Warszawa, 22 kwietnia 2024 r.

Fundacja Panoptykon
ul. Orzechowska 4/4, 02-068 Warszawa
fundacja@panoptykon.org

oraz

Fundacja „Internet. Czas działać!”
ul. Dąbrowskiego 77A, 60-529 Poznań
kontakt@internet-czas-dzialac.pl

Sz.P. Krzysztof Gawkowski
Minister Cyfryzacji

PETYCJA

w sprawie wykorzystywania technologii śledzących na stronach internetowych prowadzonych przez organy administracji publicznej

Fundacja Panoptykon jest organizacją społeczną, której celem jest ochrona praw człowieka, w szczególności prawa do prywatności, w kontekście rozwoju nowych technologii. W swojej działalności zajmuje się m.in. kwestią uprawnień policji i służb specjalnych, a także innymi formami nadzoru, jakie państwo i internetowe korporacje sprawują nad społeczeństwem.

Fundacja „Internet. Czas działać!” działa na rzecz ochrony praw cyfrowych i edukacji technologicznej, mając na celu zwiększanie kontroli ludzi nad technologią i zapobieganie używania technologii do wywierania wpływu na ludzi.

Obie organizacje – działając na styku praw człowieka i nowych technologii – zwróciły uwagę na zakres danych zbieranych za pomocą technologii śledzących, m.in. skryptów śledzących oraz ciasteczek (*cookies*), o użytkownikach i użytkowniczkach odwiedzających strony internetowe administracji publicznej.

Skrypty działające na stronach internetowych mają rozmaity charakter – od tych, które są kluczowe dla funkcjonowania stron internetowych, po takie, które służą celom marketingowym i skuteczniejszemu profilowaniu reklam. W niniejszej petycji koncentrujemy się na skryptach śledzących, których wspólną cechą jest zbieranie informacji o osobach odwiedzających stronę internetową.

Zbieranie informacji o użytkownikach i użytkowniczkach w przypadku wszystkich stron internetowych rodzi wyzwania prawne i konieczność weryfikacji, czy jest to zgodne z ustawą

z 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34; dalej: „Prawo telekomunikacyjne") oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE z 4.5.2016, L 119/1; dalej: „RODO").

Funkcjonowanie technologii śledzących wiąże się często z przekazywaniem informacji na temat użytkowników i użytkowniczek strony do podmiotów trzecich, nierzadko mających swoje serwery poza Europejskim Obszarem Gospodarczym. Niektóre strony internetowych polskich instytucji publicznych albo w ogóle nie pozyskują zgody na stosowanie technologii śledzących (nie jest wyświetlany żaden banner z zapytaniem o zgodę), albo ich administratorzy przyjmują, że „zgodą" jest brak zmiany przez użytkownika ustawień przeglądarki (co jest niezgodne zarówno z Prawem telekomunikacyjnym, RODO, jak i z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej). W innych przypadkach użytkownikom są wyświetlane bannery z zapytaniem o zgodę, które nie odpowiadają wymaganiom prawa ani wytycznym wyrażonym w orzecznictwie. Oznacza to, że korzystanie ze stron internetowych polskich instytucji publicznych w wielu przypadkach wiąże się z koniecznością ujawniania przez użytkowniczki i użytkowników informacji na swój temat firmom, których istota działalności polega na przetwarzaniu i wykorzystywaniu do własnych celów biznesowych różnego rodzaju informacji o aktywności ludzi w Internecie, w tym informacji stanowiących dane osobowe.

W kontekście stron internetowych prowadzonych przez organy administracji publicznej kwestia zbierania informacji o użytkownikach i użytkowniczkach ma szczególny wymiar, bowiem państwo nie może kierować się tą samą logiką, co właściciele prywatnych witryn internetowych zbierający dane w celu realizacji swoich celów biznesowych. Po stronie państwa leży szczególny ciężar i obowiązek troski o prywatność osób odwiedzających prowadzone przez administrację publiczną strony internetowe, zwłaszcza, że za ich pośrednictwem przetwarzane są często wrażliwe dane (np. o stanie zdrowia).

W związku z powyższym na podstawie art. 2 ust. 1 i 2 ustawy z 11 lipca 2014 r. o petycjach (tj. Dz.U. 2018 poz. 870) zwracamy się do Pana Ministra o:

1) zbadanie stosowanych przez podmioty administracji publicznej praktyk w zakresie wykorzystywania technologii śledzących na ich stronach internetowych;
2) przygotowanie – we współpracy z Urzędem Komunikacji Elektronicznej oraz Urzędem Ochrony Danych Osobowych – wytycznych wskazujących dobre praktyki w tym zakresie.

UZASADNIENIE

1. Czym są technologie śledzące i jakie jest ich zastosowanie

Internet jest siecią opartą na ciągłej interakcji między użytkownikami a serwerami. Wymaga przesyłania i odbierania danych, a w niektórych sytuacjach dodatkowo weryfikacji i potwierdzania, czy wraca ten sam użytkownik lub użytkowniczka. Strony internetowe nie tylko dostarczają treści, ale także zbierają informacje o urządzeniach końcowych użytkowniczek i użytkowników, jak i o samych tych osobach. Te dane mogą być przechowywane i przetwarzane na różne sposoby. Wykorzystywane w tym celu są tzw. skrypty śledzące, które dla uskutecznienia śledzenia nierzadko korzystają z tzw. ciasteczek (ang. „cookies"). *Cookies* są informacjami zapisywanymi przez odwiedzaną stronę na urządzeniu końcowym za pośrednictwem przeglądarki, a następnie, w przyszłości, również odczytywane przez odwiedzane strony. Skrypty śledzące mogą wykorzystywać *cookies*, aby przechowywać w nich unikalne identyfikatory nadawane odwiedzającym, aby odróżniać ich od siebie i móc łatwiej gromadzić ich historię przeglądania np. w celu profilowania.

Administratorzy stron internetowych, w tym stron internetowych podmiotów administracji publicznej, wykorzystują technologie śledzące do optymalizacji działania stron oraz do monitorowania zachowań osób odwiedzających stronę. W przypadku podmiotów komercyjnych skrypty śledzące pozwalają np. na analizę, skąd przychodzą odwiedzający, jak długo pozostają na stronie i jakie treści preferują. Zbierają takie informacje na temat aktywności użytkowników i użytkowniczek jak kliknięcia, przeglądane strony, czas spędzony na poszczególnych stronach oraz interakcje z treściami. Dzięki zebranym informacjom administratorzy mogą odpowiednio dostosować stronę, aby skuteczniej realizowała zakładane cele.

Ze względu na funkcję możemy rozróżnić trzy kategorie informacji zbieranych o użytkownikach i użytkowniczkach oraz o urządzeniach, z których korzystają:

- dane techniczne (np. rozdzielczości ekranu czy preferowanych ustawieniach w zakresie kolorystyki strony czy wielkości tekstu, jeśli strona takie ustawienia wspiera), które pozwalają lepiej dopasować wyświetlaną treść czy usprawnić działanie strony;
- informacje autoryzacyjne (kiedy w grę wchodzi logowanie za pomocą hasła, koszyk zakupów itp.);
- dane pośrednio identyfikujące użytkownika/użytkowniczkę (ale niekoniecznie używane do autoryzacji), które umożliwiają śledzenie ich działań w Internecie (np. kliknięcia w banner reklamowy; wyszukiwane hasła, historia przeglądania, dane demograficzne, ilość czasu spędzonego na stronie).

Przeciętna strona internetowa wykorzystuje kilka czy nawet kilkanaście technologii śledzących (skryptów, ciasteczek). Najtrudniej zorientować się, jaką funkcję one pełnią, kiedy są serwowane

przez tę stronę, na którą wchodzimy. W grę może wchodzić zarówno poprawne wyświetlanie treści, autoryzacja, jak i sprawdzenie, czy osoba zareagowała na reklamę. Jeśli na danej stronie pojawiają się ciasteczka stron trzecich (ang. third party cookies), może dochodzić dośledzenia w celach marketingowych. Ciasteczka stron trzecich pojawią się także wtedy, gdy strona zawiera treści hostowane na zewnętrznym serwerze (YouTube, Vimeo itp.).

2. Technologie śledzące a prywatność i dane osobowe

Na gruncie RODO zdecydowaną większość informacji, jakie zbiera na temat użytkowników i użytkowniczek strona internetowa można potencjalnie uznać za dane osobowe. Przykłady takich danych znajdziemy w motywie 30 RODO, zgodnie z którym:

„Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób".

Zgodnie z przepisami RODO, identyfikator nie musi mieć jednoznacznego charakteru, jak ciasteczka z określonym numerem. Nawet połączenie różnych cech, które osobno nie identyfikują osoby, takich jak ustawienia przeglądarki, zainstalowane czcionki i oprogramowanie, może prowadzić do pośredniej identyfikacji (taki proces nazywa się „fingerprintingiem"). W kontekście RODO istotny jest cel i zakres przetwarzania danych, a nie konkretna metoda ich zbierania.

Oczywiście to, czy i jakie dane są zbierane, zależy od konkretnego narzędzia oraz decyzji administratora strony. Jednak w przypadku skryptów śledzących stron trzecich ani użytkownik/użytkowniczka – ani nawet właściciel serwisu – nie mają kontroli nad tym, jakie informacje zostaną zapisane i odczytane przez skrypty, chociażby dlatego, że mają one dynamiczną naturę i ich treść może być zdalnie aktualizowana, bez udziału administratora strony.

Pragniemy także podkreślić, że obowiązujące powszechnie przepisy prawa chronią nie tylko dane osobowe, lecz szerzej – prywatność użytkowników Internetu. Poza RODO istotnym aktem prawnym, którego celem jest ochrona prywatności, jest Prawo telekomunikacyjne. Przepisy te wprowadzają ograniczenia dotyczące stosowania ciasteczek bez względu na to, czy stanowią one dane osobowe. W przypadku stosowania na stronach internetowych technologii śledzących choćby w celach analitycznych, wymagana jest uprzednia zgoda użytkownika/użytkowniczki. Powinna ona odpowiadać wymaganiom przepisów o ochronie danych osobowych. W szczególności powinna być poprzedzona przekazaniem jasnych i zrozumiałych informacji na temat celów, w jakich dane będą przetwarzane, jak również jakim podmiotom trzecim zostaną udostępnione. Nieprzestrzeganie przez administratorów stron internetowych wymogów

w zakresie pozyskiwania zgód użytkowniczek i użytkowników w sposób oczywisty narusza ich prywatność. Tracą oni bowiem kontrolę nad tym, jakie podmioty uzyskują dostęp do informacji o nich, w tym potencjalnie do danych osobowych. Jest to szczególnie problematyczne w przypadku stron internetowych administracji publicznej, na których przetwarzany jest szeroki zakres informacji o ludziach, w tym szczególne kategorie danych (np. dane dotyczące zdrowia).

3. Bezpieczeństwo i wiedza użytkowników stron

Zarysowana sytuacja rodzi z perspektywy użytkownika i użytkowniczki problem weryfikacji, jakie dane, w tym osobowe, na jej temat pozyskuje administrator strony internetowej oraz podmioty trzecie. Podstawowym źródłem informacji na ten temat mogą być polityki prywatności poszczególnych stron, które powinny wskazywać, jakie dane pozyskuje administrator i komu je przekazuje. Jednak nie zawsze są one w pełni zrozumiałe i przejrzyste. Niekiedy też zapoznanie się z nimi jest utrudnione, ponieważ banner dotyczący zgody na stosowanie technologii śledzących przesłania stronę, na której znajduje się polityka prywatności. Niektóre strony administracji publicznej, na których stosowane są technologie śledzące, nie mają w ogóle polityki prywatności, a użytkownik nie jest nawet pytany o zgodę na stosowanie tych technologii (tym bardziej nie może jej zatem odmówić).

Innym źródłem wiedzy mogą specjalne narzędzia, jak np. przygotowana przez Fundację „Internet. Czas działać!" wtyczka do przeglądarki – Rentgen. Wtyczka automatycznie analizuje, jakie dane zostały wysłane do podmiotów trzecich przez odwiedzane strony – wskazuje też listę domen podmiotów trzecich, z jakimi komunikowała się witryna. Mogą to być domeny, dla których dokonano zapisu i odczytu ciasteczek, a także domeny, którym udostępniono część historii przeglądania. **Wtyczka dokonuje wstępnej oceny istotności danych i automatycznie zaznacza potencjalne rekordy, którą mogą stanowić dane osobowe**. Jednak analiza pozyskanych za jej pośrednictwem informacji wymaga wiedzy technicznej.

W obecnej sytuacji użytkownicy i użytkowniczki stron internetowych nie mają pełnej wiedzy, jakie informacje na ich temat zbierają administratorzy stron publicznych.

Co więcej, można mieć wątpliwości, czy pozyskiwanie danych (oraz ich zakres) jest na jakimkolwiek etapie weryfikowane przez administratorów stron pod kątem celowości i niezbędności.

Problem ma szczególnie duże znaczenie w sytuacji, w której korzystanie ze stron internetowych administracji publicznej wiąże się z przetwarzaniem danych potencjalnie wrażliwych, np. pośrednio wskazujących na konkretne problemy zdrowotne. Taka sytuacja może mieć miejsce m.in. podczas odwiedzania witryny internetowej „uzaleznieniabehawioralne.pl" (administratorem danych osobowych w tym wypadku jest Krajowe Centrum Przeciwdziałania Uzależnieniom).

4. Suwerenność cyfrowa

Wiele spośród technologii śledzących obecnych na stronach administracji publicznej to narzędzia firmy Google (np. Google Analytics, Google Tag Manager). Ich obecność na stronach internetowych może wiązać się z przekazywaniem danych osobowych do USA. W tym kontekście istotne są podnoszone przez wiele organizacji (np. austriacki NOYB) wątpliwości dotyczące zgodności takiego transferu danych z RODO. Od 10 lipca 2023 r. obowiązuje co prawda porozumienie *EU-US Data Privacy Framework*, które formalnie daje podstawy do przekazywania danych do USA. Jednak należy pamiętać, że dwa poprzednie rozwiązania (*Safe Harbour* i *Privacy Shield*) zostały uznane za niezgodne z Kartą praw podstawowych, a względem obecnej podstawy transferów danych również podnoszone są wątpliwości. W świetle nowych zasad pojawiają się obawy, czy powołany do rozpatrywania naruszeń Sąd ds. Ochrony Danych jako organ administracji rządowej USA będzie spełniał standardy zapewniające skuteczne środki prawne, zgodnie z art. 47 Karty praw podstawowych (prawo do sądu).

Wykorzystywanie przez strony administracji publicznej narzędzi dostarczanych przez firmy z branży ad-tech jest de facto wspieraniem tych firm w ich działalności biznesowej – i to poprzez przekazywanie wskazanym podmiotom danych o Polkach i Polakach.

5. Przykłady

Oto kilka przykładów opisanego wyżej problemu:

Z Polityki prywatności oraz analizy danych z wykorzystaniem wtyczki Rentgen wynika, że strona Internetowe Konto Pacjenta korzysta m.in z Google Analytics oraz skryptu Google Tag Manager. Google Analytics to narzędzie do śledzenia i analizowania interakcji użytkowniczek i użytkowników z witryną i aplikacją. Google Tag Manager to system zarządzania tagami (kodami śledzenia), który ułatwia ich dodawanie i edytowanie. W polityce prywatności wskazuje się, że dane przekazywane do Google Analytics dotyczą m.in. „identyfikacji urządzenia, na którym [użytkownik korzysta] z serwisu pacjent.gov.pl lub aplikacji mobilnej mojeIKP".

Z kolei wspomniana wcześniej strona „uzaleznieniabehawioralne.pl", na której administratorem danych osobowych jest Krajowe Centrum Przeciwdziałania Uzależnieniom, w polityce prywatności informuje, że „pliki cookie mogą być wykorzystane przez sieci reklamowe, w szczególności sieć Google, do wyświetlenia reklam dopasowanych do sposobu, w jaki użytkownik korzysta z serwisu. W tym celu mogą zachować informację o ścieżce nawigacji Użytkownika lub czasie pozostawania na danej stronie". Natomiast w polityce prywatności serwisu „116sos.pl", która pozwala osobom w kryzysie emocjonalnym połączyć się z konsultantem, można przeczytać, że podczas przeglądania strony moduł analityczny zbiera takie dane, jak adres IP, dane lokalizacyjne czy typ urządzenia. Odbiorcami danych osobowych

mogą być podmioty świadczące usługi na rzecz NASK, z którymi zostały zawarte stosowne umowy powierzenia przetwarzania danych.

Problemy nie ograniczają się do stron internetowych, które wiążą się z przekazywaniem informacji o stanie zdrowia; są one obecne także na stronach internetowych różnych instytucji publicznych i samorządów. Na przykład oficjalna strona internetowa Wrocławia zawiera skrypty śledzące YouTube, a strona Łodzi – Google Analytics.

6. Podsumowanie

Stoimy na stanowisku, że podmioty administracji publicznej powołane do realizacji zadań publicznych powinny z najwyższą starannością dbać o ochronę prywatności, w tym ochronę danych osobowych użytkowników i użytkowniczek swoich stron internetowych. Jednym z elementów tej troski jest uporządkowanie praktyk dotyczących śledzenia tych osób z wykorzystaniem ciasteczek i skryptów śledzących na stronach internetowych. Ministerstwo Cyfryzacji ma w naszej ocenie narzędzia, żeby dokonać kompleksowego przeglądu tych praktyk.

Celem tego przeglądu powinno być zarówno wyjaśnienie, jakie narzędzia są aktualnie wykorzystywane przez administratorów, jak i potrzeb, na które te narzędzia mają odpowiadać.

Efektem przeglądu praktyk powinno być przygotowanie konkretnych wytycznych dla administratorów stron internetowych instytucji publicznych uwzględniających najwyższe standardy ochrony prywatności, a następnie ich wdrożenie w sektorze. Zależy nam na tym, by strony internetowe instytucji publicznych działały zgodnie z prawem i stanowiły wzór dla sektora prywatnego w zakresie ochrony prywatności, w tym ochrony danych osobowych użytkowników i użytkowniczek.

Wyrażamy zgodę na umieszczenie naszych danych na stronie internetowej (lub w innym miejscu publicznym) zawartych w niniejszej petycji.

PODPIS ZAUFANY
JAN
ORLIK
22.04.2024 11:34:42 [GMT+2]
Dokument podpisany elektronicznie podpisem zaufanym

Jan Orlik
Prezes Zarządu
Fundacja „Internet. Czas działać!”

PODPIS ZAUFANY
KATARZYNA
SZYMIELEWICZ
22.04.2024 12:02:13 [GMT+2]
Dokument podpisany elektronicznie podpisem zaufanym

Katarzyna Szymielewicz
Prezeska
Fundacja Panoptykon

Do wiadomości:

1. Prezes Urzędu Ochrony Danych Osobowych
2. Prezes Urzędu Komunikacji Elektronicznej
3. Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy