TOM LXXII • NR 3 (849) • DOI 10.33226/0137-5490.2019.3.16

Ochrona danych w marketingu internetowym — mechanizmy przetwarzania danych w Internecie

Data protection in internet marketing — mechanisms of data processing on the Internet

mgr Agata M. Kaczyńska-Kral

E-mail: a.kaczynska@wpia.uw.edu.pl

Streszczenie

W niniejszym opracowaniu opisano współczesne sposoby wykorzystywania danych osobowych przez systemy informatyczne i technologie za pośrednictwem Internetu na przykładzie rozwiązania *lookalike* oraz ich wpływ na ujawnianie informacji dotyczących sfery prywatności osób, których dane dotyczą. Celem tej pracy jest przedstawienie ochrony danych osobowych przetwarzanych na masową skalę za pośrednictwem Internetu na podstawie 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, zwanego dalej: „RODO".

Słowa kluczowe: ochrona danych osobowych, Internet, marketing, RODO, *lookalike*.

Summary

This report describes modern ways of using personal data by IT systems and technologies via the Internet on the example of a lookalike solution and their impact on disclosing information about the private sphere of data subjects. The aim of this work is to present the protection of personal data processed on a mass scale via the Internet on the basis of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereinafter: 'RODO'.

Key words: personal data protection, Internet, marketing, GDPR, lookalike.

1. Wprowadzenie

Celem niniejszego opracowania jest przedstawienie prawnych aspektów zautomatyzowanego przetwarzania danych za pośrednictwem Internetu z uwzględnieniem przykładów najbardziej popularnych technik masowego zbierania i przetwarzania danych w globalnej sieci.

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, zwane dalej: „RODO" jest unijną regulacją, której celem jest zapewnienie swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi oraz wprowadzenie jednolitych, dla całej UE, zasad przetwarzania danych osobowych. W motywie szóstym RODO wskazano, że celem regulacji jest również uwzględnienie postępu technologicznego, który przyczynia się do nowych sposobów zbierania i przetwarzania danych, uwzględniając przy tym dużą skalę przetwarzania. Dlatego też, mając na względzie rosnące znaczenie zautomatyzowanego przetwarzania danych osobowych, wśród form przetwarzania wyróżniono „profilowanie". Jest ono częścią zautomatyzowanego przetwarzania, które może, ale nie musi wywoływać względem, osoby, której dane dotyczą, skutków prawnych lub takich, które w podobny sposób istotnie na nią wpływają (art. 22 ust 1 RODO). RODO wprowadziło definicję legalną „profilowania" i zgodnie z art. 4 pkt 4 RODO jest to *dowolna forma zautomatyzowanego przetwarzania danych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osobowy fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań*,

wiarygodności, zachowania, lokalizacji lub przemieszczania się. Należy tutaj zaznaczyć subtelną różnicę pomiędzy definicją legalną zawartą w art. 4 pkt 4 RODO a definicją uwzględnioną w motywie 71 RODO, w którym uznano, że „profilowanie" polega *na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej* (…). Zgodnie z definicją legalną profilowanie polega na *wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej* (…), co wyraźnie wskazuje na konkretną czynność techniczną oznaczającą porównywanie danych, grupowanie cech, analizy, prognozy lub oceny. Motyw 71 RODO uznaje profilowanie jako dowolne przetwarzanie danych, które w przyszłości pozwalają ocenić czynniki osobowe osoby fizycznej. Jest to szerokie ujęcie tego pojęcia uzależniające jego istnienie bardziej od możliwości jakie daje zebranie określonych danych aniżeli faktycznej czynności „wykorzystania do oceny". Należy uznać, że definicja legalna zawarta w art. 4 pkt 4 RODO trafniej opisuje techniczne ujęcie „profilowania", dlatego w niniejszym artykule to ta definicja będzie punktem odniesienia do dalszych rozważań.

W art. 2 ust. 1 RODO odróżnia się „całkowicie" i „częściowo" zautomatyzowane przetwarzanie danych, choć takie rozróżnienie nie jest uzasadnione ze względu na brak w dalszej części RODO odniesień do częściowego zautomatyzowania danych. W takim przypadku bez względu na to jaka część procesu jest zautomatyzowana to powinniśmy odnosić się do tego jak do całkowitego zautomatyzowania przetwarzania w ograniczeniu do określonego fragmentu procesu (Litwiński, 2017, komentarz do art. 2). Przetwarzanie danych osobowych można podzielić zgodnie z zaprezentowanym schematem na rysunku 1 ze względu na formę oraz skutek.

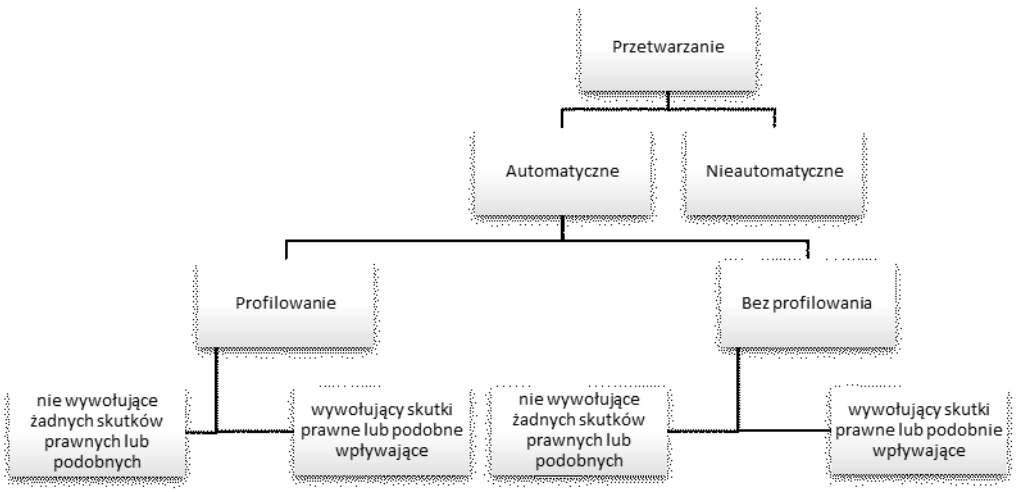
Przetwarzanie niezautomatyzowane w dużej mierze odnosi się do procesów wykonywanych ręcznie (biblioteki, archiwa papierowe), ale może odbywać się także za pomocą komputera i przy użyciu Internetu. W takich przypadkach sieć ogólnoświatowa używana jest jako sposób magazynowania danych, np. w postaci plików programu Excel zawierających dane osobowe przechowywanych w chmurze obliczeniowej (np. OneDrive lub GoogleDoc). Takie przetwarzanie, co do zasady, nie jest powiązane z przetwarzaniem danych użytkowników Internetu i masową aktywnością tych użytkowników w sieci.

Zautomatyzowane przetwarzanie danych osobowych, w szczególności profilowanie wywiera istotny wpływ na prawa i wolności obywatelskie. Użytkownik Internetu, który na portalu internetowym wyraził zgodę na śledzenie jego ruchu w sieci może nie być świadomy, że przy obecnej technologii jest możliwość powiązania jego danych z innymi portalami i urządzeniami, na których jest zarejestrowany i uzyskać przy tym informacje, których użytkownik nie chciałby udostępniać szerszemu gronu odbiorców.

2. Profilowanie a śledzenie

W świetle RODO, każdy użytkownik Internetu przeglądający strony WWW powinien mieć możliwość podjęcia świadomej zgody na zbieranie danych osobowych, w tym służących do śledzenia i profilowania. Powinien także, zostać poinformowany o celu przetwarzania oraz jakiego rodzaju dane w wyniku takiego profilowania będą zbierane — motyw 60 (RODO, 2016). Użytkownik powinien uzyskać za pośrednictwem odpowiedniej klauzuli (art. 13 i 14 RODO), informacje, kto i w jaki sposób będzie administrował pozyskanymi w wyniku śledzenia danymi. W RODO nie ma zdefiniowanego terminu „śledzenia", bowiem jest to jeden ze sposobów zbierania danych uzależniony od aktywności użytkownika na stronie WWW. Jednak jego zdefiniowanie

Rysunek 1
Formy przetwarzania danych osobowych



Źródło: opracowanie własne.

jest istotne, aby określić odpowiedni moment, w którym rozpoczyna i kończy się profilowanie. Śledzenie nie wyczerpuje treści „profilowania". Śledzenie rozpoczyna się od momentu, kiedy użytkownik Internetu wyrazi zgodę na zbieranie danych w poprzez pliki cookie i kończy się wraz z usunięciem tych plików. Technicznie ujmując, użytkownik jest śledzony za pośrednictwem pliku cookie osadzonym na komputerze, a podmiot trzeci może rejestrować szereg informacji związanych z przeglądaniem przez użytkownika stron internetowych. Ten moment nazywa się prawidłowo „śledzeniem". Samo zbieranie informacji na podstawie śledzenia nie wyczerpuje jeszcze treści profilowania, które rozpoczyna się w momencie, kiedy dane zebrane podczas śledzenia zostaną wykorzystane do analizy i oceny czynników osobowych. Pliki cookie zapisujące dane sesyjne również zbierają informacje odnoszące się do działań użytkownika na stronie internetowej, np. weryfikują, czy użytkownik korzysta ze strony, czy też jest nieaktywny, celem automatycznego wylogowania na skutek braku aktywności. Mogą jednak zawierać szereg informacji, które potencjalnie mogłyby zostać wykorzystane do oceny niektórych czynników osobowych. Pliki sesyjne nie służą jednak do oceny czynników osobowych osób fizycznych i dlatego tworzenie plików sesyjnych nigdy nie mieściłoby się w pojęciu profilowania. Pliki cookie pozwalają nie tylko na zbieranie danych z urządzenia użytkownika, ale również pozwalają na przesyłanie do przeglądarki odpowiednich instrukcji dotyczących wyświetlania zindywidualizowanych treści. W związku z powyższym w ramach procesu zautomatyzowanego przetwarzania wykonuje podprocesy, które nie przetwarzają danych do oceny niektórych czynników osobowych osobowy fizycznej np.: śledzenie, łączenie danych itp. (Mayer, 2009).

3. Profilowanie behawioralne

Niezależny europejski organ doradczy w zakresie ochrony danych osobowych i prywatności, zwany Grupą Roboczą art. 29 wyróżnił, w opinii (WP171, 2010, s. 7–9) w sprawie reklamy behawioralnej, dwa podejścia do tworzenia profili użytkowników. Pierwszy, tworzony na podstawie wnioskowania z obserwacji indywidualnego i zbiorowego zachowania użytkownik w czasie, zwany profilem predykcyjnym, oraz drugi tworzony na podstawie przekazywanych w ramach usługi sieciowej przez te same osoby, których dane dotyczą (profil jawny) np. podczas wypełniania formularza (WP171, 2010, s. 7–9). Należy mieć na uwadze, że powinno się uwzględnić również trzeci rodzaj profilowania tj. profilowanie mieszane. Najczęściej bowiem dane pozyskane np. poprzez wpisanie się do klubu lojalnościowego przedsiębiorcy, wzbogaca się łącząc z danymi pozyskanymi, np. z Facebook lub Google celem uzyskania lepszych rezultatów wnioskowania.

Profilowanie behawioralne ma swoje korzenie w psychologii i analizie kryminalistycznej sprawców przestępstw. Na podstawie badań zachowań użytkowników można wyszczególnić wzorce jakimi cechują się określone grup społeczne. W taki sposób powstają reguły typu: grupa ma cechę X to jest duże prawdopodobieństwo, że jej zachowanie będzie Y. Reklama behawioralna została przez Grupę Roboczą art. 29 zdefiniowana jako złożenie dwóch form zautomatyzowanego przetwarzania: śledzenia i profilowania behawioralnego. Polega ona bowiem na *monitorowaniu użytkowników podczas korzystania z Internetu i tworzeniu z biegiem czasu profili, wykorzystywanych następnie w celu wyświetlania użytkownikom reklam odpowiadających ich zainteresowaniom.* Zatem zbierane pliki cookie są wykorzystywane przez firmy z branży reklamowej bezpośrednio do śledzenia i profilowania behawioralnego celem utworzenia grup odbiorców, którym zostanie wyświetlona odpowiednia reklama lub zaprezentowana odpowiednia treść. Grupa odbiorców wybierana jest ze względu na współdzielone cechy np. wiek, obszar zamieszkania, czy przynależność do organizacji. Takie tworzenie grup, najczęściej rozdzielnych, nazywa się segmentacją.

Z technicznego punktu widzenia pliki cookie szybko tracą swoją przydatność do analiz. Uznaje się, że „zdrowy cookie", to taki, który ma co najwyżej miesiąc. Pliki tego typu, istniejące powyżej 180 dni tracą realną wartość analityczną. Dlatego tak istotnym jest, aby zbieranie plików cookie było procesem ciągłym. Firmy reklamowe, ze względu na to, muszą korzystać ze wsparcia wielu dostawców usług. W związku z powyższym zawierają umowy z wydawcami takimi jak: ogólnokrajowe oraz ogólnoświatowe czasopisma, które mają swoje strony i portale informacyjne, stacje telewizyjne itp. Te wszystkie podmioty współpracują ze sobą celem zbierania i utrzymania, bazy plików cookies, której wielkość może sięgać nawet kilkaset milionów plików cookie.

W związku z powyższym, aby robić reklamę behawioralną potrzebny jest udział wielu podmiotów w Internecie. Co ważniejsze, współpraca sieciowa jest niezbędna, aby można było utrzymywać ciągłe zasilanie baz danych nowymi plikami cookie (zdrowymi). W ramach reklamy behawioralnej stronami są operatorzy sieci reklamowych, dystrybutorzy reklam, reklamodawcy oraz wydawcy, którzy jako właściciele stron, czerpią dochody ze sprzedaży miejsc reklamowych (WP171, 2010, s. 5).

Należy mieć na względzie, że z punktu widzenia użytkownika Internetu zdarza się często, że wyrażona zgoda na stronie internetowej X, pozwoli firmie Y na połączenie tych danych z danymi pozyskanymi, np. przez Google oraz Facebooka i może stanowić bazę danych przekraczających znacznie informacje, na których ujawnienie zgodziłby się przeciętny użytkownik Internetu. Na podstawie tak zebranych danych można uzyskać szereg informacji na temat tego jaki kolor użytkownik lubi, jakie jest jego hobby, jaki jest poziom zamożności, orientacja seksualna, czy użytkownik jest w ciąży. Technicznie jest możliwe wybranie grupy potencjalnych osób homoseksualnych, którym chcielibyśmy wyświetlić reklamę dedykowaną tylko dla tej grupy. I technicznie nie potrzeba zbierania wprost informacji od członków tej grupy o ich orientacji seksualnej. Pod względem biznesowym profilowanie behawioralne wykorzystywane jest wyłącznie do

tworzenia reklam, które danemu użytkownikowi mogłyby przypaść do gustu. Taka reklama może być dobrana nie tylko ze względu na produkt, ale również ze względu na kolor jaki lubimy, klimat, muzykę etc. Sprofilowana reklama pozwala nawet na dobranie tła pod produktem. I takich informacji dostarcza profilowanie behawioralne.

Istotną kwestią jest jednak nie tylko to, że potrafimy zbadać użytkowników, którzy już są przekonani do jakiegoś produktu albo usługi. Dużo ciekawszą kwestią jest znaleźć podobnych do tych osób i zaoferować im produkt odpowiednio przedstawiony.

4. Mechanizm *lookalike*

O ile profilowanie behawioralne odpowiada na pytanie: Co i jak przedstawić użytkownikowi? To omawiany tutaj mechanizm wskazuje: Kto mógłby ten produkt kupić? Połączenie odpowiedzi na te dwa pytania dają pożądane rezultaty marketingowe.

Mechanizm *lookalike* ma na celu wyszukanie wśród użytkowników Internetu takich osób, które są podobne w swoim zachowaniu do próbnej grupy. Próbna grupa to np. lojalni klienci firmy samochodowej, którzy podali producentowi swoje adresy e-mail, celem otrzymywania systematycznego newslettera. Producent może teraz przekazać bazę adresów do firmy reklamowej celem stworzenia profilu behawioralnego grupy jego klientów. I na podstawie takiego profilu odbywa się wyselekcjonowanie z dużej bazy plików cookie, wszystkich tych, które reprezentują użytkowników o zrachowaniach zbieżnych z profilem. Zatem spośród użytkowników Internetu wyszukuje się ludzi o zbieżnych profilach z próbnymi grupami. To właśnie kryje się pod pojęciem „*lookalike*", czyli „wyszukiwanie podobnych". W taki sposób powstaje wzorzec, na podstawie, którego, z dużej bazy, spośród użytkowników, którzy nie znają danego przedsiębiorcy, zostaną wybrani wszyscy, których zachowania zbieżne są z zachowaniami próbnej grupy. Mechanizm *lookalike*, pozwala na wyszukiwanie podobnych sobie użytkowników do tych, których zachowanie jest nam znane. Na tej samej zasadzie można wydzielić grupę zwolenników jednej, albo drugiej partii spośród wszystkich użytkowników Internetu. Taki mechanizm wykorzystywany jest do wyświetlania reklam odpowiednim grupom odbiorców, bowiem łatwiej jest przekonać osobę przeglądającą strony internetowe z samochodami o nowej premierze oleju napędowego aniżeli osobę, która codziennie wchodzi na stronę: jakdojade.pl.

5. Uzasadniony interes administratora a profilowanie

Największym problemem dla podmiotów przetwarzających pliki cookie jest uzyskanie zgody od użytkowników Internetu na ich śledzenie i profilowanie. Obecnie wykorzystuje się wiele sposobów na obejście konieczności pozyskiwania zgód w sposób zgodny z RODO. Jedną z możliwości jest powołanie się na uzasadniony interes administratora. W świetle art. 6 pkt 1 lit. f RODO administrator, który przetwarza dane niezbędne do celów wynikających z prawnie uzasadnionych interesów przez administratora, albo stronę trzecią nie musi uzyskiwać zgody osoby, której dane dotyczą. Wyjątkiem od tej zasady jest sytuacja, w której interesy lub podstawowe prawa i wolności osoby, której dane dotyczą mają nadrzędny charakter wobec interesów administratora. Wyjątek ten nazywany jest testem równowagi. W polskim piśmiennictwie brak jest szerszej informacji na temat tego, na czym polega test równowagi i jak powinno się go przeprowadzić. Temat ten, zasługuje na odrębne omówienie, ale można poglądowo przeanalizować przygotowany test przez ICO, tj. brytyjski odpowiednich Prezesa Urzędu Ochrony Danych Osobowych (ICO, 2018). Należy uznać ten test oraz kwestionariusz LIA (ocena uzasadnionych interesów; ICO-LIA, 2018) za pożądany krok, w stosunku do podmiotów, które chcą w swojej działalności wykorzystać uzasadniony interes. Uzasadniony interes administratora jest pojęciem ogólnym, o dużym poziomie abstrakcji. Wykonanie porównania dwóch pojęć ogólnych i abstrakcyjnych, tj. interesu administratora oraz interesu osoby, której dane dotyczą może przysporzyć problemu a to nie wpływa w sposób prawidłowy na bezpieczeństwo, prawa i wolności osób, których dane dotyczą.

W świetle art. 40 RODO m.in. grupy zawodowe, związki pracodawców mogą tworzyć Kodeksy Postępowania, które po zatwierdzeniu przez Prezesa Urzędu Ochrony Danych Osobowych stają się obowiązującymi kodeksami dla poszczególnych branż i mogą stanowić na mocy art. 40 pkt 9 RODO akt powszechnie obowiązujący. IAB Polska (IAB — *Interactive Advertising Bureau*, czyli Związek Pracodawców Branży Internetowej) na swojej stronie internetowej przedstawiła projekt Kodeksu postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej, zwanego dalej: „Kodeksem IAB" (IAB, 2018). W punkcie 3.7 Kodeksu IAB wskazuje się, że *prawnie uzasadniony interes administratora danych lub strony trzeciej będący podstawą przetwarzania danych osobowych należy rozumieć w sposób szeroki, gdyż w praktyce obejmuje on interesy gospodarcze, faktyczne oraz prawne* (IAB, 2018). Ponadto Kodeks IAB proponuje wprowadzenie w punkcie 3.7.1 test równowagi oparty na czterech pytaniach. Jest to pożądany kierunek i zbieżny z tym, co uczynił brytyjski ICO.

Zgodnie z opinią Grupy Roboczej art. 29 (WP171, 2010) za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych od celów marketingu bezpośredniego. Kodeks IAB uznaje, że „dopasowanie treści serwisu internetowego do użytkownika" (IAB, 2018) jest również dopuszczalne. Nie ma w RODO legalnej definicji marketingu bezpośredniego. GIODO (obecny PUODO) w decyzji z dnia 11 maja 2012 roku stwierdził, że istotą marketingu bezpośredniego są takie działania, które kształtują popyt poprzez poszerzanie kręgu własnych nabywców, jak również poprawienie relacji pomiędzy firmą a klientem (GIODO, 2012). Zatem wszystkie

działania bezpośrednio wiążące administratora z klientami, np. programy lojalnościowe, newslettery z nowymi ofertami, kartki okazjonalne mieszczą się w granicach uzasadnionego interesu administratora i nie wymagają zgody osób, których dane dotyczą.

Należy mieć na względzie, że najważniejszą cechą wszystkich działań marketingowych, jest jak największa skala oddziaływania. Takie działania są możliwe tylko za pomocą ogólnopolskich mediów oraz plików cookie. Jednak dyskusyjne jest, czy administrator ma prawo wykorzystać uzasadniony interes do profilowania i wykorzystania, np. mechanizmu *lookalike* do realizacji własnych potrzeb marketingowych. Co do zasady, domy mediowe, czy agencje reklamowe są podmiotami przetwarzającymi dane osobowe, a klienci występują w roli administratora, który powierza i przetwarza na własne cele dane osobowe, przy wsparciu podmiotów przetwarzających. Przy takiej konstrukcji umownej nie sposób zarzucić, że administrator nie realizuje na swoją rzecz reklamy, a zatem mieści się to w granicach marketingu bezpośredniego. Jednakże problem stanowi test równowagi. Interes administratora przy profilowaniu przekracza granicę podstawowych praw i wolności osób, których dane dotyczą. Brak jest rzeczywistej możliwości przekazania osobom, których dane dotyczą, informacji o tym jakiego rodzaju dane będą zbierane podczas śledzenia i profilowania behawioralnego. Dane zbierane są automatycznie. Ponadto w bazie mogą znajdować się — i zapewne znajdują się — pliki cookie tego samego użytkownika powiązane z innymi udzielonymi wcześniej zgodami. Nikt nie jest w stanie zagwarantować, że po analizie systemowej wszystkich tych plików, osoba, której dane dotyczą zostanie rozpoznana przez system w grupie osób o odmiennej orientacji czy przynależności politycznej. Przed zbieraniem plików cookie i przed dokonaniem profilowania nikt nie jest wstanie stwierdzić, jakiego rodzaju dane osobowe będą zebrane. Śledzenie użytkownika istotnie wkracza w sferę prywatności i konsekwencje tego śledzenia są trudne do identyfikacji.

Ponadto należy podkreślić, że jest brak możliwości stosowania uzasadnionego interesu w stosunku do dzieci. Podzielić należy pogląd doktryny (Litwiński, 2017), że w tym przypadku uzasadniony interes może odnosić się wyłącznie do osób pełnoletnich.

6. Podsumowanie

Zautomatyzowane przetwarzanie danych osobowych jest mocno rozwijającą się formą przetwarzania i zapewne niedługo będziemy obserwowali coraz bardziej wyrafinowane możliwości wpływania na nasze wybory za pośrednictwem złożonych mechanizmów inteligencji obliczeniowej (zwanej również sztuczną inteligencją).

Należy jednak mieć świadomość tego, jakie możliwości daje profilowanie behawioralne i nie lekceważyć udzielanych zgód w Internecie, choć wbrew pozorom nietrudno jest być zapomnianym przez mechanizmy plików cookie. Jak wspomniano powyżej żywotność tych plików nie jest długa. Wystarczy nie korzystać z systemów, telefonów, tabletów przez okres jednego roku i możemy mieć pewność, że użytkownik nie jest dłużej śledzony.

De lege ferenda należy mieć na względzie, że profilowanie behawioralne oraz mechanizmy takie jak *lookalike* wkraczają nie tylko w sferę danych osobowych, którymi użytkownicy chętnie się dzielą, ale wkraczają w sferę prywatności, co do której świadomi użytkownicy nigdy nie dopuściliby osób trzecich. I przyszłe zmiany regulacyjne powinny uwzględnić ten fakt.

Bibliografia

Carey, P. (2018). *Data Protection, A practical Guide to UK and EU Law*. Oxford: Oxford University Press.

Ciechomska, M. (2017). Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych. *Europejski Przegląd Sądowy,* maj 1.

GIODO, D. (2012, 5 11). *Decyzja GIODO*. Warszawa.

IAB, P. (2018, 12 2). *Kodeks IAB*. Warszawa.

ICO. (2018, 12 2). https://ico.org.uk/.Retrieved from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

ICO-LIA. (2018, 12 02). https://ico.org.uk/.Retrieved from https://ico.org.uk/media/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx

Mayer, J. R. (2009, 05 1). jonathanmayer.org. Retrieved from https://jonathanmayer.org/publications/trackingsurvey12.pdf

Litwiński, P. (2017). *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa: C.H. Beck.

Lloyd, I. J. (2017). *Information Technology Law*. Oxford: Oxford University Press.

RODO. (2016). 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.

Stanisław Dmochowski, S. R. (2008). *Komentarz do Kodeksu Cywilnego, Księga Pierwsza, Część ogólna*. Warszawa: LexisNexis.

WP171, G. (2010). *Opinia Grupy Roboczej art. 29 nr 2/2010 z 22.06.2010 r. w sprawie reklamy behawioralnej* — WP 171.