

Magdalena CZAPLIŃSKA*

 <https://orcid.org/0000-0002-1344-6779>

Marlena SAKOWSKA-BARYŁA**

 <https://orcid.org/0000-0002-3982-976X>

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH I PROFILOWANIE UWAGI NA TLE WYROKU TRYBUNAŁU SPRAWIEDLIWOŚCI UE Z DNIA 1 PAŹDZIERNIKA 2019 R. W SPRAWIE C-673/17

Abstrakt

Przedmiot badań: Przedmiotem badania jest wyrok TSUE z dnia 1 października 2019 r. w sprawie C-673/17 (Planet 49). W niniejszym artykule przedstawiona została analiza problemu przetwarzania danych osobowych w zakresie obowiązków informacyjnych i warunków udzielenia zgody, wymaganych przez RODO, w sytuacji przetwarzania danych osobowych przez informatyczne narzędzia zbierania danych, które wywierają wpływ na sferę prywatności użytkownika sieci łączności elektronicznej jako informacje, w tym dane osobowe przechowywane w urządzeniach końcowych, służące zdalnej identyfikacji i śledzeniu użytkowników końcowych.

Cel badawczy: Celem badawczym artykułu jest ocena rozwiązań prawnych dotyczących obowiązków stosowania plików cookies jako jednej z technologii, która przechowuje informacje na urządzeniach użytkowników końcowych lub uzyskuje do tych informacji dostęp. W aktualnym stanie prawnym brak jest legalnej definicji plików cookie nie tylko ze względu na to, że nie jest to jedyna technologia, pozwalająca na zbieranie informacji z urządzeń końcowych, ale także z uwagi na różne źródła pochodzenia plików cookie i ich funkcje (np. cookie analityczne, marketingowe, związane z bezpieczeństwem). Pliki cookie instalowane na urządzeniu końcowym użytkownika mogą zawierać numer przypisany do danych rejestracyjnych użytkownika. Oznacza to, że skojarzenie takiego numeru z danymi osobowymi użytkownika powoduje personalizację danych przechowywanych przez pliki cookie, wobec czego zbieranie danych za pomocą tych plików może być przetwarzaniem danych osobowych. Jedną z form zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej jest profilowanie. Przetwarzanie danych osobowych uwarunkowane jest zaistnieniem przesłanek dopuszczalności przetwarzania

* Mgr, doktorantka, Uniwersytet Łódzki, Wydział Prawa i Administracji, Katedra Prawa Gospodarczego i Handlowego; e-mail: magdalena.czaplinska@edu.uni.lodz.pl

** Dr, członkini kadry naukowej Instytutu Prawa Nowych Technologii i Ochrony Danych Osobowych Uczelni Łazarskiego; e-mail: m.sakowskabaryla@kancelariasbc.pl

danych wskazanych w art. 6 i 9 RODO, wśród których znajduje się zgoda podmiotu danych. Zgoda jako jedna z niezależnych podstaw przetwarzania danych osobowych ma na celu zagwarantowanie autonomii informacyjnej podmiotu danych w sytuacji, gdy to właśnie od jego decyzji zależy możliwość przetwarzania danych. Dla zakwalifikowania danego działania lub oświadczenia jako wyrażenie zgody konieczne jest kumulatywne wystąpienie jej elementów konstrukcyjnych, wymienionych w art. 7 RODO, których spełnienie konieczne jest także w warunkach wyrażania oświadczeń on-line.

Metoda badawcza: Stosując metodę prawnoporównawczą, przeprowadzona została analiza obowiązujących przepisów z uwzględnieniem tego, że Trybunał w Luksemburgu w wyroku z 1 października 2019 r. w sprawie C-673/17 (Planet 49) wypowiedział się na temat zgody na zamieszczenie plików cookie o funkcji marketingowej oraz zakresu informacji, jakich należy udzielić przy pozyskiwaniu takiej zgody.

Wyniki: Zamieszczenie plików cookies o treści marketingowej wymaga zgody, spełnienia warunków jej pozyskiwania oraz zachowania standardów informacyjnych zgodnych z RODO.

Słowa kluczowe: zgoda na przetwarzanie, pliki cookie.

1. Wstęp

Nie ma odwrotu od życia w sieci. Wszyscy widzimy korzyści z e-commerce, z funkcjonowania serwisów społecznościowych czy e-administracji. Koszty tych udogodnień są związane z zagrożeniem dla prywatności i autonomii woli jednostki, a także większą ekspozycją na manipulację on-line. Napięcie między jawnością życia a prywatnością zyskuje nowy wymiar, nie zawsze oczywisty dla jednostki, z której danych korzysta się w celach często dla niej niewiadomych, nieoczywistych lub wobec niej ujawnionych. Dzieje się tak w dużej mierze za sprawą naszej nieświadomości co do skutków korzystania z technologii¹. Jednym z tych skutków pozostaje powszechnie stosowane profilowanie, którego immanentną cechą jest dokonywanie zautomatyzowanego przetwarzania danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy różnych aspektów jej funkcjonowania. Przetwarzanie danych osobowych nie w każdym przypadku wymaga zgody. Wielokrotnie wynika ono z innych podstaw niż zgoda osoby, której dane dotyczą. Tym bardziej istotne wydają się kwestie będące przedmiotem dokonywanej tu analizy, czyli to, kiedy mamy do czynienia ze zgodą na przetwarzanie i z przetwarzaniem danych osobowych jako takich, a także to, kiedy mamy do czynienia z profilowaniem.

¹ Zob. A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wydawnictwo Presscom, Wrocław 2019, s. 61.

Wyrok Trybunału Sprawiedliwości UE z dnia 1 października 2019 r. w sprawie C-673/17 przesądził, że w sytuacji, w której zgoda na użycie cookie jest wymagana (choć nie na zastosowanie każdego rodzaju plików cookie), musi uwzględniać standardy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólnego rozporządzenia o ochronie danych)² – dalej: RODO. We wcześniejszym wyroku w sprawie Fashion ID z dnia 29 lipca 2019 r. C-40/17, TSUE nie wykluczył zupełnie możliwości powoływania się na prawnie uzasadniony interes w odniesieniu do wtyczki społecznościowej działającej podobnie jak cookie³. Wyrok TSUE w sprawie Planet 49 może stanowić podstawę do zmiany praktyki pozyskiwania zgód w sytuacji korzystania z informatycznych narzędzi automatycznego zbierania danych, a w konsekwencji takiegoż przetwarzania pozwalającego na dokonywanie ocen i predykcji. Uzasadnienie tego wyroku pozwala przede wszystkim powrócić do refleksji nad pojęciem zgody i profilowania w rozumieniu wynikającym z przepisów RODO.

2. Zagadnienia prawne na tle wyroku TSUE C-673/17

Przedmiotem pytań prejudycjalnych postawionych przed TSUE było m.in. zagadnienie skuteczności wyrażenia zgody, w sytuacji gdy przechowywanie informacji lub dostęp do informacji, zgromadzonych w urządzeniu końcowym użytkownika, odbywa się na podstawie domyślnie zaznaczonego okienka wyboru, z którego użytkownik musi usunąć zaznaczenie w celu odmówienia wyrażenia zgody oraz to, jakich informacji usługodawca powinien udzielić użytkownikowi w ramach jasnych i wyczerpujących informacji oraz czy informacje te obejmują również okres ważności plików cookie, a także dostęp osób trzecich do plików cookie.

Wyrok z 1 października 2019 r. zapadł w stanie faktycznym, w którym sąd odsyłający po potwierdzeniu przez Spółkę Planet 49 przyjął, że pliki cookie, które mogą być instalowane na urządzeniu końcowym użytkownika uczestniczącego w loterii promocyjnej zorganizowanej przez spółkę Planet 49, zawierają numer przypisany do danych rejestracyjnych tego użytkownika, który w formularzu uczestnictwa w tej grze musi wpisać swoje imię i nazwisko oraz adres. Sąd odsyłający uznał zatem, że

² Dz.U.UE.L.2016.119.1.

³ Szerzej zob. **M. Franke**, *Pytania wokół wyroku w sprawie cookies*, ABI Expert 2020/1, s. 17.

skojarzenie takiego numeru z tymi danymi powoduje personalizację danych przechowywanych przez pliki cookie, gdy użytkownik korzysta z Internetu, wobec czego zbieranie tych danych za pomocą plików cookie jest przetwarzaniem danych osobowych. W tak przedstawionym stanie faktycznym TSUE przesądził, że nie jest ważna zgoda, jeżeli przechowywanie informacji lub dostęp do informacji już przechowywanych w urządzeniu końcowym użytkownika strony internetowej zostały zaakceptowane za pomocą zaznaczonego domyślnie przez usługodawcę okienka wyboru, którego zaznaczenie użytkownik musi usunąć, aby odmówić udzielenia zgody. Z uzasadnienia tego wyroku wynika, że praktycznie niemożliwe wydaje się ustalenie w sposób obiektywny, czy użytkownik strony internetowej rzeczywiście wyraził zgodę na przetwarzanie jego danych osobowych poprzez to, że nie usunął domyślnego zaznaczenia okienka wyboru, a w każdym razie, czy zgoda ta została udzielona w sposób świadomy. Nie można bowiem wykluczyć, że wspomniany użytkownik nie przeczytał informacji towarzyszących domyślnie zaznaczonemu okienku wyboru, czy wręcz nie zwrócił uwagi na to okienko przed podjęciem dalszej aktywności na odwiedzanej przezeń stronie internetowej.

3. Zgoda jako przesłanka przetwarzania danych

Zgodnie z art. 4 pkt 11 RODO „zgoda” osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych. Na tle tej definicji stwierdzić można, że europejski system ochrony danych osobowych został oparty na zasadzie *opt-in* wymagającej działania podmiotu danych spełniającego warunki jednoznaczności, konkretności i wyrażności (w przypadku działania potwierdzającego). W konsekwencji tego ujęcia wykluczone zostały wszelkie modele *opt-out*, wykorzystujące bierność, milczenie osoby, której dane dotyczą, jej nieuwagę lub bezwolność, a także ustawienia domyślne, w tym domyślnie zaznaczone okienka zgód. Tak więc, dla zakwalifikowania danego działania lub oświadczenia jako wyrażenie zgody konieczne jest kumulatywne wystąpienie jej elementów konstrukcyjnych, jakimi pozostają: dobrowolność, konkretność, świadomość i jednoznaczność okazania woli podmiotom, którym osoba, której dane dotyczą, przyzwala na przetwarzanie dotyczących jej danych osobowych⁴. Ich sprecyzowanie nastąpiło w art. 7

⁴ A. Nerka, komentarz do art. 4 pkt 11, w: M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, C.H. Beck, Warszawa 2018, s. 116.

RODO, który prócz elementów wskazanych wyżej, do istotnych cech zgody zalicza również jej odwoływalność. Przepis ten osobno zatytułowany „Warunki wyrażenia zgody” przewiduje, że w przypadkach, gdy przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych (art. 7 ust. 1 RODO). Nadto, jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie RODO nie jest wiążąca (art. 7 ust. 2 RODO). Wyraźnie zaznaczono w art. 7 ust. 3 RODO, że osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę, zaś wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Przepis ten zakłada, że osoba, której dane dotyczą, jest o tym informowana zanim wyrazi zgodę, że wycofanie zgody musi być równie łatwe jak jej wyrażenie. W art. 7 ust. 4 RODO określa wymogi dotyczące oceny dobrowolności zgody poprzez wskazanie, że oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Ponieważ z normatywnego założenia zgoda musi być konkretna, cechę tę osiąga się poprzez uwydatnienie wymagań co do treści zgody. Obligatoryjnie powinna ona zawierać wyraźne i precyzyjne informacje na temat celu i zakresu przetwarzania danych. Niezgodne z prawem są zatem zgody formułowane w sposób abstrakcyjny, blankietowy bądź ogólny i w efekcie niepozwalający na określenie w sposób zrozumiały celu i zakresu przetwarzania. Zgoda powinna odnosić się do przetwarzania uzasadnionego w kontekście wskazanego celu. Konkretność zgody warunkuje możliwość realizacji zasady przejrzystości przetwarzania dla podmiotu danych⁵. Analogiczne ustalenia poczyniła Grupa Robocza Art. 29 w opinii 15/2011 w sprawie definicji zgody (WP 187), w której wskazano, że niedopuszczalna jest ogólna zgoda bez określenia dokładnego celu przetwarzania⁶. Warunek konkretności nie ogranicza się jednak tylko do

⁵ *Ibidem*.

⁶ Opinia 15/2011 Grupy Roboczej Art. 29 w sprawie definicji zgody przyjęta w dniu 13 lipca 2011 r., s. 18, <https://archiwum.giodo.gov.pl/pl/1520110/4214>; stan na 11.08.2020 r.

wskazania celu przetwarzania, ale dotyczy także innych jego aspektów, przede wszystkim zakresu danych. Konieczność konkretyzacji celu przetwarzania objętego zgodą należy analizować na gruncie art. 6 ust. 1 lit. a RODO, z którego wynika, że osoba, której dane dotyczą, powinna wyrazić zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów, a także art. 9 ust. 2 lit. a RODO, z mocy którego zgoda legalizująca przetwarzanie danych osobowych szczególnych kategorii powinna określać jeden lub kilka konkretnych celów, z zastrzeżeniem niedopuszczalności przetwarzania tych danych na podstawie zgody przewidzianej przez prawo Unii lub prawo państwa członkowskiego.

Powszechną praktykę stanowi przetwarzanie danych w oparciu o wyraźne działanie potwierdzające przez potwierdzenie chęci wejścia na stronę internetową lub skorzystanie z usługi. Zakłada się też, że opublikowanie polityki prywatności strony internetowej jest wystarczające dla poinformowania użytkownika o zakresie i celu zbierania danych oraz ich ewentualnym udostępnianiu podmiotom trzecim, a tym samym umożliwia mu podjęcie świadomej decyzji co do tego, czy zgadza się na ich przetwarzanie. Badania prowadzone zarówno w Europie, jak i USA wykazały jednak, że takie domniemanie nie ma oparcia w rzeczywistości poziomie świadomości użytkowników⁷.

Po wyroku TSUE konieczne wydaje się zweryfikowanie przyjętych praktyk i rozpoczęcie na nowo dyskusji o zakresie przetwarzania danych przez informatyczne narzędzia zbierania danych i ich skutkach. TSUE podkreślił wymóg „czynnej” zgody na cookie, ale nie wskazał, jakie zachowanie użytkownika jest wystarczające. Wydaje się jednak, zarówno na podstawie omawianego wyroku, jak i wcześniejszych stanowisk niektórych regulatorów (CNIL, ICO, AEPD, GR w wytycznych WP 259), że nadszedł kres czasów, gdy samo zamknięcie okienka lub kontynuowanie przeglądania strony stanowi zgodę wyrażoną przez ustawienia przeglądarki⁸. Proces pozyskiwania zgody wyrażonej za pomocą ustawień przeglądarki powinien obejmować co najmniej jakąś formę aktywności użytkownika wyraźnie nakierowaną na akceptację cookie.

⁷ Zob. **K. Szymielewicz, A. Walkowiak**, *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem*, Aktualne Problemy Prawnej Ochrony Danych Osobowych 2014, w: **G. Sibiga** (red.), dodatek do Monitora Prawniczego 2014/9, s. 31.

⁸ Szerzej zob. **M. Franke**, *Pytania...*, s. 17.

4. Profilowanie i tworzenie profilu osobowego osoby fizycznej

Zgodnie z art. 4 pkt „profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. To definicja niewystępująca wcześniej w poprzedzającej RODO dyrektywie 95/46/WE. Opiera się na tych samych elementach, co definicja zawarta w Rekomendacji Komitetu Ministrów Rady Europy w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili [Rekomendacja CM/Rec (2010) 13], w której określono m.in. przesłanki, jakie powinny być podstawą legalizacji procesu profilowania, wykorzystane w RODO. Istotne znaczenie dla definicyjnego sprecyzowania instytucji profilowania miała również opinia Grupy Roboczej Art. 29 w sprawie internetowych reklam behawioralnych, gdzie dokonano m.in. podziału profilowania na predykcyjne oraz formalne (jawne)⁹. Warunkiem koniecznym, aby można było mówić o profilowaniu, jest zautomatyzowane przetwarzanie danych osobowych do oceny niektórych czynników osobowych osoby fizycznej. Elementami konstrukcyjnymi w tym przypadku są takie cechy przetwarzania, jak jego zautomatyzowanie i dokonywanie oceny lub ocen, także w tenże automatyczny sposób. Tworzenie profilu osobowego osoby fizycznej, nazywane zwykle „profilowaniem”, w literaturze jeszcze sprzed obowiązywania RODO, definiowało się jako automatyczną technikę przetwarzania danych, polegającą na przypisaniu danej osobie „profilu” w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw¹⁰. „Profilem” natomiast określa się zestaw danych charakteryzujący kategorię osób, mający zostać zastosowany w odniesieniu do konkretnej osoby¹¹.

Profilowanie polega na ocenie niektórych czynników osobowych osoby fizycznej, w szczególności analizie lub prognozie pewnych aspektów. Stąd nie

⁹ Zob. **M. Sakowska-Baryła** (red.), komentarz do art. 4 pkt 4, w: **M. Sakowska-Baryła** (red.), *Ogólne rozporządzenie o ochronie danych...*, s. 88.

¹⁰ Zob. **W.R. Wiewiórowski**, *Personal Profiling Based on Generally Accessible Data*, *International Journal on Information Technology and Security* 2012/3, s. 31–46.

¹¹ Zob. **W.R. Wiewiórowski**, *Profilowanie osób na podstawie ogólnodostępnych danych*, w: **A. Mednis** (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, Warszawa 2013, s. 27.

każda czynność zautomatyzowanego przetwarzania danych będzie profilowaniem (np. automatyczne rejestrowanie czasu pracy nie będzie stanowiło profilowania). Profilowanie na gruncie RODO – jako takie – nie wiąże się z nałożeniem na administratorów bądź podmioty przetwarzające dodatkowych wymogów co do dopuszczalności przetwarzania. Spełnienia konkretnych przesłanek wymaga tylko profilowanie, o którym mowa w art. 22 RODO, a więc takie, gdy jest podstawą do podejmowania wobec danej osoby decyzji opartej na zautomatyzowanym przetwarzaniu w postaci profilowania. W pozostałych przypadkach profilowania podejmowanego środkami tradycyjnymi podlega ono ogólnym zasadom przetwarzania danych, o których mowa w art. 6 i 9 RODO. Wyjątkiem pozostaje w tym zakresie prawo do sprzeciwu, o którym mowa w art. 21 RODO, dotyczące wszelkich form profilowania¹².

Profilowaniem możemy określić dwie metody działania. Pierwsza to zbieranie z różnych źródeł takich danych, o których wiadomo, że dotyczą tej samej zidentyfikowanej osoby. Druga metoda profilowania to wnioskowanie o nieznanych cechach konkretnej osoby z cech już wcześniej jej przypisanych. Mamy tu do czynienia z tworzeniem profili grupowych, obejmujących cechy wielu osób, gdzie na podstawie przynależności do określonej grupy, za pomocą wnioskowania statystycznego, wnioskuje się o występowaniu danej cechy u konkretnej osoby fizycznej, należącej do tej grupy. Z pewnością ta metoda, polegająca na uzupełnianiu zestawu cech osobowych o cechy, których wprawdzie nie jesteśmy pewni, ale których u danej osoby można się spodziewać na podstawie analiz statystycznych, jest szczególnie niebezpieczna dla prywatności jednostki, bo może prowadzić do tworzenia profili nieprawdziwych¹³.

Oba te procesy mogą występować łącznie. Zwykle pierwszy poprzedza skorzystanie z drugiego, bo wnioskowanie o danych statystycznie prawdziwych jest szczególnie przydatne wówczas, gdy danych pewnych jest wiele i gdy można na nich przeprowadzać różnorodne symulacje co do przynależności osoby do grup wzorcowych¹⁴.

Na temat profilowania wypowiedziała się Grupa Robocza Art. 29 w opinii 2/2010 przyjętej w dniu 22 czerwca 2010 r. w sprawie internetowej reklamy

¹² P. Barta, M. Kawecki, komentarz do art. 4 pkt. 4, w: P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, C.H. Beck, Warszawa 2018, s. 205–207.

¹³ Zob. W.R. Wiewiórowski, *Profilowanie...*, s. 25–26.

¹⁴ W.R. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa*, Krajowa Rada Sądownictwa 2013/1, s. 21.

behavioralnej¹⁵, wskazując, że istnieją dwa podstawowe podejścia do tworzenia profili użytkowników – profile predykcyjne i profile jawne. Profile predykcyjne tworzy się w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie, w szczególności poprzez monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla, lub na które klika. Profile jawne natomiast tworzy się na podstawie danych osobowych przekazywanych w ramach usługi. Podejścia te można łączyć, a ponadto profile predykcyjne mogą stać się jawne później, gdy osoba, której dotyczą dane, utworzy dane logowania dla danej strony internetowej. W opinii tej wskazano jednocześnie, że sieci reklamowe tworzą profile predykcyjne, stosując do eksploracji danych połączenie technik śledzenia, technik opartych na plikach „cookie” oraz oprogramowania¹⁶. Systemy reklamy internetowej często dzielą osoby, których dane dotyczą, na segmenty, odpowiednio do obszarów zainteresowań lub kategorii marketingowych. Na tworzenie profilu istotny wpływ ma także lokalizacja osoby. Profil oparty na analizie plików „cookie” zapisanych w urządzeniu końcowym może zostać wzbogacony zagregowanymi danymi, dotyczącymi zachowania przejawiających podobne wzorce w innych kontekstach¹⁷.

Problemem profilowania zajęto się w rekomendacji Rady Europy w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili¹⁸, której przyjęcie stanowiło odpowiedź na obawy i zagrożenia związane z wykorzystaniem technologii pozwalających na profilowanie.

Profilowanie powinno spełniać standardy przejrzystości przetwarzania sformułowanej w art. 5 ust. 1 lit. a RODO i pozostałych zasad rozliczalności określonych. Dane osobowe muszą być zatem przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”). W tym kontekście warto przywołać założenia wynikające z motywu 24 RODO, który klaruje, że przetwarzanie danych osobowych znajdujących się w Unii osób, których dane dotyczą, przez administratora lub

¹⁵ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pl.pdf; stan na 3.08.2020 r.

¹⁶ Na temat plików „cookie” szerzej zob. **M. Brzozowska**, *Ochrona danych osobowych w sieci*, Wydawnictwo Presscom, Wrocław 2012, s. 37.

¹⁷ Zob. Opinia 2/2010 Grupy Roboczej Art. 29 w sprawie internetowej reklamy behavioralnej, pkt 2.3, s. 8, <https://archiwum.giodo.gov.pl/pl/1520057/3593>; stan na 11.08.2020 r.

¹⁸ Rekomendacja Rady Europy CM/Rec (2010) 13 w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, przyjęta przez Komitet Ministrów w dniu 23 listopada 2010 r. podczas 1099. posiedzenia Wiceministrów, http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec%282010%2913E_Profiling.pdf; stan na 3.08.2020 r.

podmiot przetwarzający, którzy nie mają jednostki organizacyjnej w Unii, powinno podlegać niniejszemu rozporządzeniu także w przypadkach, gdy wiąże się z monitorowaniem zachowania takich osób, których dane dotyczą, o ile zachowanie to ma miejsce w Unii. Aby stwierdzić, czy czynność przetwarzania można uznać za „monitorowanie zachowania” osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w Internecie, w tym także, czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.

W motywie 60 preambuły RODO wskazuje się m.in., że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach, w tym administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli gromadzi się dane osobowe od osoby, której dane dotyczą, należy ją też poinformować, czy ma ona obowiązek je podać oraz o konsekwencjach ich niepodania.

W powyższym kontekście istotne jest także prawo dostępu osoby fizycznej do danych i informacji o okolicznościach przetwarzania jej danych osobowych. W motywie 63 precyzuje się, że każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. W miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych.

5. Cele profilowania

Profilowanie wydaje się dość oczywistą tendencją po stronie podmiotów dysponujących danymi osobowymi, które posiadając lub mając dostęp do wielu danych osobowych, często pozornie oddzielonych od siebie i zróżnicowanych treściowo, pozyskują z nich wiedzę użyteczną z punktu widzenia prowadzonej działalności. Mamy w ten sposób do czynienia z odkrywaniem wiedzy o osobie fizycznej możliwym dzięki technologiom informatycznym poprzez znajdowanie prawidłowości wynikających w zgromadzonych danych, a także uzupełnianie poprzez znajdowanie powiązanych informacji w innych dostępnych źródłach w Internecie. Można więc wywodzić nowe informacje z agregowania danych oraz uzupełniać zasoby o dane uzyskane z ekstrakcji informacji pochodzących z zewnątrz¹⁹.

Choć zwykle profilowanie kojarzone jest z przedsiębiorcami i zasobami informacji pozostającymi w dyspozycji sektora prywatnego, to jednak obecnie źródłem informacji służących tworzeniu profilu osobowego mogą być także zasoby publiczne. Do podlegających dostępowi – często w Internecie – danych sektora publicznego należą bowiem także dane osobowe zawarte w rejestrach publicznych. Trzeba spodziewać się, że w związku z zasadą ponownego wykorzystania informacji publicznej z tych właśnie danych korzysta się i będzie się korzystać w przyszłości – najpewniej w jeszcze szerszym zakresie – do tworzenia profilu osobowego osoby fizycznej²⁰. W Polsce temat przetwarzania danych osobowych przez instytucje publiczne i ich ponownego wykorzystywania do profilowania osób fizycznych zyskał na znaczeniu w związku z implementacją dyrektywy 2003/98/WE w sprawie ponownego wykorzystania informacji sektora publicznego²¹, a następnie dyrektywy 2013/37/UE zmieniającej dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego²². Do polskiego porządku prawnego dyrektywę 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora

¹⁹ *Ibidem*, s. 25.

²⁰ Zob. **W.R. Wiewiórowski**, *Ochrona prywatności jako ograniczenie prawa do ponownego przetwarzania informacji publicznej*, Gdańskie Studia Prawnicze 2014/XXXI, s. 146–147.

²¹ Dyrektywa Parlamentu Europejskiego i Rady dnia 17 listopada 2003 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U.UE.L.2003.345.90 ze zm.).

²² Dyrektywa Parlamentu Europejskiego i Rady 2013/37/UE z dnia 26 czerwca 2013 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U.UE.L.2013.175.1).

publicznego²³ implementuje ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego²⁴, która do przetwarzania danych osobowych odnosi się głównie w art. 7 formułującym zasadę zgodności ponownego wykorzystywania z przepisami o ochronie danych osobowych²⁵.

Zważywszy na znaczącą ingerencję procesów profilowania w prywatność jednostki, zasadne są obawy stosowania zasad ponownego wykorzystania informacji publicznej w takim zakresie, w jakim obejmuje ona dane osobowe, bądź takie, które w powiązaniu z posiadanymi już danymi – przez ponowne ich wykorzystanie – stają się danymi osobowymi. Chodzi tu między innymi o ochronę podstawowych wolności i praw jednostki, jej godności, prawa do prywatności, autonomii informacyjnej, niedyskryminacji. W przypadku profilowania ochrona godności ludzkiej oraz innych praw podstawowych może być skuteczna tylko wówczas, gdy wszystkie zainteresowane strony współpracują podczas tworzenia profili osób w sposób rzetelny i zgodny z prawem. Każda osoba, której dane mogą podlegać ponownemu wykorzystywaniu wraz z ponownym wykorzystaniem informacji sektora publicznego, powinna mieć tego świadomość, a z punktu widzenia procedur ochrony danych osobowych prawo dostępu do treści danych, ich poprawiania, usuwania czy blokowania, gdy profilowanie byłoby niezgodne z prawem²⁶. Profilowanie ingeruje w autonomię informacyjną jednostki, która w jego obliczu nie ma możliwości decydowania o tym: kto, jakie informacje, kiedy i w jakim zakresie pozyskuje na jej temat. W tym przypadku prawo do samookreślenia informacyjnego okazuje się złudne. Internetowa reklama behawioralna ma bowiem na celu monitorowanie zachowań podczas korzystania z Internetu i analizę zebranych informacji dającej efekt w postaci profili użytkowników²⁷, w efekcie poprzez sięganie do informacji, nad którymi jednostka nie ma żadnej kontroli.

²³ Dyrektywa Parlamentu Europejskiego i Rady z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego Dz.U.UE.L.2019.172.5.

²⁴ Dz.U. poz. 1641.

²⁵ Szerzej zob. **B. Fischer, A. Piskorz-Ryń, M. Sakowska-Baryła, J. Wyporska-Frankiewicz**, *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Lex, Warszawa 2019, komentarz do art. 7, w: **B. Fischer, A. Piskorz-Ryń, M. Sakowska-Baryła, J. Wyporska-Frankiewicz** (red.), *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Lex, Warszawa 2019 s. 220–273.

²⁶ Zob. **W.R. Wiewiórowski**, *Ochrona...*, s. 149.

²⁷ Zob. **M. Kaczorowski**, *Przetwarzanie danych osobowych w działaniach marketingowych prowadzonych on-line*, Aktualne Problemy Prawnej Ochrony Danych Osobowych 2014, w: **G. Sibiga** (red.), dodatek do Monitora Prawniczego 2014/9, s. 34.

6. Zakończenie

Dostęp do sieci Internet i zaawansowanie technik informacyjno-komunikacyjnych (ICT) spowodowały, że pozyskiwanie i przetwarzanie różnego rodzaju danych odbywa się na niespotykaną dotychczas skalę. Zgromadzone dane są poddawane różnym metodom przetwarzania, które są następnie wykorzystywane zarówno przez przedsiębiorców do lepszego dopasowania strategii marketingowych dla swoich klientów, jak i przez organy publiczne na potrzeby związane z realizacją zadań publicznych, np. ustalenia miejsca epidemii choroby zakaźnej, zapobiegania terroryzmowi czy przestępczości. Powszechna dostępność ogromnej ilości danych w Internecie, niemal nieograniczone możliwości łączenia tych danych, wzrastająca wydajność urządzeń technicznych, które przetwarzają te dane, powoduje, że żyjemy w świecie Big data, gdzie tworzenie profili i podejmowanie automatyzowanych decyzji staje się codziennością. Z drugiej strony, coraz częściej stawia się pytania o zagrożenia związane z profilowaniem, tj. dyskryminację, deindywidualizację, asymetrię informacji, brak transparentności czy naruszenie prywatności²⁸.

Gromadzenie danych oraz przetwarzanie ich na szeroką skalę przez przedsiębiorców prowadzi do różnorodnych zmian w zakresie stosunków społeczno-gospodarczych, które wpłyną bezpośrednio na każdą jednostkę. Zgoda ustawodawcy na pewne zachowania przedsiębiorców oraz innych podmiotów czerpiących z przetwarzania danych osobowych korzyści finansowe wiąże się w pewnym stopniu z erozją praw człowieka, praw jednostek²⁹. Nie ulega wątpliwości, że prawo nie rozwiąże wszystkich problemów, jakie stawia przed nami dynamiczny rozwój technologii czy sytuacja geopolityczna. Prywatność będzie padała ofiarą komercyjnych interesów i kolejnych wojen z mniej lub bardziej realnymi wrogami. Podobnie jak w przypadku ludzkiego życia, godności i wolności – nie jest to jednak powód, aby przestać ją chronić³⁰.

²⁸ Zob. **M. Ciechomska**, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, Europejski Przegląd Sądowy, maj 2017, s. 37.

²⁹ Zob. **P. Leja**, *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, Prawo Mediów Elektronicznych 2017/3, s. 16.

³⁰ Zob. **K. Szymielewicz**, **A. Walkowiak**, *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem*, Aktualne Problemy Prawnej Ochrony Danych Osobowych 2014, w: **G. Sibiga** (red.), dodatek do Monitora Prawniczego 2014/9, s. 29.

Stanowisko TSUE zawarte w wyroku wydanym w sprawie Planet 49 powinno, w okresie oczekiwania na przyjęcie Rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego Dyrektywę 2002/58/WE – ePrivacy³¹, dać podstawę do określenia minimalnych standardów informacyjnych i warunków pozyskiwania zgody na przetwarzanie danych osobowych pozyskanych uprzednio dzięki cookie, zwłaszcza że według EROD Dyrektywa 2002/58³² stanowi o pierwszeństwie art. 5 ust. 3 przed art. 6 w odniesieniu do czynności przechowywania lub uzyskiwania dostępu do informacji przechowywanych na urządzeniu użytkownika³³, a nie o dalszym przetwarzaniu danych osobowych pozyskanych uprzednio dzięki cookie. Wyjaśnienia w tym zakresie przedstawił już francuski organ nadzorczy CNIL, wskazując, że zgoda musi przejawiać się w pozytywnym działaniu osoby uprzednio poinformowanej o konsekwencjach swojego wyboru i posiadającej środki do jej wykonania. W związku z tym należy wprowadzić odpowiednie systemy do praktycznego gromadzenia zgody, aby umożliwić użytkownikom Internetu korzystanie z przyjaznych dla użytkownika i ergonomicznych rozwiązań. Akceptacja ogólnych warunków użytkowania nie może być prawidłową metodą uzyskania zgody. Zgoda musi nastąpić przed wstawieniem lub odczytaniem plików cookie. Tak długo, jak dana osoba nie wyrazi zgody owe pliki cookie nie mogą być przechowywane ani czytane na ich urządzeniu końcowym. Wymagane jest każdorazowo dodanie nowego celu do pierwotnie planowanych celów³⁴.

Wyrok w sprawie Planet 49 pozwala ponownie wrócić do zagadnień, jak użytkownicy Internetu mają zostać poinformowani i jak mają wyrazić zgodę przed rozpoczęciem ich śledzenia oraz na ile muszą mieć zapewnioną opcję, aby nie być śledzonymi podczas odwiedzania witryny lub korzystania z aplikacji mobilnych, zwłaszcza że wyroki sądów krajowych potwierdzają konieczność zgody na przechowywanie plików cookies³⁵.

³¹ Document 52017PC0010, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010>; stan na 3.08.2020 r.

³² Dz. Urz. UE L. 201.P.0037-0047 ze zm. Document 32002L. 0058, <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32002L0058>; stan na 3.08.2020 r.

³³ **M. Franke**, *Pytania...*, s. 17.

³⁴ <https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi>; stan na 3.08.2020 r.

³⁵ Wyrok Bundesgerichtshof z dnia 28.05.2020 r. w sprawie I ZR 7/16, <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html?nn=10690868>; stan na 29.05.2020 r.

Bibliografia

Akty prawne

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólnego rozporządzenia o ochronie danych), Dz.U.UE.L.2016.119.1.
- Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.U.UE L.201.P.0037-0047).
- Dyrektywa Parlamentu Europejskiego i Rady 2013/37/UE z dnia 26 czerwca 2013 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U.UE.L.2013.175.1).
- Dyrektywa Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U.UE.L.2003.345.90 ze zm.).
- Dyrektywa Parlamentu Europejskiego i Rady z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego.
- Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U., poz. 1641).

Opracowania

- Barta P., Kawecki M.**, komentarz do art. 4 pkt 4, w: P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, C.H. Beck, Warszawa 2018, s. 205–207.
- Brzozowska M.**, *Ochrona danych osobowych w sieci*, Wydawnictwo Presscom, Wrocław 2012, s. 37.
- Ciechomska M.**, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, Europejski Przegląd Sądowy, maj 2017 r., s. 37–42.
- Fischer B., Piskorz-Ryń A., Sakowska-Baryła M., Wyporska-Frankiewicz J.**, *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Lex, Warszawa 2019, komentarz do art. 7, s. 220–273.
- Franke M.**, *Pytania wokół wyroku w sprawie cookies*, ABI Expert 2020/1, s. 16–19.
- Kaczorowski M.**, *Przetwarzanie danych osobowych w działaniach marketingowych prowadzonych on-line*, Aktualne Problemy Prawnej Ochrony Danych Osobowych 2014, w: G. Sibiga (red.), dodatek do Monitora Prawniczego 2014/9, s. 34–37.
- Leja P.**, *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, Prawo Mediów Elektronicznych 2017/3, s. 10–16.
- Mednis A.**, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wydawnictwo Presscom, Wrocław 2019, s. 61.
- Nerka A.**, komentarz do art. 4 pkt 11, w: M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Legalis, Warszawa 2018, s. 115–121.
- Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa*, Krajowa Rada Sądownictwa 2013/1, s. 21.

Opinia 15/2011 Grupy Roboczej Art.29 w sprawie definicji zgody (WP 187).

Opinia 2/2010 Grupy Roboczej Art. 29 w sprawie internetowej reklamy behawioralnej, pkt 2.3, (WP...).

Rekomendacja Rady Europy CM/Rec (2010) 13 w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili.

Szymielewicz K., Walkowiak A., *Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem*, dodatek do Monitora Prawniczego 2014/9, s. 29–33.

Wiewiórowski W.R., *Ochrona prywatności jako ograniczenie prawa do ponownego przetwarzania informacji publicznej*, Gdańskie Studia Prawnicze 2014/XXXI, s. 146–147.

Wiewiórowski W.R., *Personal Profiling Based on Generally Accessible Data*, International Journal on Information Technology and Security 2012/3, s. 31–46.

Wiewiórowski W.R., *Profilowanie osób na podstawie ogólnodostępnych danych*, w: A. Mednis (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Wydawnictwo Stow. Absolwentów WPiA UW, Warszawa 2013, s. 25–27.

Strony internetowe

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pl.pdf; stan na 3.08.2020 r.

http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec%282010%2913E_Profiling.pdf; stan na 3.08.2020 r.

<http://www.polityka.pl/tygodnikpolityka/ludzieistyle/1603593,1,za-prywatnosc-w-internecie-trzeba-placic.read>; stan na 3.08.2020 r.

<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010>; stan na 3.08.2020 r.

<https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html?nn=10690868>; stan na 29.05.2020 r.

<https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi>; stan na 29.05.2020 r.

Magdalena CZAPLIŃSKA, Marlena SAKOWSKA-BARYŁA

CONSENT TO THE PROCESSING OF PERSONAL DATA AND PROFILING. OBSERVATIONS ON THE JUDGMENT OF THE EU COURT OF JUSTICE OF 1 OCTOBER 2019 IN CASE C-673/17

Abstract

Background: The subject matter of this research is the CJEU judgment on 1 October 2019 in case C-673/17 (Planet 49). The article analyses the issue of personal data protection in respect to information obligations and conditions of consent. These are required under the GDPR in cases where personal data are processed by computerised data collection tools that affect electronic communications networks' users' private of information including personal data stored on end devices used for remote identification and tracking of end users.

Research purpose: The purpose of research in the article is to assess legal solutions relating to the obligation to use cookies as one of the technologies that store or access information on the devices of end users. In the current legal environment, there is no legal definition of cookies, not only because it is not the only technology allowing for collecting information from end devices but also due to various sources of origin as well as various functions of cookies (e.g. analytical,

marketing, safety cookies). Cookies that may be installed on the end user's device may contain a number assigned to the user's registration data, which means that if such number is matched to the user's personal data, data stored by cookies are personalised and, therefore, collection of data with the use of cookies may constitute processing of personal data. One of the forms of automated personal data processing is profiling, which consists in the use of personal data for assessment of certain personal features of a natural person. Processing of personal data is conditional upon the existence of prerequisites to lawfulness of personal data processing indicated in Article 6 and Article 9 of the GDPR, which include consent of the data subject. The purpose of consent as one of independent grounds for personal data processing is to ensure that the data subject is granted information autonomy in cases where the possibility of data processing depends on his or her decision. In order for a given act or statement to qualify as consent, it is necessary that there cumulatively exist all the structural elements of consent, listed in Article 7 of the GDPR, which must be met also if statements are made online.

Methods: The applicable provisions have been analysed using the legal comparative method, taking into account that in its judgment of 1 October 2019 in case C-673/17 (Planet 49) the Court in Luxembourg addressed the issue of consent to placing marketing cookies and the scope of information that must be provided when such consent is sought.

Conclusions: Placement of marketing cookies requires consent, meeting conditions for obtaining consent, and applying GDPR-compliant information standards.

Keywords: consent to the processing of personal data, cookies.