomniałeś o wpływie wielkich korporacji – to stosunkowo nowy problem, rozwiązania dopiero się tworzą. W przypadku służb wszystko już jest gotowe, na świecie mamy wypracowane standardy, a Polska musi tylko do nich dorównać, bo dziś w sposób oczywisty ich nie przestrzega. Jednym z takich standardów jest powołanie niezależnej instytucji zdolnej kontrolować wszystkie dziewięć służb w Polsce i rozpatrywać skargi na ich działanie. Ale najważniejszą propozycją, funkcjonującą np. w Niemczech, jest

W przypadku służb na świecie mamy wypracowane standardy, a Polska musi tylko do nich dorównać. Jednym z takich standardów jest powołanie niezależnej instytucji zdolnej kontrolować wszystkie dziewięć służb w Polsce i rozpatrywać skargi na ich działanie. Ale najważniejszą propozycją, funkcjonującą np. w Niemczech, jest obowiązek informowania o inwigilacji. Po 12 miesiącach od zakończenia działań służba musiałaby powiadomić podsłuchiwanego, że był obiektem zainteresowania.

obowiązek informowania o inwigilacji. Po 12 miesiącach od zakończenia działań służba musiałaby powiadomić podsłuchiwanego, że był obiektem zainteresowania. Służby nadal mogłyby działać skutecznie i szybko, ale ze świadomością, że ich działania zostaną prędzej czy później zweryfikowane.

Wysłaliście te propozycje do wszystkich polskich partii politycznych. Jak oceniasz odpowiedzi?
Zacznę od tego, że nie dostaliśmy odpowiedzi od partii rządzącej, ale pośrednią odpowiedzią są jej ustawy zwiększające uprawnienia służb. Wszystkie partie opozycyjne zgodziły się z naszymi postulatami. Tylko że część osób, które przygotowywały te odpowiedzi, przez lata miało decydujący wpływ na pracę służb. Pamiętam, jak ci sami politycy przekonywali nas, że obowiązek informowania o podsłuchu to wybijanie służbom wszystkich zębów, że tego się nie da zrobić. Być może zmienili poglądy, przemyśleli sprawę, nie wiem. Ważne, by presja społeczna była tak duża, by nie opłacało im się ich zmieniać z powrotem.

Panoptykon jest jedną z nielicznych organizacji zajmujących się prywatnością. Nie czujecie się jak Dawid naprzeciw Goliata?
Częściej słyszymy, że jesteśmy Don Kichotami i walczymy z cyfrowymi wiatrakami. Ja wolę porównanie do Dawida, bo on przecież na końcu pokonał Goliata. Oczywiście, dysproporcja sił bywa ogromna. W powstawaniu unijnego kodeksu usług cyfrowych biorą udział setki lobbystów zatrudnionych przez wielkie korporacje i kilkunastu z organizacji pozarządowych. Ale zmiana, której chcemy być częścią, naprawdę zachodzi. To, że RODO, choć ma złą markę, nie pozwala na pewne nadużycia; to, że w ustawie antyterrorystycznej ostatecznie nie znalazło się wiele karkołomnych propozycji, to zasługa właśnie Panoptykonu i innych organizacji.
Czasem porównuję nas do organizacji ekologicznych. One od kilku dekad mówiły o globalnym ociepleniu, a dopiero dzisiaj zmienia się świadomość społeczna. Z nami, zarówno w kwestii służb, jak i cyfrowego kapitalizmu, jest podobnie. Po prostu jesteśmy na wcześniejszym etapie. Zarówno w ograniczaniu samowoli służb, jak i władzy internetowych gigantów.

Jest jeszcze jeden aspekt tego porównania: wspominasz, że aktywiści Greenpeace'u w 2018 roku byli śledzeni przez służby, opisujecie tę historię w kampanii „Podsłuch jak się patrzy". Czy polskie służby interesowały się też Panoptykonem?
Jeszcze przed zmianą władzy mieliśmy sygnały, że nasza aktywność jest obiektem zainteresowania ze strony służb. Ja przyjąłem taką postawę: jako obywatel demokratycznego państwa zakładam, że skoro nie łamię prawa, to jestem bezpieczny. I czasami przymykam oko na rzeczywistość, bo gdybym zbyt mocno na nią patrzył, musiałbym to założenie porzucić.

Na co dokładnie musiałeś przymykać oko?
Na widoczny kryzys demokracji w Polsce. Od ataku niezależność Trybunału Konstytucyjnego i sądów po drastyczne obniżenie standardów procesu legislacyjnego, które widać także w naszej pracy. Wspominałem już o ustawie antyterrorystycznej, którą przyjęto 10 czerwca 2016 roku. Zanim ją uchwalono, rząd przez kilka miesięcy mówił, że pracuje nad tym dokumentem, ale nie opublikował żadnego projektu. Pamiętam, że w maju spotkałem się z kolegami, żeby zagrać mecz koszykówki. W środku meczu dzwoni do mnie nieznany numer i męski głos w słuchawce pyta, czy nie jestem zainteresowany poznaniem projektu nowej ustawy.

Znam kilka filmów, które się tak zaczynają.
Ja też. Zapytałem, z kim rozmawiam, ale nie odpowiedział. Zaczął mówić o budce telefonicznej w budynku Poczty Głównej w Warszawie.

Ja byłem daleko od centrum, zadzwoniłem szybko do Kasi [Katarzyna Szymielewicz, prezeska Panoptykonu – przyp. red.], ona tam pojechała. W budce telefonicznej leżał nieopublikowany przez rząd projekt ustawy o działaniach antyterrorystycznych.

Co zrobiliście?
Opublikowaliśmy go. Dwa dni później ten sam projekt opublikował rząd. Wtedy po raz pierwszy poczułem, że praca w Panoptykonie nie jest zwykłą prawniczą robotą. Bardzo wyraźnie poczułem, że jestem elementem gry sił, nad którymi nie mam żadnej kontroli i które mogą zrobić mi krzywdę.

odpowiadałem też za to, żeby całość wydrukować i wysłać. Dokument miał około 150 stron, wysyłałem go poleconym z poczty na Żoliborzu. Po dłuższym czasie dostaliśmy ze Strasburga nieoficjalną informację, że list dotarł, ale w kopercie znajdowała się tylko pierwsza strona. Ta z nazwiskami skarżących.

Później uzupełniliście wszystkie dokumenty, skarga wciąż nie jest rozpatrzona, ETPC zwrócił się o wyjaśnienia do polskiego rządu, rząd odpowiedział: „Czekamy na wyrok". Wracając do tej pustej koperty: boisz się?
Staram się tę historię jak najdalej od siebie odepchnąć.

specjalizuje. Panoptykon specjalizuje się w nadzorze. Nie możemy pominąć największej siły, która nas inwigiluje, czyli służb. Czuję, że gdybyśmy odpuścili ten temat, moglibyśmy równie dobrze zamknąć cały Panoptykon.
Jest też jedna rzecz, która mnie bardzo mocno motywuje. Mam poczucie, że wielu odbiorców docenia nasze działania. Mówią: „Sami byśmy się tym nie zajęli, dobrze, że robicie to za nas".

Spore ryzyko, małe szanse na szybki efekt – niewdzięczną masz pracę.
Gdy dowiedziałem się o tej pustej kopercie, moją pierwszą myślą było: „Tyle się

Pod koniec 2017 roku złożyliśmy wspólnie z innymi aktywistami skargę do Europejskiego Trybunału Praw Człowieka w Strasburgu, która dotyczy właśnie niekontrolowanej inwigilacji przez służby. Jestem współautorem tej skargi, logistycznie odpowiadałem też za to, żeby całość wydrukować i wysłać. Dokument miał około 150 stron, wysyłałem go poleconym z poczty na Żoliborzu. Po dłuższym czasie dostaliśmy ze Strasburga nieoficjalną informację, że list dotarł, ale w kopercie znajdowała się tylko pierwsza strona.

Dostawaliście groźby?
Mam jedną niepokojącą historię, którą można traktować jako ostrzeżenie. Pod koniec 2017 roku złożyliśmy wspólnie z innymi aktywistami skargę do Europejskiego Trybunału Praw Człowieka w Strasburgu, która dotyczy właśnie niekontrolowanej inwigilacji przez służby. Jestem współautorem tej skargi, logistycznie

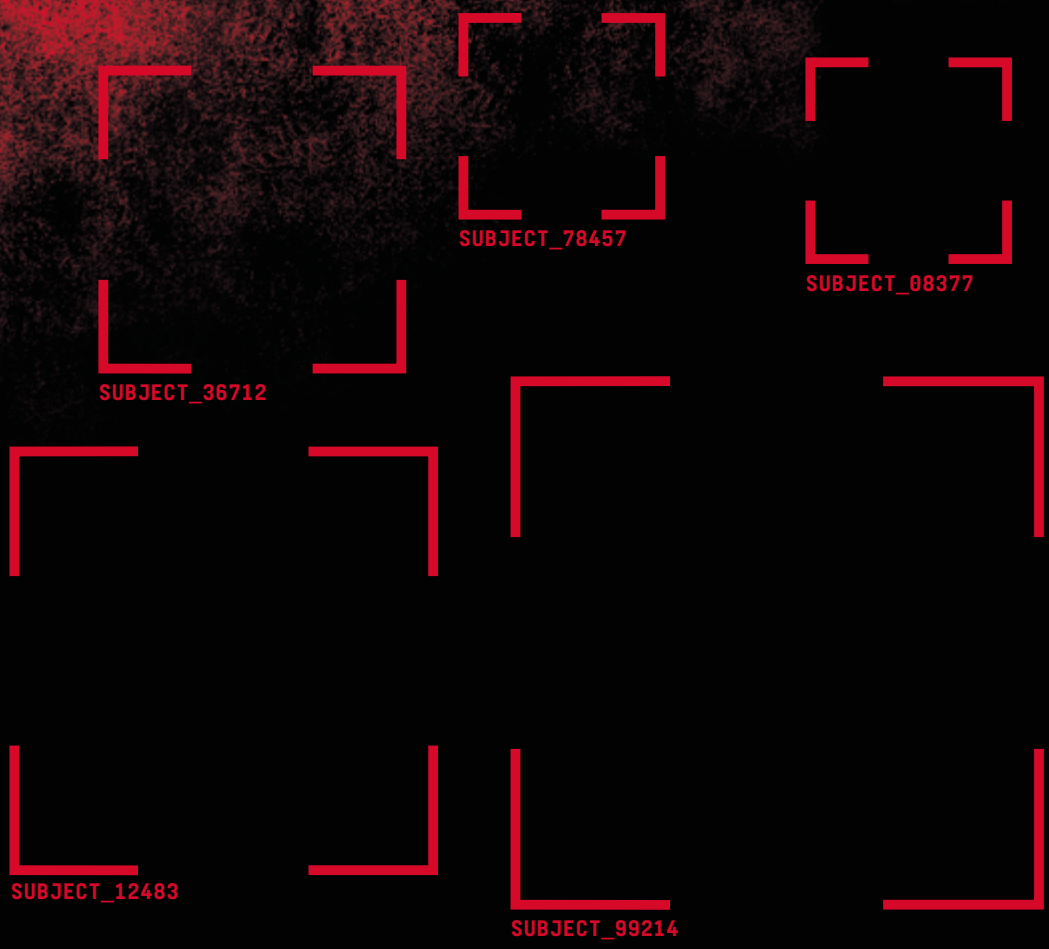
Nie wiem, co tam się stało i chyba nie chcę wiedzieć. Od paru osób usłyszałem, że po takiej historii po prostu bałyby się dalej pracować nad tym tematem. Zajmowanie się służbami i inwigilacją nie jest neutralne, jeśli chodzi o bezpieczeństwo i poczucie bezpieczeństwa. Zawsze jest trochę strachu, ale cholera, każda organizacja w czymś się

narobiłem i wszystko na marne". Czasem mówię żonie, że chciałbym być kierowcą autobusu. Z jednej strony masz poczucie, że służysz ludziom, z drugiej – po 8 godzinach wysiadasz z przegubowego mercedesa i idziesz do domu. Ona odpowiada, że umarłbym z nudów. I pewnie ma rację.

Rozmawiał Krzysztof Story.

NIKT NIE MA INTERESU W KONTROLI NAD INWIGILACJĄ ...POZA SPOŁECZEŃSTWEM.

Pomóż Fundacji Panoptykon walczyć o lepsze prawo!



FUNDACJA PANOPTYKON

Wspieraj darowiznami
(nr konta: PL 43 1440 1101 0000 0000 1044 6058)
i 1% podatku (nr KRS: 0000327613).
panoptykon.org/wspieraj

HISTORIE INWIGILOWANYCH

Wyobraź sobie, że chociaż nie wchodzisz w konflikt z prawem, trafiasz w orbitę zainteresowania służb. Nie da się wykluczyć takiego scenariusza: może klient, którego obsługujesz, ma długą policyjną kartotekę. Może twoja firma podejrzanie szybko się rozwija. Może twoja działalność społeczna jest nie w smak władzom.

Prawdopodobieństwo, że się o tym dowiesz, jest bliskie zeru.

Polskie prawo nie wymaga informowania o poddaniu inwigilacji osoby, której nie postawiono zarzutów. Jeśli sprawa wypływa, zwykle decyduje o tym przypadek.

Czasami jednak służbom zależy na tym, by obserwowana osoba zdawała sobie z tego sprawę – to ostrzeżenie: „Lepiej się nie wychylaj, obserwujemy cię".

Przedstawiamy historie i perspektywy osób, które dowiedziały się, że znalazły się na celowniku służb.

Ewelina Kycia

Koordynatorka wolontariatu w Greenpeace Polska. Podczas szczytu klimatycznego w 2018 roku w Katowicach na każdym kroku była śledzona i obserwowana. Gdziekolwiek się nie ruszyła, towarzyszyło jej dwóch tajemniczych, ubranych na czarno mężczyzn ze słuchawką w uchu. Trwało to dwa tygodnie bez przerwy.

„Takie zastraszanie może mieć różny wpływ na ludzi. Wyobrażam sobie, że ktoś nie decyduje się na aktywizm, na wyrażenie swoich poglądów, bo boi się takich konsekwencji. Może nie chce, żeby Policja pukała do domu, gdzie mieszka z mamą albo z dziećmi. Może nie chce, żeby Policja wiedziała wszystko o jego życiu. Może nie chce czuć tego oddechu na karku każdego dnia, bo myśli sobie, że jego dzisiejsze życie jest cenniejsze niż walka o przyszłość reszty świata".

Mariusz Gierszewski

Dziennikarz. Jego przekonanie, że w swojej karierze był kilkukrotnie inwigilowany, w jednym przypadku potwierdzają twarde dowody. Gdy kolejne osoby z jego otoczenia zaczęły dostawać wezwania do prokuratury, okazało się, że służby wykorzystały jego bazę numerów, by inwigilować około 30 osób: nie tylko adwokatów, polityków czy rzeczników służb, ale również kontakty prywatne. Oficjalnie powodem miało być to, że dziennikarz kontaktował się z osobą oskarżoną o udział w grupie przestępczej. On sam nie wierzy w to wyjaśnienie.

„Każdej służbie zależy na tym, by wiedzieć, czy przypadkiem dziennikarze nie grzebią w jej sprawach. Taka informacja jest bezcenna. Zaczynając od tego, że rzecznik wie, o co będzie pytany, więc może przygotować sobie odpowiednią bajeczkę, a kończąc na tym, że szef w razie nieprawidłowości może wszcząć odpowiednie postępowanie kontrolne. I potem jest w stanie od razu zgasić temat, mówiąc, że już posprzątał, już ukarał winnego. To jest niesamowita władza wiedzieć, czym dziennikarze się zajmują”.

Wojciech Bomba

Aktywista Greenpeace Polska i wolontariusz Strajku Kobiet. Policjantów regularnie spotyka pod swoim domem, kiedy wraca ze współorganizowanych przez siebie protestów. Kiedyś złożyli wizytę jego żonie: powiedzieli jej, że samochód męża brał udział w kolizji drogowej i nie ma z nim kontaktu (co było nieprawdą). Z kolei w czasie szczytu klimatycznego w Katowicach aktywista odkrył pod swoim samochodem urządzenie śledzące.

„Nawet jeżeli wydaje ci się, że nie masz nic do ukrycia, pamiętaj, że materiały pozyskane przez służby specjalne i Policję mogą zostać w taki sposób spreparowane i zmanipulowane, iż nawet rzeczy zupełnie niegroźne mogą zostać przedstawione w sposób odwracający sens historii, która się faktycznie zdarzyła”.

O historiach Eweliny, Mariusza i Wojciecha posłuchasz w podcaście Panoptykon 4.0 pt. *Inwigilacja – niewidzialna przemoc.*

panoptykon.org/podcast/historieinwigilowanych

CENA PRYWATNOŚCI

WYWIAD Z ADAMEM HAERTLE, REDAKTOREM
PROWADZĄCYM SERWISU ZAUFANA TRZECIA STRONA

„W sektorze cyberbezpieczeństwa mówi się, że rzeczywistość ma dwa stany. Albo się jest celem Mosadu, albo nie. Jeśli nie – wystarczą silne hasła, zdrowy rozsądek i absolutne podstawy bezpieczeństwa w sieci. Jeśli tak – nic nam nie pomoże. Prawda jest taka, że jeśli służby będą chciały, to nas podsłuchają, to jedynie kwestia kosztów. Jeśli chcemy czuć się bezpiecznie, musimy doprowadzić do sytuacji, w której koszty tego podsłuchu będą wyższe niż zyski dla służb z uzyskanych informacji".

Krzysztof Story: Przez 12 lat współpracował Pan z polskimi służbami.
Adam Haertle: Niestety, nie jest to materiał na film szpiegowski. Od 2004 do 2017 roku odpowiadałem za bezpieczeństwo danych klientów w UPC, jednym z największych w Polsce dostawców Internetu. Mój dział obsługiwał wszystkie pisma i żądania służb: zarówno te dotyczące dostępu do danych retencyjnych, jak i kontroli korespondencji – czyli tego, co potocznie nazywamy podsłuchami [mogą one dotyczyć zarówno treści rozmów, jak i komunikacji elektronicznej – przyp. red.].

Mieliście dużo pracy? Jak często Wielki Brat chce nas obserwować?
Tutaj musimy podzielić rozmowę na dwa osobne wątki. Zacznijmy od dostępu do danych retencyjnych: billingów telefonicznych, adresów IP i lokalizacji, z których klienci łączyli się do sieci komórkowej lub Internetu. Przez 12 lat mojej pracy zauważyłem gigantyczny wzrost liczby takich zapytań. Ona rośnie wraz ze stopniem wykorzystania technologii w naszym codziennym życiu. Służby za tym podążają, same też uczą się sięgać po te dane i odpowiednio z nich korzystać. Dziś takich zapytań jest ponad milion rocznie.

Dokładnie 1,54 miliona w 2020 roku. Uważa Pan, że to dużo?
Sama liczba nie budzi we mnie wielkich emocji. Moją uwagę przykuwa co innego: jako obywatel, nawet pracując w branży cyberbezpieczeństwa, nie miałem żadnej możliwości weryfikacji tych wniosków – ich zasadności, zgodności z prawem. Dopiero od 2016 roku służby muszą składać do sądów zbiorcze raporty o korzystaniu z tych danych. To iluzoryczna kontrola, ale wcześniej nie było nawet takiej. Często sami musieliśmy weryfikować na przykład to, czy dany policjant ma w ogóle uprawnienia do pozyskania danych retencyjnych.

Co mogliście zrobić z podejrzanymi zapytaniami?
Niewiele. Mogliśmy odrzucić lub zaskarżyć te, które nie mieściły się w granicach prawa. Zwłaszcza we wczesnych latach było ich dużo, przepisy

były mało precyzyjne, a służby same często nie wiedziały, co im wolno, a czego nie. Dostawaliśmy na przykład pytania o dane sprzed 10 lat, które każdy operator nie tylko może, ale wręcz musi kasować, inaczej grożą mu bardzo dotkliwe kary. Na przestrzeni lat widziałem, że poziom edukacji służb powoli rośnie. Pomogła też automatyzacja procesów. Kiedyś to były sterty pism, dziś większość operatorów ma elektroniczne systemy udostępniające te dane. Uniemożliwiają one składanie zapytań „z fantazją", całkowicie wykraczających poza ustawę. Ale kierunek jest tylko jeden: danych jest coraz więcej, a służby coraz chętniej z nich korzystają.

Dane retencyjne to jednak dość proste informacje na temat tego, kto jest właścicielem danego IP czy numeru telefonu. Czasami są to billingi rozmów, także geolokalizacja. Jeśli służby chcą wiedzieć więcej, korzystają z kontroli korespondencji.
To drugi wątek naszej rozmowy, w którym schodzimy o kilka rzędów wielkości. Podsłuchów jest wielokrotnie mniej, z mojej pracy pamiętam pojedyncze wnioski na przestrzeni kwartału. Tylko nieliczne służby w ogóle zgłaszały się po takie dane: przede wszystkim Policja i Agencja Bezpieczeństwa Wewnętrznego, czasami Krajowa Administracja Skarbowa.

Dziewięć uprawnionych do tego służb każdego roku zakłada łącznie około 10 tysięcy podsłuchów. Porównując te liczby do milionów zapytań o dane retencyjne, zapytam: „Dlaczego tak mało?".
Kontrola korespondencji jest dużo trudniejsza technicznie. Często nawet te służby, które wyobrażamy sobie jako najbardziej zaawansowane technicznie, nie są na to gotowe. Bardziej skomplikowane jest też uzyskanie zgody na taki podsłuch. Zgodę musi wyrazić i prokuratura, i sąd. Nawet jeśli akceptują 97 proc. wszystkich wniosków, znacząco wydłuża to procedurę. A przede wszystkim: pozyskane dane trzeba przeanalizować. Najlepszą ochroną przed nadmierną inwigilacją są ograniczone moce przerobowe służb.

Trudniejsze do analizy są dane z sieci telefonicznej czy aktywność w Internecie?
Zdecydowanie ruch internetowy. Oczywiście przesłuchanie kilku godzin rozmów telefonicznych to dużo pracy, ale wystarczą do tego uszy, mózg i notatnik. Tymczasem analiza pakietów internetowych przypomina układanie puzzli, z których tylko co setny element przedstawia jakąkolwiek wartość. Dekadę temu statystyczny klient miał łącze o prędkości 10 Mb/s, wymienialiśmy o wiele mniej danych. Dzisiaj streamujemy filmy w wysokich rozdzielczościach, a otwarcie zwykłego portalu informacyjnego powoduje połączenie z kilkudziesięcioma różnymi serwerami. Gigantyczna ilość danych bardzo utrudnia ewentualną próbę inwigilacji.

Jak często służby decydują się na układanie tych puzzli?
Rzadko. Nawet w UPC, które jest przecież głównie dostawcą Internetu, dominowały wnioski dotyczące rozmów telefonicznych. W całej mojej pracy przypominam sobie dosłownie kilka zapytań o ruch internetowy. Od kiedy większość serwisów internetowych, takich jak portale społecznościowe, banki czy dostawcy poczty elektronicznej, korzystają z szyfrowania (protokołu HTTPS), te dane są często praktycznie bezwartościowe. Jedyne znaczenie mają często metadane: nie sama treść przekazanej informacji, ale to, z jakim serwerem się łączymy. W ten sposób służby mogą ustalić na przykład, z serwerami jakich banków łączy się osoba inwigilowana. Oczywiście dobrze wyposażone służby sobie z tym poradzą. Zgaduję, że te najlepsze w Polsce mogą być w stanie kontrolować ruch internetowy kilku użytkowników miesięcznie. Zdziwiłbym się, gdyby to było znacząco więcej.

Nisko Pan to szacuje.
Bo zdaję sobie sprawę, jak wygląda życie zwykłego policjanta, który cieszy się, że ma w pracy komputer, a nie maszynę do pisania, i nie musi

przynosić z domu papieru do drukarki. Na niskim szczeblu nasze służby są bardzo ubogie technicznie. Bardzo zaawansowane narzędzia są dostępne, ale w małej skali, jak choćby słynny Pegasus czy system RCS [Remote Control System, oprogramowanie do zdalnego przechwytywania danych i komunikacji – przyp. red.], który CBA kupiło od włoskiej firmy Hacking Team. Nie bez powodu Policja najchętniej korzysta właśnie z danych retencyjnych, gdzie cała infrastruktura jest po stronie operatorów i dostawców internetowych.

Prawo zobowiązuje firmy do przechowywania danych retencyjnych przez 12 miesięcy. Kiedyś były to 24 miesiące, często słyszy się postulat wydłużenia tego okresu.
W takich dyskusjach zawsze czyha na nas fundamentalny i piekielnie trudny problem to opowieść o nieskuteczności służb. Postulat wydłużenia tego okresu to przyznanie się, że nasze organy ścigania nie są w stanie w ciągu roku czy dwóch rozwiązać sprawy. Moim zdaniem niewydolność służb nie może być argumentem na rzecz ograniczenia naszej prywatności.

Podczas każdej kolejnej dyskusji o służbach słyszymy, że do skutecznego działania potrzebują one kolejnych kompetencji.
Nadawanie kolejnych przywilejów jest najłatwiejszym rozwiązaniem problemu. Konstruktywna reforma służb jest dużo trudniejsza i – co gorsza – może się nie udać. Nie dziwię się rządzącym, że wybierają prostsze rozwiązania.

Kolejne przywileje rzadko idą w parze z rzetelnym nadzorem i kontrolą.
To oczywiste, że nie wszystkie elementy pracy służb mogą być jawne. Dzisiaj na przykład nie wiemy do końca, jakimi konkretnie narzędziami się one posługują – i to pozwala im działać skutecznie. Ale z tyłu głowy zawsze mamy to podejrzenie, że celem tego działania wcale nie musi być dobro obywateli. Jeśli kontrolę nad służbami, tak jak w Polsce, sprawują głównie politycy, obawa, że zostaną one użyte przeciwko nam, a nie przeciwko przestępcom, jest całkiem uzasadniona.

Wracamy do równowagi między bezpieczeństwem a prywatnością. Jest jakieś rozwiązanie tego dylematu?
W wielu krajach udało się wypracować mechanizmy kontroli nad służbami przez organy mianowane z klucza merytorycznego, a nie politycznego. Wyobrażam sobie powstanie takiego organu także w Polsce, ale patrząc realistycznie, wiem, że nie będzie to łatwy proces. Władza nie lubi dzielić się władzą. Taka zmiana wymaga dużej dojrzałości etycznej i politycznej, której nie spodziewam się po aktualnie istniejących w Polsce ugrupowaniach politycznych.

Czy możemy się jakoś uchronić przed taką motywowaną politycznie inwigilacją?

Jeśli kontrolę nad służbami, tak jak w Polsce, sprawują głównie politycy, obawa, że zostaną one użyte przeciwko nam, a nie przeciwko przestępcom, jest całkiem uzasadniona.

równowagi między bezpieczeństwem a prywatnością. Dzisiejszy przepis o 12 miesiącach jest efektem m.in. pracy Rzecznika Praw Obywatelskich, który w 2014 roku skierował tę sprawę do Trybunału Konstytucyjnego. Ale jeszcze w 2005 roku rozpatrywany był projekt, który mówił o 15 latach retencji. W 2006 roku projekt dotyczył 5 lat. Dla mnie W sektorze cyberbezpieczeństwa mówi się, że rzeczywistość ma dwa stany. Albo się jest celem Mosadu, albo nie. Jeśli nie – wystarczą silne hasła, zdrowy rozsądek i absolutne podstawy bezpieczeństwa w sieci. Jeśli tak – nic nam nie pomoże. Prawda jest taka, że jeśli służby będą chciały, to nas podsłuchają, to jedynie kwestia kosztów. Jeśli chcemy czuć się

bezpiecznie, musimy doprowadzić do sytuacji, w której koszty tego podsłuchu będą wyższe niż zyski dla służb z uzyskanych informacji.

Prosta rada na ograniczenie ewentualnych zysków brzmi: „Nie wychylaj się". Nie chodź na demonstracje, nie pisz artykułów, nie protestuj. Chyba nie do końca o taki efekt mrożący nam chodzi.
Podobnie sensowna jest porada: „Nie używaj telefonu komórkowego". Zgadza się, brak telefonu bardzo utrudnia podsłuchanie telefonu, ale to jest rozumowanie w stylu: „Jak ci się nie podoba, to wyjedź z Polski". Istnieje kilka mniej inwazyjnych sposobów, by utrudnić ewentualną próbę inwigilacji. Jeśli dzwonię do kogoś przez telefon i umawiam się na demonstrację, podsłuchanie takiej rozmowy to dla służb koszt zbliżony do zera. Ale jeśli zwykłą rozmowę telefoniczną zastąpię połączeniem w aplikacji Signal – koszty rosną wielokrotnie. By poznać treść takiej rozmowy, służby musiałyby mieć dostęp do któregoś z telefonów rozmówców. Albo włamać się na niego fizycznie, albo zdalnie, instalując na nim na przykład system Pegasus.

Wtedy możemy spokojnie iść na demonstrację?
W cyberbezpieczeństwie nie ma czegoś takiego jak stuprocentowa skuteczność, ale na pewno minimalizujemy ryzyko. Pegasus jest narzędziem prostym w obsłudze. Operator podaje numer telefonu i zaczyna odbierać wszystkie dane z naszego telefonu. Ich analiza jest skomplikowana, ale pozyskanie – dziecinne proste. Pegasus pozwala więc na inwigilację totalną, ale nie masową. Gdy dochodzimy do tego, że służba, by nas podsłuchać, musi zainwestować w licencję Pegasusa, a wiemy, że tych licencji jest zaledwie kilkadziesiąt, to musimy się zastanowić, czy jesteśmy w grupie kilkudziesięciu najbardziej wartych inwigilacji osób w kraju. Prawdopodobnie nie.

Signala używa też wielu dziennikarzy, ale jest to jednak mało popularna aplikacja. Co z innymi komunikatorami? Messenger, WhatsApp są dużo gorsze?
Nadając etykiety „lepsze" i „gorsze", powinniśmy patrzeć na to, jakie dane zbiera i przechowuje na nasz temat dana aplikacja, bo dokładnie te informacje może kiedyś udostępnić na żądanie służb. W przypadku Signala wszystko wskazuje na to, że przechowuje on tylko datę rejestracji i ostatniego logowania do sieci. Żadne inne ślady nie zostają poza naszym telefonem. Messenger i WhatsApp magazynują mnóstwo metadanych o tym, kiedy i do kogo dzwoniliśmy czy pisaliśmy. Messenger w dodatku nie jest szyfrowany end-to-end, co oznacza, że Facebook na żądanie amerykańskich służb może dać im dostęp do treści naszych rozmów. W przypadku Signala jest to technicznie niemożliwe.

Nawet jeśli korzystamy z Signala, archiwum rozmów zostaje na naszym telefonie. Jak go zabezpieczyć?
Niekoniecznie zostaje, bo możemy włączyć tryb znikających wiadomości, po których nie ma śladu po ustalonym czasie – godzinie czy minucie. Bezpieczniej jest też we wrażliwych kwestiach stawiać na połączenia głosowe, a nie

Jeśli dzwonię do kogoś przez telefon i umawiam się na demonstrację, podsłuchanie takiej rozmowy to dla służb koszt zbliżony do zera. Ale jeśli zwykłą rozmowę telefoniczną zastąpię połączeniem w aplikacji Signal – koszty rosną wielokrotnie. By poznać treść takiej rozmowy, służby musiałyby mieć dostęp do któregoś z telefonów rozmówców. Albo włamać się na niego fizycznie, albo zdalnie, instalując na nim na przykład system Pegasus.

czaty. Pomysłów na zwiększenie bezpieczeństwa jest zresztą wiele. Ja rekomenduję Signala, dlatego że jest prosty w obsłudze, nie wymaga konfiguracji, uruchomiony pierwszy raz na domyślnych ustawieniach działa w sposób maksymalnie bezpieczny.
Wracając do telefonów: zabezpieczajmy je, korzystając z biometrii albo z kodu PIN o co najmniej 6 cyfrach. Zabezpieczenie odciskiem palca ma jednak słaby punkt: możemy „się przypadkowo potknąć" na komisariacie (ktoś wykręci nam rękę i przyłoży ją do czytnika). W ciekawą funkcję wyposażone są iPhone'y: kiedy podejrzewam, że coś mi grozi, wystarczy pięć razy szybko nacisnąć guzik zasilania. Uruchomi się wtedy tryb awaryjny, który wyłącza biometrię. Polecam przetestować w domu!

Od kilku lat pisze Pan o tych sposobach i świecie cyberbezpieczeństwa na Zaufanej Trzeciej Stronie, prowadzi szkolenia. Czy w kontekście służb takie przeciąganie liny i szukanie nowych, bezpieczniejszych aplikacji naprawdę jest naszym obowiązkiem?
W idealnym świecie by nie było. W tym, w którym żyjemy, nawet to nie daje nam gwarancji, choć znacząco zmniejsza ryzyko. W historii wpadki zdarzały się nawet pracownikom najlepszych agencji wywiadowczych. Nawet ci ludzie, całe życie szkoleni do tego, by nie zostawiać śladów, robili błędy, zapominali o zasadach, naruszali procedury. Nic dziwnego, że będą to też robić zwykli obywatele. Tutaj wszystko zależy od tego, jak wiele wysiłku służby są w stanie włożyć, by wykorzystać nasze słabości. W naszym interesie jest, by nie sprzedać się zbyt tanio.

Rozmawiał Krzysztof Story.

20 LAT POLITYKI STRACHU
OD WTC DO USNARZA GÓRNEGO

WOJCIECH KLICKI, ANNA OBEM

Wykorzystywanie strachu w polityce jest skuteczne, bo sprawia, że racjonalne argumenty przestają działać. Zamiast trzeźwo ocenić realny stopień zagrożenia – decydujemy pod wpływem emocji. Godzimy się na przyznawanie służbom kolejnych uprawnień – bez gwarancji, że zostaną wykorzystane w słusznym celu. Jesteśmy gotowi zrezygnować z wolności i prywatności, byleby tylko zwiększyć swoje poczucie bezpieczeństwa.

Mija 20 lat od zamachu na World Trade Center. Dzięki telewizjom informacyjnym wszyscy byliśmy naocznymi świadkami, niemal uczestnikami tej tragedii. Obrazki ludzi skaczących z najwyższych pięter WTC wryły się w pamięć całych pokoleń, wzbudzając strach silniejszy od mało spektakularnych zgonów, np. w wypadkach samochodowych czy na oddziałach onkologicznych.

Doświadczenie zbiorowej traumy nie skończyło się wraz z posprzątaniem zgliszczy – trwa do dziś. Zamach na WTC okazał się bowiem idealnym pretekstem dla polityków, którzy przekonali wyborców państw zachodnich, że powinni się bać.

Efektem ubocznym tej polityki jest zgoda na to, że terroryści znajdują się poza marginesem praw człowieka – można ich pozbawić prywatności czy torturować. Czas pokazał, że „terrorystami" mogą stać się nawet osoby uciekające przed wojną, biedą i prześladowaniami w swoim kraju. 20. rocznica zamachu na World Trade Center to doskonały moment na podsumowanie długofalowych efektów polityki strachu.

W ciągu ostatnich 20 lat w zamachach terrorystycznych w Europie zginęło ok. 600 osób. Tylko w ubiegłym roku na polskich drogach poniosło śmierć 2 500 osób. W latach 2005–2014 w Stanach Zjednoczonych co roku średnio 737 osób umierało na skutek... upadku z łóżka, 11 000 w strzelaninach, a tylko 9 w zamachach islamistycznych[1]. Jeśli patrzeć na same liczby, strach przed terroryzmem jest bez pokrycia. Dlaczego zatem się boimy? Odpowiedź jest równie prosta, co – nomen omen – straszna: bo podsycanie strachu opłaca się politykom. Wystarczy wskazać wroga i pokazać, jak skutecznie będzie się z nim walczyło.

Fałszywa alternatywa

Po zamachu na WTC polityka strachu – nie tylko w USA, ale też w Europie – nabrała wiatru w żagle.

[1] https://www.huffpost.com/entry/the-freakonomics-of-extre_b_11821634

Przestraszeni ludzie od 20 lat usprawiedliwiają programy masowej inwigilacji przekonani, że „albo wolność, albo bezpieczeństwo". Nie był w stanie tego zmienić Edward Snowden, który w 2013 roku ujawnił, że inwigilacja prowadzona jest na tak szeroką skalę, że właściwie każdy i każda z nas może być podejrzany o terroryzm.

Nie udało się też Williamowi Binneyowi, sygnaliście z amerykańskiej Agencji Bezpieczeństwa Narodowego, który udowodnił, że amerykański wywiad – zamiast skutecznie typować osoby mające związek z przestępczością i im się przyglądać – gubi się w masie gromadzonych przez siebie informacji. Funkcjonariusze przygnieceni niepotrzebnie rejestrowanymi danymi zarzucili analizę kierunkową na rzecz prostego przeszukiwania baz danych, co daje mnóstwo nic nieznaczących trafień. To właśnie dlatego amerykańska Agencja Bezpieczeństwa Narodowego nie była w stanie zapobiec zamachowi zorganizowanemu w Bostonie przez braci Carnajewów, mimo że przechwyciła ich e-maile i rozmowy.

„Ujawniliśmy, że to jest system szpiegowski skierowany nie przeciwko terrorystom, ale niewinnym ludziom na całym świecie. Nie ma to nic wspólnego ze zwalczaniem terroryzmu" – Glenn Greenwald[2].

W Europie sytuacja wygląda niewiele lepiej. Pod pretekstem ścigania terrorystów służby mogą sięgać po informacje o lokalizacji i aktywności telefonicznej oraz internetowej każdego i każdej z nas. Niedawno takie szerokie pozyskiwanie danych telekomunikacyjnych zakwestionował Trybunał Sprawiedliwości Unii Europejskiej jako niezgodny z Kartą praw podstawowych. Co nie oznacza, że służby w państwach członkowskich zaprzestały takich praktyk (np. w Polsce od lat uprawnienia służb są zwiększane pod pretekstem m.in. zagrożenia terrorystycznego).

Strach narzędziem polityki

Wykorzystywanie strachu w polityce jest skuteczne. Strach sprawia, że poszukujemy obrońcy. Racjonalne argumenty przestają do nas trafiać, zamiast trzeźwo ocenić realny stopień zagrożenia – działamy pod wpływem emocji. Potrzebny jest tylko Inny: wróg, przed którym trzeba nas ochronić.

Polityka zarządzania strachem w Polsce przybrała na sile w 2015 roku – podczas kampanii przed wyborami parlamentarnymi, która nałożyła się w czasie na trwający w Europie kryzys uchodźczy. To wtedy politycy postawili znak równości między uchodźcami a terrorystami. „Na uchodźcę – muzułmanina należy patrzeć jak na potencjalnego terrorystę" (Beata Szydło), „Będą wysadzać w powietrze polskie niemowlęta" (Jarosław Gowin) i „Doprowadzą do upadku cywilizacji łacińskiej" (Jarosław Kaczyński)[3]. Zadziałało: PiS wygrał wybory, po czym ustawą inwigilacyjną i antyterrorystyczną zwiększył uprawnienia służb. Dziwnym trafem akurat w czasie prac legislacyjnych nad tym drugim aktem prawnym doszło w Polsce do dwóch prób zamachów: we wrocławskim autobusie podłożono bombę, próbowano też podpalić komisariat w Warszawie. Trudno o wygodniejszy zbieg okoliczności.

Strach podsycony przy okazji kryzysu uchodźczego został z nami na dłużej. W 2017 roku zamach terrorystyczny okazał się najczęściej wybieraną odpowiedzią na pytanie, czego Polki i Polacy boją się najbardziej. Tę odpowiedź wskazało 38 proc. ankietowanych. Okazało się, że boimy go bardziej niż utraty pracy (22 proc.) czy tego, że zostaniemy ofiarą przestępstwa (18 proc.)[4].

Odwet na prawach człowieka

Amerykanie wzięli srogi odwet za zamach na swój kraj – ale nie tylko na organizacji, która za niego odpowiadała. Podczas tzw. wojny

[2] https://edition.cnn.com/videos/world/2013/10/28/glenn-greenwald-amanpour.cnn
[3] https://www.batory.org.pl/upload/files/Programy%20operacyjne/Forum%20Idei/Zarzadzanie%20strachem.pdf
[4] https://www.polityka.pl/tygodnikpolityka/kraj/1702906,1,sondaz-polityki-czego-polacy-boja-sie-najbardziej.read

z terroryzmem wielokrotnie dopuszczali się tortur zwanych enigmatycznie „rozszerzonymi metodami przesłuchiwania". W więzieniu Guantanamo latami przetrzymywani i torturowani byli ludzie niemający jakiegokolwiek związku z terroryzmem. Jednym z nich był Jemeńczyk Mansoor Adayfi – niedoszły student, który podczas badań w Afganistanie został porwany przez afgańskich watażków i przekazany w ręce CIA. Miał wtedy 19 lat. W Guantanamo spędził ich ponad 14.

Wszystko wskazuje na to, że swój udział w torturach miały też władze Polski, które pozwoliły na to, by w naszym kraju mieściło się tajne więzienie CIA. Przebywał w nim m.in. Abu Zubajda, który do dziś jest osadzony w Guantanamo, mimo że nie został oficjalnie oskarżony o żadne przestępstwo.

Mimo wieloletnich starań obrońców praw człowieka nikt w Polsce nie poniósł konsekwencji za przyzwolenie na tortury. A opinia publiczna w ogóle się tym nie interesuje, bo problem dotyczy Innych, którym prawa człowieka nie przysługują.

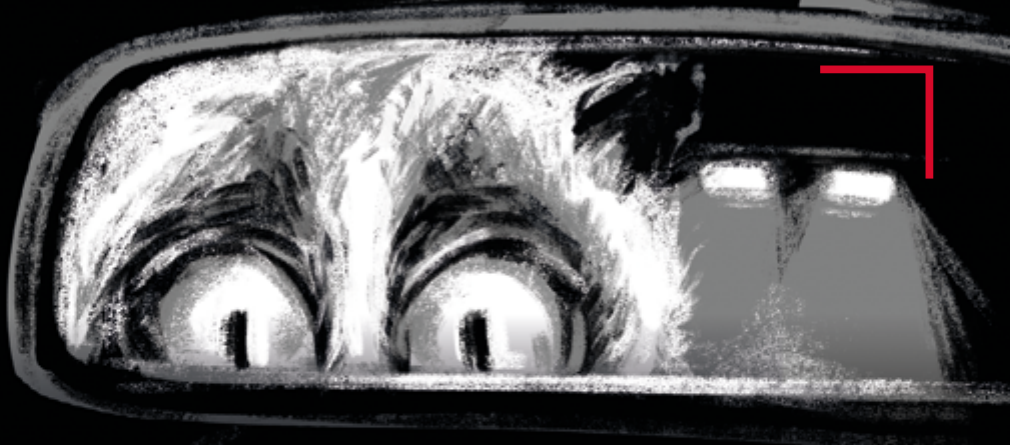
Strach na granicy

Polscy politycy dostali ostatnio nową amunicję do swojej polityki: na granicy polsko-białoruskiej pojawili się uchodźcy m.in. z Afganistanu. Los desperacko poszukujących pomocy ludzi wielu osobom nie jest obojętny – o czym świadczy aktywność organizacji społecznych wspieranych zbiórkami na pomoc prawną i rzeczową. Jednak na każdą osobę sympatyzującą z uchodźcami na granicy znajdzie się przynajmniej jedna, która – tak jak politycy kilka lat temu – stawia znak równości między uchodźcami a terrorystami. Los Innego jest bez znaczenia, jeśli tylko oddalimy zagrożenie.

Na kryzys na granicy nie ma łatwych rozwiązań, ale czy konieczność „ochrony integralności granic Rzeczypospolitej" to wystarczający powód, żeby odmawiać człowieczeństwa ludziom potrzebującym pomocy? Zamiast pozwalać im umierać na granicy i wprowadzać stan wyjątkowy, należałoby – zgodnie z obowiązującymi w Polsce przepisami – przyjąć ich wnioski o przyznanie statusu uchodźców. I wykorzystać szerokie uprawnienia służb do weryfikacji, czy wśród przybyłych znajdują się takie, które mogą stanowić realne zagrożenie.

Inwigilacja i tortury są możliwe, bo oficjalnie wymierzone są nie w nas, tylko w Innych: „terrorystów" i „przestępców". Oczywiście to pułapka, bo masowa inwigilacja nie odróżnia nawet najbardziej praworządnego obywatela od przestępcy recydywisty. Wypchnięcie Innych – czy są podejrzanymi o terroryzm, czy po prostu bezbronnymi ludźmi na granicy – poza margines praw człowieka, z przyrodzoną każdemu godnością, to najsmutniejszy efekt minionych 20 lat.

Tekst został opublikowany na stronie panoptykon.org i w Gazecie Wyborczej we wrześniu 2021 roku.



Nie jesteś zagrożonym gatunkiem,
a twój tryb życia, umaszczenie i rytuały godowe
nie powinny nikogo interesować.

A jednak! Policja ma nieograniczony i niekontrolowany
dostęp do twojej historii kontaktów i rozmów, billingów
i lokalizacji. Podgląda cię, szufladkuje i wyciąga wnioski.

Czy naprawdę chcesz, żeby traktowano cię jak zwierzę?

Fundacja Panoptykon od ponad 12 lat rzuca
światło na działanie służb i walczy o prawo,
które zapewni kontrolę nad inwigilacją.

Dowiedz się więcej na panoptykon.org
i zamów newsletter PanOptyka
(panoptykon.org/newsletter).

FUNDACJA
PANOPTYKON

ISBN: 978-83-938554-8-3