Ciasteczka – które z nich mogą być ryzykowne dla twojej prywatności w sieci

Prawdopodobnie jednym z powodów naszej dezorientacji jest to, że ta sama nazwa: „ciasteczka" obejmuje bardzo szeroki wachlarz celów, dla których ta technologia jest wykorzystywana; począwszy od bardzo pożytecznych technicznych *cookies* sesyjnych, a skończywszy na inwazyjnych ciasteczkach instalowanych np. przez firmy zewnętrzne w celu tworzenia profili użytkownika, tak aby następnie zasypywać nasze ekrany reklamami. W tym artykule skupimy się na tym, jakie przepisy regulują *cookies* i na najprostszym ich podziale, który może pomóc orientować się w dzisiejszym internetowym labiryncie.

1. Cookies – najważniejsze informacje

Zacznijmy jednak od garści podstawowych informacji, które będą dla nas punktem wyjścia do głównego problemu.

A. Czym są ciasteczka

Z technicznego punktu widzenia, ciasteczka to małe pliki (zbiór danych składający się z ciągu cyfr i liter), które są zapisywane na naszych urządzeniach (komputerach, tabletach, smartfonach) za pośrednictwem naszej przeglądarki podczas łączenia się z danym serwisem internetowym. Mówiąc o serwisach internetowych mam na myśli zarówno różnego rodzaju portale informacyjne i e-sklepy, jak również wyszukiwarki takie jak Google. Upraszczając sprawę – prawie cały internetowy świat, dostępny dla konsumenta, używa *cookies*. Ciasteczka, które znalazły się w naszym urządzeniu, zbierają informacje o tym jakie czynności podejmujemy w Internecie (np. informacje o odwiedzanych przez nas stronach), a następnie nasza przeglądarka odsyła taką „paczkę ciastek", wraz z zebranymi informacjami, przy kolejnym połączeniu się z danym serwisem. Przeglądarki mają tu istotne znaczenie, ponieważ to one zarządzają ciasteczkami, my natomiast możemy zmienić ich ustawienia w taki sposób, aby uniemożliwić instalowanie poszczególnych ciasteczek.

B. Klasyfikacje ciasteczek

Przeglądając witryny zawierające polityki *cookies*, możemy zauważyć, że zazwyczaj zamieszczona jest tam cała lista różnych kategorii ciasteczek. Taki katalog często zaczyna się od *niezębnych cookies*. Poza tym typem *cookies* często możemy przeczytać o ciasteczkach permanentnych lub sesyjnych, ciasteczkach stron trzecich lub ciasteczka

własnych, *cookies* analitycznych, funkcjonalnych czy reklamowych. Ciasteczka używane przez daną witrynę zazwyczaj można zakwalifikować do więcej niż jednej kategorii (np. ciasteczka niezbędne sesyjne lub ciasteczka własne analityczne). Najważniejszą jednak sprawą podczas przeglądania tych długich list, jest zorientowanie się, które ciasteczka nie są konieczne do prawidłowego korzystania z danego serwisu, a służą jedynie np. reklamodawcom.

C. Jakie przepisy bezpośrednio regulują cookies?

Jeżeli chodzi o polskiego e-konsumenta powinniśmy zwrócić uwagę na dwa poziomy regulacji. Na poziomie unijnym korzystanie z *cookies* uregulowane jest przede wszystkim w Dyrektywnie UE e-prywatność (z ang. e-privacy) w art. 5 ust. 3, a na poziomie krajowym w art. 173 ustawy Prawo Telekomunikacyjne (dalej: Ustawa). Przepisy krajowe oczywiście współgrają z prawem unijnym (normy prawne zawarte w Dyrektywie zostały implementowane, czyli wprowadzone do polskiego sytemu prawnego, właśnie poprzez Ustawę).

> *Jedną z najważniejszych reguł ustanowionych przez te przepisy jest to, że* ***przechowywanie lub uzyskanie dostępu do informacji przechowywanej na urządzeniu użytkownika jest dozwolone pod*** *warunkiem* ***(i)*** *dostarczenia użytkownikowi* ***jasnej i wyczerpującej informacji*** *m.in. o celach* ***przetwarzania*** *tych informacji i* ***(ii)*** *umożliwienia* ***odmówienia zgody na takie przetwarzania.*** *Na poziomie krajowym ustawa pogłębia tę zasadę wprowadzając obowiązek* ***uzyskania zgody*** *i dodatkowo* ***poinformowania*** *o warunkach korzystania z tych informacji za pomocą ustawień oprogramowania oraz ustanawiając* ***zakaz dokonywania zmian*** *konfiguracyjnych w urządzeniu użytkownika (dlatego też „informacje", o których tu mowa powinny być bezpieczne dla naszych laptopów, smartfonów czy tabletów).*

Omawiane przepisy są sformułowane w sposób bardzo techniczny, ponieważ uwzględniają różne technologie śledzące nas w sieci, dlatego na potrzeby naszego artykułu możemy zwrot **„przechowywanie lub uzyskanie dostępu do informacji"** zastąpić zwrotem: „przechowywanie lub uzyskanie dostępu do cookies".Teraz powinniśmy mieć jasność, że **podstawy** legalnego wykorzystywania *cookies* to po pierwsze, **obowiązek informacyjny**, a po drugie **uzyskanie uprzedniej zgody** (stąd wyskakujące na stronach okienka z pytaniem czy chcemy zaakceptować wszystkie *cookies*, czy może chcemy przejść do ustawień zaawansowanych).

Ale od tej głównej zasady są dwa wyjątki **zwalniające z obowiązku uzyskiwania zgody** na instalowanie ciasteczek. Chodzi o sytuacje, w których wykorzystanie *cookies* jest niezbędne do:

- „***wykonania transmisji komunikatu*** *za pośrednictwem publicznej sieci telekomunikacyjnej*” oraz
- „***dostarczania usługi*** *telekomunikacyjnej lub usługi świadczonej drogą elektroniczną,* ***żądanej*** *przez abonenta lub użytkownika końcowego*

W obu przypadkach mamy do czynienia z **niezbędnością** wykorzystania ciasteczek w celu prawidłowego nadania danej transmisji lub w celu wykonania usługi (chodzi o np. niezbędne *ciasteczko koszyka zakupowego* potrzebne do zawarcia transakcji sprzedaży online). W tym przypadku będziemy mówić głównie o **niezębnych ciasteczkach sesyjnych**. Widzimy więc, że termin „**cookies”** dotyczy nawet takiego użycia informacji zapisywanych na naszych urządzeniach**, które jest wyłączone spod regulacji ustawy.**

2. Co ma wspólnego RODO z cookies?

Odpowiadając na to pytanie, powinniśmy zwrócić uwagę na dwie ważne kwestie.

Po pierwsze związek przepisów bezpośrednio regulujących ciasteczka z RODO jest bardzo wyraźny. Możemy powiedzieć, że Dyrektywa e-prywatność i przepisy Ustawy są w pewien sposób „odpowiednikiem” RODO w cyfrowym świecie. Ponadto, same *cookies* w wielu przypadkach mogą zostać uznane za dane osobowe (o czym mowa w art. 30 preambuły RODO) i wówczas w grę wchodzi bezpośrednie stosowanie RODO. Związek między regulacjami możemy też zobaczyć w art. 174 Ustawy, zgodnie z którym do uzyskania zgody przez użytkownika stosuje się właśnie przepisy o ochronie danych osobowych.

Po drugie na dzień publikacji tego artykułu mówimy jeszcze o Dyrektywie e-prywatność, która została implementowana do porządków prawnych poszczególnych krajów UE, natomiast od trzech lat trwają prace nad Rozporządzeniem EU e-prywatność, które ma zastąpić obecną Dyrektywę i będzie stosowane bezpośrednio jako regulacja współgrająca i uzupełniająca RODO w sferze elektronicznej. Wejście w życie tego rozporządzenia ma nam dostarczyć kompleksowej regulacji nie tylko w kwestii bezpośredniej ochrony naszych danych i zarządzaniem ustawieniami dotyczącymi prywatności w sieci, ale też w innych sferach takich jak np. ochrona tzw. metadanych (czyli „danych o danych”, które również mogą być zawarte w ciasteczkach). W trakcie prac nad rozporządzeniem pojawiło się wiele propozycji; np. umożliwienie „płacenia” naszymi danymi za korzystanie z poszczególnych witryn, czyli tzw. *cookie wall* (która spotkała się z bardzo mocną krytyką jako praktyka naruszająca prawa użytkowników sieci; m.in. Europejska Rada Ochrony Danych postuluje wyraźny zakaz stosowania *cookie wall*). Poza tym, nadal sygnalizuje się kolizję wielu innych punktów projektu E-privacy z RODO, które powinny być zniwelowane tak aby zapewnić spójność obu regulacji. Prawdopodobnie z tych powodów mamy do czynienia z dużym opóźnieniem we wprowadzeniu rozporządzenia, mimo że w dobie tak mocnego przyspieszenia cyfryzacji naszego życia, obecnie funkcjonujące przepisy w formie dyrektywy (a nie rozporządzenia) nie

są już wystarczające.

3. Cookies podzielone – stopniowanie ryzyka

Teraz wróćmy do głównego problemu, czyli do ryzyka związanego z zapisywaniem *cookies* na naszych urządzeniach

> *Nasza prywatność w przypadku sesyjnych ciasteczek niezbędnych do funkcjonowania strony (essential cookies) nie powinna być zagrożona. Tutaj sprawa jest dość prosta, ponieważ – jak wskazaliśmy wyżej – ten typ ciasteczek nie wymaga naszej zgody, właśnie ze względu na swój niezbędny i podstawowy charakter.*

Jak więc traktować resztę *cookies?* Dla uproszczenia podzielę pozostałą pulę stałych ciasteczek „nie niezbędnych" (*non-essential permanent cookies*) na ciasteczka własne i ciasteczka osób trzecich.

Ciasteczka własne należą do odwiedzanej przez użytkownika domeny oraz są generowane i instalowane przez tę domenę. Pomimo, że zwyczajowo kojarzymy własne *cookies* z prawidłowym funkcjonowaniem strony i usprawnieniem poruszania się po niej (np. poprzez zapamiętanie naszego języka na wielojęzycznych stronach), to możemy też znaleźć wśród tej dużej grupy również ciasteczka analityczne (do monitorowania ruchu na stronie), a nawet ciasteczka o charakterze marketingowym (*first and third-party advertising cookies*).

Jeżeli natomiast chodzi o ciasteczka osób trzecich, są to pliki należące do zewnętrznych domen. Mówiąc o tego rodzaju ciasteczkach, prawdopodobnie w pierwszej kolejności przychodzą nam do głowy te najbardziej inwazyjne, dzięki którym generowane są „prześladujące nas" reklamy na innych stronach internetowych. Niemniej jednak, istnieją też ciasteczka osób trzecich służące np. do zabezpieczenia strony (np. *firewall cookie*).

4. Gdzie więc jest duże ryzyko dla ochrony danych?

Jeszcze dziś możemy powiedzieć, że z punktu widzenia naszej prywatności w sieci, jedną z najbardziej inwazyjnych praktyk jest łączenie – przy pomocy **cookies stron trzecich** – danych, które samodzielnie nie mogą nas zidentyfikować z innymi danymi np. adresem e-mail lub nazwiskiem. W ten sposób firmy zewnętrzne (w stosunku do odwiedzanej przez nas witryny) mogą tworzyć nasz **indywidualny profil**. Taki profil zawiera szereg informacji na temat naszych ruchów w sieci służący do wysyłania do nas bardzo zindywidualizowanych reklam, również na innych przeglądanych stronach. Takie działanie może okazać się nie tylko

niezwykle irytujące, ale też groźne z punktu widzenia ochrony konsumentów.

Dlaczego mówimy o stanie na dziś, a nie o sytuacji, która będzie miała na pewno miejsce w przyszłości? Dlatego, że użycie ciasteczek stron trzecich powoli będzie znikało z naszej przestrzeni internetowej. W tym temacie Google Chrome już zapowiedział, że do roku 2022 zupełnie wyeliminuje użycie ciasteczek osób trzecich. Wówczas szala kontroli nad zbieranymi danymi powinna przesunąć się w stronę ciasteczek stron pierwszych (które tak jak wspomniałam wcześniej, też mogą zbierać najróżniejsze dane, nawet w celach marketingowych) i innych technologii śledzących. Takie zmiany i użycie coraz to nowych (nieznanych nam tak dobrze jak *cookies*) technologii, może powodować pewien stan niepewności. Te wątpliwości powinno rozwiązać jednak tak bardzo oczekiwane rozporządzenie e-Privacy. Czekamy zatem najdalszy rozwój wydarzeń.

Autorka: Paulina Sewerzyńska

Foto from: Snappa