KONTROLUJEMY KONTROLUJĄCYCH

FUNDACJA PANOPTYKON

Publikacja powstała dzięki wsparciu:
programu Obywatele dla Demokracji finansowanego z Funduszy EOG

ICELAND
LIECHTENSTEIN
NORWAY
eea grants

FUNDACJA
BATOREGO

POLSKA FUNDACJA
DZIECI I MŁODZIEŻY

Trust for Civil Society in Central and Eastern Europe

TRUST FOR CIVIL SOCIETY
IN CENTRAL AND EASTERN EUROPE

KONTROLUJEMY KONTROLUJĄCYCH

5 LAT FUNDACJI PANOPTYKON

SPIS TREŚCI

Tak się złożyło, że kiedy Fundacja Panoptykon rozpoczynała swoją działalność, miałam okazję rozmawiać z grupką inicjatorów. Byłam trochę sceptyczna, bo już się napatrzyłam na różne inicjatywy pełne słomianego zapału: dużo szumu, mało porządku, systematyczności, uporczywego, powtarzalnego, mozolnego ociosywania rzeczywistości. I tu się gruntownie pomyliłam: w przypadku Panoptykonu systematyczność, konsekwencja, powtarzalność i cierpliwość zagwarantowały nie tylko obecność w życiu publicznym, ale i przesądziły o wyrobieniu sobie wysokiej marki wśród organizacji pozarządowych i zadecydowały o sukcesach w walce z administracją, niecierpiącą przejrzystości.

Panoptykon ostrzega przed oswojeniem z kolejnymi przejawami kontroli nad naszym życiem i erozją wolności – w obliczu nowych technologii i starych przyzwyczajeń rządzących. Wiele zrobił na rzecz uświadomienia skali zjawisk nadzorczych, propagowania przejrzystości życia publicznego (zwłaszcza w zakresie ujawniania skali zjawiska inwigilacji, zbierania danych o obywatelach, działań policji i służb specjalnych), ujawnienia patologii i nieefektywności istniejących prawnych gwarancji dla jednostek i iluzoryczności zapór chroniących przed ekspansją władzy gromadzącej informacje „na wszelki wypadek” i niechętnej jakiejkolwiek kontroli.

Ewa Łętowska, pierwsza Rzecznik Praw Obywatelskich, sędzia Trybunału Konstytucyjnego w stanie spoczynku

WPROWADZENIE

W ciągu pięciu lat Fundacja Panoptykon przeszła długą drogę: od kilkuosobowej inicjatywy do profesjonalnej organizacji. W tym czasie nasz zespół powiększył się z dwóch do dziewięciu osób, kawiarniany stolik zamieniliśmy na biuro, a spontaniczne akcje obudowaliśmy systematycznymi metodami, standardami i procedurami. Nie wszystko jednak się zmieniło – pozostało przekonanie, że dzięki wiedzy, zaangażowaniu i determinacji naprawdę można zmienić rzeczywistość. A przynajmniej trochę ją „ociosać".

Zapraszamy na ekspresowy przegląd pięciu lat z życia organizacji, która postanowiła zmierzyć się z wyzwaniami związanymi z życiem w społeczeństwie przesiąkniętym nadzorem. Tłumaczymy misję Fundacji Panoptykon; przypominamy nasze najważniejsze działania, sukcesy, z których jesteśmy dumni, i porażki, na których najwięcej się nauczyliśmy; opisujemy wyzwania i zdradzamy plany na przyszłość.

Mamy nadzieję, że to będzie inspirująca lektura!

ŻYCIE POD NADZOREM

Niezliczone bazy danych, kamery monitoringu, Internet pełen cyfrowych śladów, informacje z kart płatniczych, statusy na portalach społecznościowych, inteligentne domy, telefony pamiętające nasze kroki. Niemal każdy ruch to nowe dane, które są zapisywane, wymieniane i kojarzone ze sobą. Tak rodzi się nadzór: możliwość przewidywania naszych decyzji i kontrolowania zachowań.

W rozgrywce o kontrolę nad naszym życiem biorą udział i państwo, i biznes. Ich działania coraz głębiej się przenikają: biznes wkracza w sfery wcześniej zarezerwowane dla instytucji publicznych, a państwo korzysta z informacji, które dobrowolnie powierzamy firmom. Sami również ulegamy pokusie kontrolowania innych: obserwujemy, nagrywamy, namierzamy – w ten sposób rozbudowujemy bazę informacji, jakimi dysponują najwięksi gracze. I nakręcamy spiralę nadzoru.

Krok po kroku jesteśmy oswajani z kolejnymi przejawami nadzoru. W imię wygody lub poczucia bezpieczeństwa oddajemy coraz więcej wolności. Czasem dobrowolnie, czasem pod presją rynku lub państwa. Skoro nie robisz nic złego, chyba nie masz nic do ukrycia? Przecież to wszystko dla Twojego bezpieczeństwa (wygody, oszczędności).
W czym problem?

Wierząc, że więcej mamy do zyskania niż stracenia, łatwo ulec tej manipulacji. Tymczasem gra toczy się o najwyższą stawkę: wolność. Nie tylko abstrakcyjną wartość, ale przede wszystkim realną możliwość decydowania o sobie i własnym życiu: od błahych wyborów konsumenckich, przez decyzje polityczne, aż po fundamentalne życiowe wybory (jak te dotyczące pracy czy kierunku studiów). W dłuższej perspektywie to batalia o kształt społeczeństwa, w którym żyjemy i w którym będą żyć kolejne pokolenia.

Jakie największe problemy niesie współczesny nadzór?

1. **Ingerencje w prywatność:** śledzeni na każdym kroku, czy sobie tego życzymy, czy nie, stopniowo tracimy kontrolę nad naszymi danymi i ich „podwójnym życiem" w kolejnych bazach danych. Przekazywane z rąk do rąk odrywają się od naszego prawdziwego „ja". A jednak to na ich podstawie instytucje publiczne i firmy podejmują decyzje, które bezpośrednio nas dotyczą.

2. **Złudzenie wolności:** wielu z nas żywi przekonanie, że możemy dokonywać wolnych wyborów; tymczasem coraz częściej stajemy się towarem na rynku wymiany informacji i jesteśmy sterowani tak, by podejmować decyzje zgodne z naszym „profilem". Oswaja się nas z życiem w społeczeństwie pełnym bierności i konformizmu.

3. **Pozorne rozwiązania:** słyszymy, że dzięki nowoczesnym rozwiązaniom można łatwo rozwiązać skomplikowane społeczne problemy – tymczasem większość z nich jedynie te problemy maskuje, pochłaniając zasoby, które można przeznaczyć na wdrażanie mniej oczywistych, ale skuteczniejszych rozwiązań.

4. **Dyskryminacja i błędy systemu:** nie mamy kontroli nad tym, jak nasze dane zostaną zinterpretowane i jakie będą tego konsekwencje: uznanie za osobę podejrzaną? ograniczenie dostępu do informacji? wykluczenie? Im bardziej ufamy algorytmom, tym więcej ryzykujemy, korzystając z systemów opartych na automatycznej analizie danych i profilowaniu.

5. **Manipulacja strachem:** mamieni obietnicami, że kolejne narzędzia nadzoru zapewnią nam spokój i poczucie bezpieczeństwa, pielęgnujemy własne lęki i coraz bardziej uzależniamy się od „środków uspokajających".

Nie jesteśmy gotowi na to, by mierzyć się z nadzorem, który przenika wszystkie dziedziny życia: z początku wsiąka w nie dyskretnie, z czasem wkracza coraz odważniej. Nie wykształciliśmy społecznych mechanizmów obrony przed nadużyciami. Nie chroni nas dostatecznie również prawo – wręcz przeciwnie: pod hasłem bezpieczeństwa czy nowoczesności jest ono instrumentalnie wykorzystywane do wprowadzania kolejnych systemów nadzoru.

Czy wzrost nadzoru jest cywilizacyjną koniecznością, z którą trzeba się po prostu pogodzić? Wiele osób tak uważa Jednak nie wszyscy…

Szczegóły naszego codziennego życia zaczynają być coraz bardziej przejrzyste dla inwigilujących nas instytucji, za to ich działania stają się dla nas coraz mniej uchwytne. (…) Władza przemieszcza się z szybkością sygnału elektronicznego, co sprawia, że transparentność jednych rośnie, a innych maleje.

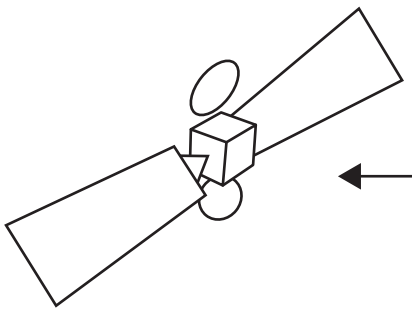
Zygmunt Bauman, twórca teorii płynnej nowoczesności

Subtelne, na początku niewidzialne, szkody, erozja wolności polegają na tym, że człowiek zaczyna zmierzać w kierunku konformizmu, dostosowania swojego zachowania. (…) Nadzór zabija zmianę, odwagę zmiany, odwagę innych zachowań. (…) Zaczynamy hodować społeczeństwo nadzorowane, które jest przede wszystkim społeczeństwem kalkulującym: „Jak wypadam w oczach tego Wielkiego Brata, który mnie nieustająco monitoruje? Jak to zostanie wykorzystane w odniesieniu do moich szans zawodowych i społecznych?”.

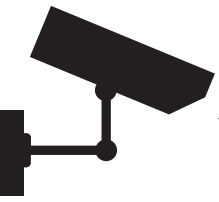
Irena Lipowicz, Rzecznik Praw Obywatelskich

JAK JESTEŚMY NADZOROWANI ?

Z dala od naszego pola widzenia mają nas wszystkich na oku. Kontrolują sygnały naszych telefonów, obserwują trasy naszego przemieszania się i robią coraz więcej zdjęć.



Towarzyszą nam niemal wszędzie: miejskie, sklepowe, szkolne, kawiarniane. Oficjalnie – mają poprawiać bezpieczeństwo, choć do tej pory nie udało się dowieść, że naprawdę to robią. W praktyce prowokują podglądactwo i oswajają nas z poczuciem, że w monitorowaniu każdego naszego kroku nie ma nic dziwnego.



Czasem sami wchodzimy w rolę nadzorujących (korzystając z Google Glass i innych narzędzi). Możliwość podglądania i rejestrowania jest naprawdę kusząca. Dokumentujemy więc wszystko, wszędzie, zawsze, dostarczając firmom i państwu informacji o nas, o naszych bliskich i o nieznanych nam ludziach znajdujących się w zasięgu naszych nadzorujących narzędzi.

Nigdy nie możemy być pewni, jak, gdzie i przez kogo jesteśmy obserwowani i nadzorowani. Jedno nie ulega wątpliwości: nasze myśli, opinie, pomysły i plany interesują tych, którzy chcieliby nimi kierować: zarówno biznes, jak i państwo.

Najpowszechniejsze narzędzie rozrywki, pracy i komunikacji – wie o nas prawie wszystko. Wiecznie podłączony do Internetu pozwala zbierać o nas dowolne dane: i te, które sami udostępniamy, i te, o których istnieniu nawet nie wiemy. Dzięki „cyfrowemu łupieżowi” można nas zidentyfikować i śledzić. W sieci cała nasza komunikacja przechodzi przez czyjeś ręce: nawet prywatne maile są tylko pocztówką, z której treścią może się zapoznać każdy, kto pośredniczy w jej doręczeniu.

Bardzo osobiste narzędzie, zawsze przy nas – w każdej chwili może poinformować, gdzie jesteśmy i z kim się komunikujemy: operatora (który przechowuje dane o naszych połączeniach), policję i inne służby (gdy tylko się nami zainteresują), producentów oprogramowania, które kupujemy razem z telefonem lub ściągamy, a czasem również naszych bliskich, którzy chcieliby mieć nas na oku.

Do naszych emocji (najczęściej strachu) odwołują się ci, którzy chcą zaostrzać nadzór nad społeczeństwem. Obietnica życia w bezpiecznym świecie, bez lęku i ryzyka, ma uzasadniać odbieranie nam kolejnych swobód i wolności.

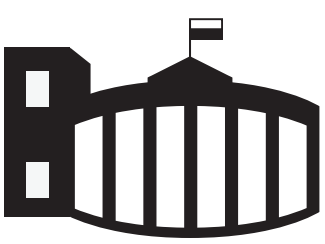
Palec to najpopularniejszy nośnik naszego biometrycznego śladu (innymi są: tęczówka oka, głos, tętno krwi, siatka żył). Odcisk palca wykorzystujemy już nawet do odblokowywania telefonu i drobnych płatności. Ignorujemy przy tym fakt, że zostawiamy go wszędzie, a jego podrobienie dla osoby znającej się na rzeczy nie jest szczególnym wyzwaniem.

Nasz portfel jest coraz cieńszy, ale mieści kolejne karty, które dokładnie liczą, ile i na co wydajemy. Wszystko po to, by biznes mógł jeszcze skuteczniej podsuwać nam kolejne produkty. Do tego karty wyposażone w czipy RFID są podatne na zdalne przejęcie kontroli.

Dowód osobisty, karta miejska, identyfikator z pracy pozwalają nas zidentyfikować, a jednocześnie zasilają ogromne bazy wiedzy o nas i naszych działaniach. W wielu z nich przechowuje się więcej informacji, niż to niezbędne, wiele podmiotów wymienia się tymi danymi bez naszej kontroli.

Oczywisty obiekt, który można wykorzystać do śledzenia tego, gdzie w danym momencie jesteśmy. Dlatego w samochodach coraz częściej znajdziemy nadajniki GPS. Ruch drogowy to też jeden z ulubionych kadrów kamer monitoringu, które nie ograniczają się do namierzania kierowców przejeżdżających na czerwonym świetle. Standardem staje się automatyczne odczytywanie numerów rejestracyjnych.

Rządzący podejmują decyzje, kogo, jak, po co i za ile nadzorować. Do publicznych instytucji trafia też najwięcej informacji pochodzących „z nadzoru”. Jednocześnie to właśnie one są w stanie ochronić nas przed nieuczciwym i głodnym danych biznesem.



Fundacja Panoptykon jest wciąż młoda i niespokojna, jednak swoje palące pytania stawia w przemyślany sposób. Potrzeba mocnych nerwów i rzetelnego rozpoznania, żeby mierzyć się z nadzorem (*surveillance*) – jednym z najbardziej wymagających i aktualnych wyzwań w sferze etyki i polityki.

David Lyon, czołowy badacz i teoretyk społeczeństwa nadzorowanego

Panoptykon jest wzorcowym przykładem nowego typu organizacji społecznej i obywatelskiej. Nowym, bo Katarzyna Szymielewicz, prezeska Fundacji, wraz ze swymi współpracownikami wie, że najważniejszym orężem w promowaniu ważnych spraw jest wiedza. Nie wystarczy stwierdzić, że kwestie prywatności, inwigilacji mają kluczowe znaczenie w cyfrowym świecie. Trzeba to jeszcze udowodnić, docierając do opinii publicznej precyzyjnymi, racjonalnymi argumentami.

Obserwowałem przez lata, jak Panoptykon cierpliwie i konsekwentnie buduje zasoby wiedzy, rozwija eksperckie kompetencje i uczy się praktyk skutecznego zaangażowania w sprawy publiczne. W rezultacie organizacja ta stała się niezbędnym punktem referencyjnym każdej debaty o problemach i wyzwaniach społeczeństwa informacyjnego.

Edwin Bendyk, publicysta

OTWIERAMY PANOPTYKON

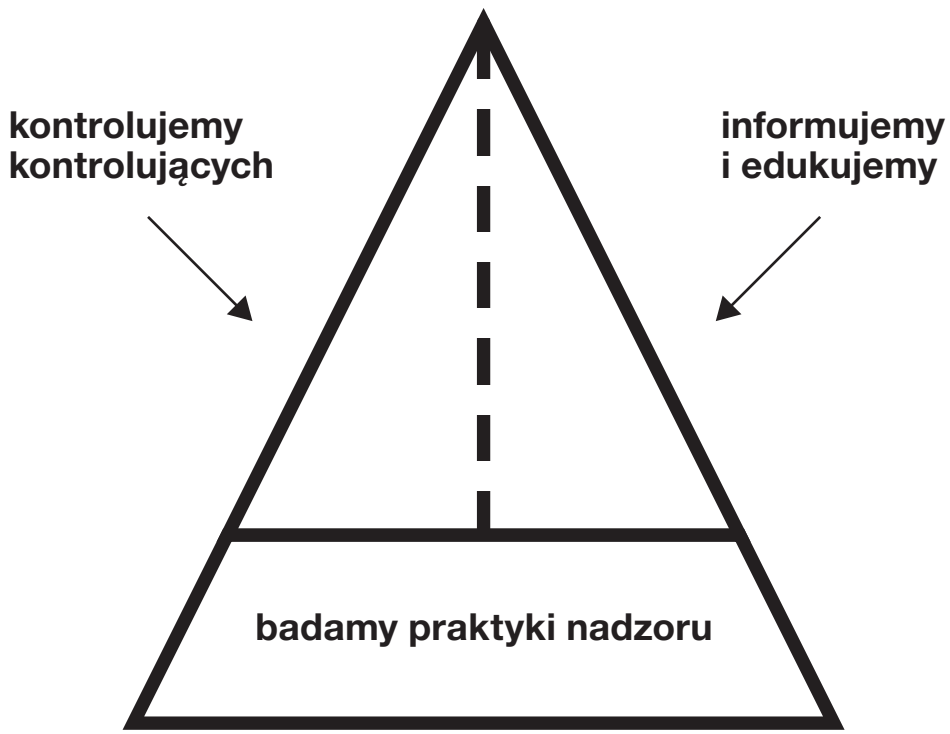
Jesteśmy przekonani, że nadzór powinien mieć granice. Nie powinien być stosowany bez naszej wiedzy, poza społeczną kontrolą, poza ramami prawnymi. Nowe technologie powinny służyć ludziom, a nie być wykorzystywane przeciwko nim. Fundacja Panoptykon wyrosła z poczucia, że negatywnych społecznych zjawisk nie powinno się ignorować, oraz z przekonania, że dzięki wiedzy, zaangażowaniu i determinacji można je ograniczać, wpłynąć na otaczającą rzeczywistość.
Za cel postawiliśmy sobie stanie na straży wolności i praw człowieka w społeczeństwie nadzorowanym.

Staramy się ten cel osiągnąć, działając na trzech poziomach:

1. **Badamy praktyki nadzoru** – śledzimy doniesienia medialne i badania naukowe, współpracujemy z ekspertami i prowadzimy własne badania. Korzystamy z dostępu do informacji publicznej – uparcie zadajemy kolejne pytania. Słuchamy tego, co inni mają do powiedzenia. Staramy się zrozumieć i wyjaśnić, jak działa nadzór i jakie pociąga za sobą konsekwencje. To jest nasza baza i punkt wyjścia do podejmowania innych działań.

2. **Kontrolujemy kontrolujących** – obserwujemy tworzone i obowiązujące prawo, działania władz publicznych i prywatnych firm. Opiniujemy projekty aktów prawnych, krytykujemy niebezpieczne rozwiązania i zabiegamy o systemową zmianę prawa. Piętnujemy nadużycia i zaniedbania związane z nadzorem. Działamy samodzielnie i w koalicjach z innymi organizacjami.

3. **Informujemy i edukujemy** – zwracamy uwagę na problemy związane z nadzorem w debacie publicznej. Informujemy o zagrożeniach i niepokojących praktykach na stronie internetowej, w newsletterze, mediach społecznościowych i na naszym blogu. Współpracujemy z mediami, odpowiadając na pytania dziennikarzy i zachęcając ich do podejmowania trudnych panoptykonowych tematów. Organizujemy seminaria, dyskusje, warsztaty. Tworzymy i udostępniamy materiały edukacyjne, opracowania tematyczne, infografiki i materiały filmowe.



Przy tak zróżnicowanych metodach działania Fundacja Panoptykon musi łączyć w sobie elementy i kompetencje z różnych światów. Działamy jak:

§ kancelaria prawna,

firma lobbingowa,

portal informacyjny,

agencja reklamowa,

ośrodek badawczy,

firma szkoleniowa i agencja eventowa w jednym.

Od nich wszystkich różni nas jednak podstawowa cecha organizacji pozarządowej: jesteśmy niezależni w wyznaczeniu celów i nie działamy dla zysku. Jednak jak każda profesjonalna organizacja musimy znać się też na

zdobywaniu finansowania i zarządzaniu oraz – co w naszej „branży" szczególnie ważne –

nowych rozwiązaniach technologicznych.

W przypadku niedużej organizacji, dysponującej ograniczonym budżetem, połączenie tych licznych kompetencji stanowiło spore wyzwanie. Naszą odpowiedzią było zbudowanie mocnego merytorycznie i zaangażowanego zespołu, w którym każdy jest w stanie działać na kilku frontach i podejmować zróżnicowane zadania.

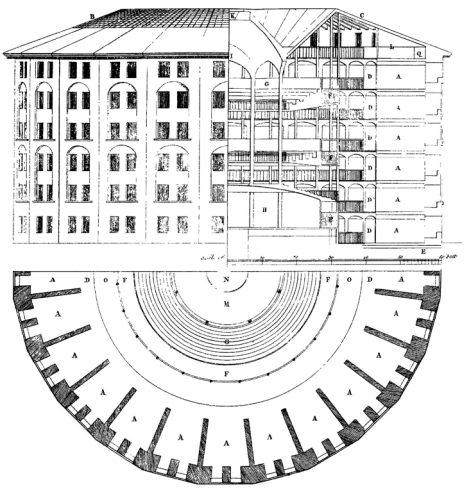
W naszej codziennej pracy liczą się standardy. Te trzy są dla nas najważniejsze:

1. **Niezależność** – w oparciu o naszą misję sami wyznaczamy cele, metody działania i konkretne zadania do zrealizowania. Dla organizacji strażniczej jest to podstawa rzetelnego i odpowiedzialnego działania, ale również wyzwanie – i w codziennej pracy, i w poszukiwaniu źródeł finansowania.

2. **Otwartość** – mamy swoje przekonania, ale zawsze jesteśmy otwarci na dyskusję i argumenty naszych adwersarzy. Chętnie rozmawiamy z przedstawicielami służb bezpieczeństwa, biznesu internetowego i każdym, kto zna nadzór od drugiej strony. Staramy się też działać w możliwie przejrzysty sposób, regularnie publikując informacje o tym, co robimy, udostępniając raporty finansowe, prowadząc Biuletyn Informacji Publicznej i cierpliwie odpowiadając na zadawane pytania.

3. **Współpraca** – działamy zespołowo – i w ramach organizacji, i kiedy wychodzimy na zewnątrz. Dlatego aktywnie angażujemy się w prace koalicji European Digital Rights i współpracujemy z kilkunastoma organizacjami z różnych krajów (np. Electronic Frontier Foundation, La Quadrature du Net, Bits of Freedom, Chaos Computer Club, Digitale Gesellschaft). W Polsce również współdziałamy z wieloma organizacjami (w tym Helsińską Fundacją Praw Człowieka, Amnesty International Polska, Centrum Edukacji Obywatelskiej, Fundacją Nowoczesna Polska, Centrum Cyfrowym, Fundacją Wolnego i Otwartego Oprogramowania) oraz instytucjami o zbieżnej misji (Rzecznikiem Praw Obywatelskich, GIODO, Najwyższą Izbą Kontroli).

Przewrotną inspiracją dla nazwy Fundacji Panoptykon była XVIII-wieczna koncepcja idealnego więzienia stworzona przez Jeremy'ego Benthama. Panoptykon to budynek w kształcie pierścienia, podzielony na cele skazańców, którzy zawsze pozostają w polu widzenia strażnika. Sam strażnik – nadzorca – miał przebywać w centralnej wieży i pozostać niewidoczny, tak by nigdy nie było wiadomo, w którą stronę spogląda. Bentham był przekonany, że nieprzerwana kontrola więźniów w praktyce nie jest możliwa, ale zakładał, że ten sam efekt można osiągnąć, wzbudzając w nich poczucie, że w każdej chwili mogą być obserwowani. Projekt Benthama posłużył za inspirację przy tworzeniu zamkniętych instytucji, a dla Michela Foucaulta okazał się również użyteczną metaforą otaczającej rzeczywistości. Obecność Panoptykonu w nazwie fundacji ma przypominać o ciemnym obliczu nadzoru, a logo – symbolizować otwarcie więziennych murów.



Projekt Panoptykonu
według Jeremy'ego Benthama

Zespół Fundacji Panoptykon, fot. Roch Forowicz

Katarzyna Szymielewicz – współzałożycielka i prezeska Fundacji Panoptykon

§

Małgorzata Szumańska – współzałożycielka i wiceprezeska

§

Anna Obem – w zespole od 2011 roku

Kamil Śliwowski – od 2009 roku współpracownik, od 2014 członek zespołu

Wojciech Klicki – w zespole od 2012 roku

§

Jędrzej Niklas – od 2011 roku wolontariusz, od 2012 członek zespołu

§

Karolina Szczepaniak – od 2011 roku wolontariuszka, w zespole od 2012 roku

Anna Walkowiak – w zespole od 2013 roku

§

Michał „Czesiek" Czyżewski – od 2013 roku członek zespołu

OBSZARY DZIAŁANIA

I. Ochrona prywatności

Rozwój techniki i biznesu opartego na masowym przetwarzaniu danych niesie poważne wyzwania dla prywatności. Problem pogłębia społeczny brak świadomości tych procesów i wiedzy, jak się bronić, oraz prawo nieprzystające do realiów cyfrowego świata. W Unii Europejskiej trwają prace nad przyjęciem nowych regulacji. Jednak postulaty obywateli z trudem przebijają się przez zmasowany lobbing części biznesu, której zależy na powstrzymaniu zmian.

Wybrane działania

1. Śledziliśmy zmiany przepisów dotyczących prywatności w Polsce, losy europejskiej reformy i działanie prawa w praktyce.
2. Informowaliśmy o toczących się w Brukseli pracach (liczne artykuły i wypowiedzi w mediach, infografika). Animowaliśmy debatę publiczną i braliśmy aktywny udział we wszystkich ważnych wydarzeniach.
3. W ramach koalicji European Digital Rights opiniowaliśmy setki poprawek zgłaszanych do projektu unijnego rozporządzenia i przygotowywaliśmy materiały dla decydentów i dziennikarzy. Podjęliśmy też dyskusję z przedstawicielami biznesu, która zaowocowała wspólnym stanowiskiem Fundacji Panoptykon i KPP „Lewiatan".
4. Jako jedyna organizacja niebiznesowa włączyliśmy się w prace nad reformą na poziomie krajowym: współprowadziliśmy serię warsztatów eksperckich dotyczących prywatności w Internecie, a przez prawie rok niemal co tydzień uczestniczyliśmy w spotkaniach roboczych w Ministerstwie Administracji i Cyfryzacji.
5. Realizowaliśmy też w działania edukacyjne, dostarczając konkretnej wiedzy dotyczącej ochrony prywatności. Przygotowaliśmy scenariusze zajęć („Cyfrowa Wyprawka"), prowadziliśmy lekcje w szkołach, warsztaty dla nauczycieli i trenerów, organizacji pozarządowych oraz studentów.

Pozytywne zmiany

1. Temat ochrony prywatności zaistniał w debacie publicznej. W opiniotwórczych mediach (np. Gazeta Wyborcza, Polityka, Polskie Radio, TOK FM) rozpoczęła się poważna dyskusja dotycząca reformy.
2. Nasze postulaty zostały uwzględnione w stanowisku wypracowanym przez Parlament Europejski i przebiły się do europosłów, którzy publicznie je przywoływali.
3. Polskie władze aktywnie zaangażowały się w prace nad reformą i zorganizowały konsultacje społeczne. Połowa istotnych dla nas rekomendacji została uwzględniona w polskich instrukcjach negocjacyjnych.

93% użytkowników naszej strony internetowej uważa, że naszymi działaniami zwiększamy wiedzę obywateli na temat ochrony danych osobowych i bezpieczeństwa w sieci, 82% – że skutecznie inicjujemy debatę nad reformą ochrony danych osobowych, a 71% – że nasze działania mają pozytywny wpływ na regulacje prawne chroniące prywatność.

II. Wolność w Internecie

Biznes w Internecie opiera się na śledzeniu użytkowników. Każdy klik uruchamia przepływ informacji: część z nich udostępniamy sami, z istnienia części naszych cyfrowych śladów nawet nie zdajemy sobie sprawy. Wiele proponowanych zmian prawa może jeszcze pogłębić problem inwigilacji w sieci, ograniczyć swobodę korzystania z niej oraz wolność słowa.

Wybrane działania

1. Zbadaliśmy, jak chętnie instytucje publiczne sięgają po dane użytkowników usług internetowych, jak dostawcy takich usług radzą sobie z problemem spornych treści (kiedy je usuwają, a kiedy nie) i w jaki sposób biblioteki publiczne korzystają z programów filtrujących.

2. Śledziliśmy i opiniowaliśmy dziesiątki krajowych i unijnych inicjatyw: projektów ustaw i rozporządzeń, programów europejskich, dyrektyw, rezolucji i konwencji. Reagowaliśmy na każdą próbę wprowadzenia niepokojących rozwiązań. Namierzaliśmy różne inicjatywy blokowania stron internetowych i krytycznie je opiniowaliśmy. W koalicji organizacji sprzeciwiliśmy się stworzeniu Rejestru Stron i Usług Niedozwolonych oraz podobnym projektom na poziomie unijnym: braliśmy udział w spotkaniach z rządem, organizowaliśmy dyskusje, prowadziliśmy działania informacyjne w sieci i w mediach.

3. Od początku monitorowaliśmy prace nad ACTA i zaangażowaliśmy się w działania przeciwko temu porozumieniu. Uruchomiliśmy akcję informacyjną w sieci – w czasie wybuchu protestów społecznych nasza strona była jednym z nielicznych rzetelnych źródeł wiedzy w języku polskim (korzystało z niej wtedy nawet kilkadziesiąt tysięcy osób dziennie). Odpowiadaliśmy na pytania mediów i zabieraliśmy głos w publicznych dyskusjach. Mobilizowaliśmy obywateli do kontaktu z władzami i sami wywieraliśmy nacisk na decydentów. Współorganizowaliśmy Improwizowany Kongres Wolnego Internetu – nieformalny zlot ACTA-wistów.

4. Na froncie edukacyjnym przygotowaliśmy przewodnik „Perypetie informacji w Internecie", infografiki, teksty poradnikowe, scenariusze zajęć („Cyfrowa Wyprawka"), prowadziliśmy lekcje w szkołach i warsztaty.

Pozytywne zmiany

1. Upadł pomysł stworzenia Rejestru Stron i Usług Niedozwolonych. W Polsce nie wprowadzono blokowania stron internetowych, a w Unii Europejskiej zrezygnowano z planów obowiązkowego blokowania.

2. Rząd wycofał swoje poparcie dla ACTA, a następnie umowę tę odrzucił Parlament Europejski.

3. Upadły inne niepokojące inicjatywy (np. porozumienie w sprawie egzekwowania praw autorskich i wymiany informacji).

4. Ujawniono liczne trzymane wcześniej w tajemnicy dokumenty (dotyczące np. ACTA).

5. Decydenci przekonali się, że ignorowanie głosu obywateli w sprawie regulacji Internetu jest ślepą uliczką – w efekcie otworzyli się na dialog i konsultacje proponowanych zmian.

Spotkanie dotyczące regulacji Internetu,
źródło: strona Kancelarii Prezesa Rady Ministrów

Radio TOK FM doceniło nasze zaangażowanie w sprawę ACTA i inne działania: przyznało Katarzynie Szymielewicz i Fundacji Panoptykon nagrodę im. Anny Laszuk za 2012 rok, za „czujność i podjęcie walki w ważnych i nie zawsze łatwych czy medialnie popularnych sprawach".

Wręczenie nagrody radia TOK FM,
źródło: Agencja Gazeta

III. Polityka bezpieczeństwa

Bezpieczeństwo to prawdziwy wytrych. Jeśli jakiś przejaw nadzoru można nim uzasadnić – choćby tylko w teorii – obowiązkowo pojawia się na sztandarze i zamyka usta oponentom. Jest to na rękę służbom, które mogą korzystać z coraz bardziej zaawansowanych narzędzi nadzoru, jednocześnie pozostając poza demokratyczną kontrolą. Tak jest w przypadku danych telekomunikacyjnych, które operatorzy telekomunikacyjni mają obowiązkowo przechowywać w celach bezpieczeństwa – zgodnie z unijną dyrektywą – i przekazywać instytucjom państwowym na każde żądanie.

Wybrane działania

1. Zbieraliśmy informacje na temat pozyskiwania i wykorzystywania danych obywateli przez państwo; skierowaliśmy dziesiątki wniosków o informacje publiczną, przeprowadziliśmy szereg rozmów z przedstawicielami służb i prokuratury. Analizowaliśmy polskie i zagraniczne regulacje prawne.

2. Upubliczniliśmy pierwsze dane na temat skali „billingowania", rozpoczynając merytoryczną debatę publiczną. Przeprowadziliśmy akcje informacyjne w sieci i w mediach, przedstawialiśmy problem w trakcie wydarzeń publicznych, najważniejsze informacje zebraliśmy w przewodniku „Telefoniczna kopalnia informacji".

3. Naciskaliśmy na zmianę zasad dostępu do danych telekomunikacyjnych zarówno w Polsce – współpracując z Rzecznikiem Praw Obywatelskich, GIODO, Najwyższą Izbą Kontroli; jak i w Unii Europejskiej – w ramach koalicji European Digital Rights. Przygotowywaliśmy stanowiska prawne i opinię dla Trybunału Konstytucyjnego.

4. Monitorowaliśmy prace nad wszystkimi ustawami regulującymi funkcjonowanie służb i opiniowaliśmy zgłaszane propozycje.

5. Przyglądaliśmy się organizacji EURO 2012: krytykowaliśmy niepokojące zmiany prawa i praktyki. Wnioski zebraliśmy w opracowaniu: „Ile wolności kosztował nas »stan wyjątkowy« w czasie EURO 2012?".

6. Śledziliśmy doniesienia związane z PRISM i innymi amerykańskimi programami masowej inwigilacji i dzieliliśmy się informacjami. We współpracy z Helsińską Fundacją Praw Człowieka i Amnesty International Polska skierowaliśmy do polskich instytucji 100 pytań dotyczących inwigilacji obywateli. Włączaliśmy się w międzynarodowe akcje protestu i sami napisaliśmy do prezydenta Stanów Zjednoczonych.

Pozytywne zmiany

1. Światło dzienne ujrzały ważne informacje dotyczące korzystania z danych telekomunikacyjnych i związków polskich służb z amerykańskimi. Z czasem dostęp do informacji stawał się coraz bardziej otwarty – większość służb zmieniła praktykę, a najbardziej tajemnicza z nich (Służba Kontrwywiadu Wojskowego) przegrała z nami spór w sądzie.

2. Dane dotyczące „billingowania" poruszyły opinię publiczną. Rzecznik Praw Obywatelskich, GIODO, Najwyższa Izba Kontroli, Naczelna Rada Adwokacka i inne podmioty zaczęły aktywnie zabiegać o zmianę prawa.

3. Rzecznik Praw Obywatelskich zakwestionowała konstytucyjność zasad udostępniania państwu danych telekomunikacyjnych. Trybunał Sprawiedliwości Unii Europejskiej stwierdził nieważność dyrektywy retencyjnej.

4. Okres obowiązkowego przechowywania danych telekomunikacyjnych skrócono z 24 do 12 miesięcy. Po krytycznym raporcie Najwyższej Izby Kontroli senat pracuje nad dalej idącymi zmianami.

Akcja „Płot Narodowy", fot. Jędrzej Niklas, Barbara Gubernat

Mówisz o billingach. Najpierw Cię ignorują. Później twierdzą, że nie potrafisz czytać danych. Następnie, że manipulujesz i jesteś radykalna. Potem, że może jednak warto rozmawiać. Wzajemnie się zrozumieć. Wytłumaczyć. Uzasadnić. Zapraszają na konferencje i seminaria. Próbują zmiękczyć. Ale Twoje pytania przejmują inni. Instytucje państwowe. Media. Stają się częścią normalnej debaty. Dopytuje się Trybunał Konstytucyjny. Służby, policja, sądy się nieudolnie tłumaczą. Zmienia się prawo, wrażliwość, podejście społeczeństwa. To jest siła 5-letniego sukcesu Panoptykonu. W tej i w innych sprawach.

Adam Bodnar, wiceprezes Helsińskiej Fundacji Praw Człowieka

IV. Śledzenie i obserwacja

Rozwój technologii zaowocował upowszechnieniem się nowych narzędzi inwigilacji. Najpopularniejszym są kamery monitoringu; dzięki nim państwo na szeroką skalę podgląda obywateli, firmy – pracowników i konsumentów, szkoły i rodzice – dzieci, sąsiedzi – siebie nawzajem. Oficjalnie to wszystko ma służyć bezpieczeństwu, w praktyce niewiele ma z nim wspólnego. Za to prowokuje do podglądactwa, naruszeń prywatności i niesie negatywne skutki społeczne. W Polsce problem pogłębia brak prawnych zasad korzystania z monitoringu.

Wybrane działania

1. Analizowaliśmy zasady działania monitoringu w Polsce i za granicą oraz publikacje naukowe dotyczące jego (nie)skuteczności. Zbadaliśmy, co Polacy sądzą o kamerach i jak wpływają one na codzienne życie. Zebraliśmy dane dotyczące działania miejskich systemów monitoringu i kamer na basenach.

2. Śledziliśmy i opiniowaliśmy wszystkie propozycje zmian prawa dotyczące korzystania z kamer monitoringu. We współpracy z Rzecznik Praw Obywatelskich i GIODO wywieraliśmy nacisk na przyjęcie kompleksowych regulacji prawnych. Byliśmy jedyną organizacją niezwiązaną z biznesem kamerowym zaangażowaną w prace nad nowymi rozwiązaniami: przedstawialiśmy własne analizy i opiniowaliśmy propozycje Ministerstwa Spraw Wewnętrznych.

3. Interweniowaliśmy w przypadkach nadużyć (np. kamery na basenie, nagrywanie spotkań w szkole). Weszliśmy w dyskusję z Ministerstwem Spraw Wewnętrznych na temat jego udziału w projekcie badawczym INDECT (który ma na celu rozwój „inteligentnych” kamer).

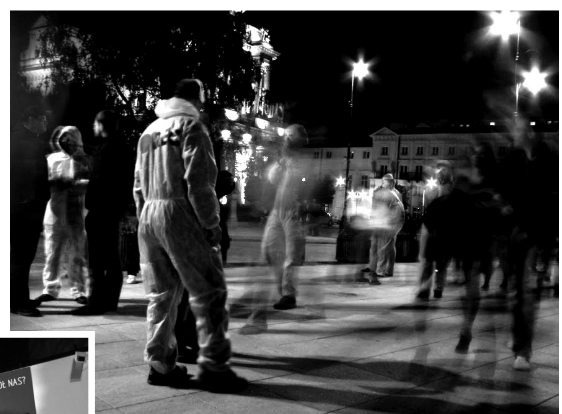
4. Zwracaliśmy uwagę na problemy związane z niekontrolowanym rozwojem monitoringu. Informowaliśmy, współpracowaliśmy z mediami, organizowaliśmy seminaria, dyskusje, happeningi, stworzyliśmy przewodnik „Życie wśród kamer”.

Pozytywne zmiany

1. W debacie publicznej pojawił się krytyczny głos dotyczący wszechobecności kamer monitoringu.

2. Rzecznik Praw Obywatelskich, GIODO i Najwyższa Izba Kontroli zaangażowali się w działania na rzecz prawnego ograniczenia monitoringowej samowoli.

3. Decydenci dostrzegli, że nie mogą ignorować problemów związanych z niekontrolowanym działaniem kamer. Ministerstwo Spraw Wewnętrznych przygotowało projekt założeń do ustawy regulującej monitoring, który uwzględnia część naszych postulatów.



Happening z okazji „Freedom not Fear Day”, fot. Alicja Szymczak

V. Zarządzanie i polityka społeczna

Dzięki nowym narzędziom możliwe staje się gromadzenie informacji i ich kojarzenie na coraz szerszą skalę. Dla wielu instytucji staje się to uniwersalną metodą zarządzania i rozwiązywania problemów. Często bez refleksji nad tym, jakie są ich źródła i jak najskuteczniej je rozwiązać. W pogoni za modernizacją i cyfryzacją brakuje czasu na analizę, jakie wartości poświęcamy po drodze. W efekcie rozrastają się publiczne bazy danych o obywatelach – zarówno na poziomie centralnym (np. systemy informacji medycznej i oświatowej), jak i lokalnym (np. karty miejskie).

Wybrane działania

1. Zaangażowaliśmy się w prace nad projektami wprowadzenia centralnych systemów informacji w oświacie i ochronie zdrowia. Opiniowaliśmy projekty ustaw i rozporządzeń. Zwracaliśmy uwagę na zagrożenia ministerstwom, posłom, senatorom, prezydentowi, Rzecznik Praw Obywatelskich i GIODO. Zaangażowaliśmy we wspólne działania inne organizacje społeczne.

2. Zbieraliśmy informacje na temat funkcjonowania inteligentnych liczników energii i kontaktowaliśmy się z ekspertami. Śledziliśmy prace nad ustawami, które ich dotyczyły, i opiniowaliśmy wszystkie projekty. Braliśmy udział w wydarzeniach publicznych i dyskutowaliśmy z lobby zainteresowanym wdrażaniem inteligentnych liczników.

3. Wystąpiliśmy przeciwko obowiązkowej personalizacji kart miejskich w Warszawie – zwróciliśmy się w tej sprawie do władz miasta, Rzecznika Praw Obywatelskich, GIODO, UOKiK-u. Zachęcaliśmy warszawiaków do wyrażania sprzeciwu (protestacyjne hasło: „Mam Cię, bo muszę"), media – do zainteresowania się tematem, a radnych – do zmiany prawa.

Pozytywne zmiany

1. Rzecznik Praw Obywatelskich zakwestionowała konstytucyjność części przepisów ustawy o systemie informacji w ochronie zdrowia.

2. W ustawie o systemie informacji oświatowej wprowadzono wyższy standard ochrony danych wrażliwych. Rzecznik Praw Obywatelskich podzieliła nasze wątpliwości dotyczące systemu i zwróciła na nie uwagę ministrowi edukacji.

3. Rząd zrezygnował z pomysłu wprowadzenia obowiązku powszechnej instalacji inteligentnych liczników, a parlament wprowadził gwarancje ochrony prywatności osób, u których zostały one zainstalowane.

4. W debacie publicznej pojawił się temat kart miejskich. Decyzja GIODO przerwała część z najbardziej kontrowersyjnych praktyk warszawskiego ZTM.

Karta miejska z panoptykonowym hasłem, fot. Piotr Waglowski

KALENDARIUM: SUBIEKTYWNY WYBÓR 100 NAJWAŻNIEJSZYCH DZIAŁAŃ 5-LECIA

IV 2009 Oficjalnie rozpoczynamy działalność

V 2009

1. Rusza strona internetowa Panoptykon.org

2. Pierwsza akcja – sprzeciw wobec obowiązkowej personalizacji kart miejskich w Warszawie: występujemy do władz miasta, RPO, GIODO
→ VII 2009: decyzja GIODO ogranicza praktyki warszawskiego ZTM ☺

VII 2009

3. Pierwszy artykuł w ogólnopolskiej prasie: Rzeczpospolita, „Czy spersonalizowane karty miejskie zagrażają prywatności"

X 2009

4. Rusza „Seminarium Panoptykon": organizujemy pierwsze z cyklu 13 spotkań

5. Sprzeciw wobec personalizacji kart miejskich: promujemy wśród warszawiaków protestacyjne tło kart: „Mam cię – bo muszę"
→ I 2010: zaproszenie na spotkanie z premierem ☺

XI 2009

6. Rozpoczynamy serię szkoleń na temat prawa do prywatności dla studentów udzielających darmowych porad prawnych w klinice prawa

7. Negatywnie opiniujemy projekt stworzenia Rejestru Stron i Usług Niedozwolonych: angażujemy się w działania koalicji organizacji sprzeciwiających się blokowaniu (początek współpracy z grupą organizacji zajmujących się Internetem)*

8. Pierwszy wywiad – opowiadamy o ciemnych stronach nadzoru: Gazeta Stołeczna, „Jakie są granice naszej wolności i prywatności?"

II 2010

9. Pierwsze spotkanie organizacji społecznych i blogerów z premierem Donaldem Tuskiem: dyskutujemy o regulacji Internetu*
→ II 2010: rząd wycofuje się z projektu stworzenia Rejestru Stron i Usług Niedozwolonych; premier oglasza, że w Polsce nie będzie blokowania stron internetowych ☹

V 2010

10. Sprzeciw wobec projektu wprowadzenia obowiązkowych badań ginekologicznych: występujemy do ministra zdrowia i RPO*
→ VII 2010: RPO podejmuje interwencję ☺
→ IX 2010: Ministerstwo Zdrowia rezygnuje z projektu ☺

11. Rozpoczynamy monitoring wyborów GIODO*

VI 2010

12. Angażujemy się w działania przeciwko ACTA: apel do europosłów o przejrzystość procesu negocjacyjnego*
→ IX 2010: Parlament Europejski przyjmuje deklarację krytyczną wobec ACTA ☺

13. Zaczynamy uwagę na problemy związane z przekazywaniem danych bankowych: apel o odrzucenie porozumienia między UE a USA w sprawie SWIFT
→ VII 2010: Parlament Europejski akceptuje porozumienie ☹

VII 2010

14. Dołączamy do koalicji European Digital Rights (EDRi); z czasem Katarzyna Szymielewicz wchodzi do zarządu organizacji

VIII 2010

15. Negatywnie opiniujemy propozycje poszerzenia uprawnień Żandarmerii Wojskowej
→ Dalsze prace nad projektem nie zostają podjęte ☹

IX 2010

16. Pierwsze obchody Freedom not Fear Day w Warszawie: organizujemy happening antymonitoringowy

X 2010

17. Dzięki zdobyciu finansowania rozpoczynamy systematyczne działania strażnicze: z kawiarni przenosimy się do biura!

18. Rozpoczynamy zbieranie informacji o praktyce korzystania z danych telekomunikacyjnych przez państwo: seria wniosków o informację publiczną
→ Początkowo tylko nieliczne instytucje odpowiadają na nasze pytania; z czasem się to zmienia ☹

XI 2010

19. Upubliczniamy pierwsze informacje na temat skali „billingowania" i pierwszy raz trafiamy na „jedynkę": Gazeta Wyborcza, „Milion billingów"
→ XI 2010: poruszenie mediów, opinii publicznej i decydentów: RPO interweniuje u premiera, premier powołuje specjalny zespół do zbadania sprawy; swój sprzeciw wyraża szereg podmiotów ☺
→ VII 2011: RPO kieruje do TK wniosek o stwierdzenie niekonstytucyjności zasad dostępu do danych telekomunikacyjnych ☺
→ VI 2012: kolejny wniosek w tej sprawie składa Prokurator Generalny ☺
→ IV 2014: rusza sprawa przed TK ☺

20. Zaczynamy naciskać na zmianę prawa dotyczącego dostępu państwa do danych telekomunikacyjnych na poziomie Polski i UE; pierwszy raz jedziemy w tym celu do Brukseli
→ IV 2011: Komisja Europejska publikuje krytyczny raport z ewaluacji obowiązującej dyrektywy; ale nie proponuje jej rewizji ☺
→ X 2013: rząd proponuje stworzenie Komisji Kontroli Służb Specjalnych ☹
→ IV 2014: Trybunał Sprawiedliwości UE uznaje dyrektywę retencyjną za nieważną ☺

21. Włączamy się w prace nad zasadami odpowiedzialności pośredników za treści publikowane w Internecie: uwagi do projektu dyrektywy e-commerce i ustawy o świadczeniu usług drogą elektroniczną
→ VI 2011: projekt przyjęty przez rząd uwzględnia szereg naszych postulatów, jednak z czasem prace nad nim zostają zawieszone ☹

22. Występujemy przeciwko unijnemu projektowi blokowania stron internetowych*
→ X 2011: europosłowie odrzucają pomysł obowiązkowego blokowania stron w UE; ale nie wykluczają takich działań na poziomie państw członkowskich ☹

XII 2010

23. Włączamy się w prace parlamentarne nad przyjęciem ustawy o systemie informacji w oświacie i ochronie zdrowia

24. Angażujemy się w prace nad reformą zasad ochrony prywatności w UE: pierwsze stanowisko*

25. Pierwszy raz występujemy na Chaos Communication Congress w Berlinie

I 2011

26. Sprzeciwiamy się próbie zwiększenia kontroli nad materiałami audiowizualnymi publikowanymi w sieci (nowelizacja ustawy o radiofonii i telewizji)
→ III 2011: senat usuwa z nowelizacji kontrowersyjne propozycje ☺

II 2011

27. Organizujemy debatę „Blokowanie stron internetowych – rok po: początek cenzury czy odpowiedź na realne zagrożenia?"

28. Publikujemy materiały edukacyjne „Szkoła z klasą 2.0" (początek współpracy z Centrum Edukacji Obywatelskiej)*

III 2011

29. Negatywnie opiniujemy projekt ustawy o wymianie informacji między organami ścigania UE
→ IX 2011: projekt ustawy zostaje przyjęty bez najbardziej kontrowersyjnych rozwiązań ☹

30. Rusza pierwsza z trzech serii badań społecznych dotyczących nadzoru (monitoring wizyny, ochrona danych i prywatność w Internecie)

IV 2011

31. Kolejne spotkanie z premierem i początek serii spotkań roboczych w ministerstwach: kontynuujemy dyskusję o regulacji Internetu

32. Sprzeciw wobec ustawy o systemie informacji oświatowej: przekazujemy krytyczną opinię posłom, a następnie apelujemy do prezydenta*
→ I 2012: grupa posłów kwestionuje konstytuczność części ustawy przed TK ☺
→ VII 2012: parlament nowelizuje ustawę i ogranicza przetwarzanie danych wrażliwych w centralnym systemie ☺

V 2011

33. Pierwszy raz uczestniczymy w konferencji re:publica w Berlinie

VI 2011

34. Po raz pierwszy bierzemy udział w konferencji Computers, Data Protection and Privacy w Brukseli

VIII 2011

35. Opiniujemy projekt ustawy o bezpieczeństwie EURO 2012
→ VIII 2011: ustawa zostaje przyjęta w ekspresowym tempie ☹

36. Interweniujemy w sprawie kamer monitoringu w przebieralni łódzkiego basenu

37. „Czy żyjemy w społeczeństwie nadzorowanym?" – organizujemy spotkanie z Davidem Lyonem

IX 2011

38. Organizujemy konferencję „Internet na rozdrożu" i publikujemy raport „Internet a prawa podstawowe"

39. Apelujemy do sejmu i prezydenta o odrzucenie poprawek senatu ograniczających dostęp do informacji publicznej*
→ IX 2011: prezydent podpisuje ustawę, ale przekazuje ją to TK ☹
→ IV 2012: TK uznaje ograniczenie za niezgodne z konstytucją ☺

40. Pierwszy raz aktywnie bierzemy udział w Internet Governance Forum w Nairobi

X 2011

41. Organizujemy konferencję „Nadzór niekontrolowany" i publikujemy raport „Nadzór 2011. Próba podsumowania"

42. Interweniujemy przeciwko nieformalnemu porozumieniu o „współpracy i wzajemnej pomocy w sprawie ochrony praw własności intelektualnej w środowisku cyfrowym" negocjowanym pod egidą MKiDN*
→ Prace nad porozumieniem zostają zarzucone ☹

XII 2011

43. Rozsyłamy 1. numer newslettera „PanOptyka"

44. Działamy przeciwko przyjęciu nowego porozumienia UE–USA dotyczącego przekazywania danych pasażerów linii lotniczych: zwracamy się do europosłów i ministrów
→ IV 2012: porozumienie zostaje przyjęte ☹

I 2012

45. Upubliczniamy informacje o planach podpisania ACTA bez dalszych konsultacji i uruchamiamy kampanię informującą o porozumieniu; odpowiadamy na zainteresowanie mediów i obywateli

Angażujemy się w działania rzecznicze przeciwko ACTA*
→ I 2012: rusza lawina medialna, bezprecedensowe poruszenie w sieci i na ulicach; nasza strona staje się ważnym źródłem informacji ☺
→ II 2012: RPO krytycznie opiniuje ACTA ☺
→ II 2012: rząd ujawnia dokumenty negocjacyjne, a premier opowiada się za odrzuceniem ACTA ☺

II 2012

46. Współorganizujemy Improwizowany Kongres Wolnego Internetu – nieformalny „zlot" ACTA-wistów"
Spotkanie zwolenników i przeciwników ACTA u premiera – odmawiamy obecności „na salonach" i bierzemy udział przez Internet*

47. Włączamy się w prace legislacyjne dotyczące inteligentnych liczników: pierwsze krytyczne uwagi do nowego prawa energetycznego
→ IV 2013: zostajemy zaproszeni do dyskusji przez Ministerstwo Gospodarki i Urząd Regulacji Energetyki ☺

48. Angażujemy się w prace nad nowelizacją prawa telekomunikacyjnego
→ III 2013: strony internetowe mają obowiązek informować o ciasteczkach ☹

III 2012

49. Sprzeciw wobec propozycji wprowadzenia zakazu zasłaniania twarzy: opiniujemy projekt ograniczający wolność zgromadzeń i bierzemy udział w wysłuchaniu publicznym
→ V 2012: posłowie rezygnują z propozycji zakazu zasłaniania twarzy ☺

50. Przedstawiamy opinię przyjaciela sądu dla TK dotyczącą uprawnień państwa do dostępu do danych telekomunikacyjnych

51. Rusza seria warsztatów organizowanych przez Ministerstwo Administracji i Cyfryzacji – współprowadzimy prace grupy „Ochrona danych osobowych i prywatność"

IV 2012

52. Publikujemy kolejne dane dotyczące skali sięgania po dane telekomunikacyjne i rozpoczynamy akcję informacyjną
→ I 2013: dane telekomunikacyjne mają być przechowywane krócej: 12 zamiast 24 miesięcy ☺
→ X 2013: NIK przedstawia wnioski z kontroli: prawo nie chroni obywateli ☺
→ II 2014: senat przygotowuje propozycję ograniczenia uprawnień policji i służb ☺

53. Przekazujemy opinię prawną sądowi badającemu „billingowanie" dziennikarza Bogdana Wróblewskiego
→ IV 2013: dziennikarz wygrywa z CBA ☺

54. Pytamy MSW o zaangażowanie policji w projekt INDECT i przygotowujemy analizę zagrożeń, które może on stwarzać dla praw człowieka
→ VI 2012: MSW powołuje zespół, który ma wyjaśnić zaangażowanie policji w dotychczasowe prace; projekt jest kontynuowany ☹

V 2012

55. Pierwszy raz zabieramy głos w sprawie rewizji Międzynarodowych Przepisów Telekomunikacyjnych (ITR)*
→ VIII 2012: Ministerstwo Administracji i Cyfryzacji ujawnia polskie stanowisko negocjacyjne w sprawie ITR i przeprowadza konsultacje społeczne ☺
→ XI 2012: ostateczna wersja polskiego stanowiska negocjacyjnego uwzględnia nasze postulaty ☺

56. Noc Muzeów: współtworzymy antynadzorczą instalację artystyczną

57. Interweniujemy u RPO w sprawie zasad przyznawania akredytacji w trakcie EURO 2012
→ VII 2012: RPO interweniuje u ministra spraw wewnętrznych ☺

58. Rozpoczynamy akcję nawołującą do pisania do europosłów w sprawie ACTA
→ VI 2012: komisje europarlamentu głosują przeciwko ACTA ☺
→ VII 2012: ACTA przepada w głosowaniu plenarnym ☺

VII 2012

59. Podsumowujemy: Ile wolności kosztował nas „stan wyjątkowy" w czasie EURO 2012?

60. Ruszają badania miejskiego monitoringu: we współpracy z RPO i GIODO wysyłamy ankiety do wszystkich miast powiatowych
→ Ponad 200 miast udziela odpowiedzi ☹

VIII 2012

61. Angażujemy się w akcję „Plot Narodowy"*

62. Interweniujemy u komendanta głównego policji w sprawie zasad upubliczniania nagrań z telefonu alarmowego 112
→ VIII 2012: komenda główna zleca przygotowanie analizy prawnej i przekazanie jej oficerom prasowym policji ☹

IX 2012

63. Kolejne obchody Freedom not Fear Day w Warszawie: piknik pod „plotem narodowym" i debata „Miasto wolne od strachu"*

X 2012

64. Współorganizujemy seminarium „Kto na nas patrzy? Obywatel pod obserwacją kamer" i podsumowujemy badania dotyczące monitoringu wizyjnego
→ X 2012: wiceminister spraw wewnętrznych publicznie obiecuje przygotowanie przepisów dotyczących monitoringu ☺

XI 2012

65. Opinia dotycząca ustawy o cudzoziemcach: zwracamy uwagę na niski standard ochrony prywatności
→ I 2013: jedna z naszych uwag zostaje uwzględniona ☹

XII 2012

66. Interweniujemy u GIODO w sprawie przetwarzania numerów rejestracyjnych pojazdów przez Zarząd Dróg Miejskich w Warszawie
→ XII 2012: GIODO rozpoczyna kontrolę w ZDM ☺

67. Badamy, w jaki sposób biblioteki publiczne korzystają z oprogramowania filtrującego ruch w Internecie

I 2013

68. Krytykujemy projekt ustawy dotyczącej instalacji kamer monitoringu w izbach wytrzeźwień
→ I 2014: wszystkie izby mają być wyposażone w kamery ☹

69. Rozpoczynamy bardzo intensywne działania na rzecz unijnej reformy ochrony prywatności w Brukseli (w koalicji z EDRi)*
Ruszamy z kampanią informacyjną w polskich mediach i zachęcamy do kontaktu z europosłami
→ X 2013: kluczowa komisja Parlamentu Europejskiego (LIBE) przyjmuje kompromisową opinię, uwzględniającą część naszych postulatów ☹

II 2013

70. Przygotowujemy kompleksowe stanowisko dotyczące regulacji monitoringu wizyjnego
→ XII 2013: część naszych propozycji zostaje uwzględniona w projekcie założeń do ustawy ☹

III 2013

71. Katarzyna Szymielewicz i Fundacja Panoptykon docenione przez radio TOK FM – odbieramy nagrodę za 2012 rok

72. Strona Panoptykon.org rusza w nowej odsłonie

73. Krytykujemy poselski projekt obowiązkowej instalacji inteligentnych liczników
→ V 2013: obowiązek instalacji liczników znika z projektu; pojawiają się za to gwarancje ochrony prywatności ☺

IV 2013

74. W Ministerstwie Administracji i Cyfryzacji ruszają cotygodniowe warsztaty poświęcone reformie ochrony prywatności
→ Wiele z naszych postulatów trafia do polskich stanowisk, prezentowanych na forum UE ☺

75. Przekazujemy RPO krytyczne opinie dotyczące centralnych systemów informacji w oświacie i ochronie zdrowia
→ VII 2013: RPO kieruje do TK wniosek kwestionujący konstytucyjność części ustawy o systemie informacji w ochronie zdrowia ☺

VI 2013

76. Organizujemy dyskusję „Anonimowi, wolni użytkownicy sieci czy sprofilowani odbiorcy usług internetowych"

VII 2013

77. Ruszamy z badaniem zasad wykorzystywania danych użytkowników Internetu przez państwo: kierujemy pytania do służb i firm

VIII 2013

78. Badamy praktyki korzystania z kamer monitoringu na basenach

IX 2013

79. Kolejne obchody Freedom not Fear Day: organizujemy debatę pod hasłem: „NSA a sprawa polska: czy świat bez inwigilacji jest jeszcze możliwy?"*

80. Bierzemy udział w corocznej konferencji rzeczników ochrony danych osobowych – Privacy Conference w Warszawie

X 2013

81. Uruchamiamy stronę internetową z materiałami dla nauczycieli „Cyfrowa Wyprawka"

82. Rusza akcja „100 pytań o inwigilację": wysyłamy serię wniosków o informację publiczną – pytamy o współpracę polskich służb z amerykańskimi i reakcję polskich władz na informacje upublicznione przez Edwarda Snowdena*
→ Niektóre instytucje odpowiadają, inne uchylają się od tego obowiązku ☹

83. Przedstawiamy krytyczne opinię projektu nowelizacji ustawy o statystyce publicznej
→ IV 2014: większość naszych uwag zostaje uwzględniona ☺

84. Rozpoczynamy publikację serii tekstów edukacyjno-poradnikowych „Cyfrowa Wyprawka dla Dorosłych"

85. PRISM z polskiej perspektywy: publikujemy artykuł na łamach brytyjskiego Guardiana*

86. Krytykujemy tryb prac nad nowym porozumieniem handlowym na szczeblu UE–USA (TTIP) – domagamy się większej przejrzystości
→ IV 2014: Ministerstwo Gospodarki nawiązuje dialog z organizacjami społecznymi ☺

XI 2013

87. Rusza seria warsztatów dla nauczycieli oraz lekcji pilotażowych prowadzonych w szkołach na bazie materiałów „Cyfrowa Wyprawka"

88. Organizujemy dyskusję z blogerami i dziennikarzami „Słowa w sieci"; promujemy pierwszy z serii przewodników „Perypetie informacji w Internecie"; następne – „Życie wśród kamer" i „Telefoniczna kopalnia informacji" ukazują się w kolejnych miesiącach

XII 2013

89. Publikujemy raport „Dostęp państwa do danych użytkowników usług internetowych"; z czasem ukazuje się też angielska wersja opracowania

90. Opiniujemy rozporządzenie zakładające niebezpieczne rozszerzenie uprawnień Straży Granicznej
→ II 2014: wszystkie nasze uwagi zostają uwzględnione ☺

I 2014

91. Krytycznie opiniujemy rządową koncepcję profilowania bezrobotnych
→ IV 2014: projekt zostaje przyjęty ☹

92. Wraz z aktywistami na całym świecie czekamy na lotnisku na Edwarda Snowdena

93. Z okazji europejskiego dnia ochrony danych osobowych publikujemy poradnik „Prywatność – zrób to sam"

II 2014

94. Dzień niezgody na inwigilację: nasze pytania o współpracę polskich i amerykańskich służb kierujemy do prezydenta USA Baracka Obamy

95. Pierwsze starcie w sądzie ze służbami specjalnymi: skarżymy SKW o bezczynność i brak odpowiedzi na nasze pytania o współpracę z zagranicznymi służbami
→ II 2014: WSA orzeka bezczynność SKW ☺

96. Publikujemy raport z badań „Monitoring wizyjny w życiu społecznym"

III 2014

97. Rusza seria tekstów dotyczących bezpieczeństwa w Warszawie

IV 2014

98. Rozpoczynamy realizację nowego projektu edukacyjnego: Akademii Praw Cyfrowych

99. Przygotowujemy debatę z kandydatami do europarlamentu i zadajemy trudne pytania o ochronę praw cyfrowych

100. Kończymy prace nad serią filmów animowanych dotyczących nadzoru

---

Badamy praktyki nadzoru | Kontrolujemy kontrolujących | Informujemy i edukujemy
* Działania podejmowane w koalicji organizacji społecznych

JESTEŚMY DUMNI Z TEGO, ŻE...

1.
Udało się zbudować prężną i stabilną organizację – mimo ograniczonych źródeł finansowania i niskiej społecznej świadomości problemów, którymi się zajmujemy.

2.
Nadzór zaistniał jako temat w debacie publicznej – rozpoczęliśmy dyskusję na trudne panoptykonowe tematy i zainteresowaliśmy nimi media, co w przypadku młodej i niedużej organizacji było sporym wyzwaniem.

3.
Nawiązaliśmy współpracę z wieloma organizacjami i instytucjami zarówno w Polsce, jak i za granicą – problem nadzoru w polskim wydaniu zaistniał na międzynarodowej mapie.

4.
Ujawniając trzymane w tajemnicy informacje, zwiększyliśmy przejrzystość działania państwa; przyczyniliśmy się też do zatrzymania wielu niebezpiecznych inicjatyw i wprowadzenia pozytywnych zmian w prawie.

5.
Zbudowaliśmy ekspercką pozycję: na nasze analizy i wyniki badań powołują się takie instytucje, jak Rzecznik Praw Obywatelskich, Prokurator Generalny, Rada Legislacyjna czy Najwyższa Izba Kontroli.

6.
Efekty naszej pracy są doceniane: 93% czytelników naszej strony uważa nasze teksty za interesujące, 90% – za wiarygodne, 89% – za przydatne; wszyscy uczestnicy warsztatów, którzy korzystali z naszych scenariuszy zajęć dla dzieci i młodzieży, oceniają je pozytywnie – najbardziej chwalą praktyczne rady, ciekawe pomysły i prostotę.

7.
Regularnie spotykamy osoby, które przyznają, że nasze działania zwróciły ich uwagę na nowe problemy, skłoniły do refleksji, a nawet zmiany codziennych praktyk – każdy taki przypadek to dla nas dowód, że ta praca ma sens!

Fundacja Panoptykon odkrywa coraz to nowe obszary kluczowe dla ochrony wolności i prawa człowieka w ciągle rozwijającym się świecie nowych technologii. W bardzo krótkim czasie organizacja obudziła opinię publiczną w Polsce i otworzyła nam wszystkim oczy na szereg zagrożeń, m.in. dla naszej prywatności i dostępu do informacji, wynikających z niewłaściwego zastosowania technik nadzoru w życiu codziennym. Rzetelność i innowacyjność pracy Fundacji sprawiły, że jest ona ważnym partnerem i źródłem inspiracji dla innych organizacji nie tylko w Polsce, ale też w Europie.

Draginja Nadaždin, dyrektorka Amnesty International Polska

Koty również lubią panoptykonowe gadżety, fot. Joanna Łojas

PANOPTYKON W LICZBACH

PIĘĆ LAT NASZEJ DZIAŁALNOŚCI ZAOWOCOWAŁO POWSTANIEM WIELU MATERIAŁÓW. W TYM CZASIE:

Do instytucji publicznych (od premiera i ministrów, przez policję i inne służby, po miejskie instytucje) skierowaliśmy ponad

520

wniosków o udostępnienie informacji publicznej

Opracowaliśmy i przekazaliśmy organom mającym wpływ na tworzenie i działanie prawa ponad

160

opinii prawnych, stanowisk i wystąpień

Na naszej stronie internetowej opublikowaliśmy ponad

1300

artykułów i notek

Występowaliśmy na konferencjach, seminariach, spotkaniach publicznym bądź zorganizowaliśmy własne wydarzenie ponad

150

razy

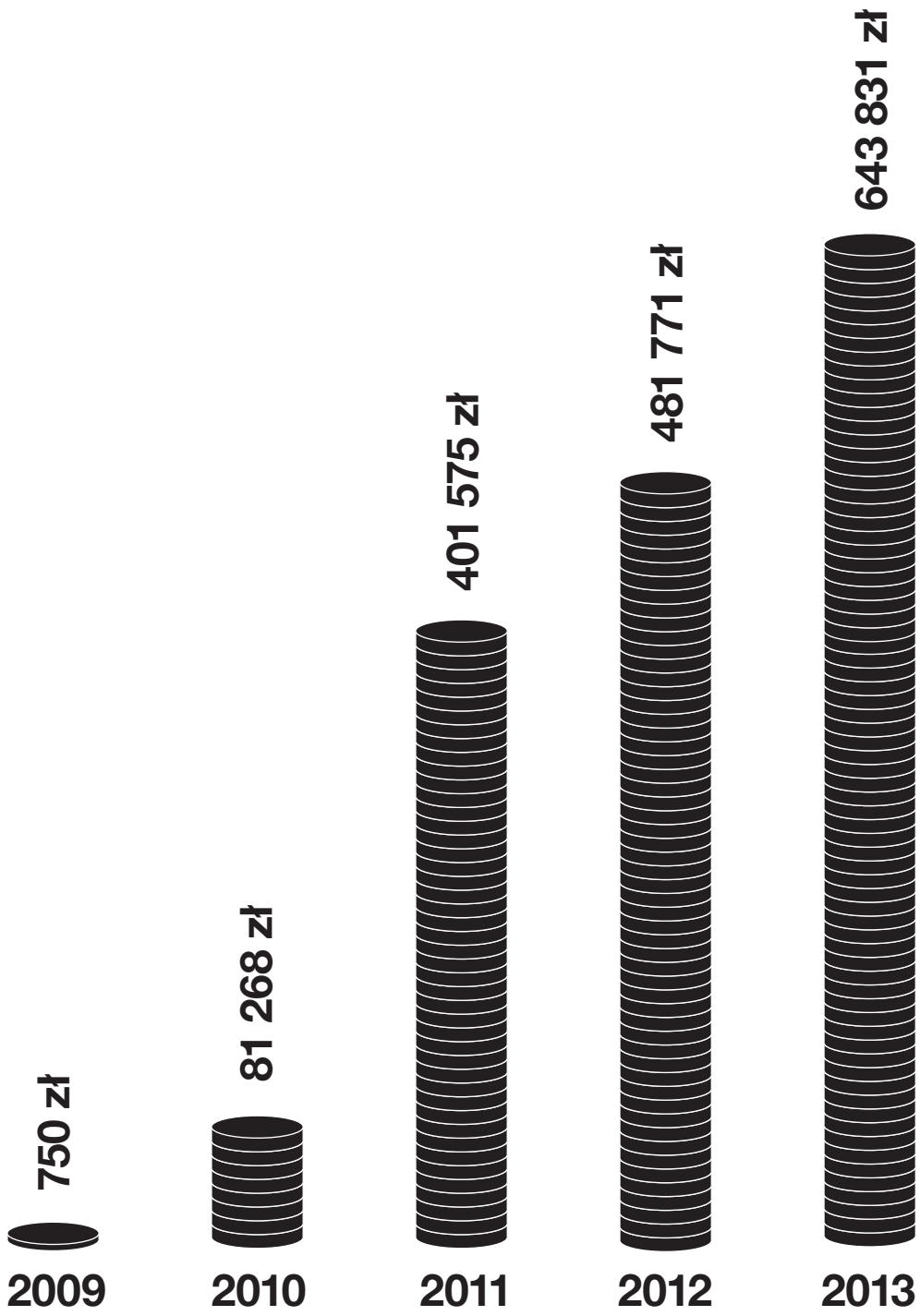
Dzięki artykułom własnym, przedrukom, wywiadom, cytowaniom itp. ponad

1000

razy pojawiliśmy się w mediach (prasie, radiu, telewizji, Internecie)

Nasza działalność rozwijała się z roku na rok. Ruszaliśmy bez jakiegokolwiek zewnętrznego finansowania – pierwsze granty udało nam się zdobyć dopiero po ponad roku pracy i pierwszych sukcesach.

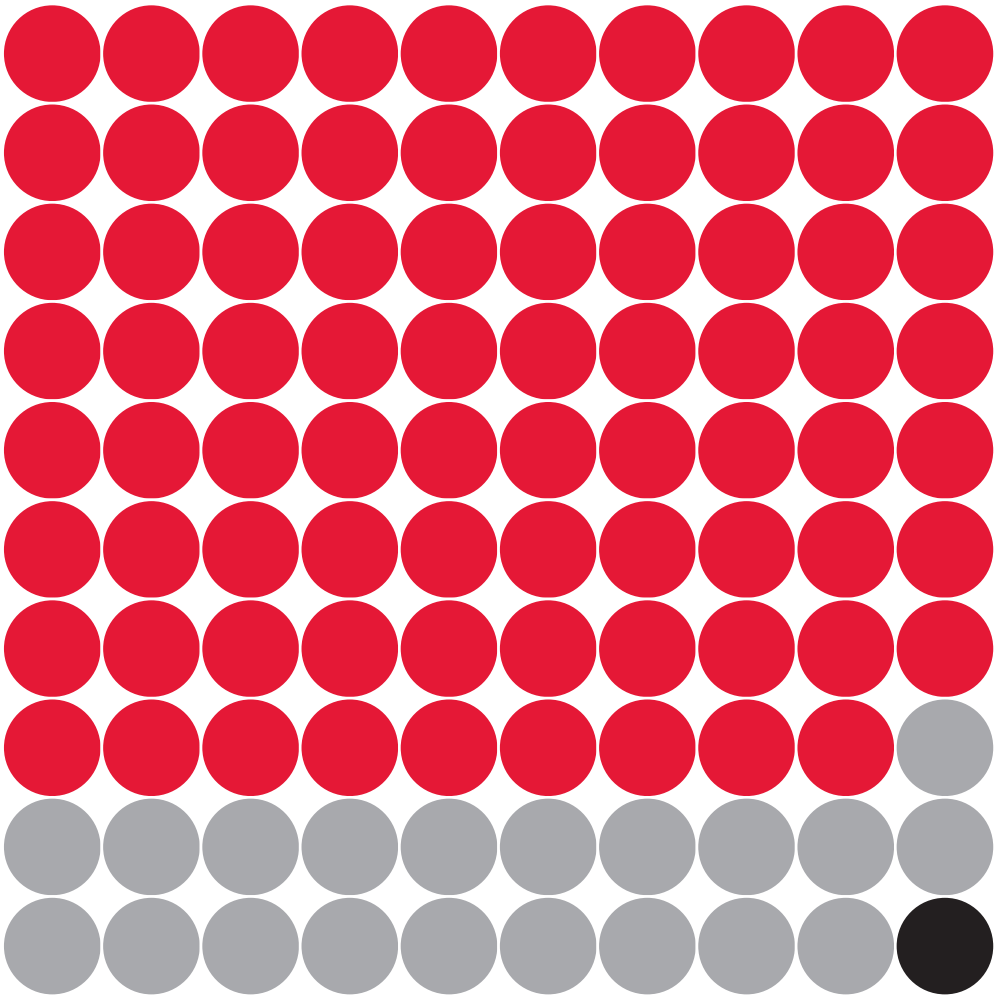
ŚRODKI FINANSOWE, KTÓRE MIELIŚMY DO DYSPOZYCJI W KOLEJNYCH LATACH*:



* Zestawienia przygotowane na potrzeby raportu – szczegółowe informacje na temat finansów Fundacji Panoptykon, w tym sprawozdania finansowe, dostępne są na stronie internetowej w zakładce „Organizacja".

Większość naszych środków finansowych pochodzi od instytucji grantodawczych, które ogłaszają konkursy na realizację projektów. Jedynie ułamek naszego budżetu to darowizny od indywidualnych osób. Są one jednak ważnym elementem stabilności finansowej organizacji – pozwalają sprawnie reagować na nowe zagrożenia i realizować zadania, które wykraczają poza ramy projektów finansowanych przez grantodawców instytucjonalnych.

ŹRÓDŁA FINANSOWANIA W 2013 ROKU*:



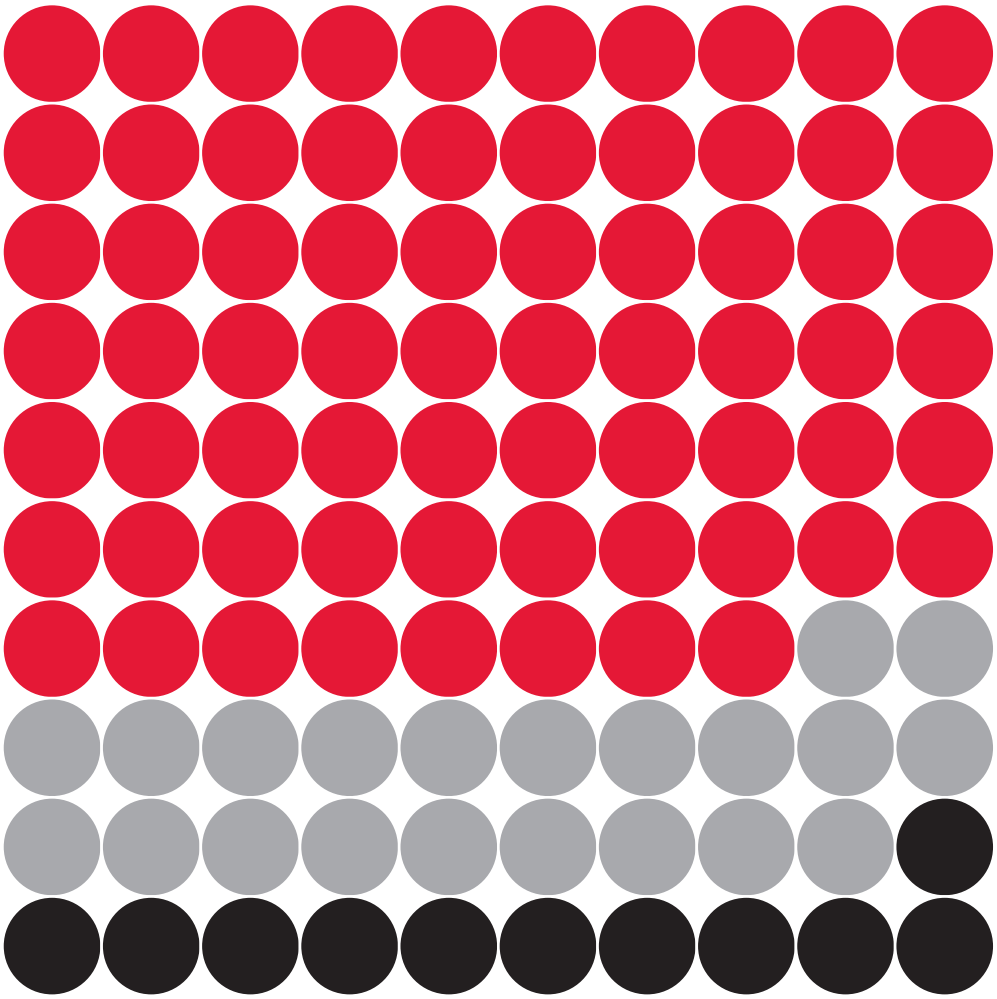
pochodzące z grantów prywatnych instytucji – **79,8%**

pochodzące z grantów publicznych instytucji – **19,2%**

pozaprojektowe – **1%**

Wszystkie działania organizacji opierają się na sprawnie działającym i kompetentnym zespole. Dlatego większość środków przeznaczamy na wynagrodzenia. Przy zachowaniu odpowiednich standardów działania staramy się minimalizować koszty administracyjne.

WYDATKI W 2013 ROKU*:



koszty wynagrodzeń zespołu – **67,7%**

inne koszty niezbędne do realizacji zadań (np. usługi graficzne, druk materiałów, zakup publikacji) – **22,3%**

koszty administracyjne (np. utrzymanie biura, Internet, księgowość) – **10%**

* Zestawienia przygotowane na potrzeby raportu – szczegółowe informacje na temat finansów Fundacji Panoptykon, w tym sprawozdania finansowe, dostępne są na stronie internetowej w zakładce „Organizacja".

PLANY I WYZWANIA

W najbliższych latach planujemy rozwinąć dotychczasowe działania, szczególnie w dziedzinie edukacji. Zamierzamy:

1) patrzeć na ręce kontrolującym i badać codzienne problemy związane z nadzorem;

2) namierzać kolejne niebezpieczne inicjatywy i naciskać na przyjęcie lepszych rozwiązań prawnych w sferze ochrony prywatności, kompetencji służb i monitoringu wizyjnego;

3) coraz szerzej informować o naszych działaniach i o tym, czego udało nam się dowiedzieć;

4) rozwinąć praktyczne i atrakcyjne zasoby edukacyjne: poradniki, infografiki, gry; przygotowywać do pracy trenerów w ramach Akademii Praw Cyfrowych;

5) „wychodzić na zewnątrz" – tworzyć okazje do dyskusji i nowe możliwości zaangażowania dla tych, którzy też mają potrzebę zmiany kawałka świata wokół siebie.

Oto kluczowe wyzwania, z którymi się przyjdzie nam się zmierzyć:

1. Problemów związanych z nadzorem jest coraz więcej – przyrastają geometrycznie wraz z rozwojem nowych narzędzi i ilością dostępnych na nasz temat danych. Nie ze wszystkimi będziemy mogli się zmierzyć, dlatego wiemy, że czekają nas niełatwe wybory.

2. Mówimy rzeczy trudne, obnażamy ciemną stronę rzeczywistości. Dlatego musimy liczyć się ze społecznym wyparciem: z tym, że nie każdy ma ochotę mierzyć się z nieprzyjemną prawdą o społeczeństwie nadzorowanym.

3. Po drugiej stronie barykady mamy państwo i biznes, które dysponują nieporównanie większymi zasobami. Dlatego nigdy nie możemy sobie pozwolić na moment nieuwagi. O naszej „pozycji negocjacyjnej" decydują merytoryczne argumenty – to nasze jedyne oręże.

4. Nie jest łatwo zdobyć środki finansowe na tego typu działalność, zwłaszcza że wielu instytucjom nasza misja jest nie na rękę, a w Polsce brakuje tradycji wspierania organizacji strażniczych.

WESPRZYJ NAS!

Fundacja Panoptykon jest jedyną w Polsce organizacją, która odpowiada na wyzwania związane z nadzorem. By skutecznie działać, bardzo potrzebujemy wsparcia finansowego wszystkich, którym bliska jest ta misja. Oto trzy główne powody, dlaczego wkład indywidualnych darczyńców jest dla nas tak ważny:

1. Dla organizacji strażniczej niezależność i wiarygodność to podstawa. Żeby je zachować, nie możemy korzystać ze wszystkich potencjalnych źródeł finansowania. Szczególnie ogranicza nas to, że patrzymy na ręce zarówno władzy publicznej, jak i firmom.

2. Aby działać sprawnie i skutecznie, musimy sprawnie reagować na pojawiające się problemy. Wielu z nich nie jesteśmy w stanie przewidzieć na etapie przygotowywania wniosków i projektów. Bez środków pochodzących z darowizn trudno o elastyczne i szybkie działania.

3. Mimo że problemy, którymi się zajmujemy, dotyczą każdego, nie należą do prostych i przystępnych. Nasza praca bywa porywająca, jednak na co dzień wymaga przede wszystkim żelaznej konsekwencji, cierpliwości i samozaparcia; rzadko przynosi szybkie i spektakularne sukcesy. Dlatego nie możemy liczyć na masowe okazjonalne datki, a jedynie regularne wsparcie osób, które wierzą, że to, co robimy, ma sens.

Pomóż nam sprawnie działać i rozwinąć przedsięwzięcia edukacyjne! Przekaż darowiznę na konto: 43 1440 1101 0000 0000 1044 6058 Nordea Bank Polska S.A. (w tytule przelewu wpisz „Darowizna”) lub ustaw stałe zlecenie w swoim banku. Bardzo liczymy na Twoje wsparcie!

Możesz nam pomóc również na inne sposoby:

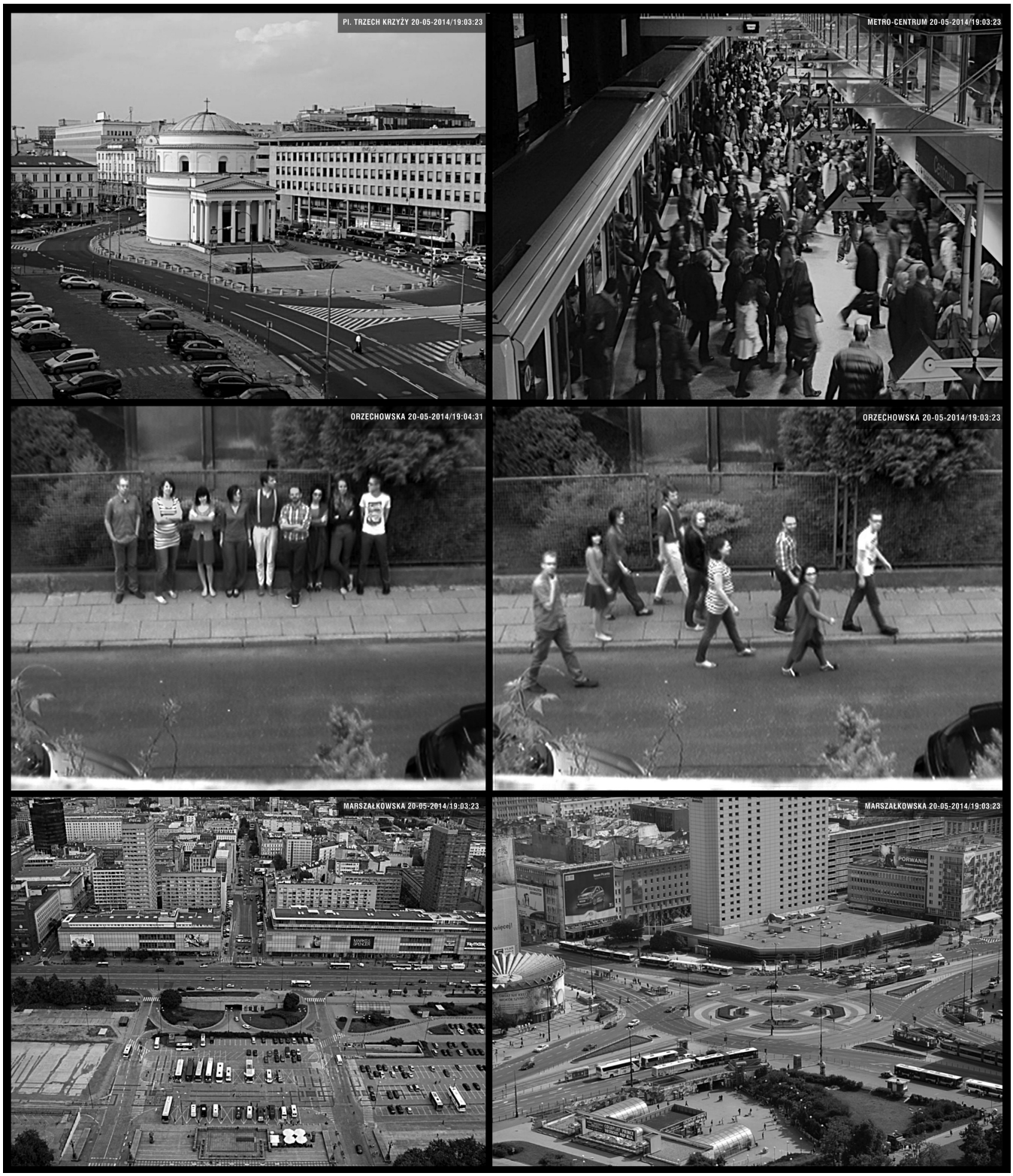
1. Wyrażaj swój sprzeciw wobec nadzoru i poparcie dla naszych działań: włączaj się w akcje i koalicje rzecznicze!

2. Podziel się wiedzą: przekazuj nam ciekawe informacje i wspieraj ekspercko!

3. Pomóż nam dotrzeć do nowych odbiorców: podsyłaj innym nasze materiały, informuj o działaniach!

Zespół Fundacji Panoptykon,
fot. Kamil Śliwowski

Serdecznie dziękujemy wszystkim, którzy nas wspierają: przyjaciołom i sympatykom angażującym się w nasze działania, służącym radą i pomocą, ale też konstruktywną krytyką, wolontariuszom, darczyńcom, grantodawcom. Bez Was nie byłoby Fundacji Panoptykon. To dzięki Wam możemy świętować 5-lecie naszej działalności. Robimy wszystko, by nie zawieść Waszego zaufania i skutecznie realizować panoptykonową misję.

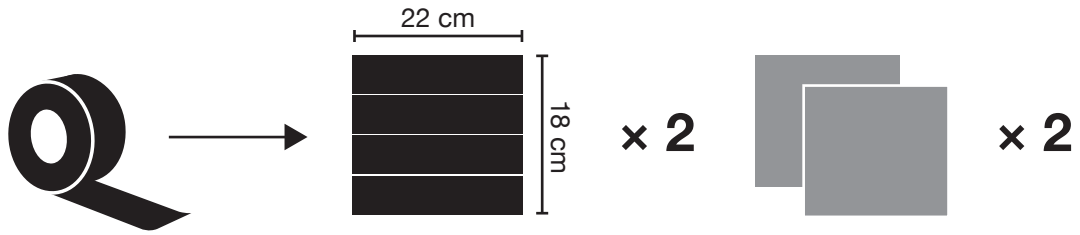


Fot. Roch Forowicz

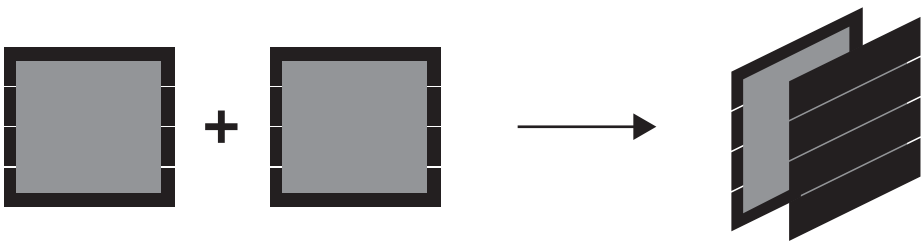
ZRÓB BEZPIECZNY PORTFEL

Zabezpiecz swoje karty przed nieautoryzowanym odczytem. Wystarczy umieścić w wewnątrz portfela metalową (np. z aluminium) warstwę, która będzie odbijać sygnały wysyłane do czipów RFID znajdujących się w Twoich kartach*.

1. Przygotuj z oderwanych pasów srebrnej taśmy klejącej (tzw. *ducttape*) dwa prostokąty o rozmiarach ok. 22 × 18 cm. Potem wytnij z folii aluminiowej dwa odrobinę mniejsze.

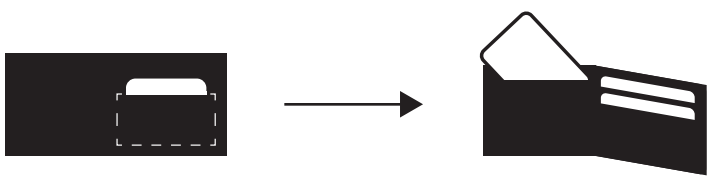


2. Sklej dwie warstwy taśmy z dwiema warstwami folii w środku.



3. Złóż prostokąt na pół i sklej boki tak, aby zrobić główną kieszeń.

4. Doklej w środku pasy taśmy, by utworzyć dodatkowe kieszenie na karty.



5. Przetestuj: włóż telefon komórkowy do środka, szczelnie zamknij portfel i spróbuj z innego aparatu zadzwonić na swój numer. Jeśli telefon pozostaje głuchy, to znaczy, że Twój portfel działa.

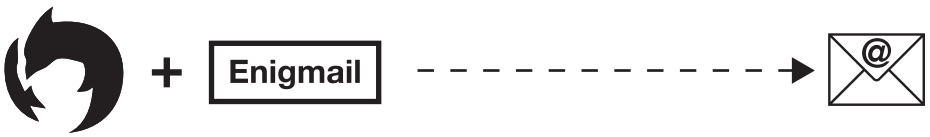
* Przykładowe zdjęcia: http://howto.wired.com/wiki/Make_a_Faraday_Cage_Wallet

ZACZNIJ SZYFROWAĆ SWOJĄ POCZTĘ

PGP (czyli *Pretty Good Privacy*) oraz GPG (*GNU Privacy Guard*) to rozwiązania pozwalające na podpisywanie Twoich wiadomości w zaufany sposób (aby każdy mógł sprawdzić, czy to na pewno Ty je wysyłasz) i szyfrowanie ich, tak aby były czytelne tylko dla Ciebie i odbiorcy maila. Dzięki temu możesz zabezpieczyć swoją korespondencję przed „okiem" pośredników (np. Twojego operatora telekomunikacyjnego lub dostawca poczty), instytucji publicznych oraz innych osób, które mogą być zainteresowane jej treścią.

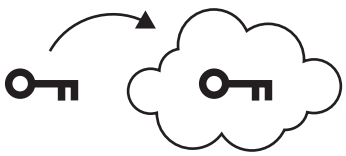
1. Będziesz potrzebować programu pocztowego, który obsługuje szyfrowanie – najpopularniejszym jest Mozilla Thunderbird z dodatkiem Enigmail. Możesz pobrać go za darmo z sieci.

2. Podłącz do programu swoją skrzynkę pocztową. Te popularne (takie jak Gmail czy Yahoo) zrobią to prawie automatycznie.

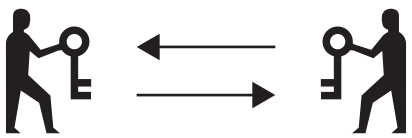


3. Za pomocą wtyczki Enigmail wygeneruj tzw. parę kluczy. Publiczny będzie służył innym osobom do szyfrowania poczty wysyłanej do Ciebie, natomiast powiązany z nim prywatny klucz, zabezpieczony Twoim hasłem, ich odszyfrowywaniu.

4. Publiczny klucz wyślij na serwer kluczy (np. za pośrednictwem programu pocztowego), możesz go też załączać do Twoich maili. Dzięki niemu będzie można zweryfikować Ciebie jako nadawcę wiadomości.



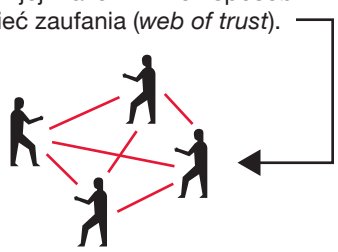
5. Wymień się kluczami publicznymi z osobami, z którymi chcesz się bezpiecznie komunikować w Internecie.



6. Aby zaszyfrować treść wysyłanych przez siebie wiadomości, używaj kluczy publicznych Twoich odbiorców (nigdy swojego).

7. Teraz możesz komunikować się bezpiecznie, pamiętaj jednak, by zawsze zweryfikować klucz osoby, z którą korespondujesz!

8. Kiedy zweryfikujesz czyjś klucz, możesz potwierdzić wirtualną tożsamość tej osoby powiązaną z jej mailem. W ten sposób rozwijasz sieć zaufania (*web of trust*).



KONTROLUJEMY KONTROLUJĄCYCH.
5 LAT FUNDACJI PANOPTYKON

OPRACOWANIE
Małgorzata Szumańska
Katarzyna Szymielewicz
Kamil Śliwowski

WSPÓŁPRACA
zespół Fundacji Panoptykon

KOREKTA
Urszula Dobrzańska

PROJEKT GRAFICZNY I SKŁAD
Filip Zagórski | filipzagorski.com

WYDAWCA

FUNDACJA
PANOPTYKON

panoptykon.org

Warszawa 2014

ISBN
978-83-938554-0-7