Nie ma czegoś takiego jak anonimowość w sieci – mówi Tomasz Izydorczyk

Posted on 2026-04-02

Jeśli ktoś korzysta z internetu, zawsze zostawia za sobą cyfrowe ślady. Od pełnych danych osobowych np. w trakcie zakupów on-line, po pliki cookies, profile użytkownika czy metadane związane z urządzeniami, które ten dostęp do sieci i usług zapewniły – mówi Tomasz Izydorczyk, członek Społecznego Zespołu Ekspertów przy Prezesie UODO.

Jak w ostatnich latach zmieniło się podejście administratorów do ochrony danych?

Podejście to zmieniło się przez ostatnie lata i nadal ewoluuje. W początkowej fazie, w latach 2016–2020, polegało ono na organizacji projektu, wdrożeniu i przygotowaniu do stosowania przepisów. Z czasem administratorzy musieli zrozumieć, że RODO to nie zestaw polityk do odłożenia na półkę, tylko procesy – tak samo jak księgowość, płace, sprzedaż czy zamówienia. Ochrona danych musiała wejść w normalne procesy operacyjno-administracyjne każdej organizacji. Oczywiście, wiele podmiotów ma jeszcze dużo elementów do wdrożenia czy udoskonalenia, jednak są i tacy administratorzy, którzy zintegrowali swoje procesy ochrony danych w normalnej codziennej pracy operacyjnej.

Nie ma czegoś takiego jak anonimowość w sieci – mówi Tomasz Izydorczyk

Nie mam żadnych statystyk, aby podeprzeć swoje twierdzenia, ale aktualnie obserwuję kilkadziesiąt dużych i średnich podmiotów, w których funkcjonujący system ochrony danych naturalnie się rozwija, łączy i przeplata z innymi działaniami, których celem jest zapewnienie zgodności z przepisami dotyczącymi nowych technologii. Mam tu na myśli (w zależności od sektora i branży) wymagania m.in. dotyczące cyberbezpieczeństwa czy sztucznej inteligencji.

Skoro RODO jest silnie związane z technologią, to jej rozwój i pojawiające się nowe technologiczne akty prawne naturalnie łączą się z przepisami o ochronie danych. Uważam też, że postawienie przez UODO wyraźnych granic działalności inspektorów ochrony danych oraz mnogość nowych regulacji w dziedzinie gospodarki cyfrowej opartej na wiedzy sprawiła, że administratorzy zaczynają dostrzegać i rozumieć potrzebę oddzielenia funkcji inspektora ochrony danych od funkcji wykonawczych, decyzyjnych i wdrożeniowych, które zapewnią szeroko rozumianą zgodność z takimi przepisami jak RODO, DSA, DGA, NIS2/KSC, AIA. Nawet jeśli przyjąć, że inspektor ochrony danych posiada wszechstronne i interdyscyplinarne kompetencje, to jednak samodzielnie nie udźwignie takiej liczby regulacji i wdrożeń. Administratorzy chyba zaczynają to rozumieć i budować swoje komórki, działy, departamenty i piony zgodności regulacyjnej.

Jakie znaczenie dla ochrony danych osobowych ma przyjęcie ustawy implementującej NIS2 w Polsce (ustawa o KSC)?

Tu także nie dysponuję statystykami, ale dzięki obserwacjom własnym oraz wielu koleżanek i kolegów – inspektorów ochrony danych – mogę przewidywać pewne zjawiska w ochronie danych i prywatności. Uważam, że NIS2 (znowelizowane przepisy Ustawy KSC) będzie miało dwa główne efekty z punktu widzenia ochrony danych. Po pierwsze, nastąpi pewnego rodzaju „odkurzenie” lub udoskonalenie procesów oceny ryzyka. Nic tak nie wymusza na organizacji przeglądu i aktualizacji polityk, procedur, analiz, jak zmiany w przepisach.

Medialna i branżowa dyskusja pomaga nam w zdobywaniu budżetów na wewnętrzne

projekty, szkolenia, edukację czy zakup profesjonalnych usług lub systemów wsparcia zarządzania bezpieczeństwem informacji. Świadomość najwyższego kierownictwa z pewnością się poprawi, a co za tym idzie, większość personelu administratorów także będzie bardziej odpowiedzialnie podchodziła do szeroko rozumianego bezpieczeństwa danych. Po drugie, NIS2 może realnie wesprzeć ochronę danych osobowych w istotnym aspekcie – zachowania poufności, integralności i dostępności tych danych. Nic tak nie skupia uwagi na tej triadzie, jak właśnie systemy zarządzania bezpieczeństwem informacji, które są najistotniejszym elementem przepisów KSC.

W jednym z postów na LinkedIn pisał Pan o „końcu pseudo-anonimowości" w internecie. Czy faktycznie nowe regulacje, jak NIS2 czy DSA, sprawią, że platformy internetowe będą powszechnie weryfikować tożsamość użytkowników?

Może zacznę od wyjaśnienia, dlaczego w ogóle użyłem pojęcia „pseudo-anonimowość". Otóż uważam, że nie ma czegoś takiego jak anonimowość w sieci. Jeśli ktoś korzysta z internetu, zawsze zostawia za sobą cyfrowe ślady. Od pełnych danych osobowych np. w trakcie zakupów on-line, po pliki cookies, profile użytkownika czy metadane związane z urządzeniami, które ten dostęp do internetu i usług zapewniły.

To, co pozwala zidentyfikować konkretną osobę fizyczną, to czasami „okruchy" informacji, które przy odpowiednich umiejętnościach, chęciach, ale i zasobach czasowych czy finansowych dają możliwość wskazania konkretnego człowieka. Nie bez powodu w samej definicji danych osobowych w RODO zostało użyte pojęcie „możliwości identyfikacji" osoby fizycznej, a katalog informacji, które identyfikują konkretną osobę, pozostaje otwarty.

Internet staje się coraz bardziej niebezpieczną domeną funkcjonowania człowieka. Chyba wszyscy możemy się zgodzić z takim twierdzeniem. A skoro jakaś przestrzeń działań jednych ludzi staje się niebezpieczna dla innych, politycy, eksperci, a na końcu prawodawcy wprowadzają prawo, które ma chronić ludzi i określone wartości. Skoro tak łatwo można skrzywdzić drugiego człowieka on-line, społeczeństwa wprowadzają roz-wiązania

pomagające nie tylko zapobiegać, ale też wykrywać i karać sprawców tych niepożądanych działań.

Organy regulacyjne i organy ścigania nie mogą działać wobec „użytkownika cyfrowego", tylko muszą ustalić personalia osoby fizycznej lub prawnej stojącej za konkretną aktywnością w internecie. Skoro jako społeczeństwo żądamy, aby platformy były bardziej bezpieczne dla nas, naszych transakcji, naszych pieniędzy czy naszych danych osobowych, a przede wszystkim dla słabszych grup społecznych, jak dzieci czy osoby starsze, administratorzy muszą zaostrzyć swoje działania wobec użytkowników platform.

I na czym ma polegać to zaostrzenie?

Jednym z wielu środków bezpieczeństwa, jakie serwisy internetowe mogą wdrożyć, to obniżenie anonimowości kont internetowych. To prowadzi wprost do zbierania większej ilości danych, aż po weryfikację wieku użytkowników. Skoro media społecznościowe mają być bezpieczne dla dzieci, platformy muszą wprowadzić weryfikację wieku. A skoro platformy sprzedaży on-line mają być bardziej bezpieczne dla osób kupujących w internecie, muszą prowadzić polityki KYC, KYB (Know Your Customer) i KYB (Know Your Business).

Dostawcy platform społecznościowych chyba także są zainteresowani samą weryfikacją wieku, bo to daje im jeszcze większy wgląd do tego, kim jesteśmy my – ich użytkownicy. Źródła OSINT, na podstawie danych publicznych dotyczących lobbingu i zeznań podatkowych, donoszą, że Meta tylko w USA wydała ponad 2 mld dolarów na lobbowanie przepisów wprowadzających obowiązek weryfikacji wieku w internecie. Oczywiście wszystkie te działania mają szczytny cel: bezpieczeństwo dzieci i innych użytkowników w sieci.

Czy można to pogodzić z prywatnością i bezpieczeństwem danych użytkowników? W zeszłym roku doszło do dużego wycieku danych z Discorda, wysłanych przy okazji weryfikacji tożsamości. Wówczas wielu komentatorów mówiło, że takich danych nie da się całkowicie

zabezpieczyć i jest tylko kwestią czasu, aż wyciekną. Rzeczywiście tak jest?

Uważam, że można pogodzić prywatność i bezpieczeństwo danych użytkowników w internecie. Aby to nastąpiło, musimy zrobić tylko i aż trzy rzeczy. Każdy z nas powinien sam wyznaczyć swoją granicę prywatności – czyli jako świadomy użytkownik udostępniać tyle danych, ile uważa za właściwe, i wybierać takich dostawców usług cyfrowych, którym ufa. Druga sprawa – administratorzy muszą ustawić odpowiedni, a słowami RODO – adekwatny – poziom bezpieczeństwa klientów (użytkowników), który będzie odpowiadał temu społecznemu i indywidualnemu poczuciu prywatności.

I żeby te dwie rzeczy się wydarzyły, czyli: „świadomy użytkownik" i „bezpieczny administrator", musi zaistnieć trzeci, równie ważny element: masowa edukacja zarówno w ramach systemu oświaty, jak i innych działań uświadamiających wszystkich zainteresowanych bezpieczną cyberprzestrzenią. W tak idealnie zbudowanym świecie tak głośne i duże wycieki danych nie będę miały większego wpływu na nas jako użytkowników sieci.

Każdy internauta będzie świadomie udostępniał informacje o sobie, a administratorzy będą wdrażać odpowiednie środki, aby nasze dane i prywatność odpowiednio zabezpieczyć.

Jak więc weryfikować tożsamość, by rodziło to jak najmniejsze zagrożenia dla prywatności? Jakie dane zbierać w tym celu i jak je zabezpieczać?

Istnieją przynajmniej cztery techniki weryfikowania tożsamości w taki sposób, aby rodziło to jak najmniejsze zagrożenia dla prywatności. Pierwszą z nich są dowody z wiedzą zerową (Zero-Knowledge Proofs). To metoda pozwalająca udowodnić, że dana informacja jest prawdziwa (np. użytkownik ma ukończone 18 lat) bez ujawniania konkretnych danych, np. daty urodzenia czy numeru PESEL.

Inną techniką jest weryfikacja atrybutowa (w odróżnieniu od „tożsamościowej"). Przykładowo, zamiast prosić użytkownika o skan dowodu osobistego, system pyta jedynie o

konkretną cechę potrzebną – adekwatną do usługi (np. prawo jazdy, czyli uprawnienie, a nie adres zamieszkania).

Kolejnym sposobem jest zdecentralizowana identyfikacja (Decentralized Identity Self-Sovereign Identity). To technika, w której użytkownik przechowuje swoje dane w cyfrowym portfelu (np. mObywatel w polskim kontekście) i udostępnia tylko niezbędne klucze do ich potwierdzenia, zamiast kopiować dane na serwer firmy.

A ostania metoda weryfikacji, jaką polecam administratorom, to weryfikacja lokalna (Edge Verification). Biometria (odcisk palca, Face ID) powinna być przetwarzana wyłącznie na urządzeniu użytkownika, np. naszym smartfonie. Serwer usługodawcy otrzymuje jedynie informację „TAK/NIE”, a nie wzorzec biometryczny. To nie są nowe techniki, ale wymagają przemyślanego wdrożenia. Co mamy w zamian? Checkbox potwierdzający, że użytkownik ma 18 lat albo zbieranie ogromnego zakresu danych na tak zwany „zapas”, czyli z naruszeniem zarazy minimalizacji danych.

Wspomniany Discord ogłosił wprowadzenie podejścia „Teen-by-Design”. Jeśli dobrze rozumiem, zakłada ono, że treści na platformie dostępne domyślnie będą odpowiednie dla nastolatków. A jeśli ktoś chce mieć dostęp do tych „nieodpowiednich”, to musi sam się zweryfikować jako dorosły. Może tą drogą powinny iść wszystkie platformy, zamiast starać się wyłapać konta niepełnoletnich?

Trudno mi ocenić, w którym kierunku rozwiną się proponowane rozwiązania. Z jednej stromy mamy ogromne lobby powiązane z mediami społecznościowymi, które chce jak najwięcej zbierania danych – bo właśnie na naszych danych zarabiają największe pieniądze. Z drugiej strony mamy mniejszych administratorów, którzy nie chcą wdrażać skomplikowanych rozwiązań, które tylko utrudniają szybki i łatwy dostęp do ich usług. Jeszcze kilka lat temu zrozumiałbym wdrożenie podejścia „Teen-by-Design” na takiej platformie jak Discord.

Nie ma czegoś takiego jak anonimowość w sieci – mówi Tomasz Izydorczyk

Dziś Discord nie jest już tylko usługą dla dzieci i nie służy wyłącznie rozrywce. Stał się narzędziem budowania ogromnych społeczności internetowych także dla dorosłych. Jest jeszcze jedna sprawa z podejściem „Teen-by-Design" lub szeroko rozumianym bezpieczeństwem w internecie: a mianowicie cenzura i monitorowanie absolutnie wszystkiego. Pod płaszczykiem bezpieczeństwa zawsze były pokusy wprowadzania narzędzi inwigilacji. Tutaj musimy nieustannie poszukiwać złotego środka pomiędzy bezpieczeństwem jednych a prawami i wolnością innych.

Branża gier, zwłaszcza mobilnych i on-line, wydaje się rodzić zagrożenia dla małoletnich – korzysta z niej wiele dzieci i to często miejsce polowań dla przestępców seksualnych. Jak można walczyć z tymi zagrożeniami?

Znowu mam tylko jedną odpowiedź: edukacja zarówno dzieci, jak i rodziców. To przede wszystkim rodzice powinni wziąć pełną odpowiedzialność za to, co ich dzieci robią w internecie i jak z niego korzystają. Jeśli edukacja nic nie da, a rodzice nie będę odpowiednio nadzorować i edukować swoje dzieci, zostanie nam wprowadzenie prawa przerzucającego całą odpowiedzialność na platformy internetowe i dostawców usług. Jak wiemy z lektur George'a Orwella, może to się skończyć permanentną inwigilacją i monitorowaniem wszystkiego, co robimy w internecie.

Wiele gier ma mechaniki, które mają uzależniać użytkowników, wymuszać działania, zachęcać do wnoszenia opłat (mikropłatności) czy proponować mechanizmy hazardowe, dark patterns. Jednak gry to nie tylko samo zło. Jak można bronić się przed tymi mechanizmami i co mogą nam dać gry, poza rozrywką?

W tym miejscu chciałbym bardzo mocno podkreślić, że gry internetowe czy mobilne nie są złe same w sobie. Wręcz przeciwnie, mogą być nie tylko rozrywką, ale i wspaniałym uzupełnieniem podstawowej edukacji matematyki, geografii czy historii, a zaawansowane gry dla dorosłych uczą zarządzania logistyką, sterowania samolotem, pociągiem, dronem czy nawet strategii wojennej osadzonej w realnych zdarzeniach współczesnych czasów. W tym

miejscu chciałbym się odwołać do wykładów i manifestów dr. Krzysztofa M. Maja z Akademii Górniczo-Hutniczej w Krakowie, polonisty uczącego młode pokolenie inżynierów, przyszłych twórców gier. To on właśnie piętnuje to, co jest złego w grach, czyli uzależniające i niebezpieczne mechaniki, oraz uczy, jak należy projektować gry.

O ile jest dużo gier dobrych i wspierających edukację oraz przyszłe kompetencje młodych ludzi, o tyle będą i te, które mają negatywny lub niebezpieczny wpływ na użytkowników. Jak walczyć z zagrożeniami w grach? Ponownie odpowiem: edukacja, edukacja i jeszcze raz edukacja. Jeśli nie zainwestujemy we właściwą edukację, w tym nie zaplanujemy odpowiednich budżetów dla organów regulacyjnych, przemysł gier z mechanikami uzależniającymi będzie niszczył kolejne pokolenia użytkowników.

A co z weryfikacją wieku? W grach i nie tylko. Wszyscy mamy świadomość, że to ważna i konieczna sprawa. Czy jest to realne, jak należy to zrobić, kto powinien być za to odpowiedzialny? Ostatnio pojawiły się głosy sugerujące, że powinno się to odbywać na poziomie systemu operacyjnego. Czy to dobry pomysł? No i co z ogromną ilością danych o użytkownikach? To dane osobowe, ale też dane o preferencjach i gustach, łakomy kąsek dla platform.

Zacznijmy od tego, że nie każda gra wymaga założenia konta użytkownika czy weryfikacji wieku. Projektanci i producenci mają swoje cele, które chce osiągnąć poprzez publikację konkretnego tytułu. Zazwyczaj platformy z grami dbają o odpowiednie oznaczenia wieku i opis gry. Uważam jednak, że to my – społeczeństwo i użytkownicy, powinnyśmy wymuszać poprzez nasze decyzje konsumencie, które gry są wartościowe, a które powinny być napiętnowane, aby zniknęły z rynku. Zachęcam rodziców do wspólnego grania ze swoimi dziećmi właśnie po to, aby lepiej zrozumieli i poznali gry, z których korzystają ich pociechy, oraz aby świadomie decydowali, w jakie powinny grać, a w jakie nie.

Uważam, że jeśli jako społeczeństwo zgodzimy się na weryfikację wieku na poziomie systemu operacyjnego komputera, przekroczymy pewną granicę, która będzie miała wpływ

na naszą prywatność. Weźmy pod uwagę, że system operacyjny to nie tylko komputer osobisty czy telefon. W telewizorach czy samochodzie też są komputery z systemem operacyjnym. Wiemy z raportów Fundacji Mozilla, jak bardzo producenci IoT (Internetu Rzeczy, w tym samochodów) łakną naszych danych osobowych. Skoro telewizory i samochody mające systemy operacyjne też będą weryfikować wiek, to w jaki sposób powstrzymamy innych producentów urządzeń, jak lodówka, kuchenka, pralka, zmywarka, przed dostępem do informacji o nas i weryfikacji wieku użytkowników?

Przecież te urządzenia także są przeznaczone dla użytkowników w odpowiednim wieku. Jak daleko będziemy przesuwać granicę zbierania dużej ilości danych o nas – użytkownikach, żebyśmy odważyli się nazwać to inwigilacją? Ja nie twierdzę, że mamy nic nie robić, ale uważam, że rozwiązywania problemów wąskiej grupy użytkowników nie można wdrażać kosztem całej społeczności. Tym bardziej że, jak wskazałem wcześniej, istnieją techniki potwierdzania wieku bez zbędnego zbierania danych osobowych.

Na koniec chciałbym zapytać o mObywatela, potężne narzędzie cyfrowego państwa, z którego korzysta ponad 11 mln użytkowników. Jeszcze w tym roku do ekosystemu ma dołączyć Europejski Portfel Tożsamości Cyfrowej (EUDI Wallet), który umożliwi obywatelom bezpieczne potwierdzanie tożsamości oraz korzystanie z usług w całej Unii Europejskiej. Jak Pan to ocenia?

Brałem udział w projektach Komisji Europejskiej związanych z budową i testowaniem rozwiązań cyfrowych portfeli i rozproszonych rejestrów cyfrowych. Zdaję sobie sprawę z tego, że jednym z kluczowych czynników tego typu rozwiązań jest prostota interfejsu i łatwość korzystania.

Jako aktywny użytkownik mObywatela jestem bardzo zadowolony z jego funkcjonalności, w szczególności potwierdzania swojej tożsamości w załatwianiu codziennych spraw.

Jednak jako gorący zwolennik transparentności mam duże obawy o bezpieczeństwo i

prywatność usługi mObywatel. Wielu ekspertów badających bezpieczeństwo tego typu aplikacji uważa, że nadal nie mamy dostępu do wszystkich informacji i całości dokumentacji, na podstawie których można byłoby zweryfikować działanie tej aplikacji pod kątem zabezpieczenia danych. Uważam, że nic tak nie poprawia jakości i bezpieczeństwa systemów jak możliwość transparentnej weryfikacji przez społeczeństwo i ekspertów niezależnych.

Pełna transparentność i rozwiązania typu open source, rozwijane przez społeczność internetową, dają gwarancję, które nie zawsze otrzymujemy od komercyjnych dostawców. Jakby nie było, cały internet jest zbudowany wyłącznie na standardach RFC – Request for Comments, publikowanych od 1969 r. przez internetową społeczność ekspertów bez nadzoru i własności jakiejkolwiek korporacji czy państwa. Darzę ogromnym zaufaniem społeczeństwo internetowe jako całość i mechanizmy w nim drzemiące. Dlatego zachęcam twórców wszelkich aplikacji, aby poddawali swoje rozwiązania krytyce społecznej użytkowników, a co za tym idzie również ocenie niezależnych ekspertów.

Dziękuję za rozmowę

Nie ma czegoś takiego jak anonimowość w sieci – mówi Tomasz Izydorczyk

Nie ma czegoś takiego jak anonimowość w sieci – mówi Tomasz Izydorczyk

Tomasz Izydorczyk