Czym jest ślad cyfrowy i jak nim zarządzać

Posted on 2025-06-30

Zarządzanie śladem cyfrowym wymaga świadomego i odpowiedzialnego funkcjonowania w przestrzeni cyfrowej. Wyrobienie właściwych nawyków oraz znajomość przysługujących nam praw umożliwiają skuteczne ograniczenie nadmiernego gromadzenia danych oraz wzmocnienie ochrony prywatności w środowisku cyfrowym.

W erze cyfryzacji wszelka aktywność w przestrzeni wirtualnej zostawia tzw. ślad cyfrowy. Terminem tym określa się wszystkie informacje, które użytkownicy – często nieświadomie – pozostawiają pod-czas korzystania z internetu, aplikacji webowych, mobilnych oraz innych usług cyfrowych. Ponieważ dane te są zapisywane, na ich podstawie możliwe jest ustalenie zachowań danej osoby i stworzenie jej profilu. Informacje te mogą być wykorzystane przez wiele różnych podmiotów w bardzo różnych celach. Od przedstawiania nam spersonalizowanych ofert przez firmy, poprzez analizę naszych zachowań przez policję, urzędy skarbowe czy potencjalnych pracodawców, a na możliwości podszywa-nia się pod nas lub przeprowadzania ataków phishingowych przez cyberprzestępców kończąc. Dlatego świadome zarządzanie cyfrowym śladem jest niezmiernie ważne.

Rodzaje śladów

Ślady cyfrowe – w zależności od tego, w jaki sposób zostały pozostawione lub zapisane – dzieli się na dwie kategorie:

- • aktywne – obejmują dane, które samodzielnie podajemy w internecie, lub czynności, które tam wykonujemy (np. publikacje w mediach społecznościowych, zakupy w internecie),
- • pasywne – obejmują dane gromadzone automatycznie bez naszej wiedzy za pośrednictwem plików cookies, które są używane za każdym razem, gdy wchodzimy na jakąś stronę internetową. Takie pliki mogą śledzić, ile razy odwiedzamy stronę, z jakiego urządzenia, jaki mamy adres IP, jakie są nasze dane geolokalizacyjne itp.

Ślad cyfrowy jako dane osobowe

Ponieważ znaczna część elementów składających się na ślad cyfrowy umożliwia bezpośrednią lub pośrednią identyfikację osoby fizycznej, może zostać zakwalifikowana jako dane osobowe w rozu-mieniu art. 4 pkt 1 RODO. Do takich elementów należą w szczególności:

- • adresy IP,
- • identyfikatory plików cookies,
- • dane geolokalizacyjne
- • czy unikatowe identyfikatory urządzeń elektronicznych (tzw. fingerprint).

Stanowisko takie jest prezentowane zarówno w orzecznictwie Trybunału Sprawiedliwości Unii Euro-pejskiej (TSUE), jak i wyrokach WSA czy NSA. Również Prezes Urzędu Ochrony Danych Osobowych w wydawanych decyzjach administracyjnych jednoznacznie przesądzał o takim charakterze wielu cyfrowych śladów.

Przykładowo TSUE w wyroku C-582/14 z 19 października 2016 r. uznał, że dynamiczne adresy IP mogą być klasyfikowane jako dane osobowe w sytuacji, gdy administrator dysponuje środkami umożliwiającymi identyfikację osoby fizycznej. Powoduje to, że nawet dane, które same nie pozwa-lają na identyfikację osoby, mogą podlegać ochronie na

podstawie przepisów RODO, jeżeli istnieje realna możliwość powiązania ich z konkretnym podmiotem danych.

Z kolei Prezes UODO w decyzji z 1 lipca 2021 r. (DKE.523.29.2021), powołując się m.in. na krajowe orzecznictwo, wyjaśnił, że „informacją dotyczącą osoby jest zarówno informacja odnosząca się do niej wprost, jak i taka, która odnosi się bezpośrednio do przedmiotów czy urządzeń, ale poprzez możliwość powiązania tych przedmiotów czy urządzeń z określoną osobą pośrednio stanowi infor-mację także o niej samej. Adres IP (Internet Protocol Address) jest unikalnym numerem przyporząd-kowanym urządzeniom sieci komputerowych. Jest zatem informacją dotyczącą komputera a nie konkretnej osoby fizycznej, zwłaszcza wtedy gdy możliwe jest współużyczenie jednego adresu IP przez wielu użytkowników w ramach sieci lokalnej. Adres IP nie zawsze wobec tego może być trak-towany jako dane osobowe w rozumieniu rozporządzenia 2016/679. Jednak tam gdzie adres IP jest na dłuższy okres czasu lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisa-ne jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej [wyrok Naczelnego Sądu Admini-stracyjnego z dnia 19 maja 2011 r., sygn. akt I OSK 1079/10]”.

W innej z decyzji (ZSPR.440.331.2019) Prezes UODO przesądził, że informacje dotyczące „kategorii marketingowych” (profilu behawioralnego) przypisanych użytkownikowi na podstawie plików cookies oraz dane skorelowane z tymi informacjami stanowią dane osobowe. W konsekwencji administrator jest zobligowany do udostępnienia tych danych osobie, której dotyczą, na podstawie art. 15 RODO.

W kontekście kontroli śladu cyfrowego przez użytkowników warto zwrócić uwagę na wyrok TSUE z 1 października 2019 r. w sprawie C-673/17, w którym Trybunał doprecyzował wymogi dotyczące wyrażania zgody na instalację plików cookies. Jak wskazał, zgoda nie jest ważna, jeżeli przechowy-wanie informacji lub dostęp do informacji już przechowywanych w urządzeniu końcowym użytkow-nika strony internetowej, za pośrednictwem plików cookie,

zostały zaakceptowane za pomocą do-myślnie zaznaczonego okienka wyboru, którego zaznaczenie użytkownik ten musi usunąć, aby od-mówić udzielenia zgody.

Zarządzanie śladem cyfrowym

Mając świadomość tego, że każda nasza aktywność w środowisku wirtualnym generuje dane podle-gające potencjalnemu przetwarzaniu, analizie i profilowaniu i biorąc pod uwagę, jakie rodzi to kon-sekwencje, warto świadomie zarządzać swoim śladem cyfrowym.

1. Świadome udostępnianie informacji

Fundamentalnym działaniem jest świadome podejmowanie decyzji odnośnie do zakresu oraz od-biorców udostępnianych informacji. Rekomendowane jest ograniczenie przekazywania danych oso-bowych do niezbędnego minimum. Gdy podanie jakichś danych (np. adresu e-mail lub numeru tele-fonu) nie jest konieczne, lepiej ich nie udostępniać.

2. Zarządzanie zgodami na

pliki cookies

Większość współczesnych witryn internetowych wymaga wyrażenia zgody na stosowanie plików cookies, przy czym często domyślnie aktywowane są pliki marketingowe lub analityczne. Użytkownik ma prawo do ich odrzucenia bez konsekwencji w postaci ograniczenia dostępu do serwisu. Wskazane jest również korzystanie z funkcji prywatności w przeglądarkach, umożliwiających blokowanie śledzących plików cookies podmiotów trzecich, a także systematyczne usuwanie historii przeglądania oraz danych przeglądarki.

3. Wykorzystanie narzędzi zwiększających prywatność

Warto też korzystać z rozwiązań technologicznych wzmacniających ochronę prywatności, takich jak:

- • wtyczki do przeglądarek blokujące mechanizmy śledzące,
- • przeglądarki zoptymalizowane pod kątem ochrony danych,
- • tryb incognito podczas przeglądania,
- • sieci VPN podczas korzystania z sieci publicznych, które zapewniają szyfrowanie połączenia, maskowanie adresu IP oraz zabezpieczenie przed atakami typu MITM (Man in the middle).

4. Egzekwowanie uprawnień wynikających z RODO

Nieodzownym elementem kontroli śladu cyfrowego jest aktywne korzystanie z praw przysługują-cych nam na mocy RODO. Każdy z nas ma prawo do informacji o zakresie przetwarzanych danych, celach przetwarzania oraz potencjalnych odbiorcach. Ponadto możliwe jest żądanie sprostowania, ograniczenia przetwarzania, przeniesienia lub usunięcia danych. W przypadku wątpliwości warto wyjaśniać je z administratorem. Ponadto przysługuje nam również prawo złożenia skargi do Prezesa UODO oraz możliwość dochodzenia swoich praw przed sądem cywilnym.