FUNDACJA PANOPTYKON

Śledzenie i profilowanie w sieci:

W czym problem? Co się zmieni w prawie?
Jak może wyglądać przyszłość?

Katarzyna Szymielewicz
Współpraca: Weronika Adamska
Wrzesień 2017

Wprowadzenie

Dużymi krokami zbliża się moment, w którym firmy opierające swój model biznesowy na wykorzystywaniu danych osobowych będą musiały dostosować się do nowych reguł gry. Generalne rozporządzenie o ochronie danych osobowych (RODO) obowiązuje już od 2016 r., a po 25 maja 2018 r. zacznie być w pełni stosowane. Podstawowe zasady przetwarzania danych nie zmienią się w sposób znaczący, ale pojawią się nowe – jednolite na całym europejskim rynku – obowiązki dla firm, połączone z silniejszymi uprawnieniami dla osób, których dane są przetwarzane (np. prawo do przeniesienia danych). Zwiększą się wymagania, jeśli chodzi o przejrzystość (np. automatycznego podejmowania decyzji) i ocenę ryzyka, jak również samo projektowanie technologii i domyślne ustawienia prywatności.

Jednocześnie trwają prace nad rozporządzeniem o prywatności w łączności elektronicznej (ePrivacy Regulation), które ma doprecyzować reguły i standardy techniczne dla komunikacji elektronicznej i usług realizowanych przez Internet. To rozporządzenie przeniesie ogólne zasady ochrony prywatności wynikające z RODO na poziom praktycznych wyzwań, takich jak dopasowywanie reklam do preferencji użytkowników Internetu w czasie rzeczywistym, profilowanie wyników wyszukiwania i strumieni aktualności czy monitorowanie aktywności użytkowników za pośrednictwem „inteligentnych" sensorów.

> **Europejski regulator dostrzega wszechobecność i problematyczność gromadzenia danych o użytkownikach nowych technologii poza ich kontrolą. Próbuje na to wyzwanie odpowiedzieć w zrównoważony sposób, szanując różne modele biznesowe i tworząc równe pole dla wszystkich przedsiębiorców. Trudno jednak przewidzieć, jak na zaproponowane reguły gry zareaguje rynek, szczególnie branża marketingu internetowego i wiodące platformy internetowe. Czy dostrzegą w nich szansę na rozwój, czy tylko przeszkodę, którą trzeba ominąć?**

Od początku prac nad reformą prawa o ochronie danych osobowych organizacje reprezentujące interesy internetowych wydawców i reklamodawców w alarmistycznym tonie przestrzegały przed „końcem Internetu, jaki znamy". Argumentowały, że usługi internetowe – w szczególności serwisy informacyjne – utrzymują się głównie dzięki targetowanej reklamie i że ten model generowania zysku „musi zostać". Odpowiadały im organizacje reprezentujące samych użytkowników i odbiorców treści, pytając, czy rynek

reklamowy musi się rozwijać w oparciu o nieprzejrzyste i nieetyczne praktyki, takie jak śledzenie ludzi bez ich wiedzy i zgody.

> **O ile z perspektywy wydawców i reklamodawców główne wyzwanie sprowadza się do utrzymania wysokiej klikalności banerów reklamowych, o tyle dla wielu użytkowników stało się jasne, że ich osobista stawka w Internecie naszpikowanym śledzącymi skryptami jest o wiele wyższa. Nie chodzi już o to, czy nabędą kolejną parę butów albo nowszy telefon, ale o to, kto i w jakim celu kupi ich profil oraz co się w nim znajdzie.**

Techniki śledzenia i profilowania stają się coraz bardziej inwazyjne, nie oszczędzając żadnej sfery życia prywatnego. Dane dotyczące zdrowia (także intymnego czy psychicznego), sytuacji finansowej, pochodzenia etnicznego, relacji osobistych, nałogów, słabości, marzeń i aspiracji miliardów ludzi są zbierane lub generowane (na zasadzie predykcji) oraz integrowane w sposób, który nie uwzględnia możliwych ryzyk. Kojarzeniem tego typu danych poza kontrolą ludzi, których one dotyczą, są zainteresowani nie tylko ubezpieczyciele czy potencjalni pracodawcy, ale coraz częściej także partie konkurujące w wyścigach wyborczych.

Na progu europejskiej reformy ochrony danych osobowych warto spojrzeć trzeźwo na wyzwania stojące nie tylko przed regulatorem, ale także (czy wręcz przede wszystkim) przed samymi uczestnikami internetowego rynku. Czy będziemy w stanie znaleźć kompromis między interesami komercyjnych graczy, przyzwyczajonych do swobodnej eksploatacji danych, a oczekiwaniami ludzi, którzy w obecnym modelu generowania zysku utracili podmiotowość, ale chcą ją odzyskać? Czy lepsza wersja komercyjnego Internetu jest możliwa? Jeśli tak, jak powinna działać? Jeśli nie, jakie czekają nas konsekwencje i ryzyka pozostania przy obecnym modelu?

—

Celem tego opracowania jest zwięzłe omówienie najpoważniejszych problemów związanych z praktykami śledzenia i profilowania w sieci, tak jak wyglądają one z perspektywy 2017 r. (rozdział 1), przedstawienie koncepcji europejskiego regulatora odpowiadających na te wyzwania (rozdział 2) oraz zarysowanie możliwych przyszłych scenariuszy w sferze ich implementacji (rozdział 3).

Rozdział 1

Komercyjny Internet

Rzut oka z perspektywy 2017 r.

Dane osobowe pod różnymi postaciami stały się nową walutą. Szacuje się, że wartość rynkowa ogółu danych przetwarzanych online na terenie Unii Europejskiej osiągnie do 2020 r. wartość 739 miliardów euro[1]. Od kilku dekad różne branże (handlu detalicznego, turystyczna, dóbr konsumpcyjnych, mediów, telekomunikacyjna, bankowa, ubezpieczeniowa i inne) gromadzą i wykorzystują informacje o swoich klientach, a częściowo także wymieniają się nimi. Firmy nauczyły się skutecznie wykorzystywać techniki śledzenia w sieci do identyfikowania, zdobywania i przywiązywania do siebie atrakcyjnych klientów, wyliczania ich wartości oraz do „efektywnego inwestowania środków" w „najbardziej dochodowe grupy klientów".

Analiza zainteresowań, potrzeb i słabości użytkowników Internetu służy w praktyce do ich kategoryzowania i hierarchizowania. Ta wiedza – czy też raczej przeświadczenia – na temat (potencjalnych) klientów są następnie wykorzystywane do ich pozyskiwania i obsługiwania. Firmy opracowały strategie włączania całych grup klientów do określonych działań promocyjnych i wyłączania ich z nich, taktyki wpływania na ich zachowania (odtworzone na podstawie zebranych danych) oraz metody mierzenia i optymalizowania wyników takich działań. Strategie i modele biznesowe firm w coraz większym stopniu opierają się na ilości i jakości danych osobowych, jakie są w stanie pozyskać lub sprzedać innym.

> **Bezpośrednią ofiarą tej pogoni za danymi jest prywatność użytkowników cyfrowych technologii, nieświadomych toczonej za ich plecami gry.**

[1] Komisja Europejska, *European Data Market Study*, https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy.

> **Najdrobniejsze i najpoważniejsze decyzje zakupowe, codzienne zachowania w sieci (od pojedynczego ruchu myszką i kliknięcia po zalogowanie na stronie internetowej), schematy przemieszczania się, relacje społeczne, zainteresowania oraz najbardziej intymne chwile miliardów ludzi są na bieżąco rejestrowane, analizowane i oceniane.**

W tym kontekście nie powinno nikogo dziwić, że sektor obsługujący przetwarzanie i przechowywanie danych osobowych ma wkrótce osiągnąć tak zawrotną wartość. Nadal jednak tylko wierzchołek góry lodowej, jaką tworzą internetowe systemy śledzenia, jest znany użytkownikom. Zdecydowana większość procesów zachodzących na „zapleczu" Internetu odbywa się w cieniu, a ustalenie ich realnego znaczenia i możliwych konsekwencji sprawia trudność nawet badaczom i technicznym ekspertom.

Świadomi tych trudności i ograniczeń, na potrzeby tego opracowania pokusiliśmy się o zebranie przynajmniej podstawowych informacji, jakie posiadamy dzięki badaniom akademickim i raportom niezależnych ekspertów, a które pokazują skalę, metody i techniki śledzenia w kontekście usług internetowych.

1.1. Urządzenia mobilne, aplikacje i sensory

Katalizatorem i kluczowym narzędziem śledzenia i profilowania na potrzeby komercyjne stały się smartfony – komputery osobiste nowej generacji, z którymi większość użytkowników nie rozstaje się przez całą dobę, w jednym urządzeniu łącząc sferę osobistą i zawodową oraz angażując się w setki (o ile nie tysiące) drobnych interakcji dziennie. Standardowo korzystanie z aplikacji mobilnych generuje metadane: adres IP, czas dostępu, długość trwania sesji, rodzaj używanego oprogramowania, lokalizację urządzenia[2]. Z metadanych – w połączeniu z informacjami o tym, w jaki sposób dana osoba korzystała z aplikacji czy usługi (gdzie kliknęła, czego szukała, co kupiła) – powstaje dokładny profil użytkownika, obejmujący także jego cechy osobowości i opis przyzwyczajeń i indywidualnego trybu życia. Takie dane mają niejednokrotnie wrażliwy charakter i głęboko ingerują w prywatność: wystarczy wspomnieć o aplikacjach typu *fitness tracker* czy zdobywających coraz większą popularność aplikacjach rejestrujących cykl menstruacyjny i seksualne zachowania kobiet.

[2] Me and My Shadow, *Location Tracking,* https://myshadow.org/location-tracking.

Przeciętny użytkownik smartfona korzysta aktywnie z około 27 aplikacji miesięcznie. Tylko nieliczni inwestują czas i uwagę w zapoznanie się z ich regulaminami i politykami prywatności. Badanie przeprowadzone przez naukowców z Carnegie Mellon University wykazało, że przeciętna polityka prywatności liczy aż 2518 słów[3], a jej przeczytanie zajmuje ok. 10 minut. Jak wskazują autorzy raportu „Appfail Report"[4], zrealizowanego przez norweską Radę ds. Konsumentów, polityki prywatności najpopularniejszych aplikacji są nie tylko długie, ale też często nieczytelne i niezrozumiałe dla potencjalnego użytkownika.

W efekcie większość użytkowników aplikacji i urządzeń mobilnych rozpoczyna korzystanie z nich bez świadomości podstawowych funkcji i procesów związanych z przetwarzaniem ich danych osobowych. Wielu z nich zapewne nigdy nie wyraziłoby zgody na bardziej ryzykowne transakcje (np. przekazanie ich danych innym podmiotom bez związku z istotą usługi czy permanentne lokalizowanie) – ale wychodzą z założenia, że nie mają wyboru[5]. Do głębszej analizy polityk prywatności zniechęca adhezyjny charakter umów: jedyne, co użytkownicy mogą zrobić, to pójść gdzie indziej. Często tylko po to, by się przekonać, że czeka na nich równie zły regulamin i pełna wytrychów prawnych polityka prywatności, albo zderzyć się z faktycznym brakiem konkurencyjnych usług. Ostatecznie korzystanie z wielu urządzeń mobilnych nie jest dziś możliwe bez konta na serwerze Google'a, Microsoftu czy Apple'a.

Na co „zgadzają się" użytkownicy?

Wystarczy pobieżnie przejrzeć polityki prywatności najpopularniejszych aplikacji mobilnych, aby odtworzyć rynkowy „standard przetwarzania danych osobowych", z jakim mierzy się typowy użytkownik smartfona. I tak – bez względu na rodzaj i funkcje zainstalowanej aplikacji – ów użytkownik zapewne będzie musiał zezwolić jej na:

- dostęp do swoich kontaktów,
- dostęp do kalendarza,
- dostęp do historii przeglądanych stron i zakładek,
- dostęp do wrażliwych logów aplikacji systemowych,

---

[3] Por. raport A. M. McDonald, L. F. Cranor, *The Cost of Reading Privacy Policies,* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[4] The Norwegian Consumer Council, *Appfail Report – Threats to Consumers in Mobile Apps*, https://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/.

[5] Por. J. A. Obar, A. Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465.

- dostęp do aplikacji aktywnych na danym urządzeniu,
- dostęp do historii wybieranych numerów,
- dostęp do wszystkich profili użytkownika na danym urządzeniu,
- dostęp do treści i metadanych wysyłanych SMS-ów,
- dostęp do załączników e-maili,
- możliwość zmiany ogólnych ustawień telefonu.

Nie wszystkie z powyższych upoważnień i nie w każdym kontekście muszą być problematyczne. Na przykład uprawnienie do dostępu do aktywnych aplikacji zapewne nie wzbudzi zastrzeżeń w przypadku aplikacji służących do zarządzania zadaniami (często zintegrowanych z kalendarzem czy kontem pocztowym). Jeśli jednak o taki dostęp „prosi" oprogramowanie typu latarka czy fitness tracker, jest to już powód do niepokoju. Aktywność innych aplikacji to przecież bogate źródło wiedzy o preferencjach i przyzwyczajeniach użytkownika.

Tę samą logikę można odnieść do udostępniania kontaktów zgromadzonych w telefonie – do czego jest on potrzebny aplikacji, która nie oferuje żadnej funkcji związanej z zarządzaniem kontaktami? I tak dalej. Oczywiście, natura tych pytań jest retoryczna. Twórcy aplikacji nie kryją, że często ich główną intencją i powodem, dla którego oferują coś za darmo, jest zebranie danych, których sama aplikacja nie wykorzystuje, ale które mają realną, rynkową wartość. Dlatego większość aplikacji dostępnych na rynku przekazuje dane stronom trzecim.

Lokalizacja poza kontrolą użytkowników

Nagminność śledzenia lokalizacji przez aplikacje mobilne to jeden z najpoważniejszych problemów w sferze ochrony prywatności. Powszechność tego zjawiska wiąże się ze względną łatwością pozyskania tego typu danych po stronie projektantów aplikacji i obiektywną trudnością po stronie użytkownika, który chciałby takie śledzenie powstrzymać. Niewiele w tym zakresie pomogą zmiany samodzielnie wprowadzone w ustawieniach telefonu czy konkretnej aplikacji. Skutecznych sposobów na ustalenie lokalizacji bez wiedzy i zgody użytkownika jest wiele: w grę może wchodzić np. dostęp do technicznych danych o logowaniu telefonu do stacji przekaźnikowych, śledzenie przy pomocy czipu GPS zainstalowanego w telefonie lub wewnętrznego rejestru lokalizacji (*location logs*).

Przybliżone dane o położeniu użytkownika można również odtworzyć na podstawie historii zapamiętanych sieci WiFi (nawet jeśli nie doszło do połączenia z siecią), historii

przypisanych danemu urządzeniu adresów IP czy metadanych zapisanych na tym urządzeniu zdjęć, które standardowo zawierają współrzędne geograficzne ustalone w momencie robienia zdjęcia. W praktyce mało który użytkownik jest w stanie zapanować nad wszystkimi śladami ujawniającymi jego lokalizację. Ewentualna próba ochrony swojej prywatności kończy się zwykle na wyłączeniu w telefonie funkcji lokalizacji GPS. Twórcy aplikacji doskonale to wiedzą i dlatego tak chętnie zastrzegają sobie dostęp do mniej oczywistych wskaźników.

Nowa jakość śledzenia: wszechobecne sensory

Techniki mobilnego śledzenia, mimo wysokiej skuteczności, stale ewoluują. W ostatnich latach weszły na kolejny poziom dzięki możliwości wykorzystania sensorów w rozmaitych urządzeniach, które wkroczyły do biur i mieszkań. Czytniki e-booków, smart TV, termostaty, czujniki gazu, inteligentne lodówki, okulary, szczoteczki do zębów i zabawki, a ostatnio nawet autonomiczne odkurzacze zasilają bazy danych nowymi wskaźnikami, zbieranymi i nierzadko przekazywanymi dalej w czasie rzeczywistym. Tego typu urządzenia, analogicznie do smartfonów, zapewniają firmom rosnący dostęp do informacji na temat preferencji i przyzwyczajeń ich klientów w wielu obszarach życia codziennego.

Zbierane dane mogą być kontrolowane przez jedną firmę (tak jest np. w przypadku czytnika Kindle), jak również udostępniane stronom trzecim, najczęściej w celach marketingowych (w tym zaproponowania kolejnych, także śledzących, aplikacji). Do baz danych, puchnących dzięki wszechobecnym sensorom, dostęp mogą mieć również tzw. platformy IoT – zaawansowane aplikacje ułatwiające firmom analizowanie i zarządzanie danymi, dostarczane i obsługiwane przez wyspecjalizowane korporacje.

W ekosystemie opartym na komercjalizacji danych osobowych nic się nie marnuje, a zysk z niego może czerpać wiele niezależnych podmiotów. Dobrym przykładem jest wykorzystanie sensorów i inteligentnego oprogramowania w samochodach. Terabajty danych generowane przez inteligentne auta to realna wartość dla producentów, dealerów samochodowych, leasingodawców, autorów wyspecjalizowanych w tej branży aplikacji, producentów oprogramowania do telefonów komórkowych takich jak Google czy Apple, brokerów danych, agencji reklamowych, jak również służb porządkowych czy windykatorów (a lista jest znacznie dłuższa). Każdy z tych profesjonalnych graczy jest w stanie znaleźć coś dla siebie, nie odbierając wartości innym.

W najgorszej pozycji jest sam użytkownik, którego żaden z wymienionych powyżej podmiotów nie ma ochoty informować o swoich interesach ani tym bardziej prosić o zgodę na skorzystanie z tak łatwo dostępnego bogactwa. Jeśli ten trend nie zostanie odwrócony, systemy połączonych urządzeń, działające w ramach tzw. Internetu rzeczy (ang. IoT –

Internet of Things), mogą stać się najpoważniejszym, bezprecedensowym zagrożeniem dla prywatności, a w niektórych przypadkach (np. inteligentnych samochodów czy sprzętu medycznego) także fizycznego bezpieczeństwa ich użytkowników.

1.2. Skrypty śledzące i targetowane reklamy

Dostawcy treści w Internecie (wydawcy gazet, właściciele blogów, media społecznościowe) utrzymują się przede wszystkim ze sprzedaży przestrzeni reklamowej. Ten model finansowania oznacza, że ich realnym klientem jest nie ten, kto odwiedza stronę, ale ten, kto płaci za wyświetlenie na niej reklamy. Marketingowa przewaga tych mediów nad tradycyjną prasą i telewizją wzięła się z nieporównanie lepszych możliwości targetowania przekazu. Czasy, w których reklamodawcy inwestowali w kampanie kierowane do „kobiet z dużych miast" czy „mężczyzn w pewnym przedziale wiekowym", są daleko za nami. Wygrywa reklama kontekstowa, skierowana do zdefiniowanego odbiorcy – i to w momencie, w którym jest szansa, że ten konkretny człowiek kupi oferowany mu produkt.

Rosnący popyt na jak najlepiej stargetowaną reklamę przekłada się nie tylko na konieczność wykrojenia atrakcyjnej przestrzeni reklamowej, ale przede wszystkim – śledzenia użytkowników. Tylko znając ich zainteresowania, siłę nabywczą i sposoby reagowania, dostawcy treści są w stanie zapewnić swoim klientom odpowiedni wskaźnik klikalności (ang. *click through rate*) i uzyskać dobrą cenę za wyświetlane reklamy. Taka operacja marketingowa wymaga rzetelnych danych na temat wieku, płci, miejsca zamieszkania, zainteresowań, sytuacji życiowej, sytuacji majątkowej, historii zakupów, sieci społecznościowej, a nawet cech osobowości[6] potencjalnego klienta. Ilu z nich ujawnia je świadomie, z własnej woli? Niewielu. Nawet świadomość tego, że tak szczegółowe dane są zbierane lub generowane (na zasadzie predykcji) w celach marketingowych, nie jest powszechna[7].

[6] https://en.wikipedia.org/wiki/Big_Five_personality_traits

[7] Por. badania The Chartered Institute of Marketing, *Whose data is it anyway?*, https://exchange.cim.co.uk/blog/consumers-in-the-dark-about-their-own-data/.

„Some 92% of respondents did not fully understand how information that companies gleaned about them was being used, and they were highly sceptical about marketing practices" oraz raport: T. Morey, A. Schoop, *Customer Data: Designing For Transparency And Trust*, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust, potwierdzający, że aż 69% respondentów jest zaniepokojnych samą informacją, że ich dane mogłoby być wykorzystywane do innych celów niż zadeklarowane (w tym marketingowych). Według Eurobarometru aż 71% badanych uważa, że niedopuszczalnym jest, by firmy dzieliły się danymi o nich, nawet gdyby miało to poprawić jakość usług, z których lubią korzystać.

Profile marketingowe stanowią zbiór wielu pozornie nieistotnych okruchów danych, które nieświadomi użytkownicy zostawiają za sobą w sieci: numerów IP, logów, informacji o lokalizacji, pojedynczych kliknięć, drobnych transakcji online, historii odwiedzanych stron i pytań zadawanych wyszukiwarce. W jaki sposób i przez kogo są wykorzystywane? Rzetelna odpowiedź na to pytanie nie jest prosta. Wymaga zagłębienia się w dyskretny, działający na „zapleczu" Internetu ekosystem reklamy behawioralnej. W żargonie marketingowym określa się go poprzez kluczową funkcję, jaką pełni: *real time bidding* (RTB) – w wolnym tłumaczeniu: 'licytacje w czasie rzeczywistym'. Przedmiotem owych licytacji są profile osobowe użytkowników Internetu, czyli potencjalnych odbiorców reklam.

Jak działa mechanizm real time bidding (RTB)?

Dostawcy treści internetowych wystawiają na sprzedaż profile swoich użytkowników oraz wyświetlaną im przestrzeń reklamową za pośrednictwem tzw. platform podaży (ang. Supply Side Platforms) – wyspecjalizowanego oprogramowania, które w czasie rzeczywistym umożliwia komunikację z innymi graczami na giełdzie reklam.

Oferowany profil nie zawiera danych bezpośrednio identyfikujących użytkownika, takich jak nazwisko czy adres. Te informacje z perspektywy reklamodawców mają niewielką wartość. Liczą się tylko cechy decydujące o skłonności użytkownika do dokonania konkretnego zakupu. Dlatego pośrednicy posługują się unikatowym numerem użytkownika, do którego przypisany jest profil o znaczeniu marketingowym (zainteresowania, siła nabywcza, stan zdrowia, ważny moment w życiu etc.).

Dane wystawiane przez sprzedawców przestrzeni reklamowej odbierają i analizują tzw. platformy popytu (ang. Demand Side Platforms), zaprogramowane w celu znalezienia użytkowników o określonym profilu. Profile poszukiwanych użytkowników określają agencje mediowe – kluczowi rozgrywający po tej stronie rynku reklamowego. Ich klienci przychodzą ze standardowym zleceniem: „Daj mi klienta, który kupi po jak najlepszej cenie to, co mam do sprzedania". Zadaniem agencji jest określenie, jakie cechy ma taka osoba i gdzie ją można znaleźć w sieci. Podstawą ich wiedzy o potencjalnych klientach są dane o zakupach pochodzące bezpośrednio od reklamodawców. Aby je wygenerować, większość firm utrzymuje systemy zarządzania relacjami (CRM), programy lojalnościowe i własne sklepy internetowe.

Z informacji o tym, kto i co kupił w przeszłości, wyciągane są cechy typowego klienta. To punkt wyjściowy dla agencji mediowych, które mierzą dalej: próbują ustalić, jakie cechy i zachowania charakteryzują osoby, które jeszcze reklamowanego produktu nie kupiły, ale

mogą to zrobić w przyszłości. W żargonie reklamowym ten hipotetyczny profil klienta to *look-alike*.

> ***Look-alike* to mieszanka twardych danych pochodzących od reklamodawców („taki człowiek już u mnie kupił") i statystycznej wiedzy o ludziach („taki człowiek może chcieć to kupić"). Komponent statystyczny pochodzi z analizy tzw. *big data*, które agencje mediowe pozyskują od dostawców treści, mediów społecznościowych i brokerów danych.**

Profile *look-alike*, wystawiane przez agencje mediowe, i profile faktycznych użytkowników, wystawiane przez dostawców treści (jednocześnie sprzedawców przestrzeni reklamowej), spotykają się na internetowych giełdach. Zadaniem giełdy jest optymalnie dopasować reklamę do użytkownika, który powinien ją zobaczyć. Mają na to ułamki sekund.

Standardowa transakcja w modelu RTB rozpoczyna się w momencie nawiązania przez przeglądarkę połączenie ze stroną, którą ktoś właśnie próbuje załadować na swoje urządzenie. Strona ustala profil tego użytkownika, przypisuje mu unikatowy numer i notyfikuje serwer reklam. Serwer reklam łączy się z platformą podaży i przekazuje jej dane o dostępnej przestrzeni reklamowej oraz o profilu użytkownika, który czeka na jej załadowanie. Platforma podaży wystawia ten profil na giełdzie i czeka na ofertę.

Giełda reklam rozsyła unikatowy numer sprofilowanego użytkownika do współpracujących z nią platform popytu. Ten moment w żargonie to *ad call*. Potencjalni oferenci dowiadują się, że osoba o danym profilu właśnie czeka na wyświetlenie strony internetowej i że mogą dołączyć do niej swoją reklamę. Czy się na to zdecydują i ile zapłacą, zależy od tego, na ile ten profil pokrywa się z poszukiwanym przez nich *look-alike*.

W ułamkach sekund, które mają na zawarcie transakcji, platformy popytu zaciągają dodatkowe dane na temat wystawionego profilu. Co wiemy o jego przeszłych transakcjach? Jakie strony odwiedził przed chwilą? Czy porównywał ceny? Czego szuka i ile jest w stanie zapłacić? Korzystając ze skryptów śledzących, a czasem też dodatkowych informacji pozyskanych od brokerów danych, podejmują decyzję (tak/nie) i wysyłają ofertę. Oferent, który zaproponował najwyższą stawkę, wygrywa prawo do wyświetlenia reklamy.

> **Ten proces jest w pełni zautomatyzowany i zdominowany przez algorytmy. Z punktu widzenia profilowanego użytkownika pozostaje całkowicie niezauważalny. Dlatego tylko nieliczni interesują się tym, co się dzieje na komercyjnym „zapleczu" Internetu. W rezultacie mamy do czynienia z niebezpieczną asymetrią informacyjną, którą profesjonalni gracze**

> **wykorzystują, by – w nieujawniony sposób – wpływać na zachowania nieświadomych użytkowników.**

Kim są kluczowi gracze?

Szybkie i precyzyjne dopasowanie profilu użytkownika, który w danym momencie przegląda strony internetowe, do poszukiwanego przez reklamodawców (*look-alike*) jest łatwiejsze, jeśli obie strony rynku reklamowego mają dostęp do tych samych danych o ludziach i tych samych technik profilowania. Z tej prawidłowości wynika przewaga firm z najbardziej rozwiniętą analityką i dostępem do największych baz danych, szczególnie danych behawioralnych.

Niekwestionowanymi liderami w zautomatyzowanym handlu przestrzenią reklamową są największe platformy internetowe: Facebook i Google. Ich przewaga polega nie tylko na gigantycznych ilościach danych, jakie zebrały o ludziach, ale też na dostępie do technologii, która gwarantuje odpowiednią prędkość transakcji. Google stworzył rynek targetowanej reklamy, na którym kontroluje wszystkie kluczowe role: sprzedaje i kupuje przestrzeń reklamową oraz dostarcza dane i analizę danych po obu stronach transakcji. W tym momencie żaden inny gracz nie może z nim konkurować.

W drugim szeregu działają brokerzy danych, czyli pośrednicy w handlu danymi, którzy zdobywają dane o użytkownikach Internetu za pośrednictwem innych firm (banków, sklepów, ubezpieczycieli etc.). Najwięksi gracze w tej kategorii to firmy amerykańskie, takie jak Acxiom, Experian czy Datalogix. Lokalizacja głównych siedzib nie przeszkadza im zbierać, na masową skalę, danych o konsumentach na całym świecie, również w Europie. Wykorzystują do tego publiczne i komercyjne bazy danych oraz media społecznościowe. Sam tylko Acxiom zebrał informacje o 700 milionach konsumentów, przy średniej liczbie danych na temat jednej osoby na poziomie 3000. Przy takiej skali i głębokości śledzenia ludzkich zachowań nawet nietypowy konsument staje się przewidywalny.

1.3. Skala i głębokość śledzenia

Zakres danych, jakie są dostępne na temat konkretnych użytkowników (w systemie RTB każdy ma przypisany unikatowy numer identyfikacyjny), w dużej mierze zależy od rodzaju usług, z których taka osoba korzysta. W szczególności od tego, czy korzysta z mediów społecznościowych lub innych platform (e-commerce, poczta elektroniczna), które wymagają zalogowania i podania prawdziwych danych, a zarazem umożliwiają ciągłe

gromadzenie danych behawioralnych. Jednak nawet wobec braku tak zweryfikowanych i łatwo dostępnych danych dostawcy treści internetowych (a zarazem sprzedawcy przestrzeni reklamowej) i brokerzy danych próbują tworzyć wielowarstwowe profile użytkowników, na które standardowo składają się:

- imię i nazwisko, adresy, numer telefonu, kod pocztowy, płeć, wiek, stan cywilny, poziom edukacji, sektor zatrudnienia, poziom dochodów, liczba osób pozostających na utrzymaniu użytkownika (i ich wiek), stan posiadania (samochody, nieruchomości etc.), profil etniczny i religijny;
- szczegółowe dane o lokalizacji ustalone na podstawie współrzędnych GPS, sieci Wi-Fi i adresów IP, z którymi łączyło się urządzenie użytkownika;
- dane techniczne, takie jak rodzaj systemu operacyjnego, ustawienia przeglądarki i rozdzielczość ekranu, które składają się na (coraz bardziej unikatowy) „odcisk palca" urządzenia;
- historia aktywności na stronie: w co użytkownik kliknął, co przykuło jego uwagę (i na jak długo), co ostatecznie kupił (i za ile).

Budując profil możliwego klienta (*look-alike*), agencje mediowe próbują ustalić nawyki, zainteresowania, słabości, ważne momenty z życia (takie jak ślub czy ciąża), cechy osobowościowe i demograficzne użytkowników. Na tej podstawie tworzą wąsko zdefiniowane kategorie, powiązane z cechami usługi czy produktu, który mają za zadanie sprzedać: „aktywny styl życia i SUV", „dom, zdrowe jedzenie", „przede wszystkim dzieci", „miejski styl życia, singiel" czy „ponadprzeciętny dochód, dobra luksusowe". Podobnie działają brokerzy danych, którzy w swoich ofertach dla agencji mediowych i innych nabywców wyodrębniają segmenty klientów odpowiadające określonym cechom lub przewidywanym zachowaniom oraz punktację (ang. *score*) wskazującą na prawdopodobieństwo, że takie cechy lub zachowania się potwierdzą.

Facebook w ramach oferty dla swoich klientów (reklamodawców) jest w stanie wygenerować tysiące szczegółowych kategorii związanych z określonymi markami produktów, zainteresowaniami (rodzajem uprawianego sportu, śledzonymi serialami, ulubioną muzyką), konkretnym stylem czy momentem życia (np. para bez dzieci w dużym mieście, świeżo upieczeni rodzice), siłą nabywczą, a nawet precyzyjnie określonymi zamiarami zakupowymi (np. planowany zakup BMW w ciągu 2 miesięcy wraz z budżetem, jaki klient jest skłonny w ten zakup zainwestować).

Dane osobowe zbierane i przetwarzane w celach marketingowych mają różne źródła i charakter. Mogą pochodzić bezpośrednio od użytkowników, jeśli zostały przez nich udostępnione w sposób dobrowolny (np. na etapie zawierania umowy) lub zadeklarowane

(np. w ramach badania). Inną kategorię stanowią dane „zaobserwowane", wynikające z monitorowania realnej aktywności użytkowników w sieci, często w sposób niejawny lub enigmatycznie wspomniany w ogólnych warunkach świadczenia usług. Bez względu na źródło pozyskania dane, które odnoszą się do zweryfikowanych cech i zachowań użytkowników, są uważane za „rzeczywiste". Obok nich coraz większą wartość marketingową zyskują dane „wywnioskowane" (czy też: „wymodelowane"), czyli przypuszczenia na temat ukrytych cech lub przewidywanych zachowań użytkownika generowane na podstawie danych rzeczywistych.

Na opisane powyżej kategorie danych nakłada się jeszcze inny podział: na „dane z pierwszej ręki" (pozyskane przez firmy mające bezpośredni związek z klientem) i „dane strony trzeciej" (zgromadzone czy nabyte od innych podmiotów).

> **Z regulacyjnego punktu widzenia dane pochodzące od stron trzecich są szczególnie problematyczne, ponieważ użytkownicy, których te informacje charakteryzują, mają nad ich gromadzeniem i wykorzystywaniem najmniejszą kontrolę. W tym miejscu pojawia się największe ryzyko błędów i nadużyć. Ten problem dostrzegł europejski regulator i dlatego zmiany przewidziane w RODO i ePrivacy Regulation w największym stopniu wpłyną na obieg danych od „stron trzecich", przy zachowaniu zasad, jakie do tej pory obowiązywały w bezpośrednich relacjach klient–firma.**

1.4. W czym problem? Ciemna strona śledzenia i profilowania użytkowników sieci

Podsumowując perspektywę użytkowników urządzeń mobilnych i odbiorców usług internetowych – dominujący model generowania zysku w oparciu o eksploatację danych osobowych ma następujące wady:

Brak przejrzystości i kontroli

Użytkownicy nie mają realnego wpływu na zakres danych, jakie są zbierane lub generowane (na zasadzie predykcji) na ich temat, szczególnie przez tzw. strony trzecie. Tym bardziej nie mają wpływu na kryteria profilowania, któremu są poddawani, ani na dobór treści, jakie ostatecznie zobaczą na ekranie swojego urządzenia.

Powszechnie wiadomo, że za dobór wyświetlanych treści odpowiadają uczące się algorytmy i sieci neuronowe. Na tym publiczna dyskusja się kończy, pozostawiając zbyt duże pole do domysłów, jeśli chodzi o logikę działania tych systemów oraz kryteria, jakie biorą pod uwagę (w tym to, w jakim stopniu są to „decyzje redakcyjne" samych firm). Nawet wiodące firmy technologiczne, takie jak Alphabet/Google i Facebook, które w ramach swoich platform udostępniły użytkownikom interfejsy do zarządzania profilami reklamowymi, nie ujawniają pełnego zakresu danych przetwarzanych w celach marketingowych (w szczególności pozyskiwanych od tzw. stron trzecich, np. brokerów danych) ani logiki stojącej za profilowaniem wyświetlanych treści.

Na ten problem zwrócił uwagę niemiecki minister ds. ochrony konsumentów Heiko Maas[8]: „Brak przejrzystości to nasz wspólny problem. Wiemy, że niezliczone dane osobowe przepływają przez Internet, że te dane mogą być łączone i analizowane. Ale szczegóły tych transakcji pozostają dla nas niedostępne. Kto wie, jakie dane rzeczywiście przesyłają dalej nasze smartfony? Kto liczy się z tym, że nawet rytm, w jakim przesuwamy palcami po klawiaturze, może zdradzić, w jak bardzo konsumpcyjnym nastroju właśnie jesteśmy? Kto jest w stanie przewidzieć, że zdjęcia, jakie umieszcza na swoim Instagramie, mogą być użyte do oceny jego stanu emocjonalnego?". W efekcie użytkownicy urządzeń mobilnych i usług internetowych są spychani do roli przedmiotu nieprzejrzystych i nie zawsze uczciwych transakcji.

Brak przejrzystości i kontroli po stronie użytkowników na wszystkich etapach budowania ich cyfrowych osobowości przekłada się na konkretne ryzyka. W grę wchodzi nie tylko dotkliwe ograniczenie autonomii informacyjnej, będącej jednym z praw podstawowych, ale także ryzyko finansowe lub utrata niematerialnych korzyści. Obecny model zbierania i eksploatacji danych nie gwarantuje, że wygenerowane profile osobowe będą prawdziwe, a jeśli nawet będą – czy nie zostaną wykorzystane w sposób dyskryminujący lub wykluczający użytkownika.

[8] Heiko Maas, przemówienie na konferencji *Digital live – networked. measured. Sold? #values #Algorithms #IoT*, 3 lipca 2017, Berlin.

Dyskryminacja cenowa i wykluczenie

Wielokrotnie przeprowadzane eksperymenty naukowe i dziennikarskie[9] potwierdzają, że w kontekście usług internetowych dochodzi do **dyskryminacji cenowej**. A więc te same produkty (np. laptop, bilet lotniczy) lub usługi (np. abonament telefoniczny) są oferowane konsumentom na tym samym rynku (w ramach danego kraju czy nawet tego samego segmentu usług) po różnych cenach, uzależnionych od ich unikatowych cech (np. klasy urządzenia, z którego korzystają, ofert, jakie przeglądali wcześniej w sieci, czy ustalonego profilu osobowościowego).

Firmy standardowo wykorzystują systemy CRM (Customer Relationship Management) po to, by skoncentrować uwagę swoich pracowników na utrzymaniu najcenniejszych klientów. W skrajnych scenariuszach takie działania mogą prowadzić do **wykluczenia klientów uznanych za mniej wartościowych** poprzez ograniczenie kierowanych do nich ofert czy intencjonalne utrudnienia w procesie obsługi (np. długie czasy oczekiwania na infolinii, brak dostępnych terminów w placówkach banków). Znane są jednak również przykłady kampanii marketingowych obliczonych na **wykorzystanie słabości lub trudnej sytuacji życiowej** klientów dysponujących realnym kapitałem, np. mieszkaniem na sprzedaż[10]. Zręczne wykorzystanie takiej informacji, w połączeniu z ukrytymi technikami marketingowymi, może doprowadzić do zawarcia nieuczciwej transakcji.

Krzywdzący scoring

Uzasadnione kontrowersje wzbudzają także metody oceny ryzyka, w coraz większej mierze bazujące na modelach predykcyjnych i analizie korelacji statystycznych (wykorzystujących np. informacje o miejscu zamieszkania, pochodzeniu czy sieci osobistych relacji), a nie na faktycznej historii zachowań i zweryfikowanych cechach ocenianych osób. Surowe dane są wtłaczane w algorytmy, których zadaniem jest kalkulacja ryzyka kredytowego pod kątem przyszłych finansowych lub życiowych ruchów klienta.

Standardem na rynku amerykańskim staje się wykorzystywanie w scoringu niestandardowych kategorii danych, np. danych behawioralnych (sposobu wypełniania

---

[9] Por. raport Executive Office of the President of the United States, *Big Data and Differential Pricing*, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf;

D. Keats Citron, F. A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209; *Data And Discrimination: Collected Essays*, https://na-production.s3.amazonaws.com/documents/data-and-discrimination.pdf, The Wall Street Journal, *Websites Vary Prices, Deals Based on Users' Information*, https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[10] Por. D. Dudek, *Jak znaleźć zadłużonego właściciela mieszkania, który chce je sprzedać? Możliwości ultraprecyzyjnego targetowania reklamy na Facebook,* http://jakrobicmarketing.pl/jak-znalezc-zadluzonego-wlasciciela-mieszkania-ktory-chce-je-sprzedac-mozliwosci-ultraprecyzyjnego-targetowania-reklamy-na-facebook/.

formularza, prędkości podejmowania decyzji, liczby popełnionych i skorygowanych błędów, urządzenia, z jakiego korzystał klient, i tego, czy miało ono naładowaną baterię). W **efekcie instytucje finansowe i ubezpieczeniowe zaczynają podejmować istotne dla swoich klientów decyzje w oparciu o niezweryfikowane i dyskusyjne podstawy**. Jednocześnie rośnie wpływ złego scoringu: życie takiej informacji nie kończy się na pojedynczej odmowie kredytu czy ubezpieczenia, ale może obciążyć profil danej osoby w relacji z organami państwa, pracodawcą czy partnerami biznesowymi.

Manipulowanie emocjami

Kolejny obszar, w którym użytkownicy usług internetowych doświadczają utraty kontroli i obawiają się manipulacji, to dostęp do informacji w postaci wyników wyszukiwania czy treści wyświetlanych przez portale społecznościowe (Facebook, Twitter, Instagram). W 2014 r. wyszło na jaw, że 700 tys. użytkowników Facebooka wzięło – nieświadomie – udział w eksperymencie badającym wpływ negatywnych i pozytywnych komunikatów na ich zachowanie w sieci. To badanie, przeprowadzone bez wiedzy i zgody użytkowników, wywołało falę niezadowolenia i protesty. A to był tylko początek. W 2017 r. za sprawą wycieku informacji handlowych z biura Facebooka w Australii opinia publiczna dowiedziała się, że portal pozwala na profilowanie reklam i innych targetowanych przekazów w oparciu o stan emocjonalny użytkowników (nawet tych 14-letnich). Według doniesień dziennika The Australian oferta skierowana do partnerów biznesowych obejmuje szerokie spektrum stanów emocjonalnych nastolatków: od „niepewny swojej wartości", „zagrożony", „beznadziejny" i „głupi" po „nieudaczny", „zestresowany" czy „przechodzący życiowy kryzys".

Wyborcza dezinformacja

Więcej światła na ryzyka związane z targetowaniem przekazu, nie tylko reklamowego, w mediach społecznościowych rzuciła dyskusja, jaka przetoczyła się po wyborze Donalda Trumpa na prezydenta USA i brytyjskiej kampanii Leave.EU. Mimo że oba sztaby korzystały z od dawna znanych i sprawdzonych technik marketingowych, po raz pierwszy na taką skalę zainteresowała się nimi opinia publiczna. Śledztwa dziennikarskie dowodziły, że mieliśmy do czynienia z **szeroko zakrojoną i precyzyjnie wyreżyserowaną manipulacją**, w dużej mierze za sprawą mikrotargetowania użytkowników Facebooka i taktycznego wykorzystania *fake news*.

Te zarzuty w dużej mierze potwierdzali architekci obu kampanii, publicznie chwaląc się możliwościami **niejawnego wpływania na poglądy i postawy wyborców** m.in. poprzez dark posts (treści widoczne tylko dla konkretnych użytkowników, intensywnie

wykorzystywane do ich zmobilizowania lub zdemobilizowania w dzień głosowania). Na ile te działania przesądziły o wyniku wyborów, pozostaje kwestią spekulacji. Faktem jest, że Facebook dużo obiecuje specjalistom od marketingu politycznego, oferując im, nawet w Europie, dedykowane usługi.

Rozdział 2

Odpowiedź unijnego regulatora

Internet zmienił się w komercyjne przedsięwzięcie, gdy firmy nie znalazły innego sposobu na zysk poza reklamami, a potem profilowaniem oraz wynalezieniem ciasteczek i przeglądarek w celu zarabiania jeszcze więcej. To prawo zezwalało na taki model biznesowy. Ale nie ma nic świętego w strukturze prawnej regulującej Internet, możemy to zmienić.

Bruce Schneier[11]

Problemy i ryzyka związane z rozwojem technik śledzenia i profilowania w sieci, opisane w poprzednim rozdziale, nie narodziły się wczoraj. Dzięki pracy niezależnych ekspertów i badaczy z różnych dziedzin dysponujemy dziesiątkami raportów i opracowań analizujących zjawiska i ich możliwe konsekwencje[12]. W tym kontekście warto podkreślić, że decyzja unijnego regulatora, by zreformować i zmodernizować istniejące regulacje w sferze ochrony danych i usług elektronicznych, z pewnością nie była pochopna.

Przygotowane przez Komisję Europejską projekty generalnego rozporządzenia o ochronie danych osobowych (RODO) i rozporządzenia o prywatności w łączności elektronicznej (ePrivacy Regulation) zostały poprzedzone oceną wpływu dotychczasowych mechanizmów

[11] Światowej sławy kryptograf i specjalista z zakresu bezpieczeństwa teleinformatycznego. *Inwigilacja to model biznesowy internetowych korporacji*. Agne Pix rozmawia z Brucem Scheneierem, http://krytykapolityczna.pl/gospodarka/inwigilacja-to-model-biznesowy-internetowych-korporacji/.

[12] Por. np. raporty: Access, *The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy*, https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf, The Canadian Internet Policy and Public Policy Clinic, *On the data trail: How detailed information about you gets into the hands of organizations with whom you have no relationship. A report on the Canadian data brokerage industry*, https://idtrail.org/files/DatabrokerReport.pdf, J. Deighton, P. A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy*, https://www.ipc.be/~/media/documents/public/markets/the-value-of-data-consequences-for-insight-innovation-and-efficiency-in-the-us-economy.pdf, *Credit-Based Insurance Scores: Impacts on Consumers of Automobile Insurance*, https://www.ftc.gov/sites/default/files/documents/reports/credit-based-insurance-scores-impacts-consumers-automobile-insurance-report-congress-federal-trade/p044804facta_report_credit-based_insurance_scores.pdf.

regulacyjnych na sytuację na rynku i na prawa podstawowe obywateli[13]. Komisja Europejska na podstawie przeprowadzonych badań doszła do wniosku, że interwencja regulacyjna jest konieczna w obu tych sferach.

> **Europejska reforma przepisów o ochronie prywatności była zatem projektowana z jednej strony z myślą o firmach, które w ramach wspólnego rynku mają prawo oczekiwać prostszych procedur i jednakowych reguł gry (bez względu na państwo pochodzenia firmy czy usługi), z drugiej – o obywatelach, których pozycja w ekosystemie usług elektronicznych wymagała wzmocnienia i których prawa w sieci do tej pory nie były skutecznie egzekwowane.**

2.1. RODO

Ogólne rozporządzenie o ochronie danych (RODO)[14] konsekwentnie realizuje zamierzenia Komisji Europejskiej. Z jednej strony zapewnia jednolity, ogólnoeuropejski standard w sferze ochrony danych osobowych, zastępując niespójne i skomplikowane ustawodawstwo poszczególnych krajów. Regulacja wymusza, żeby wszystkie przedsiębiorstwa chcące oferować swoje usługi na terenie Unii Europejskiej – bez względu na to, czy mają swoją siedzibę w kraju członkowskim, czy nie – stosowały europejskie prawo ochrony danych osobowych. Na tym polega tzw. wyrównanie pola (*level playing field*). Z drugiej strony rozporządzenie rzeczywiście wzmacnia gwarancje ochrony praw użytkowników, szczególnie poprzez stworzenie twardych mechanizmów ich egzekwowania.

Nowe rozporządzenie nie dyskryminuje podmiotów, które oparły swój model biznesowy na komercjalizacji wielkich danych (*big data*); nie zakazuje też profilowania jako jednej z operacji, jakie można przeprowadzać na danych. Ale wymaga w tej sferze więcej **przejrzystości, odpowiedzialności i rozliczalności**. W tym kontekście kluczowe znaczenie będą miały zasady **ochrony danych osobowych w fazie projektowania i domyślnie** (*data protection by design & by default*). Mają one zachęcić aktorów biznesowych do wprowadzania innowacyjnych rozwiązań (na poziomie technologicznym

[13] Por. Komisja Europejska, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, http://ec.europa.eu/newsroom/document.cfm?doc_id=41232, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_en.pdf.

[14] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679.

i organizacyjnym) zabezpieczających dane osobowe przed wyciekami i nieautoryzowanym wykorzystaniem, także przez strony trzecie. Wczesnej identyfikacji takich ryzyk miało służyć inne zalecenie – przeprowadzania oceny wpływu przetwarzania danych na prawa osób, których to dotyczy (*data protection impact assessment*).

RODO promuje również takie techniki jak **anonimizacja** (usuwanie wszelkich danych pozwalających na identyfikację użytkownika, o ile nie są one niezbędne), **pseudonimizacja** (zastępowanie danych indywidualizujących sztucznie wygenerowanymi identyfikatorami) i **szyfrowanie** (kodowanie danych tak, by tylko osoba upoważniona mogła je odczytać). W założeniach Komisji Europejskiej takie rozwiązania, zwiększające bezpieczeństwo danych, powinny być szczególnie atrakcyjne dla firm przetwarzających dane na masową skalę i intensywnie korzystających z transferów danych, tak jak ma to miejsce w ekosystemie reklamy behawioralnej.

Z myślą o samych użytkownikach RODO wzmacnia lub utrzymuje w mocy **podstawowe zasady przetwarzania danych**, które mają zapewnić podmiotom przetwarzania danych realną kontrolę nad tym procesem. W kontekście śledzenia i profilowania kluczowe znaczenie będzie miało wdrożenie następujących zasad:

Ograniczenie celem

Dane mogą być zbierane wyłącznie w (z góry) określonych celach, a po zebraniu nie mogą być przetwarzane w innym celu bez dodatkowej zgody podmiotu danych. W szczególności nie mogą być przekazywane innym podmiotom w ich celach marketingowych.

Adekwatność i minimalizacja danych

Zbierane dane muszą być adekwatne, istotne i niezbędne w kontekście celów, w których są przetwarzane. W praktyce oznacza to, że administrator nie może zbierać więcej, niż rzeczywiście potrzebuje. Nie może zbierać informacji, które nie mają bezpośredniego związku z oferowanym produktem czy usługą (np. lokalizacji, o ile świadczona usługa jej nie wymaga). Regulator wyszedł z założenia, że im mniej danych zostanie zebranych, tym mniejsze ryzyko dla osób, których one dotyczą, i samych administratorów.

Przejrzystość i prawo dostępu do informacji

Administratorzy danych muszą w jasny i przystępny sposób poinformować osoby, których dotyczą zbierane dane, o celach, sposobie i czasie ich przetwarzania, jak również o logice stojącej za automatycznym podejmowaniem decyzji, jeśli do niego dochodzi (w tej kategorii powinno się znaleźć dopasowywanie ofert w czasie rzeczywistym do profili użytkowników), oraz o wszystkich podmiotach, z którymi dzielą się danymi (stronach trzecich). Muszą także udostępnić wszystkie przetwarzane dane (w tym profil

marketingowy) na żądanie osoby, której to dotyczy, i zapewnić jej prawo do poprawienia tych danych (np. skorygowania profilu marketingowego).

Centralną wartością, na jakiej zbudowane zostało RODO, jest **ochrona autonomii informacyjnej** użytkowników, a więc zagwarantowanie im realnej kontroli nad tym, w jaki sposób ich dane są przetwarzane. Stąd **stosunkowo wysoki standard, jaki rozporządzenie przewiduje dla udzielenia skutecznej zgody na przetwarzanie danych** osobowych. Zgoda użytkownika musi być:

- dobrowolna (*freely given*),
- jednoznaczna (*unambiguous*),
- konkretna (*specific*),
- oparta na rzetelnych informacjach (*informed*),
- wyraźnie wyodrębniona (*by a statement or by a clear affirmative action*)[15].

Ten standard w jednym aspekcie jest niższy niż obowiązujący obecnie w Polsce: RODO nie wymaga, by zgoda była zawsze wyrażona w sposób dosłowny (np. poprzez klauzulę „zgadzam się na…"). A więc w praktyce będzie ją można wywnioskować z innego wyraźnego zachowania użytkownika (np. faktu wypełnienia określonego pola w formularzu lub kliknięcia w określone miejsce na stronie).

> **Mimo tego wyłomu standard wyrażania zgody na przetwarzanie danych przewidziany w RODO jest dość szczelny i powinien ograniczyć najgorsze praktyki śledzenia użytkowników w sieci. Nieważne będą arbitralne postanowienia regulaminów i tzw. polityk prywatności, mówiące o tym, że użytkownik akceptuje śledzenie przez strony trzecie. Brokerzy danych będą musieli wyjść z cienia i ujawnić swoje praktyki po to, by móc powalczyć o zgodę użytkowników na ich śledzenie i profilowanie. Natomiast – co ważne – zgoda na śledzenie w celach reklamowych nie jest wymagana, jeśli takie dane o swoich użytkownikach zbiera i wykorzystuje na własne potrzeby właściciel serwisu. Ma do tego prawo na podstawie tzw. uzasadnionego interesu.**

[15] Por. art. 4 punkt 11 RODO.

2.2. Rozporządzenie ePrivacy

Zasady zawarte w RODO zostały rozwinięte i uszczegółowione pod kątem specyfiki komunikacji elektronicznej i usług internetowych w projekcie rozporządzenia w sprawie prywatności i łączności elektronicznej (tzw. ePrivacy Regulation)[16]. Opierając się na ocenie skutków wcześniejszej regulacji (tzw. ePrivacy Directive), Komisja Europejska zaproponowała następujące reguły:

- każdy administrator danych (strona internetowa, aplikacja mobilna, operator sieci Wi-Fi etc.) ma aktywny obowiązek dbania **o przejrzystość przetwarzanych danych** i informowania o tym użytkowników w przystępny sposób, np. poprzez wyświetlanie ostrzeżeń w rodzaju „usługa finansowana przez reklamę targetowaną, w związku z czym dane o historii przeglądania stron przez użytkownika będą użyte w celu dopasowania reklamy";
- **zgoda na przetwarzanie danych** (np. w celach marketingowych) może zostać wyrażona **przy pomocy odpowiednich ustawień przeglądarki** lub innej aplikacji;
- przeglądarki i podobne platformy mają zapewniać **przyjazne dla użytkownika** ustawienia już w wersji domyślnej, by wzmocnić jego kontrolę nad danymi wypływającymi z jego komputera;
- praktyki polegające na blokowaniu dostępu do strony lub innej usługi online w przypadku braku zgody na śledzenie (tzw. *cookie wall*) **są niedozwolone**;
- wszystkie rodzaje **niezamówionych komunikatów, łącznie z targetowaną reklamą** w mediach społecznościowych i marketingiem bezpośrednim przez telefon, wymagają jednoznacznej, aktywnie wyrażonej zgody (*opt-in*);
- **poufność komunikacji elektronicznej jest zagwarantowana zarówno w odniesieniu do treści, jak i metadanych**; ten sam standard ochrony obowiązuje w przypadku wszelkich rodzajów danych lokalizujących użytkowników, także pośrednio (np. dane o historii logowania do sieci Wi-Fi);
- wszelkie **urządzenia końcowe**, takie jak telefony komórkowe, komputery i inne sprzęty z kategorii Internet of Things, należą do **sfery prywatnej użytkownika**. Ta reguła rozciąga się na wszelkie dane przechowywane i emitowane przez takie urządzenia.

[16] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010.

W kontekście praktyk marketingowych te reguły oznaczają, że usługodawcy internetowi, operatorzy telekomunikacyjni i brokerzy danych nie będą mogli w dowolny sposób zbierać i przetwarzać danych generowanych przez rozmaite urządzenia podłączone do sieci (w tym wskaźników lokalizacji – np. adresów IP i nazw sieci Wi-Fi). Za każdym razem będą **musieli wykazać podstawę prawną** takiej operacji.

Jedną z możliwych podstaw przetwarzania danych generowanych przez urządzenia końcowe będzie jednoznaczna i aktywnie wyrażona **zgoda użytkownika** (dokładnie tak jak w RODO). Choć, oczywiście, nie jedyną!

Dane generowane przez urządzenia końcowe użytkowników będą mogły być przetwarzane (nawet bez konieczności uzyskania dodatkowej zgody użytkownika) wtedy, gdy okaże się to niezbędne dla:

- zapewnienia płynnej transmisji danych;
- realizacji zamówionej przez użytkownika usługi;
- lub mierzenia wejść na stronę i monitorowania ruchu (jeśli będzie to robione przez samego dostawcę usługi, a nie strony trzecie).

—

Projektując oba rozporządzenia, europejski regulator nie przesądził, jak powinien wyglądać w przyszłości ekosystem targetowanej reklamy, w jakim kierunku powinny pójść praktyki wydawców i brokerów danych ani jaki model biznesowy najlepiej spełnia wymagania wynikające z unijnych regulacji. Firmy i organizacje branżowe mają duże pole do rozwijania istniejących i testowania nowych modeli reklamy behawioralnej.

Komentarz Anny Streżyńskiej, Minister Cyfryzacji

Bez wątpienia wejście w życie w najbliższym czasie tzw. RODO, a więc rozporządzenia unijnego reformującego unijny i krajowy system ochrony danych osobowych, budzi duże zainteresowanie wszystkich środowisk – również przedsiębiorców. Nie ma się co dziwić, bo z jego stosowaniem bez wątpienia wiążą się zmiany konieczne do wdrożenia w każdej organizacji. Bardzo negatywnie podchodzę jednak do coraz częściej budowanej narracji zastraszania nową regulacją, w tym w związku z wprowadzoną do niej możliwością nakładania kar za naruszenie przepisów o ochronie danych.

Po pierwsze, **reforma systemu ochrony danych osobowych nie jest o karach**. Kary są jednym z możliwych do zastosowania przez organ środków, równorzędnym do decyzji nakazujących usunięcie naruszenia, wydawanych upomnień czy ostrzeżeń.

Po drugie, niemal każdy z sektorów gospodarki jest dzisiaj nadzorowany przez organ mający możliwość nakładania kar, co w żadnym zakresie nie wpływa negatywnie na funkcjonowanie tego sektora.

Po trzecie, w mojej ocenie **na reformę można również spojrzeć probiznesowo**. Przykładowo: wprowadzone do RODO mechanizmy certyfikacji i akredytacji są rozwiązaniem stymulującym rozwój konkurencyjności na rynku. Powstanie grupa podmiotów, które (dzięki uzyskanemu certyfikatowi) mają być wzorem dla innych. I tutaj jest otwarte pole dla marketingowców, by sprzedać w odpowiedni sposób przynależność do takich grup.

RODO wprowadza również możliwość realizacji części obowiązków informacyjnych przez tzw. infografiki, a nie nudne opisy. To jest **ogromne pole do popisu dla kreatywności działów marketingu** różnych firm, by tworzyć ciekawe grafiki – zachęcające i pokazujące przedsiębiorcę jako otwartego, dbającego o prywatność i wyróżniającego się na tle innych.

Po raz pierwszy w obszarze sektora ochrony danych osobowych to właśnie RODO wprost uprawnia część przedsiębiorców do pobierania opłat za realizację niektórych obowiązków. I wreszcie – skuteczne zastosowanie w polskiej przestrzeni prawnej RODO będzie skutkować reformą wielu sektorów, w tym również obszarów, które zmian wymagały od lat (tj. sektora pracy, ubezpieczeń czy sektora bankowego).

Rozdział 3

Odpowiedź rynku: możliwe scenariusze

Co się zmieni, kiedy na śledzenie naszych ruchów w sieci i budowanie profili marketingowych będzie potrzebna świadoma i dobrowolna (niewymuszona przez tzw. *cookie walls*) zgoda użytkownika? Jak inaczej można ukształtować relacje pomiędzy reklamodawcami, brokerami danych, użytkownikami i platformami, na których reklamy są wyświetlane? Czy nowe reguły gry da się sensownie przełożyć na praktykę?

> **Odpowiedź na te pytania nie leży już w gestii regulatora ani interpretujących przepisy prawników. Architektami docelowych rozwiązań będą sami wydawcy mediów elektronicznych, agencje marketingowe i pracujący dla nich brokerzy danych. To oni będą się musieli zmierzyć z ryzykiem, które już teraz głośno sygnalizują: że użytkownicy – nierozumiejący, jak działa reklama behawioralna, i zaskoczeni pytaniem o zgodę na przekazywanie danych firmie, o której istnieniu do tej pory nie mieli pojęcia – automatycznie klikną „nie pozwalam".**

Zanim ulegniemy pokusie determinizmu i stwierdzimy, że „tego nie da się zrobić", warto poważnie rozważyć możliwe scenariusze rozwoju reklamy, która wykorzystuje śledzenie użytkowników przez tzw. strony trzecie, po wejściu w życie nowych regulacji. Z pewnością jest ich więcej niż jeden.

3.1. Scenariusz I – wdrożenie pozorowane

Aby uniknąć wysiłku organizacyjnego związanego z dostosowaniem do nowych reguł gry, firmy eksploatujące dane – dostawcy treści, brokerzy danych, reklamodawcy – mogą przyjąć taktykę pozorowanego wdrożenia.

Sprowadzałaby się ona do **wyboru najbardziej liberalnej interpretacji przepisów i wykorzystania elastyczności, jaką ma w sobie nowa definicja zgody na przetwarzanie danych osobowych**. Działając na granicy prawa, firmy mogą utrzymywać, że już samo wejście użytkownika na stronę, na której „gdzieś w widocznym miejscu" znajduje się klauzula informująca o mechanizmach szpiegujących stron trzecich, stanowi zgodę na tego typu śledzenie i dalszą eksploatację danych.

Takie potraktowanie nowych przepisów byłoby niezgodne z ich celem i z pewnością nadawało się do podważenia w sądzie. Jednak część graczy na rynku reklamy interaktywnej może podjąć to ryzyko tylko po to, by kupić czas. W odpowiedzi na nieetyczne praktyki niektórzy użytkownicy i reprezentujące ich organizacje będą się skarżyć do organów ochrony danych i wnosić sprawy do sądów. To oznacza wieloletnie i kosztowne, głównie dla firm, batalie prawne. A więc w pierwszej fazie tego scenariusza najwięcej stracą użytkownicy, a najwięcej do zyskania mają prawnicy, wyspecjalizowani w omijaniu regulacji prawnych i prowadzeniu sądowych sporów.

> **Przeciętni użytkownicy technologii tego pozorowanego wdrożenia w początkowej fazie raczej nie zauważą: albo zdążyli się już przyzwyczaić do nieetycznych praktyk śledzenia, albo nauczyli się je omijać. Ich obojętność wobec praktyk marketingowych, wbrew pozorom, dla biznesu żyjącego z reklamy nie wróży rosnących zysków. Z czasem na tym scenariuszu zacznie tracić także branża interaktywna, która już odczuwa symptomy tego zmęczenia po stronie odbiorców.**

Podczas gdy dla jednych użytkowników problemem jest nieadekwatność targetowania („znowu reklama viagry!"), innych bardziej niepokoi trafiona reklama, jeśli pojawia się w sferze, którą uważają za prywatną („skąd wiedzą, że akurat potrzebuję tego środka na porost włosów?"). Wspólny mianownik jest ten sam: ludzie woleliby mieć wpływ na to, jaka reklama jest im wyświetlana i jakie dane są do tego wykorzystywane. W tym scenariuszu nie mogą na niego liczyć.

Stąd rosnąca popularność Adblocka i podobnych wtyczek, która z roku na rok będzie się przekładać na spadające dochody w branży wydawniczej i wzmocnienie duopolu marketingowego Google & Facebook, który doskonale sobie radzi nawet bez danych od tzw. stron trzecich i nie zawaha się, by wykorzystać tę przewagę konkurencyjną.

Erozja debaty publicznej i postępujący kryzys prywatności

Scenariusz pozorowanego wdrożenia nowych regulacji oznacza także brak impulsu do rozwoju (płatnych) serwisów z treściami wysokiej jakości, w tym serwisów informacyjnych z prawdziwego zdarzenia. Użytkownicy mają słabą motywację, by sięgać do portfela, skoro tak czy inaczej są skazani na oglądanie reklam i na wymuszone klikanie. Dopóki liczy się liczba odsłon, a nie ilość czasu spędzona nad jednym tekstem, jesteśmy w pułapce kiepskiego produktu. Ta „kapitulacja z jakości" po obu stronach rynku – czytelników, którzy pogodzili się z rozrywką w miejsce wiadomości, i wydawców, którzy równają do dołu – przekłada się na niski poziom debaty publicznej. Skutki tego stanu rzeczy dla współczesnej demokracji już są widoczne i nie napawają optymizmem.

> **Przy założeniu, że wydawcy nie znajdą innej drogi finansowania treści niż targetowana reklama, nieuchronnie zmierzamy do zbierania coraz większych ilości danych behawioralnych i pogłębiającej się inwigilacji użytkowników w ramach platform, do których muszą się logować (sklepów internetowych, mediów społecznościowych, poczty elektronicznej). To wypadkowa rosnącego popytu na dane i coraz bardziej ograniczonych możliwości śledzenia za pomocą *cookies* czy podobnych skryptów, które przeciętny użytkownik potrafi zablokować.**

Zwiększająca się inwazyjność śledzenia musi z kolei przełożyć się na postępujący spadek zaufania do firm internetowych. To tylko kwestia czasu, żeby użytkownicy zorientowali się, że są osaczeni: albo ujawnią, kim tak naprawdę są, czego potrzebują i ile są gotowi za to zapłacić, ze wszystkimi intymnymi i wrażliwymi sprawami włącznie, albo taka wiedza na ich temat będzie generowana w oparciu o statystyczne korelacje. Tak czy inaczej to ich cyfrowy profil – rzeczywisty albo wygenerowany na zasadzie predykcji – stanie się kluczem do rynku pracy, usług finansowych, ubezpieczeń i nieruchomości.

> **Nietrudno sobie wyobrazić, że tak rozwijający się scenariusz w ciągu dekady doprowadzi do ostrego kryzysu zaufania pomiędzy użytkownikami Internetu a brokerami danych i podmiotami korzystającymi z ich usług. W efekcie może nas czekać również realny kryzys ekonomiczny wywołany załamaniem w sferze usług internetowych lub gwałtowny zwrot w polityce regulacyjnej państwa, którego skutki dla biznesu dziś trudno przewidzieć.**

3.2. Scenariusz II – wdrożenie złośliwe

Ten scenariusz to wariant pierwszego: zamiast omijać prawo firmy działające na rynku reklamy behawioralnej i wydawcy mogą podjąć próbę ośmieszenia lub wypaczenia nowej regulacji poprzez **agresywne wymuszanie zgód na zwykłych użytkownikach**. Już w tej chwili część internetowych mediów odmawia wyświetlania treści strony, jeśli użytkownik nie wyłączy oprogramowania blokującego reklamy. Na tej samej zasadzie można wymusić zgodę na przetwarzanie danych osobowych – chcesz czytać, zgódź się na wszystko.

To wypaczenie sensu nowej regulacji, ponieważ zgoda na przetwarzanie danych nie powinna być nadużywana ani tym bardziej wymuszana. Świadoma i dobrowolna zgoda polega na tym, że użytkownik może wybrać jedną z dwóch ścieżek: pozwolić tzw. stronom trzecim na wykorzystywanie jego danych w celach reklamowych albo nie. Niezależnie od podjętej decyzji powinien mieć dostęp do oferowanej usługi – tym bardziej, że nowe regulacje nie ograniczają prawa właściciela serwisu do zbierania danych użytkowników we własnych celach marketingowych!

Fala frustracji

Lawina irytujących pop-upów, blokujących normalną możliwość przeglądania strony, to sprawdzony sposób na zniechęcenie użytkowników usług internetowych do jakiejkolwiek regulacji. Znamy ten scenariusz z nieudanego wdrożenia poprzedniczki rozporządzenia ePrivacy, tzw. Dyrektywy ciasteczkowej (cookie directive). Wtedy też skończyło się na głośnej frustracji i fali bezsensownego klikania, które zmierzało do usankcjonowania złych praktyk na rynku. Ludzie klikali, by pozbyć się wyskakujących okienek, a nie by odzyskać kontrolę nad swoimi danymi. Ta druga możliwość zwyczajnie nie została im przedstawiona: w praktyce mogli tylko zaznaczyć „zgadzam się". Jeśli ten scenariusz się powtórzy, użytkownicy znowu zostaną postawieni pod ścianą.

> **Jak zareagują? U większości pojawi się frustracja wywołana kolejnymi wymuszonymi kliknięciami. Jej skutkiem ubocznym może być rosnąca niechęć do instytucji unijnych – źródła całego zamieszania. Konieczność codziennego przedzierania się przez okna blokujące dostęp do treści internetowych będzie pożywką dla populistów i eurosceptyków.**

Dla tych, którzy jeszcze nie zainstalowali Adblocka, może to być moment przełamania się i podjęcia próby – przynajmniej częściowego – wypisania się z rynku reklamy behawioralnej. Zgodnie z logiką: skoro reklama ma być okupiona tak wysoką ceną,

a w dodatku nie daje mi realnego wyboru, czy chcę ją oglądać, czy nie, wybieram nieoglądanie jej wcale. Taka postawa użytkowników niczego nie rozwiąże, ale z pewnością przyspieszy „wyścig zbrojeń" – z jednej strony wydawcy i reklamodawcy będą szukać innych sposobów na śledzenie opornych, z drugiej – innowacyjni deweloperzy będą proponować kolejne blokady i sposoby obejścia *cookie walls*.

Wzmocnienie mocnych i zagłada słabych

Długofalowe konsekwencje tego wyścigu po wiedzę o zirytowanych i nieufnych użytkownikach będą analogiczne do opisanych w pierwszym scenariuszu. Warto w tym miejscu podkreślić, że najboleśniej te skutki odczują lokalni gracze (np. polskie serwisy), podczas gdy globalny duopol Google & Facebook może tylko zyskać. Ci internetowi giganci zbudowali model pozyskiwania i komercjalizacji danych w oparciu o własne usługi, co powoduje, że są w mniejszym stopniu zależni od danych dostarczanych przez strony trzecie.

Wręcz przeciwnie: to Facebook i Alphabet/Google mają wiedzę, której pożądają brokerzy danych. Możliwość ciągłego obserwowania zachowań użytkowników (w większości zalogowanych), których liczą już w miliardach, daje im bezkonkurencyjną pozycję w targetowaniu. W praktyce oznacza to, że największe platformy internetowe nie będą musiały prowadzić agresywnej kampanii nakierowanej na pozyskanie zgód na przetwarzanie danych osobowych. Zgodnie z prawem na śledzenie swoich użytkowników we własnych celach takiej zgody przecież nie potrzebują.

> **Na złośliwym scenariuszu wdrożenia nowych regulacji najwięcej mogą zatem stracić właśnie ci, którzy zaserwują użytkownikom irytujące pop-upy: wydawcy i mniejsi gracze na rynku reklamy behawioralnej. W krótkim horyzoncie będzie to ciężar przede wszystkim dla użytkowników, ale z czasem konsekwencje wywołanego przez wymuszone zgody kryzysu zaufania rozleją się po lokalnych rynkach, wzmacniając globalny duopol reklamowy.**

3.3. Scenariusz III – optymalne wdrożenie, czyli współpraca

Internet nie musi się popsuć: optymalne wdrożenie nowych reguł gry – na którym wszyscy mogą coś zyskać – również jest możliwe. To optymistyczny scenariusz, w którym użytkownicy sami zdecydują, jakim firmom z branży interaktywnej chcą przekazać swoje dane osobowe, a te firmy zyskają lepiej stargetowanych odbiorców. Fundamentem takiego rozwiązania musi być jednak **mądrze zaprojektowany proces – od edukacji użytkowników po samoregulację rynku reklamy behawioralnej**.

W tym scenariuszu rolą firm będzie, w pierwszym kroku, aktywna edukacja użytkowników, którzy muszą zrozumieć, w jaki sposób ich dane są zbierane oraz komu i do czego służą w skomplikowanym ekosystemie reklamy behawioralnej. Dopiero w drugim kroku będą mogły zaproponować – już uświadomionym – użytkownikom narzędzia do zarządzania ustawieniami prywatności, w tym udzielenia zgody na śledzenie i targetowanie.

Po stronie użytkowników pozostanie podjęcie wysiłku, by zacząć zarządzać swoją prywatnością w sieci, a nie tylko kontestować jej brak lub instalować Adblocki. Przy czym zarządzanie, w tym kontekście, odwołuje się do zupełnie innego porządku niż upraszczający podział na totalną inwigilację i totalną prywatność. Użytkownicy zarządzający swoimi danymi w sieci będą mogli zdecydować, jakie dane osobowe udostępniają poszczególnym firmom oraz jaki rodzaj reklamy chcą otrzymać w zamian.

Konsole do zarządzania prywatnością

Szansą dla brokerów danych i firm z branży marketingowej specjalizujących się w targetowaniu reklam jest wyjście z cienia i współpraca na zasadzie **samoregulacji i dobrowolnej certyfikacji**. Branża interaktywna już dziś tworzy wspólne platformy, w ramach których użytkownicy mogą wyrażać i zmieniać swoje preferencje dotyczące targetowania. Najlepszym przykładem jest portal Your Online Choices, firmowany przez European Interactive Digital Advertising Alliance (EDAA), do którego na zasadzie konsensusu przyłączyło się kilkadziesiąt wiodących firm z branży interaktywnej. Podobną platformę, w ramach swojego wewnętrznego imperium, oferuje użytkownikom Google.

Dziś są to usługi „dla zainteresowanych", świadomych i aktywnych użytkowników, w dodatku oparte na zasadzie *opt-out* (jeśli ci się nie podoba to, co robimy z twoimi danymi, możesz wyrazić sprzeciw). Po wejściu w życie nowych przepisów branża interaktywna powinna wykonać kolejny krok: przejść na model *opt-in*, zgodnie z którym śledzenie i targetowanie użytkowników przez tzw. strony trzecie (czyli firmy, z którymi

użytkownik nie ma bezpośredniej relacji i od których nie zamawiał żadnej usługi) wymaga zgody.

> **Do pozyskiwania zgody na przetwarzanie danych i zarządzania profilami reklamowymi użytkowników świetnie się nadają platformy skupiające jak największą liczbę graczy na rynku. Z perspektywy użytkownika ich zaletą jest to, że określa swoje preferencje raz i nie musi (choć zawsze może) do tego wracać. Firmy mają korzyść w tym, że nie muszą pytać o możliwość zainstalowania ciastka (czy innego skryptu śledzącego) na każdej stronie internetowej i przy każdej okazji. Zamiast atakować klienta irytującymi pop-upami nawiązują z nim merytoryczną rozmowę w przeznaczonym do tego miejscu.**

Opt-in w przeglądarce

Oczywiście, platforma z kilkudziesięcioma rubrykami do zaznaczenia i dużą liczbą informacji to nie jest rozwiązanie dla każdego. W dobrze działającym modelu powinny się znaleźć także prostsze narzędzia. Na przykład możliwość wyrażenia jednorazowej, generycznej zgody na śledzenie przez strony trzecie w ustawieniach przeglądarki. Ta opcja ma wiele wad, przede wszystkim taką, że wszystkie firmy z branży interaktywnej pakuje do jednego worka, w wyniku czego firmy o wysokich standardach mogą ucierpieć na złej reputacji pozostałych. Ale niewątpliwie jest to rozwiązanie dla użytkowników, którzy preferują jedno kliknięcie zamiast mierzenia się z pełnymi ustawieniami prywatności.

Bez względu na to, jakie narzędzie zyska popularność wśród użytkowników – prosta opcja „tak/nie" w ustawieniach przeglądarki czy konsola do zarządzania relacjami z konkretnymi firmami – jedno wydaje się pewne: branża reklamy interaktywnej będzie musiała wyjść z cienia i opowiedzieć ludzkim językiem o swoich modelach biznesowych. Tylko w ten sposób może zbudować zaufanie i bazę pod dalszy rozwój swoich usług.

Pozytywny efekt domina

Wbrew lamentom firm z branży marketingowej sensowne **wdrożenie nowych regulacji może się przełożyć na większą skuteczność targetowanych reklam**. Ludzie, którzy zdecydują się dobrowolnie i świadomie udostępnić swoje dane brokerom, własnoręcznie będą weryfikować i ulepszać swoje profile reklamowe. W efekcie kierowane do nich kampanie będą dobrane do ich rzeczywistych, a nie hipotetycznych potrzeb. Skończy się era cold callingu, w ramach którego anonimowi telemarketerzy obdzwaniają

przypadkowych ludzi z propozycjami niepotrzebnych produktów, oraz firm, z których baz danych nie sposób się wypisać.

Rosnąca świadomość dotycząca technik śledzenia, jak również wartości, jaką na rynku internetowym mają dane osobowe, będzie miała skutki wykraczające poza ekosystem reklamy behawioralnej. Świadomi użytkownicy staną się mniej chętni do udostępniania swoich danych w zamian za tzw. darmowe usługi, w tym info-papkę oferowaną przez portale internetowe. To realna **szansa dla mediów, które chcą i są w stanie oferować treści wysokiej jakości w zamian subskrypcję lub jednorazowe opłaty**. W tym modelu będą w stanie finansować pracę swoich redakcji bez zwodzenia użytkowników („tylko kliknij!") i krótkowzrocznej pogoni za coraz bardziej agresywną powierzchnią reklamową.

Komentarz Michała Boniego, eurodeputowanego, członka komisji LIBE

Trzeba rozróżnić wdrażanie RODO i prace nad ePrivacy. RODO jest przyjętym aktem prawnym, zaczyna być w pełni stosowane 25 maja 2018 r. i trzeba dołożyć wszelkich starań, by te rozwiązania zostały wdrożone jak najlepiej. Duże firmy nad tym pracują, małe zaczynają. Trzeba im pomóc wielką akcją promocyjną i doradczą, zaadresowaną do różnych sektorów.

Prace nad ePrivacy jeszcze trwają. Ich cel jest ważny: chronić i zachowywać poufność nie tylko danych, ale i ich przesyłu w całej komunikacji elektronicznej oraz tego, co znajduje się w swoistej „pamięci" naszych urządzeń, których jesteśmy ostatnimi użytkownikami. I nie pozwalać na rozpowszechniające się „trakowanie" nas za pomocą urządzeń, bez naszej zgody, poza naszą wiedzą. Z drugiej strony nie można przez zero-jedynkowość rozwiązań zabić rozwoju usług.

Ochrona prywatności w sieci nie może być sprowadzana do prostego „tak/nie". To wypadkowa wielu wyborów, jakich dokonujemy. Na coś się mogę zgadzać, a na coś nie. Ale jeśli już podejmę tę decyzję, to ona powinna wyznaczać horyzont tego, co faktycznie dzieje się z moimi danymi – bez ambarasującego nagabywania do udzielenia zgody na każdym kroku. Natomiast ustawienia prywatności dla użytkowników powinny być szeroko i łatwo dostępne. Świadomy i korzystający z nich użytkownik to jest coś, na czym wszystkim stronom debaty nad ePrivacy powinno zależeć.

Całe to natręctwo reklam musi być poddane naszej kontroli. Ale trzeba znaleźć równowagę między naszą zgodą i wyborem a prawem firm do budowania modelu biznesowego w oparciu o reklamę albo subskrypcję (jeśli nie chcę reklam, mogę wybrać inny model).

Każde rozwiązanie prawne musi dbać o równowagę. Bo dotyczy – szczególnie w tym wypadku – tego, co dzieje się w interakcji; tego, co dzieje się pomiędzy. A więc w grę wchodzą prawa, obowiązki i korzyści po obu stronach. Zakładam przy tym, że mówimy o uczciwych podmiotach.

W ePrivacy jest mnóstwo szczegółów, nad którymi trzeba się jeszcze zastanowić. Potrzebujemy spokojnego namysłu nad tym, jak dalej (już po uzyskaniu zgody) mogą być przetwarzane dane, np. jeśli służy to badaniom nad zdrowiem społeczeństwa przez porównywanie danych jednostkowych o przebiegu chorób, najlepiej po uprzedniej ich anonimizacji.

Z pewnością byłoby lepiej, jaśniej i łatwiej, gdyby wdrażanie rozporządzenia ePrivacy było oparte już na doświadczeniach wdrożonego RODO. Natomiast obie te regulacje mają sens, bo budują jednolitość na europejskim rynku cyfrowym. Krajowymi rozwiązaniami nie wolno tego podważać i wracać do zmory fragmentacji.

W oparciu o pozyskane dane można budować nowe usługi. Kluczem i szansą jest personalizacja usług – możliwa właśnie dzięki pracy z danymi. Dotyczy to ochrony zdrowia, lepszego zarządzania sieciami miasta – np. wiemy, jakie są potoki samochodów, zużycie wody o różnych porach. Dotyczy to wygody zamawiania usług online, na żądanie. Dotyczy to badań naukowych i lepszych możliwości edukacyjnych dla ludzi. Dotyczy to bezpieczeństwa naszych dzieci – możemy wiedzieć, gdzie są, ale też możemy monitorować stan ich zdrowia, jeśli to potrzebne. W tych wszystkich kontekstach pozytywne efekty są możliwe, bo pracują na nie nasze dane, a my sami możemy monitorować ich przepływ. Ale właśnie: w zgodzie z regułami, które wspólnie przyjmiemy.

Na koniec jedna uwaga. Debata o prywatności powinna otwierać dyskurs o pozytywnych funkcjach Internetu łączącego użytkowników z usługodawcami biznesowymi oraz państwowymi, a nie go zamykać. W tym kontekście powinna się też toczyć dyskusja o swobodzie przepływu danych w Unii Europejskiej, o ochronie bezpieczeństwa bez łamania zasad kryptograficznych użytych dla naszego bezpieczeństwa, dyskusja o eZdrowiu.

Podsumowanie

Czy grozi nam ekologiczny kryzys prywatności?

Sytuacja, w której dane odrywają się od ludzi i zaczynają krążyć w cyfrowym ekosystemie poza ich wiedzą i kontrolą, nie jest bezpieczna. W dłuższym horyzoncie czasowym może się okazać, że jakość i wiarygodność cyfrowych profili nie nadąża za ich rosnącym wpływem na decyzje biznesowe, relacje firm z konsumentami i państwa z obywatelami.

Realne wydaje się ryzyko „zanieczyszczenia" Internetu danymi, które wyciekają z rozmaitych baz lub są przedmiotem transakcji między zorientowanymi na zysk brokerami, przekraczając prawnie wyznaczone i etyczne granice. I tak błędnie wyliczony scoring czy przypadkowy ślad w policyjnej bazie danych może wpłynąć na czyjąś szansę zatrudnienia, a stare zdjęcie z imprezy lub ujawnione poglądy polityczne na reputację w środowisku zawodowym.

> **Dane pod wieloma względami przypominają izotop radioaktywny, który mądrze i odpowiedzialnie wykorzystany kryje w sobie duży potencjał, ale z definicji wymaga też szczególnej ochrony. Ta ochrona powinna się zaczynać już na etapie pozyskiwania danych i gwarantować kontrolę nad tym procesem samym użytkownikom. W tym momencie ten ochronny parasol mocno przecieka.**

Cytowany już minister Heiko Maas tak podsumowuje problem, z którym jako społeczeństwo właśnie się mierzymy:

> *Wszyscy jesteśmy połączeni w sieci. Wszyscy jesteśmy poddawani ocenom w cyfrowym świecie. I wszyscy musimy wziąć odpowiedzialność za to, by – przy wszystkich szansach, jakie oferuje Internet – nie*

> *sprzedać i nie poświęcić tych wartości, których potrzebuje wolne i demokratyczne społeczeństwo.*
> **Heiko Maas**

Jedną z tych wartości jest prywatność, w prawniczym żargonie częściej określana mianem autonomii informacyjnej. Jej istotą nie jest ukrycie się za przysłowiową firanką czy pseudonimem, ale realna możliwość kontrolowania obiegu informacji na swój temat, zarządzania różnymi tożsamościami (rodzinną, zawodową, towarzyską) i różnymi relacjami, które nie powinny się przenikać (z bankiem, ubezpieczycielem, urzędem skarbowym, pracodawcą, opieką zdrowotną etc.). Wartość takiej ochrony we współczesnym świecie trafnie podsumował Bruce Schneier, światowej sławy kryptograf i wykładowca na Uniwersytecie Harvarda:

> *Prywatność zapewnia mi możliwość decydowania o tym, z kim dzielę się różnymi aspektami mojej osoby i informacjami o mnie. Oznacza to, że jestem niezależną ludzką istotą w społeczeństwie. Kiedy ktoś mówi mi: „Wiem coś o tobie", gwałci moją prywatność, ale także mnie osobiście.*
>
> **Bruce Schneier**

W kontekście tych zagrożeń działania podjęte przez europejskiego regulatora wydają się konieczne, choć o kilka lat spóźnione. Tym większą wagę będzie miała sensowna i szybka implementacja tych ram prawnych i ich przełożenie na konkretne praktyki rynkowe. To zadanie nie tylko dla firm, ale też dla organów je wspierających, w tym rządu i Generalnego Inspektora Ochrony Danych Osobowych, oraz partnerów społecznych, takich jak Fundacja Panoptykon. Jesteśmy gotowi podjąć to wyzwanie.

Polecane źródła:

Komisja Europejska, *Proposal for a Regulation on Privacy and Electronic Communications*, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Komisja Europejska, *Comparative Study on Different Approaches to New Privacy Challenges, in particular in the light of Technological Developments*, http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_en.pdf

Komisja Europejska, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, http://ec.europa.eu/newsroom/document.cfm?doc_id=41232.

Cracked Labs, *Report – Corporate Surveillance in Everyday Life*, http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf.

Me and My Shadow, *Location tracking*, https://myshadow.org/location-tracking.

The Norwegian Consumer Council, *Appfail Report – Threats to Consumers in Mobile Apps*, https://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/.

Share Labs, *Invisible Infrastructures: Mobile permissions*, https://labs.rs/en/invisible-infrastructures-mobile-permissions/.