SŁOWO WSTĘPNE. JESZCZE MOŻEMY ODZYSKAĆ KONTROLĘ

Prywatność, wersja cyfrowa

Nie ma nic dziwnego w tym, że w cyfrowym świecie chcemy prowadzić normalne życie. Pracować, rozmawiać, przyjaźnić się, szukać pracy i informacji, nawiązywać znajomości i romanse. Kłócić się i kochać. Czasem mówić prawdę, a czasem kłamać. Możemy zechcieć podzielić się konkretną myślą czy obrazem z całym światem, ale niektóre przekażemy tylko najbliższym. Bez względu na to, jak wiele pokazujemy, i na ile prawdziwy lub wystylizowany jest to obraz, chcemy mieć nad nim kontrolę – im bardziej zależy nam na widoczności w sieci, tym większą uwagę przykładamy do tego, co do niej trafia. Chcemy dzielić się informacjami i kreować nasz wizerunek, jednocześnie zachowując to, co naprawdę intymne lub prywatne, tylko dla siebie.

Nieporozumieniem, natrętnie powracającym w debacie publicznej, jest pogląd, jakoby prawo do prywatności było równoznaczne z chęcią ukrycia się za firanką w oknie czy pod internetowym pseudonimem. Taka retoryka ma na celu zdewaluowanie prywatności, ma pokazać, że nie przystaje ona do potrzeb nowoczesnego społeczeństwa, a wręcz stawia człowieka, który jej poszukuje, w pozycji podejrzanego. Skoro nie chcesz być widoczny, zapewne

masz coś do ukrycia, prawda? A jeśli tak, to powinieneś się z tego wytłumaczyć.

Żaden człowiek nie musi tłumaczyć się z chęci zachowania prywatności. To jedno z naszych podstawowych praw, zagwarantowanych w narodowych konstytucjach i międzynarodowych konwencjach. Istotą prywatności, w wymiarze prawnym, nie jest możliwość zachowania sekretu, lecz autonomia informacyjna: samodzielne decydowanie o tym, kto, po co i w jaki sposób może przetwarzać informacje, które nas dotyczą. W praktyce oznacza to, że ze swoimi danymi możemy zrobić wszystko: od udostępnienia ich na stronie internetowej po zachowanie w ścisłej tajemnicy. Z perspektywy prawa ważne jest, aby była to nasza świadoma, niewymuszona decyzja, oparta na rzetelnych informacjach.

Tyle, jeśli chodzi o teorię. A jaka jest rzeczywista kondycja naszej prywatności w cyfrowym świecie? Najkrócej ujmując: bardzo słaba. Przede wszystkim dlatego, że podstawową infrastrukturą jest dla nas internet – sieć, która nie była tworzona z myślą o zachowaniu anonimowości jej użytkowników. Przeświadczenie, że w internecie możemy schować się za pseudonimem, a nawet udawać kogoś innego, wynika z subiektywnego doświadczenia, z gry pozorów, trwającej tak długo, jak długo nikomu nie zależy na jej przerwaniu. Dla serwerów i routerów – czyli urządzeń tworzących właściwą infrastrukturę internetu, które kierują ruchem i przekazują nam treści, których szukamy –

nasze pseudonimy nie są żadną przeszkodą. W internecie faktycznie funkcjonujemy jako numer, na tyle unikalny, by w razie potrzeby można było do nas trafić.

Na warstwę „infrastrukturalną", zapamiętującą wszystkie urządzenia i miejsca, z których łączymy się z siecią, nakłada się warstwa oprogramowania – aplikacji i skryptów, zdolnych zapamiętać jeszcze więcej. Są wśród nich aplikacje służące do wysyłania maili i wiadomości, wrzucania treści na portale społecznościowe czy robienia zakupów. Łatwo zapomnieć, że te kolorowe, przyjazne i dobrze znane interfejsy to tylko powierzchnia internetu. Pod nią nie jest już ani tak ładnie, ani przejrzyście. Niepoliczalne linijki kodu, dzięki którym wszystko na powierzchni działa tak, jak powinno, to świat dostępny już tylko programistom i geekom. Co jakiś czas po internecie rozchodzi się ostrzeżenie, że smartfonowa latarka wyciąga z naszego telefonu prywatne dane, a całkiem zabawna gra czy quiz na Facebooku używa naszej sieci kontaktów. W rzeczywistości śledzenie naszych ruchów i wyciąganie danych to dla internetowych aplikacji chleb powszedni. A kiedy próbujemy się buntować, słyszymy, że jest już za późno: innego internetu nie będzie.

Cyfrowa pańszczyzna

Eric Schmidt, dyrektor zarządzający Google'a, wywołał duże poruszenie stwierdzeniem: „Jeśli jest coś, o czym

wolałbyś, żeby inni nie wiedzieli, może przede wszystkim nie powinieneś tego robić". Chwilę później Mark Zuckerberg, założyciel i szef Facebooka, zaryzykował jeszcze dalej idącą tezę: „Pojawienie się serwisów społecznościowych w sieci oznacza, że ludzie nie oczekują już prywatności". To nie przypadek, że szefowie dwóch największych (jeśli chodzi o zasięg i wartość udziałów) firm, świadczących usługi w internecie, prowadzą retoryczną batalię, której celem jest podważenie naszej autonomii informacyjnej. Ich model biznesowy zakłada przejęcie pełnej kontroli nad cennym zasobem, jakim stały się informacje na temat ludzi.

Tezom Zuckerberga przeczą jednak reakcje jego klientów na zmiany tzw. polityki prywatności Facebooka. Za każdym razem, kiedy portal ograniczał kontrolę użytkowników nad tym, dokąd trafiają ich dane i kto może zobaczyć publikowane przez nich informacje, powstawały silne grupy protestujących, które straszyły opuszczeniem serwisu. Na nic się to zdało. Mark Zuckerberg nikomu nie obiecywał demokracji. Z perspektywy właściciela serwisu jego użytkownicy są towarem, a nie podmiotem, mogącym negocjować warunki. Faktycznym klientem jest ten, kto płaci za możliwość skomercjalizowania naszych danych, a więc przede wszystkim firmy zainteresowane tworzeniem reklam dopasowanych do naszego profilu.

Mimo tego, że jesteśmy skazani na regulaminy, których nie możemy negocjować, nie rezygnujemy z najpopularniejszych serwisów i codziennie zasilamy tę cyfrową

farmę świeżymi okruchami swojego życia. Koszt porzucenia internetowego świata okazuje się bowiem – przynajmniej w węższej perspektywie – wyższy, niż cena, jakiej żąda od nas Zuckerberg. Wszechobecny cyfrowy nadzór jest jak zanieczyszczone powietrze lub dym papierosowy: jego obecność dostrzegamy dopiero wtedy, gdy powraca jako choroba, dysfunkcja, realne ograniczenie, a w przypadku utraty kontroli nad własnymi danymi jako brutalna konfrontacja z tym, że pewien obszar praw i swobód został nam odebrany.

Czy jesteśmy w stanie zachować tę przestrzeń wolności lub – tam, gdzie bardzo się skurczyła – skutecznie o nią walczyć? Co zrobić w sytuacji, gdy nie mamy realnego wpływu na politykę państwa, w którym żyjemy, czy na warunki świadczenia usług internetowych, z których korzystamy? Te pytania stanowią punkt wyjścia dla Finna Bruntona i Helen Nissenbaum. „Nie ulega wątpliwości, że gromadzenie danych wplątane jest w asymetryczną relację władzy: rzadko mamy wybór, czy chcemy, czy też nie chcemy być monitorowani, co dzieje się ze zbieranymi informacjami albo jakie działania są podejmowane wobec nas w oparciu o wnioski wyciągane z tych informacji" – konstatują autorzy. Na tym jednak nie poprzestają. Szukają działającego, realnego i względnie prostego remedium na sytuację skrajnie asymetrycznej władzy nad informacjami, dotyczącej nas jako obywateli i konsumentów cyfrowego świata.

Nie chodzi o sytuację, jak tłumaczą autorzy, w której ktoś – ciekawska sąsiadka czy ksiądz w małym mieście – po prostu wie więcej niż reszta otoczenia. Mowa tu o zjawisku systemowym, nazywanym przez Bruntona i Nissenbaum „konwergencją asymetrii", czyli sytuacji, w której zbiega się wiele asymetrycznych relacji władzy. Nawet jeśli wiemy, kto zbiera o nas informacje, nie możemy ustalić, w jakim celu i z jakim skutkiem. Bardzo często nie mamy nawet świadomości, że dane na nasz temat prowadzą „podwójne życie" poza naszym laptopem czy telefonem. Co ważne, nasze dane funkcjonują nie tylko na serwerach znanych nam firm, takich jak Google czy Facebook. W złożonym ekosystemie handlu danymi o wiele większą rolę odgrywają tacy potentaci jak (raczej unikający rozgłosu) Acxiom, który na zamówienie klienta jest w stanie dostarczyć mu tysiące „internetowych dusz", chętnych lub wręcz zdesperowanych, by zapłacić za oferowany produkt.

Nadzór nasz powszedni

Konwergencja asymetrii powoduje, że podlegamy władzy, której nie dostrzegamy i na którą nie mamy rzeczywistego wpływu. Nie oznacza to jednak, że faktycznie jej nie odczuwamy. Brunton i Nissenbaum pokazują całe spektrum sytuacji, kiedy władza oparta na danych wkracza do naszego życia: od utraty kredytu (niska ocena w systemie

ratingowym) czy uniemożliwienia nam pracy w atrakcyjnym miejscu (niewiarygodny profil w sieciach społecznościowych), przez ograniczenie naszej mobilności (dodatkowe kontrole, a nawet zakaz wstępu na pokład samolotu w związku z podejrzanym profilem podróżnego lub wpisem w międzynarodowej bazie danych), pozbawienie członkostwa w ważnej dla nas grupie czy możliwości zdobycia wykształcenia (niewłaściwy profil na etapie rekrutacji), aż po blokadę środków finansowych, przesłuchanie, a nawet areszt motywowane podejrzaną transakcją czy zachowaniem.

Autorzy *Zmyl trop. Na barykadach prywatności w sieci. Przewodnik* nie pozostawiają wątpliwości: świat zbudowany na przeświadczeniu, że każdy może być terrorystą, a przynajmniej stanowi zakłócenie dobrze działającego systemu, nie jest dla nas bezpieczny. Wystarczy pomyłka lub nieco nadgorliwy algorytm, aby każdy z nas mógł stać się obiektem śledztwa, zostać zatrzymany, napiętnowany czy ukarany. Wystarczy zła wola polityków, by dzięki władzy nad informacjami sparaliżować procesy ważne dla demokracji i rządów prawa – stłumić protest, zaszantażować liderów legalnej opozycji, ocenzurować medialną krytykę. Nawet jeśli z perspektywy względnie stabilnej i działającej demokracji takie zagrożenia mogą wydawać się abstrakcyjne, warto pamiętać, że rząd w każdej chwili może się zmienić, a z nim wola polityczna i szacunek dla demokratycznych procedur.

Wszechogarniający cyfrowy nadzór to zasada działania nie tylko usług, na których wyrosły internetowe imperia, lecz także nowoczesnego państwa, chcącego i coraz lepiej potrafiącego zarządzać społeczeństwem. Gromadzenie, łączenie i analiza danych dzięki coraz bardziej wyrafinowanym algorytmom to kluczowe narzędzie w pracy policji i służb, których zadaniem jest wykrycie zagrożenia, zanim zmaterializuje się ono w formie zamachu terrorystycznego. Czy podczas kupowania większego zapasu syntetycznego nawozu w internecie, sprawdzania w kilku źródłach niepokojących doniesień z Syrii czy tłumaczenia na polski arabskiego słowa, które nas zaintrygowało, nie stajemy się potencjalnymi podejrzanymi? Z tych samych technik, używanych przez banki do wykrywania podejrzanych transakcji na kontach swoich klientów, chętnie korzysta urząd skarbowy, chcący namierzyć nierzetelnych podatników. Ministerstwo Finansów utworzyło spółkę celową, mającą analizować dane podatników pod kątem „prawdopodobieństwa wyłudzenia VAT". Czy przy okazji tych analiz zajrzy także na nasze profile społecznościowe i porówna majątek widoczny na zdjęciach z wykazanym w zeznaniach podatkowych?

W każdej sferze, w której państwo prowadzi aktywną i obciążającą budżet politykę, otwiera się obszar do gromadzenia i analizy danych motywowanej oszczędnościami lub chęcią sprawnego, racjonalnego zarządzania. Analizy, która z uwagi na stosowane metody i skalę musi opierać się na

prostych statystycznych korelacjach, pomija tym samym specyfikę indywidualnych życiorysów i motywacji, a nierzadko powiela utarte, krzywdzące stereotypy. To, co wydaje się racjonalne i korzystne z perspektywy państwa, dla konkretnego obywatela łatwo przybiera formę niesprawiedliwego traktowania. W optyce policji czy Agencji Bezpieczeństwa Wewnętrznego cudzoziemiec, a szczególnie muzułmanin mieszkający w Polsce, to osoba, której warto się przyglądać. Z perspektywy praw człowieka mamy tu do czynienia z niczym innym, jak nieuzasadnionym i dyskryminującym profilowaniem etnicznym. Dla urzędu pracy, mającego za zadanie optymalnie rozporządzać środkami otrzymanymi z centralnego budżetu na wsparcie osób bezrobotnych, samotna matka niepełnosprawnego dziecka to osoba, której nie ma sensu pomagać, ponieważ i tak nie znajdzie ona stałej pracy. Z jej perspektywy taka klasyfikacja będzie krzywdząca i niezrozumiała, bo przecież chce i potrzebuje wrócić do pracy. System, opierający się na korelacjach statystycznych, osobistych motywacji po prostu nie dostrzega.

W poszukiwaniu podmiotowości

Czy wobec władzy działającej według nieprzejrzystych algorytmów i gromadzącej informacje, nad którymi dawno utraciliśmy kontrolę, mamy jakieś prawa? Istotną różnicą

między światem, opisywanym przez autorów *Zmyl trop. Na barykadach prywatności w sieci. Przewodnik*, a Unią Europejską są ramy prawne, w których funkcjonujemy. W przeciwieństwie do obywatela Stanów Zjednoczonych, Europejczyk dysponuje wieloma prawami, które pomagają mu w relacjach z państwem czy korporacją. Przede wszystkim mamy prawo do informacji o tym, kto i jakie dane na nasz temat przetwarza. Powinno nas to interesować szczególnie wówczas, gdy nasze dane zmieniają właścicieli i zaczynają funkcjonować w internetowym obiegu. Mamy też prawo sprzeciwić się wykorzystywaniu przez firmę naszych danych w celach marketingowych, co może przybrać formę zaawansowanego profilowania, także w oparciu o dane wrażliwe (np. informacje o naszym zdrowiu czy nałogach). Ile firm dobrowolnie przestrzega tych standardów? Ile osób ma świadomość swoich praw i determinację, by z nich skorzystać, a w razie potrzeby – upominać się o ich respektowanie przed odpowiednimi organami?

Jako konsumenci i obywatele cierpimy na chroniczne niedoinformowanie, jesteśmy zaabsorbowani swoimi sprawami, niezorganizowani. Nie chcemy tracić czasu i pieniędzy na prawne batalie. Po drugiej stronie najczęściej występuje podmiot wyposażony w wiedzę, zasoby finansowe i stałą obsługę prawną, który nie boi się zaryzykować. Ta asymetria powoduje, że nawet jeśli formalnie przysługują nam różne prawa, to rzadko z nich korzystamy. Wiele firm zbudowało swój model biznesowy właśnie na tej

bierności lub niewiedzy. Sytuacja obywateli i konsumentów mieszkających w Europie nie jest więc radykalnie odmienna od tej, którą opisują Finn Brunton i Helen Nissenbaum – również jesteśmy słabi.

Czy mamy do dyspozycji jakieś inne narzędzia niż skomplikowane procedury prawne? Jak najbardziej. Podobnie jak śledzące nas państwa i korporacje, my również możemy sięgnąć po możliwości, jakie stwarza technologia. Nie jest to wiedza tajemna, dostępna tylko dla zaawansowanych użytkowników. To podważający naszą inteligencję mit; korzystają z niego firmy, oferujące masowe rozwiązania za cenę, która wielokrotnie przebija realną wartość ich usług. Najwspanialszą cechą internetu jest to, że nadal możemy się po nim poruszać bez pośrednictwa komercyjnych firm, nie powierzając nikomu naszych sekretów i odrzucając śledzenie jako „warunek świadczenia usług". By wysłać maila czy opublikować treść nie potrzebujemy wcale „usługi" – możemy zrobić to sami. Istnieją również poradniki tłumaczące nam krok po kroku, jak w świadomy, bezpieczny i niezależny sposób korzystać z internetu, tworzone przez grupy aktywistów i organizacje pozarządowe, np. Tactical Technology Collective czy Fundację Panoptykon.

Możemy szyfrować maile (za pomocą PGP lub aplikacji takich jak Proton Mail), korzystać z szyfrowanych komunikatorów (np. Signala), zainstalować wtyczki do przeglądarek, blokujące reklamy oraz śledzące nas „ciasteczka", przetestować Wirtualne Sieci Prywatne (VPN)

czy sieci anonimowe (np. TOR), dające nam możliwość „zgubienia" internetowej tożsamości. A przede wszystkim przejść z komercyjnego, zamkniętego oprogramowania dostarczanego przez firmy oczekujące zysków na software rozwijany w ramach internetowych społeczności, otwarty i niekomercyjny (jak np. Linux).

Każdy z tych eksperymentów wymaga pewnego poziomu świadomości oraz determinacji, aby poradzić sobie z początkowymi trudnościami i przyzwyczaić się do nowego, technologicznego doświadczenia. Trzeba też pamiętać o tym, że niektóre zabezpieczenia mogą nas narazić na nieoczekiwane ryzyko, paradoksalnie uczynić „bardziej widocznymi". Na przykład szyfrowane maile lub fakt korzystania z sieci TOR mogą sprowokować zwiększone zainteresowanie służb (zgodnie z logiką: „skoro próbujesz się schować, to zapewne masz coś do ukrycia"). Prościej na pewno więc nie będzie, jednak satysfakcja z tego, że udało nam się wyzwolić z cyfrowej pańszczyzny i urządzić cyfrowe życie na naszych własnych zasadach, będzie wielka.

Sztuka mylenia tropów

Dla osób szukających innej drogi Finn Brunton i Helen Nissenbaum mają ciekawą propozycję. I co ważne, nie jest to rozwiązanie przeznaczone tylko dla zaawansowanych użytkowników. Sztukę „znikania w cyfrowej mgle" może

opanować każdy. Bardziej niż obycie z technologią, przyda się w niej odwaga, cierpliwość i wyobraźnia. Autorzy zdają się mówić: jeśli nie możesz albo nie potrafisz się ukryć, nadal jesteś w stanie zmylić tropy lub zniknąć w tłumie.

Kto powiedział, że na swoim profilu społecznościowym możesz publikować tylko to, co faktycznie myślisz, robisz lub chcesz przekazać innym? Czy nie zabawniej i ciekawiej byłoby umówić się ze znajomymi na kod, w którym są w stanie rozpoznać, co jest na serio, a co jest tylko grą lub żartem? To bardzo prosty sposób, by oszukać profilujący algorytm, dla którego intencje nie mają znaczenia. Dlaczego mielibyśmy zawsze uczciwie oznaczać swoją lokalizację, czy też pozwalać, by nasze urządzenie robiło to automatycznie za nas? Wystarczy jedno kliknięcie i nasz post czy zrobione przez nas zdjęcie zostaną „wysłane" z dowolnego miejsca na świecie. Wystarczy, że łącząc się z internetem, skorzystamy czasem z wirtualnego serwera (VPN), by nasz geograficzny profil został poważnie zaburzony („co ten spokojny i przewidywalny użytkownik nagle robi na drugiej półkuli?").

Brunton i Nissenbaum nie obiecują, że opisywane przez nich techniki mylenia tropów to odpowiedź na każdy problem, jaki napotkamy w sieci lub w relacji z inwigilującym nas państwem. Uczciwie podkreślają, że stosowane techniki muszą być dobrze dopasowane do kontekstu i celu. Mogą ostatecznie nie uchronić nas przed namierzeniem, ale z pewnością wydłużą czas operacji lub zwiększą

koszt pracy namierzającego. Niekoniecznie sprawią, że dostaniemy upragnioną pracę lub kredyt, ale ochronią nas przed sprofilowaniem na potrzeby internetowej reklamy, zwiększą chaos informacyjny i zaburzą działanie algorytmów, czekających na proste prawidłowości. Podrzucanie fałszywych tropów to wreszcie sztuka sama w sobie i zabawa, więc warto ich czasem spróbować.

Dlaczego mielibyśmy podjąć wysiłek i zagrać w tę grę? Kluczowym powodem, do którego często powracają autorzy, jest sam fakt, że żyjemy w świecie pełnym „nieznanych nieznanych" (*unknown unknowns*). Nie jesteśmy w stanie przewidzieć, w jaki sposób informacja o nas zostanie wykorzystana i na ile okaże się to dla nas niebezpieczne lub niekomfortowe. W sytuacji dużej niepewności i wysokiego ryzyka mądry człowiek porusza się ostrożnie i uważa na ślady, jakie za sobą zostawia. Z myślą o takich – raczej rozważnych niż szalonych – odbiorcach Finn Brunton i Helen Nissenbaum przygotowali swoisty poradnik kreatywnego korzystania z cyfrowych technologii, który można dopasować do różnych potrzeb, filozofii życiowych i szerokości geograficznych. Inspirującej lektury!

Katarzyna Szymielewicz