Anna Nowak*, Magdalena Węgłowska**, Miłosz Gapsa***

Profilowanie na podstawie danych osobowych konsumentów przetwarzanych przez pojazd autonomiczny[1]

Spis treści

Streszczenie

Profilowanie w coraz większym stopniu wkracza w życie konsumentów, a równolegle z nim postępuje zjawisko gromadzenia i wykorzystywania danych konsumentów pochodzących z różnych źródeł, w tym przetwarzanych przez autonomiczne pojazdy. Niniejszy artykuł ma na celu scharakteryzowanie kluczowych zagrożeń dla konsumentów, które mogą wynikać z procesu profilowania w oparciu o dane osobowe pozyskane z pojazdów autonomicznych, ze szczególnym uwzględnieniem praktyki personalizacji. W tym kontekście szerzej omówione zostaną dwa akty prawne – ogólne rozporządzenie o ochronie danych, na którego podstawie scharakteryzowany zostanie proces pozyskiwania danych osobowych z pojazdów autonomicznych oraz dyrektywa 2005/29/WE o nieuczciwych

* Studentka V roku prawa na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego; kontakt e-mail: anna.nowak2@edu.uni.lodz.pl; ORCID: https://orcid.org/0000-0001-6274-3895.

** Studentka V roku prawa na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego; kontakt e-mail: magdalena.weglowska@edu.uni.lodz.pl; ORCID: https://orcid.org/0000-0003-0180-6930.

*** Student V roku prawa na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego; kontakt e-mail: milosz.gapsa@edu.uni.lodz.pl; ORCID: https://orcid.org/0000-0002-0986-5591.

[1] Artykuł powstał w związku z uczestnictwem autorów w „Klinice Prawa Technologii Przyszłości", organizowanej w ramach współfinansowanego przez Erasmus+ projektu TechLawClinics (nr projektu 2019-1-FR01-KA203-062630) na Wydziale Prawa i Administracji UŁ w roku akademickim 2019/2020 i koordynowanego przez dr hab. Monikę Namysłowską, prof. UŁ. Autorzy tekstu chcieliby szczególnie podziękować mgr Annie Urbanek, doktorantce w Katedrze Europejskiego Prawa Gospodarczego UŁ za jej nieocenioną pomoc przy tworzeniu artykułu.

praktykach handlowych, w ramach której przeanalizowana zostanie możliwość zakwalifikowania personalizacji reklam oraz wykorzystywania profilowania do optymalizacji warunków umownych jako nieuczciwych praktyk handlowych.

Słowa kluczowe: sztuczna inteligencja; dane; dane osobowe; pojazdy autonomiczne; nowy ład dla konsumentów; ochrona konsumentów; nieuczciwe praktyki handlowe; personalizacja; profilowanie; prawa konsumenta.

JEL: K15, K24, K42

I. Wprowadzenie

Nieustanny rozwój nowych technologii opartych na sztucznej inteligencji doprowadził do wzrostu znaczenia danych pozyskiwanych przez algorytmy z otoczenia. W ramach ogólnej kategorii danych można wyróżnić dane osobowe oraz dane nieosobowe, czyli tzw. metadane. Złożone zbiory danych zawierające niejednokrotnie zarówno dane osobowe, jak i metadane są konieczne do zapewnienia poprawności działania algorytmów sztucznej inteligencji oraz ich ciągłego ulepszania, jednak w przypadku danych osobowych nie jest to jedyny cel ich pozyskiwania i przetwarzania.

Na znaczeniu zyskuje bowiem wykorzystanie danych osobowych do działań opierających się na mechanizmie zautomatyzowanego podejmowania decyzji, w tym profilowania. Technika przetwarzania danych oparta na profilowaniu, zgodnie z motywem 71 ogólnego rozporządzenia o ochronie danych (dalej: RODO)[2], polega na zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej związane m.in. z jej preferencjami, sytuacją ekonomiczną oraz zachowaniem. Stworzone na tej podstawie profile służą administratorom, jak również są przekazywane odpłatnie osobom trzecim. Profilowanie może być wykorzystywane w celu podjęcia decyzji dotyczących określonej osoby oraz analizowania lub prognozowania jej osobistych preferencji, zachowań i postaw[3]. Niezauważalną dla konsumentów konsekwencją profilowania może być zjawisko optymalizacji cen oferowanych mu produktów oraz usług, a także dostosowanie przekazu reklamowego do indywidualnych potrzeb klienta, czyli tzw. personalizacja. Algorytmy sztucznej inteligencji potrafią stworzyć w oparciu o dane profile behawioralne częstokroć w sposób lepszy, niż gdyby tworzył je sam konsument i wykorzystywać je w przekazie reklamowym (Jabłonowska i in., 2018, s. 59–74).

Skuteczność wymienionych powyżej działań jest ściśle powiązana z ilością i jakością danych osobowych zebranych na temat konkretnej osoby. Jedną z technologii umożliwiających zbieranie kompleksowego spektrum danych osobowych są pojazdy autonomiczne. Nowoczesne samochody niejednokrotnie już teraz są wyposażone w inteligentne systemy wspomagania kierowcy, m.in. oprogramowanie odpowiedzialne za automatyczne powiadamianie o wypadku[4], ostrzeżenia

[2] 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 (Dz. Urz. UE L 119/1); dalej: RODO, ogólne rozporządzenie o ochronie danych.

[3] Zob. art. 4 pkt 4 RODO.

[4] Zgodnie z rozporządzeniem Parlamentu Europejskiego 2015/758 nowe pojazdy wyposażane są w system eCall.

o przekroczeniu prędkości, wykrywanie zmęczenia[5] lub ostrzeżenia przed używaniem telefonu w czasie jazdy. Na szeroką skalę testowane są również pojazdy, w których sztuczna inteligencja ma pełną kontrolę nad ruchem pojazdu. Pojazdy te, z uwagi na wykorzystywaną w nich sztuczną inteligencję, nieustannie zbierają różnego typu dane, w tym dane osobowe na temat kierowcy i pasażerów, wywnioskowane z obserwacji otoczenia.

Mimo niewątpliwych korzyści płynących z zastosowania profilowania, praktyka ta, w połączeniu z wszechstronnym zakresem danych osobowych pozyskiwanych przez pojazdy autonomiczne, niesie ze sobą również ryzyko dyskryminacji[6] oraz manipulacji[7]. Zebrane przez pojazdy autonomiczne dane (np. o geolokalizacji) pozwalają na wyciągnięcie wniosków dotyczących m.in. stylu życia danego konsumenta, jego zainteresowań, poglądów politycznych, orientacji seksualnej lub wyznawanej religii. Często są to informacje, których konsument w sposób świadomy sam by nie ujawnił lub podzielił się nimi z przedsiębiorcą tylko w ściśle określonym celu. Wymienione powyżej zagrożenia dają asumpt do zastanowienia się w niniejszym artykule nad zagadnieniem nadużywania wobec konsumentów profilowania oraz będącej jego konsekwencją personalizacji.

II. Zbieranie danych jako podstawa działania pojazdu autonomicznego

Fundamentalną częścią działania sztucznej inteligencji jest gromadzenie i generowanie ogromnych ilości danych[8]. Proces analizy dużej ilości i dobrej jakości danych jest kluczowy dla poprawności działania pojazdu autonomicznego. W zależności od sposobu interakcji można mówić o: bezpośredniej komunikacji pojazdu z urządzeniem, takim jak smartfon, smart watch lub komputer (*Vehicle to Device Communications* – V2D), komunikacji pojazdu z infrastrukturą drogową, taką jak m.in. kamera prędkości, fotoradar, sygnalizacja drogowa (*Vehicle to Infrastructure Communications* – V2I) oraz najbardziej zaawansowanej technologicznie komunikacji pojazdu z innym pojazdem (*Vehicle to Vehicle Communications* – V2V), będącej docelowym sposobem koegzystencji pojazdów w pełni autonomicznych (Gaeta, 2019). Zwiększone zapotrzebowanie na dane zaspokajane jest przez zastosowanie większej ilości czujników w pojeździe. W tym celu wykorzystywane mogą być takie nowoczesne technologie, jak LiDAR, MobilEye, NTRIP lub PolySync (Pogorzelski i Zygmunt, 2016, s. 800–801; Budzeń, 2020). Ruch pojazdu autonomicznego wymaga nie tylko kontrolowania toru pasa ruchu, analizy znaków drogowych i sygnalizacji świetlnej. Dla poprawnego działania niezbędna jest także analiza stanu nawierzchni, parametrów ruchu lub postoju innych pojazdów drogowych oraz stałe wymienianie informacji zarówno z infrastrukturą drogową, jak i z innymi pojazdami. Oczywistym jest, że dane gromadzone przez pojazd autonomiczny będą przekazywane do zewnętrznych serwerów, gdzie będą przechowywane i analizowane. O ile manipulacje danymi pogodowymi lub o stanie nawierzchni nie zagrażają obecnym standardom ochrony danych osobowych, o tyle operacje na danych zawierających

[5] Szerzej na ten temat: https://www.auto-swiat.pl/wiadomosci/aktualnosci/volvo-przyjrzy-nam-sie-dokladnie-kamery-do-obserwacji-kierowcy/408nhg (14.09.2020).

[6] Na przykład poprzez ograniczenie widoczności ofert dla określonych grup konsumentów.

[7] Na przykład poprzez kierowanie przekazu do osób szczególnie podatnych emocjonalnie i wpływanie poprzez to na ich zachowania. Zob. też EDPB guidelines 8/2020 on the targeting of social media users Version 1.0 adopted on 2 September 2020 s. 5–6.

[8] W przypadku pojazdów autonomicznych może być to nawet 1 GB na sekundę.

aktualną lokalizację pojazdu i jego pasażerów, a nawet wizerunki pieszych oraz innych użytkowników pojazdów ruchu drogowego budzą zasadne wątpliwości. Zgromadzone w ten sposób dane mogą być bowiem wykorzystywane m.in. w celu późniejszego profilowania.

Kontrowersje wywoływane przez pojazdy autonomiczne mają związek z szerokim zakresem gromadzonych przez nie danych, obejmującym zarówno kategorię danych osobowych, jak i nieosobowych. Podział ten jest istotny, gdyż przepisy RODO regulują problematykę zbierania, przetwarzania i wymiany jedynie danych osobowych[9]. Nie oznacza to jednak, że Unia Europejska nie zdaje sobie sprawy z roli, jaką odgrywają dane nieosobowe – w ramach strategii jednolitego rynku cyfrowego postuluje się wprowadzenie, obok swobodnego przepływu towaru, usług, osób i kapitału, swobody przepływu danych[10]. Jej celem jest stworzenie europejskim przedsiębiorcom optymalnych warunków do rozwijania projektów opartych na nowych technologiach, takich jak pojazdy autonomiczne, przez zapewnienie im niezakłóconego dostępu do danych nieosobowych[11].

Dane osobowe określić można jako wszelkie informacje o osobie fizycznej zidentyfikowanej albo możliwej do zidentyfikowania[12]. Przykładowo jest to numer IP, który w przypadku pojazdu autonomicznego z zespoloną płytą główną będzie stanowił identyczną daną weryfikacyjną, jak ma to miejsce w przypadku komputerów (zob. Voss i Houser, 2019). Ze względu na swój charakter oraz wartość ekonomiczną dane osobowe muszą podlegać bardziej rygorystycznej regulacji mającej na celu zwiększenie ochrony podmiotów, których dane dotyczą. Z kolei dane nieosobowe nie prowadzą w sposób bezpośredni do identyfikacji konkretnej osoby fizycznej. W odniesieniu do pojazdów autonomicznych, do tej grupy zakwalifikować można m.in. informację o prędkości, dystansie, pogodzie (Everett, du Boulay i Brown, 2019). Czasami status danej kategorii danych może mieć charakter względny. Jest tak np. z numerem VIN, który jest uznawany za daną osobową, jednak z zastrzeżeniem, że jedynie w odniesieniu do podmiotów mających dostęp do Centralnej Ewidencji Pojazdów i Kierowców (Odlanicka-Poczobutt i Szyszka-Schuppik, 2018).

Ze względu na sposób funkcjonowania pojazdów autonomicznych szczególnie istotne znaczenie ma lokalizacja, która zapewnia prawidłowe działanie systemu GPS, ale pozwala również na analizę odwiedzonych przez użytkownika pojazdu miejsc, przebytych tras, a przez to dostarcza wiedzy o sposobie i stylu życia, poglądach politycznych lub orientacji seksualnej. W konsekwencji powodować może identyfikację konkretnego użytkownika pojazdu, a także stworzenie na podstawie tych informacji profilu danej osoby. Analiza danych lokalizacyjnych jest immanentna dla automatyzacji pojazdów, jednak wiązać się musi z zapewnieniem wyższych standardów ochrony ze względu na potencjalne zagrożenia, jakie może generować. Koniecznie jest rozróżnienie przypadków koniecznej identyfikacji użytkownika pojazdu i jego lokalizacji w celu realizacji przewozu, od potencjalnie nadmiernego wykorzystywania lokalizacji jako źródła informacji o danej osobie.

[9] Zob. art. 1 RODO.

[10] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów, Strategia jednolitego rynku cyfrowego dla Europy. (COM/2015/0192 final).

[11] Pozyskano z: https://ec.europa.eu/commission/presscorner/detail/pl/IP_15_4919.

[12] Zob. art. 4 pkt 1 RODO.

III. Przetwarzanie danych osobowych w pojazdach autonomicznych

1. Administrator danych osobowych zbieranych przez pojazdy autonomiczne

W odniesieniu do pojazdów autonomicznych administratorem danych będzie osoba, która określa zarówno cele, jak i sposoby przetwarzania przez pojazd autonomiczny danych. Do tej kategorii zakwalifikować można m.in. dostawców poszczególnych usług wymieniających dane z otoczeniem pojazdu oraz zewnętrzne podmioty dokonujące analizy tych danych, ubezpieczycieli samochodów oferowanych w ramach usługi „samochód na minuty", producentów pojazdów zbierających dane o ich eksploatacji lub nawet organy państwa w przypadku kolizji drogowej z udziałem pojazdu autonomicznego. Mnogość potencjalnych administratorów danych stanowi niewątpliwe zagrożenie dla zapewnienia właściwej ochrony danych osobowych i może utrudniać podmiotom danych egzekwowanie przysługujących im praw[13].

2. Podstawy przetwarzania danych osobowych i ochrona konsumenta

Na gruncie przepisów RODO, poza samą klasyfikacją danych, istotne znaczenie ma dokładne określenie celu ich przetwarzania. Dane mogą być przetwarzane przez administratora jedynie w oparciu o konkretną podstawę prawną. Należy wprowadzić w tym miejscu rozróżnienie danych wykorzystywanych do prawidłowego funkcjonowania pojazdu (Milczarek, 2020, s. 76–77) od tych, których przetwarzanie nie stanowi *conditio sine qua non* korzystania z pojazdu autonomicznego. Te drugie mogą zostać wykorzystane np. do świadczenia dodatkowych usług lub być przekazywane osobom trzecim do realizacji celów komercyjnych (VDA, 2014, s. 2–3).

Domyślnie, przetwarzanie danych niezbędnych do funkcjonowania pojazdu powinno się odbywać na innych niż zgoda podstawach prawnych, takich jak: niezbędność do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej; zapewnienie ochrony żywotnych interesów administratora danych; przetwarzanie danych niezbędnych w celu wykonania przez administratora umowy[14]. Przykładem już stosowanego systemu, który przetwarza dane osobowe na tych podstawach jest urządzenie eCall[15] (Gaeta, 2019). Błędna byłaby jednak ekstrapolacja powyższego przykładu na całokształt funkcjonowania pojazdów autonomicznych. Prowadziłoby to do wniosku, że ogólne umożliwienie bezpiecznego korzystania z pojazdu wymaga przetwarzania danych osobowych wszystkich osób wewnątrz pojazdu oraz osób postronnych. Administratorzy danych nie powinni nadużywać możliwości przetwarzania danych bez zgody osoby, której dotyczą, uzasadniając to choćby ochroną swojego własnego interesu.

W przypadku danych osobowych wykorzystywanych w innych niż zapewnienie bezpieczeństwa pojazdu celach, podstawą przetwarzania powinna być zgoda osoby, której dane dotyczą. Zgoda na przetwarzanie powinna być dobrowolna, konkretna, świadoma, będąc przy tym jednoznacznym oświadczeniem woli[16], przy czym nie wolno jej domniemywać. Dodatkowo, zawsze istnieje prawo do odmowy udzielenia zgody, które nie może pociągać za sobą negatywnych reperkusji

[13] Zob. EDPB guidelines 8/2020 on the targeting of social media users adopted on 2 September 2020.

[14] Zob. art. 6 ust. 1 RODO.

[15] W sytuacji wypadku system autonomicznie wykonuje „telefon alarmowy" w celu zawiadomienia służb ratunkowych.

[16] Grupa Robocza Art. 29, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679, 17/PL WP259 rev.01, s. 5.

(IT Governance Privacy Team, 2017). Zgoda na przetwarzanie danych osobowych musi być udzielana oddzielnie na poszczególne cele przetwarzania i nie może być wiązana automatycznie z umową kupna lub leasingu samochodu. Przyjmuje się, że mogłaby być udzielona nawet w formie odrębnej umowy. Przed wyrażeniem zgody podmiot powinien zostać poinformowany o tym, kto jest administratorem danych osobowych, w jakim celu są one zbierane, do kogo trafią, przez jaki okres będą przechowywane oraz jakie prawa mu przysługują na podstawie przepisów RODO[17]. W przypadku przetwarzania danych z wykorzystaniem profilowania konieczne jest również poinformowanie podmiotu danych o ewentualnych konsekwencjach zastosowania wobec niego profilowania[18].

Raz udzielona zgoda na przetwarzanie danych fakultatywnych powinna obowiązywać przy każdym kolejnym korzystaniu z pojazdu. Gdyby proces ten miał bowiem polegać na uzyskiwaniu zgody kierowcy przy każdorazowym uruchomieniu pojazdu autonomicznego, byłby co najmniej uciążliwy, a w odniesieniu do osób trzecich wręcz niemożliwy (Everett i in., 2019).

RODO wprowadza trzy rozwiązania zapobiegające negatywnym skutkom wykorzystywania danych przez sztuczną inteligencję (Lubasz, 2020), które dotyczą wdrażania technologii chroniących dane osobowe już na etapie projektowania, zapewnienia domyślnej ochrony danych[19]. Pierwsze rozwiązanie to *privacy by design*, czyli projektowanie sztucznej inteligencji, mając na względzie ochronę danych osobowych użytkownika, które powinno być nie tylko nieodłącznym składnikiem przy tworzeniu nowoczesnych systemów, lecz także fundamentem budującym zaufanie konsumentów do producenta (Glancy, 2012). Ważnym elementem *privacy by design* jest minimalizacja ilości danych zbieranych przez administratorów i przechowywanie ich tylko przez najkrótszy niezbędny czas (Bienias, 2016). Drugie rozwiązanie to *privacy by default*. Zakłada ono, że systemy, urządzenia, algorytmy, które podlegają konfiguracji, prywatność konsumenta uznają jako domyślny stan wyjściowy, a więc bierność konsumenta wobec ustawień produktu będzie nadal gwarantować należytą ochronę jego danych (Krzysztofek, 2017). Ostatnie z przyjętych rozwiązań to *data protection impact assessment*, czyli ocena skutków przetwarzania danych osobowych[20]. Proces ten ma na celu analizę danych i udowodnienie, że są używane zgodnie z RODO, a więc oceniając m.in. konieczność i proporcjonalność ich przetwarzania[21].

3. Profilowanie danych osobowych w celu późniejszej personalizacji

Zgoda użytkownika pojazdu autonomicznego na przetwarzanie danych osobowych może być powiązana z ich profilowaniem, czyli formą 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[22]. Wyróżnić można dwie postacie profilowania:

[17] European Data Protection Board Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. Wersja 1.0 przyjęta 28 stycznia 2020, pkt 46–48, 80 i nast.

[18] Zob. art. 13 ust. 2 lit. f RODO.

[19] https://www.pwc.pl/pl/artykuly/2017/rodo-data-protection-impact-assessment.html (30.08.2020).

[20] https://www.dotmagazine.online/issues/on-the-road-mobility-connected-car/making-connected-cars-safe/data-protection-for-connected-cars (30.08.2020).

[21] https://www.pwc.pl/pl/artykuly/2017/rodo-data-protection-impact-assessment.html (30.08.2020).

[22] Zob. art. 4 pkt 4 RODO.

a) bezpośrednie, czyli oparte na danych przekazanych administratorowi bezpośrednio;
b) pośrednie, tj. wywnioskowane z informacji pozyskanych ze źródeł zewnętrznych (Sakowska-Baryła, 2018).

W przypadku pojazdów autonomicznych nieustannie raportujących swoją lokalizację, łączących się z telefonami swoich użytkowników oraz komunikujących się z innymi pojazdami, większe znaczenie będzie miało profilowanie pośrednie. Pozyskane w ten sposób z różnych źródeł dane posłużą do stworzenia kompletnego profilu danego użytkownika. Tak przygotowany profil może posłużyć do podejmowania wobec podmiotu danych określonych decyzji, m.in. o optymalizacji cen produktów i usług, a nawet odmowy zawarcia określonej umowy. Konsekwencją procesu profilowania może być również personalizacja przekazu reklamowego do potrzeb oraz zainteresowań określonej osoby.

Zgodnie z art. 4 pkt 4 RODO, aby mówić o profilowaniu należy spełnić trzy przesłanki. Po pierwsze, musi być to dowolna forma zautomatyzowanego przetwarzania danych osobowych. Po drugie, na podstawie profilowania dokonywana powinna być analiza i prognoza różnych aspektów dotyczących osoby, takich jak preferencje, sytuacja ekonomiczna, lokalizacja, zachowania, zdrowie. Po trzecie, profilowaniu muszą podlegać dane osobowe[23].

Kwestię profilowania wykonywanego na potrzeby zautomatyzowanego podejmowania decyzji reguluje art. 22 RODO. Oprócz tego typu profilowania można wyróżnić jeszcze profilowanie zwykłe, które odbywa się przy udziale czynnika ludzkiego.

Z art. 22 RODO wynikają przesłanki dopuszczalności podejmowania zautomatyzowanych decyzji. Wprost mówią o tym, że podleganie zautomatyzowanej decyzji jest możliwe wtedy, gdy decyzja ta jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą a administratorem, gdy decyzja jest dopuszczona prawem Unii lub państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą lub gdy decyzja ta opiera się na wyraźnej zgodzie osoby, której dane dotyczą[24]. Wydaje się, że jedyną dopuszczalną podstawą prawną przetwarzania danych z użyciem profilowania w celu personalizacji przekazu reklamowego powinna być zgoda osoby, której dane dotyczą[25]. Przesłanka zgody legalizuje również zautomatyzowane przetwarzanie tzw. danych wrażliwych określonych w art. 9 ust. 1 RODO, które co do zasady objęte jest zakazem określonym w art. 22 ust. 4 RODO. Są to m.in. dane dotyczące stanu zdrowia, poglądów politycznych oraz przekonań religijnych lub światopoglądowych (Sakowska-Baryła, 2018).

Przepis art. 22 RODO ma zastosowanie jedynie wtedy, gdy podjęta wskutek profilowania decyzja wywołuje wobec osoby fizycznej skutki prawne lub w podobny sposób istotnie na nią wpływa (Sakowska-Baryła, 2018, s. 268). Niewątpliwie odmowa zawarcia określonej umowy dokonana w wyniku profilowania stanowi dla osoby fizycznej istotny skutek prawny. Również optymalizacja cen w wyniku profilowania istotnie wpływa na osoby fizyczne. Za ważną w skutkach decyzję w kontekście profilowania uznać można także zawarcie umowy na skutek spersonalizowanej reklamy charakteryzującej się nachalnością, specyficznym momentem jej

[23] Wytyczne Grupy Roboczej Art. 29 dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, WP251 rev.01, s. 7.

[24] Art. 22 ust. 2 RODO.

[25] Zob. EDPB guidelines 8/2020 on the targeting of social media users adopted on 2 September 2020, s. 16.

dostarczenia lub uwzględniającej podatności profilowanej osoby, takie jak depresję, uzależnienia, choroby, trudną sytuację osobistą lub finansową (Sakowska-Baryła, 2018 s. 268–275, za: Szymielewicz, 2018).

Profilowanie niesie za sobą szereg zagrożeń, jak brak przejrzystości, ryzyko dyskryminacji cenowej i wykluczenia klientów uznanych za mniej wartościowych przez oferowanie im niepełnego wachlarza usług oraz utrudnianie im skorzystania z niektórych usług (Szymielewicz i Iwańska, 2019, s. 30). Z tego względu proces ten musi się odbywać z poszanowaniem wszystkich zasad ochrony danych ujętych w RODO.

Po pierwsze, ważne jest zachowanie przejrzystości czynności, które dla konsumentów są niewidoczne gołym okiem i mogą być dla nich niezrozumiałe. Administrator powinien w sposób krótki, zrozumiały i czytelny udzielić informacji o przetwarzaniu danych i jego konsekwencjach[26]. Po drugie, zapewnienie rzetelności przetwarzania danych pozwoli uniknąć dyskryminujących procederów wobec konsumentów[27]. Dalsze przetwarzanie danych jest możliwe jedynie z zachowaniem celu, przy rozważeniu przesłanek, takich jak charakter danych, kontekst ich zbierania, wpływ dalszego przetwarzania na konsumenta oraz zabezpieczenia stosowane przez administratora[28]. Przechowywanie danych, na podstawie których uczy się algorytm może poprawiać jego funkcjonowanie, jednak mimo to powinno odbywać się w jak najkrótszym czasie i w sposób proporcjonalny do celów[29]. Mając na uwadze dużą wartość danych poddanych profilowaniu oraz łatwość ich gromadzenia, możliwa jest sytuacja, w której przedsiębiorcy w sposób sprzeczny z zasadą minimalizacji danych, zbierają ich więcej niż potrzebują[30], a także wykorzystują je do podejmowania decyzji[31].

Nawet jeśli podstawą przetwarzania danych osobowych jest zgoda, nie legitymizuje to stosowania profilowania, które jest nieproporcjonalne lub niesprawiedliwe[32]. RODO wskazuje, że profilowanie nie powinno być wykorzystywane w sposób ingerujący w prawa osób fizycznych, z czym wiąże się wprowadzenie prawa do sprzeciwienia się profilowaniu (Lubasz, 2019). Według art. 21 ust. 1 RODO, osoba, której dane podlegają przetwarzaniu ma prawo sprzeciwić się temu z przyczyn związanych z jej szczególną sytuacją. Jeśli to zrobi, administrator danych jest zobowiązany do zaprzestania procesu profilowania, chyba że udowodni istotne prawnie podstawy do przetwarzania, nadrzędne dla praw osoby fizycznej[33]. RODO nie wskazuje wprost jakie podstawy mogłyby zostać uznane za istotne w powyższym przypadku. W kontekście personalizacji reklam zasadnicze znaczenie będzie miał również art. 21 ust. 2 RODO, który stanowi o bezwarunkowym prawie do sprzeciwu przetwarzaniu danych, w tym profilowaniu, dla celów marketingowych.

[26] Guidelines on Transparency under Regulation 2016/679/EU (wp260rev.01), s. 22.

[27] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, WP251rev.01, s. 11.

[28] Art. 6 ust. 4 RODO.

[29] Ibidem.

[30] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, WP251rev.01, s.12.

[31] Ibidem.

[32] Zob. EDPB guidelines 8/2020 on the targeting of social media users Version 1.0 adopted on 2 September 2020, s. 16

[33] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, WP251rev.01, s. 21.

IV. Problemy związane z profilowaniem danych zbieranych przez pojazdy autonomiczne

1. Wykorzystanie profilowania w celu optymalizacji warunków umowy ubezpieczenia

Firmy ubezpieczeniowe coraz częściej oferują swoim klientom ubezpieczenia komunikacyjne w modelu *pay-as-you-drive*, które uzależniają wysokość składki ubezpieczeniowej od stylu jazdy użytkownika pojazdu[34].

Ubezpieczyciel posiadający dane o częstotliwości używania pojazdu, przekraczaniu dozwolonej prędkości oraz odwiedzanych miejscach może dostosować w oparciu profilowanie wysokość składki, uwzględniając ryzyko stwarzane przez danego kierowcę, a nawet odmówić zawarcia umowy. O ile powyższe dane można uznać za obiektywne, o tyle informacje o wykonywanym zawodzie, poziomie wykształcenia, zamieszkiwaniu we własnym domu lub wynajętym mieszkaniu[35] nie powinny być wykorzystywane przez ubezpieczycieli do optymalizacji składek, gdyż potencjalnie może to prowadzić do dyskryminacji cenowej (Katyal, 2019, s. 95–98).

Obecnie optymalizacja składek na podstawie profilowania danych nie jest częsta wśród ubezpieczycieli działających na terenie Unii Europejskiej, jednak mając na uwadze ochronę konsumentów uzasadnione jest objęcie działań opartych na profilowaniu danych osobowych w celu optymalizacji warunków umowy obowiązkiem przejrzystości cen wynikającym z art. 4 ust. 2 dyrektywy Rady 93/13/EWG[36] (Jabłonowska i in., 2018, s. 91).

2. Personalizacja reklam

Dane osobowe są towarem *per se*, szczególnie cennym dla branży marketingowej i nierzadko stanowią źródło dodatkowego zysku obok transakcji centralnej (Buczyński, 2016, s. 129–136). Pozwalają stworzyć dla poszczególnych konsumentów zindywidualizowaną ofertę lub reklamę w oparciu o tzw. typowanie behawioralne (Namysłowska i Jabłonowska, 2020, s. 95). Celem marketingu behawioralnego jest pokierowanie zachowaniem konsumenta w określony przez twórcę spersonalizowanego przekazu sposób, nie pozbawiając go przy tym możliwości wyboru ani nie wpływając na jego decyzję za pomocą ceny (Thaler i Sunstein, 2008). Jedną z form marketingu behawioralnego jest reklama behawioralna, która opiera się na obserwacji osób fizycznych oraz badaniu ich zachowania w celu opracowania profilu danej osoby, a następnie zapewnienia jej reklam dopasowanych do ustalonych zainteresowań[37].

Mikrotargeting jest powszechnie wykorzystywany w celach marketingowych i politycznych (zob. Bashyakarla, Hankey, Macintyre, Rennó i Wright, 2019), a za sprawą dużych ilości danych pozyskiwanych nieustannie z pojazdów autonomicznych stanie się jeszcze skuteczniejszy i dalej idący. Już teraz historia odwiedzanych przez użytkownika pojazdu miejsc, dostęp do słuchanej w trakcie jazdy muzyki lub nawet rozmowa ze współpasażerami przy czuwającym w pojeździe asystencie głosowym mogą służyć do proponowania użytkownikom pojazdów spersonalizowanych

[34] W Polsce taki model ubezpieczenia oferowany jest przez grupę Ergo Hestia we współpracy z firmą Yanosik. Dane zbierane przez aplikację obejmują m.in. częstotliwość jazdy o poszczególnych porach dnia, w terenie zabudowanym i niezabudowanym, prędkość oraz płynność jazdy.

[35] Szerzej na ten temat: https://www.washingtonpost.com/news/tripping/wp/2018/02/07/auto-insurance-rates-have-skyrocketed-and-in-ways-that-are-wildly-unfair/?noredirect=on (14.09.2020).

[36] Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz. Urz. UE L 95/29).

[37] Grupa Robocza ds. ochrony danych powołana ma mocy art. 29, Opinia 2/2010 w sprawie internetowej reklamy behawioralnej z dnia 22 czerwca 2010 r.

produktów, usług i wydarzeń. Dodatkowo, komunikaty marketingowe mogą być niebawem wyświetlane w pojeździe w trakcie jazdy wraz z możliwością kupna określonego produktu bądź propozycją postoju w danym miejscu, przez co pozyskanie nowego klienta sprowadzałoby się do jednego kliknięcia (McKinsey & Company, 2016, s. 55–57).

V. Profilowanie kwalifikowane jako nieuczciwa praktyka handlowa

Profilowanie nie pozostaje irrelewantne z punktu widzenia dyrektywy o nieuczciwych praktykach handlowych[38] (Jabłonowska i in., 2018, s. 62). Nieprawidłowy proces pozyskiwania i wycofywania zgody na przetwarzanie danych oraz uchybienia w obowiązkach informacyjnych mogą zostać zakwalifikowane jako nieuczciwe praktyki handlowe przy pomocy tzw. małych klauzul generalnych (Namysłowska i Jabłonowska, 2020, s. 102–103).

1. Niedopełnienie obowiązków informacyjnych wobec konsumenta jako zaniechanie wprowadzające w błąd

Zaniechaniem wprowadzającym w błąd jest pominięcie istotnych informacji potrzebnych przeciętnemu konsumentowi do podjęcia świadomej decyzji dotyczącej transakcji i spowodowanie lub możliwość spowodowania podjęcia przez niego decyzji dotyczącej umowy, której inaczej by nie podjął[39].

Zaniechanie to może polegać na zatajeniu istotnych informacji lub przekazaniu ich w sposób niejasny, niezrozumiały, dwuznaczny, z opóźnieniem[40]. Niewyczerpujący katalog istotnych informacji zawarty został w załączniku II dyrektywy 2005/29/WE. Katalog ten, z uwagi na pełną harmonizację, może być uzupełniany jedynie informacjami wymaganymi przez prawo Unii (Stefanicki, 2009). Do katalogu tego należy zaliczyć obowiązki informacyjne wynikające z RODO. Z finansowego punktu widzenia producentom pojazdów może zależeć na uzyskiwaniu jak największej liczby zgód na przetwarzanie i komercyjne wykorzystanie zebranych przez pojazd danych. W związku z tym, mogą uciekać się do manipulacji w procesie ich pozyskiwania, np. zatajania lub przekazywania w sposób niezrozumiały informacji o celu ich przetwarzania poprzez stosowanie ustawień domyślnych, projektowanie nieczytelnych paneli ustawień prywatności, a także oferowanie w zamian za wyrażenie zgody zniżek (Namysłowska i Jabłonowska, 2020). Producenci pojazdów autonomicznych powinni zapewnić konsumentom przejrzystą procedurę przedstawiania informacji, cofania zgody na przetwarzanie danych oraz rezygnacji z dodatkowej usługi w dowolnym momencie (Milczarek, 2020, s. 105). Warto zwrócić uwagę, że w przypadku wykorzystywania profilowania obowiązek informacyjny względem podmiotów danych został poszerzony o konieczność poinformowania ich o samym fakcie profilowania oraz o konsekwencjach takiego profilowania[41].

Pozyskiwanie, wykorzystywanie i sprzedaż danych konsumentów bez odpowiedniego poinformowania ich o tym, należy uznać za naruszenie prawa do informacji (Pachuca-Smulska, 2013,

[38] Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady (Dz. Urz. UE L 149/22); dalej: dyrektywa 2005/29/WE.

[39] Zob. art. 6 ust. 1 dyrektywy 2005/29/WE.

[40] Zob. art. 7 ust. 2 dyrektywy 2005/29/WE.

[41] Zob. art. 13 ust. 2 lit. f RODO.

s. 60–62). Podobnie przyjął włoski Regionalny Trybunał Administracyjny[42] rozpatrujący odwołanie od decyzji[43] włoskiego Urzędu ds. Konkurencji (*Autorità Garante della Concorrenza e del Mercato*). Sąd zaznaczył, że zjawisko komercjalizacji danych osobowych obliguje przedsiębiorców do przestrzegania obowiązków udzielania jasnych i kompletnych informacji w celu ochrony konsumenta. Wykorzystanie danych w celach wykraczającym poza korzystanie z serwisu bez poinformowania o tym procederze stanowi praktykę wprowadzającą w błąd. Podkreślono przy tym, że przepisy dotyczące danych osobowych oraz ochrony konsumentów w aspekcie obowiązków informacyjnych są ze sobą komplementarne.

Obowiązek podania istotnych informacji konsumentom, a tym samym możliwość zakwalifikowania zaniechań dotyczących obowiązków informacyjnych jako nieuczciwej praktyki handlowej, są ograniczone wyłącznie do etapu zaproszenia do dokonania zakupu[44]. Wydaje się, że decyzja co do wyrażenia zgody na przetwarzanie danych oparte na profilowaniu mogłaby nastąpić dopiero po tym etapie, przykładowo bezpośrednio po uruchomieniu pojazdu lub w trakcie korzystania z niego. Obowiązek informacyjny z punktu widzenia ogólnego rozporządzenia o ochronie danych zostałby tym samym skutecznie spełniony. Jeżeli jednak brak wyrażenia zgody na profilowanie wiązałby się z brakiem dostępu do określonych funkcji pojazdu, które jednocześnie zostały wcześniej przedstawione w treści zaproszenia do dokonania zakupu, to z punktu widzenia nieuczciwych praktyk rynkowych może być to zakwalifikowane jako zaniechanie wprowadzające w błąd.

Coraz częściej mamy do czynienia również ze zjawiskiem dostosowywania cen do stopnia skłonności do ich zapłaty[45]. Zaniechań wprowadzających w błąd mogą dopuszczać się przedsiębiorcy w sytuacji, gdy nie poinformują konsumenta o tym, że cena została dopasowana do niego w oparciu o pozyskane dane. Wspomnieć należy o nowym obowiązku informacyjnym wprowadzonym za sprawą „Nowego ładu dla konsumentów"[46] do dyrektywy 2011/83/UE[47]. Przed zawarciem umowy na odległość konsument powinien zostać bowiem poinformowany czy zaproponowana mu cena została indywidualnie dostosowana, tak aby mógł uwzględnić potencjalne ryzyko przy podejmowaniu decyzji o zakupie[48]. Obowiązek ten został ograniczony do sytuacji, gdy personalizacja dokonywana jest za pomocą zautomatyzowanego podejmowania decyzji, przy czym nie obejmuje on tzw. cen dynamicznych (Namysłowska i Jabłonowska, 2020, s. 109). W praktyce coraz większa liczba działań marketingowych opiera się na mechanizmie zautomatyzowanego podejmowania decyzji, a co za tym idzie – przepis będzie miał szerokie zastosowanie. Przyjęte rozwiązanie pozwala konsumentowi na zweryfikowanie, czy zaproponowana mu cena została wyświetlona wskutek profilowania, jednak niemniej ważna jest możliwość identyfikacji kryteriów,

[42] TAR Lazio, sez. I, wyr. n. 261/20 dnia 10 stycznia 2020 r. Sąd częściowo podtrzymał decyzję nakładającą na portal Facebook karę 10 milionów euro w związku ze stosowaniem nieuczciwej praktyki rynkowej polegającej na niejasnym i niekompletnym informowaniu użytkowników portalu o komercyjnym wykorzystaniu ich danych.

[43] Decyzja nr 27432 AGCM z dnia 29 listopada 2018 r. Pozyskano z: https://www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-degli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Facebook (14.09.2020).

[44] Zob. motyw 14 dyrektywy 2005/29/WE.

[45] Praktyka ta stosowana jest przez ubezpieczycieli pojazdów, którzy dopasowują cenę w zależności od tego, czy konsument jest skłonny poświecić swój czas na porównywanie cen innych ubezpieczycieli. Pozyskano z: https://www.npr.org/2015/05/08/403598235/being-a-loyal-auto-insurance-customer-can-cost-you (14.09.2020).

[46] Zob. art. 6 ust.1 lit. ea dyrektywy 2019/2161 z dnia 27 listopada 2019 r. zmieniającej dyrektywę Rady 93/13/EWG i dyrektywy Parlamentu Europejskiego i Rady 98/6/WE, 2005/29/WE oraz 2011/83/UE w odniesieniu do lepszego egzekwowania i unowocześnienia unijnych przepisów dotyczących ochrony konsumenta (Dz. Urz. UE L 304/64).

[47] Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz. Urz. UE L 328/7); dalej: dyrektywa 2011/83/UE.

[48] Zob. motyw 45 ww. dyrektywy.

w oparciu, o które cena została dostosowana, co na tę chwilę nie zostało uregulowane na szczeblu Unii Europejskiej.

Bez wątpienia nowy obowiązek informacyjny dotyczący indywidualnego dostosowania ceny wyrażony w dyrektywie 2011/83/UE wpisuje się w kryteria istotnych dla konsumenta informacji, o których stanowi dyrektywa 2005/29/WE.

Podsumowując, zarówno nieprawidłowe przekazanie konsumentowi informacji o sposobie przyszłego wykorzystania jego danych osobowych, jak i brak powiadomienia konsumenta o indywidualnym dostosowaniu ceny może stanowić nieuczciwą praktykę handlową stypizowaną w art. 7 ust. 1 dyrektywy 2005/29/WE. W dobie pogłębiającej się asymetrii informacji między przedsiębiorcą a konsumentem, mającej swoje podstawy w dużych zbiorach danych o konsumentach, prawo do informacji nabiera większego znaczenia (Jabłonowska i in., 2018, s. 15). Równocześnie zbyt duża ilość informacji może stać się źródłem dezinformacji (Pachuca-Smulska, 2013, s. 43–47). Scharakteryzowane powyżej zaniechania dotyczące obowiązków informacyjnych mogą uniemożliwiać konsumentom dokonanie świadomego i efektywnego wyboru w zakresie spersonalizowanych ofert oraz sposobu wykorzystania danych osobowych.

2. Manipulowanie zachowaniem konsumenta jako agresywna praktyka handlowa

W świetle dyrektywy 2005/29/WE z agresywną praktyką handlową mamy do czynienia, jeżeli poprzez nękanie, przymus (fizyczny lub psychiczny) lub bezprawny nacisk w znaczny sposób ogranicza się swobodę wyboru przeciętnego konsumenta i tym samym powoduje lub może powodować podjęcie przez niego decyzji dotyczącej transakcji, której inaczej by nie podjął[49].

Zgodnie z art. 9 dyrektywy 2005/29/WE przy ustalaniu agresywności danej praktyki bierzemy pod uwagę m.in. jej czas, miejsce, rodzaj i uporczywość, a także wykorzystanie przez przedsiębiorcę na tyle poważnego nieszczęścia lub okoliczności, że są one w stanie ograniczyć zdolność konsumenta do oceny. Elementy te możemy odnosić zarówno do etapu podejmowania decyzji o przystąpieniu do umowy, jak i etapu wykonywania przez konsumenta swoich praw wynikających z umowy (Stefanicki, 2009).

Bez wątpienia personalizacja reklam oraz praktyka dostosowywania cen do skłonności do ich zapłaty w pewnym stopniu ogranicza swobodę wyboru konsumenta i wpływa na jego decyzyjność. Jednak przesłanka wywierania niedopuszczalnego nacisku zostanie spełniona tylko w określonych przypadkach. Będą to sytuacje, kiedy przedsiębiorca będzie starał się dotrzeć do osób „wrażliwych", np. odczuwających stres lub kryzys emocjonalny (Namysłowska i Jabłonowska, 2020). Z tego względu personalizacja cen produktów bądź usług w oparciu o wiedzę, że dany konsument nie jest skłonny do szukania innych, korzystniejszych ofert, choć naganne, nie będzie agresywną praktyką handlową. Dodać trzeba, że branża reklamowa dostrzega problem nadużywania personalizacji wobec konsumentów i poprzez samoregulację zakazuje tworzenia reklam z uwagi na określone cechy[50].

Naruszenia występujące podczas procesu zbierania zgód na komercyjne wykorzystanie danych użytkowników pojazdów autonomicznych mają odmienny charakter i polegają głównie

[49] Art. 8 dyrektywy 2005/29/WE.

[50] Google Ads nie dopuszcza reklam personalizowanych odnoszących się do problemów osobistych, zdrowia, statusu społecznego. Pozyskano z: https://support.google.com/adspolicy/answer/143465?hl=pl (14.09.2020).

na uporczywym nękaniu konsumentów. Użytkownicy pojazdów mogą być w sposób natarczywy zachęcani do wyrażenia zgody na przetwarzanie danych pozyskanych z pojazdu w celach komercyjnych przy każdej okazji, gdy korzystają z pojazdu. Elementem decydującym przy wyrażeniu zgody może być w związku z tym chęć nieotrzymywania kolejnych komunikatów bądź nieuwaga wywołana presją czasu (Sieradzka, 2008).

Możliwa jest też sytuacja odwrotna – gdy przedsiębiorca używać będzie zwrotów (przykładowo ostrzegających, że cofnięcie zgody będzie wiązać się z utratą przez pojazd szeregu funkcjonalności) w celu zniechęcenia konsumentów do wycofania tejże zgody. W świetle przedstawionych powyżej rozważań, postawienie zarzutu agresywnych praktyk handlowych w kontekście personalizacji może być ograniczone.

VI. Ewolucja modelu przeciętnego konsumenta w związku z przetwarzaniem danych osobowych przez pojazdy autonomiczne

Przy ocenie zachowań stanowiących nieuczciwe praktyki handlowe punktem odniesienia jest pojęcie „przeciętnego konsumenta", który jest dostatecznie dobrze poinformowany, uważny i ostrożny[51]. Pojęcie to nie jest statyczne i jednolite na poziomie międzynarodowym, a nawet krajowym. Określenie jego cech należy do sądów poszczególnych państw członkowskich (Namysłowska, 2016, s. 4–9).

Z jednej strony, w dobie rozwoju nowych technologii i ogólnodostępności Internetu słuszne jest zredefiniowanie modelu przeciętnego konsumenta w kontekście możliwości stosowania wobec niego personalizacji. Konsumenci wchodzą bowiem w coraz częstsze interakcje z przedsiębiorcami i biorą aktywny udział w kreowaniu rynku (Prahalad i Ramaswamy, 2004). Zgoda na udostępnienie danych oraz zastosowanie profilowania coraz częściej jest działaniem świadomym, które przynosi konsumentowi wymierne korzyści, tym bardziej jeśli bierzemy pod uwagę przeciętnego użytkownika autonomicznego pojazdu. Model „przeciętnego konsumenta" jest bowiem kształtowany z uwzględnieniem danej kategorii produktów i usług, na temat których konsument posiada określony zasób wiedzy (Macierzyńska-Franaszczyk, 2018, s. 125–137). Przeciętny posiadacz pojazdu autonomicznego będzie świadom zakresu danych zbieranych przez pojazd i będzie mógł w sposób roztropny operować dostępem do nich. W odniesieniu do tak scharakteryzowanej grupy społecznej wymagania dotyczące praktyk handlowych będą niższe (Michalak, 2008).

Z drugiej strony, wraz z upowszechnieniem się nowych technologii rosło będzie rozwarstwienie między nowym pokoleniem konsumentów wyedukowanych i pewnie poruszających się w rzeczywistości zdigitalizowanej a konsumentami wrażliwymi, o niższej predyspozycji do przyswajania nowych technologii (Jabłonowska i in., 2019, s. 14–15).

Jeśli dana praktyka kierowana jest bezpośrednio do konsumentów wrażliwych, jej ocena jest dokonywana z perspektywy przeciętnego członka tej grupy, a zatem odstępuje się od wzorca podstawowego (Sieradzka, 2014, s. 127–128). Konsumenta szczególnie wrażliwego określa się z uwagi na jego wiek, niepełnosprawność fizyczną bądź umysłową oraz łatwowierność[52]. Katalog cech określonych w dyrektywie 2005/29/WE uznaje się za zamknięty (Namysłowska i Jabłonowska, 2020, s. 107), co należy uznać za niekorzystne z punktu widzenia upowszechniania się nowych

[51] Zgodnie z motywem 18 dyrektywy 2005/29/WE.

[52] Zgodnie z motywem 19 dyrektywy 2005/29/WE.

technologii. Konsument doświadczający wykluczenia cyfrowego nie posiada predyspozycji do szybkiego przyswajania nowych technologii i nie jest świadomy wartości swoich danych, a przez to powinien zyskać w określonych sytuacjach przymiot konsumenta szczególnie wrażliwego. Niemniej jednak, tylko niekiedy wrażliwość będzie wynikać z zamkniętego katalogu cech wskazanego w dyrektywie 2005/29/WE, tj. określonego wieku, niepełnosprawności lub łatwowierności.

Na marginesie powyższych rozważań zaznaczyć trzeba, że w przypadku daleko idącego profilowania obejmującego m.in. poziom wykształcenia, styl życia oraz uwarunkowania społeczne danego konsumenta model przeciętnego konsumenta może nie mieć zastosowania. Każda oferta, reklama bądź umowa będzie uwzględniać profil danego konsumenta, a co za tym idzie traktowanie go jako konsumenta przeciętnego może być niemożliwe.

Stosowanie profilowania na podstawie uprzednio udzielonej zgody nie jest *novum*. Pojazdy autonomiczne staną się jednak nowym środkiem do pozyskiwania zgód i wykorzystywania danych. Skonstruowanie modelu przeciętnego użytkownika pojazdu autonomicznego (o ile w ogóle będzie możliwe), będzie utrudnione z uwagi na znaczne zróżnicowanie wiedzy technologicznej konsumentów.

Wyrażamy nadzieję, że cześć przedsiębiorców wykorzysta posiadany szeroki zakres spersonalizowanych danych w słusznym celu – by skuteczniej dostosować swoje praktyki handlowe oraz sposób przekazywania informacji do poszczególnych grup konsumentów, co wpłynie pozytywnie na egzekwowanie dyrektywy 2005/29/WE.

VII. Zakończenie

Profilowanie na stałe zagościło wśród metod wykorzystywanych przez przedsiębiorców do kontaktu z konsumentami, a pojazdy autonomiczne stają się kolejnym źródłem danych, a niekiedy również platformą, przez którą może być stosowana personalizacja reklam lub optymalizacja cen. Konsekwencją upowszechnienia się tych praktyk będzie powstanie nowych zagrożeń dla konsumentów – ryzyka wykorzystania danych osobowych użytkowników pojazdów w sposób sprzeczny z pierwotnym założeniem, możliwości naruszenia prawa do prywatności oraz zagrożeń związanych ze zbyt daleko idącym profilowaniem wykorzystującym ludzkie słabości oraz nieuwagę.

Problematyka profilowania wykorzystywanego w stosunku do konsumentów jest obecna w pracach legislacyjnych toczących się na szczeblu unijnym. Uregulowania dotyczące wyświetlania spersonalizowanych cen zawarte zostały w nowelizacji dyrektywy 2011/83/UE. Z kolei w propozycji projektu Kodeksu Usług Cyfrowych z 15.12.2020 r.[53] określono obowiązki informacyjne dotyczące wyświetlania spersonalizowanych reklam. Czynione w tym zakresie działania należy uznać za pozytywne, lecz niewystarczające. Analiza dyrektywy 2005/29/WE o nieuczciwych praktykach handlowych ukazała luki, które mogą zostać zniwelowane jedynie z pomocą inicjatywy legislacyjnej na szczeblu Unii Europejskiej. W szczególności możliwość zastosowania w kontekście personalizacji przekazu reklamowego agresywnych praktyk handlowych jest zbyt ograniczona. Aktem prawnym mogącym na tę chwilę stanowić ochronę konsumentów przed nadużywaniem przez przedsiębiorców profilowania jest RODO.

[53] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. (COM/2020/825 final).

Mimo że profilowanie bywa wykorzystywane przeciwko konsumentom, z ich punktu widzenia nadal jest zjawiskiem korzystnym – wytworzone na skutek profilowania spersonalizowane reklamy są mniej uciążliwe i niejednokrotnie pozwalają ograniczyć czas potrzebny na znalezienie interesujących produktów lub usług. Szeroko pojęte śledzenie aktywności konsumentów, w tym pozyskiwanie od nich danych osobowych, coraz częściej staje się również formą zapłaty za oferowane treści, aplikacje oraz usługi, co również może wywrzeć korzystny wpływ dla sytuację konsumentów. Wydaje się zatem, że profilowanie i personalizacja są przez konsumentów pożądane w takim stopniu, że wprowadzanie regulacji opartych na zakazie ich wykorzystywania jest wykluczone. Konsumenci bezsprzecznie powinni mieć jednak łatwo dostępną możliwość zrezygnowania z tych udogodnień i to właśnie w tym kierunku powinny iść ewentualne zmiany aktów prawnych w zakresu ochrony konsumentów.

Bibliografia

Bashyakarla, V., Hankey, S., Macintyre, A., Rennó, R. i Wright, G. (2019). *Personal Data: Political Persuasion Inside the Influence Industry. How it works*. Tactical Tech's Data and Politics team. March. Pozyskano z: https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf.

Bienias, M. (2016). Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych. *Monitor Prawniczy,* (20), 53.

Buczyński, S. (2013). Konsument wobec internetowej reklamy behawioralnej. W: M. Królikowska-Olczak i B. Pachuca-Smulska (red.), *Ochrona konsumenta w prawie polskim i Unii Europejskiej*. Warszawa: Wydawnictwo C.H. Beck.

Buczyński, S. (2016). Działania na zbiorach typu big data z perspektywy ochrony praw e-konsumenta. W: M. Królikowska-Olczak i B. Pachuca-Smulska (red.), *Ochrona prawna konsumenta na rynku mediów elektronicznych*. Warszawa: Wydawnictwo C.H. Beck.

Budzeń, M. (2020). Bosch może spopularyzować technologię LiDAR w samochodach. Tabletowo.pl, 2 stycznia. Pozyskano z: https://www.tabletowo.pl/bosch-technologia-lidar-w-samochodach/ (18.11.2020).

Contissa, G., Lagioia, F., Lippi, M., Micklitz, H., Pałka, P., Sartor, G. i Torroni, P. (2018), *Towards Consumer-Empowering Artificial Intelligence*. Wystąpienie wygłoszone na międzynarodowej konferencji, Sztokholm, 13–19 lipca. http://doi.org/10.24963/ijcai.2018/714.

Everett, M., du Boulay, E. i Brown, H. (2019). *Driving Data Compliance.* Herbert Smith Freehills LLP. 20 May. Pozyskano z: https://hsfnotes.com/tmt/2019/05/20/driving-data-compliance/ (15.09.2020).

Gaeta, Maria. (2019). Data protection and self-driving cars: the consent to the processing of personal data in compliance with GDPR, *Communications Law, 24*(1).

Glancy, D.J. (2012). Privacy in Autonomous Vehicles. *Santa Clara Law Review*, *52*(4), s. 1226.

IT Governance Privacy Team. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. United Kingdom: IT Governance Publishing.

Jabłonowska, A., Kuziemski, M., Nowak, A., Micklitz, H., Pałka, P. i Sartor, G. (2018). Consumer Law and Artificial Intelligence: Challenges to the EU Consumer Law and Policy Stemming from the Business' Use of Artificial Intelligence – Final report of the ARTSY project. *EUI Department of Law Research Paper*, (11). https://doi.org/10.2139/ssrn.3228051.

Jin, G. (2018). Artificial Intelligence and Consumer Privacy. *NBER Working Paper*, (24253).

Katyal, S. (2019). Private Accountability in the Age of Artificial Intelligence. *UCLA Law Review, 66*(54).

Krzysztofek, M. (2017). Ochrona danych w fazie projektowania i domyślna ochrony danych. *Informacja w Administracji Publicznej*, (1), 33.

Lubasz, D. (2019). Big brother is watching you. Profilowanie i zautomatyzowane podejmowanie decyzji w kontekście zasad legalności i przejrzystości. W: W. Wiewiórowski, H. Wolska (red.), *Rok RODO.* Warszawa: Wydawnictwo C.H. Beck.

Lubasz, D. (2020). Zasady legalności, przejrzystości i minimalizacji danych w ogólnym rozporządzeniu o ochronie danych osobowych w kontekście sztucznej inteligencji. W: L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji* (s. 173–186). Warszawa: Wydawnictwo C.H. Beck.

Macierzyńska-Franaszczyk, E. (2018). Konsument, Internet i informacja. W: E. Sługocka-Krupa, K. Podgórski, M. Fras (red.), *Prawa konsumenta w teorii i praktyce*. Warszawa: Wydawnictwo C.H. Beck.

McKinsey & Company. (2016). *Monetizing car data. New service business opportunities to create new customer benefits.* September. Pozyskano z: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/monetizing%20car%20data/monetizing-car-data.ashx.

Megías Quirós, J.J. (2019). RGPD y actividades personales en materia de proteccion de datos. *Persona y Derecho*, *80*, 1. https://doi.org/10.15581/011.80.147-178.

Michalak, A. (2008). *Przeciwdziałanie nieuczciwym praktykom rynkowym. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Milczarek, E. (2020). *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w Internecie.* Warszawa: Wydawnictwo C.H. Beck.

Namysłowska, M. (2016). Dziesięć lat dyrektywy 2005/29/WE o nieuczciwych praktykach handlowych. *Europejski Przegląd Sądowy*, 3.

Namysłowska, M. i Jabłonowska, A. (2020). Personalizacja oparta na sztucznej inteligencji – nowe wyzwanie dla prawa konsumenckiego. W: L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji* (s. 95–109). Warszawa: Wydawnictwo C.H. Beck.

Odlanicka-Poczobutt, M. i Szyszka-Schuppik, A. (2018). Bezpieczeństwo danych osobowych w świetle nowych przepisów (RODO) – przegląd historyczny. *Zeszyty Naukowe. Organizacja i Zarządzanie/ Politechnika Śląska*, 118. https://doi.org/10.29119/1641-3466.2018.118.31.

Pachuca-Smulska, B. (2013). Prawo do informacji i edukacji podstawą ochrony interesów konsumenta. W: M. Królikowska-Olczak, B. Pachuca-Smulska (red.), *Ochrona konsumenta w prawie polskim i Unii Europejskiej.* Warszawa: Wydawnictwo C.H. Beck.

Pogorzelski, T. i Zygmunt, B. (2016). Integracja sensorów w autonomicznym samochodzie. *Mechanik*, *89*(7), 800–801.

Prahalad, C.K. i Ramaswamy, V. (2004). Co-creating unique value with customers. *Strategy & Leadership*, (32). https://doi.org/10.1002/dir.20015.

Russell, S.J. i Norvig, P. (2009). *Artificial Intelligence: A Modern Approach* (3rd ed.). New Jersey: Prentice Hall.

Sakowska-Baryła, M. (2018). *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, art. 22.* Warszawa: Wydawnictwo C.H. Beck.

Sieradzka, M. (2008). *Komentarz do ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz*. Warszawa: Oficyna a Wolters Kluwer business.

Stefanicki, R. (2009). *Ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz.* Warszawa: Wydawnictwo Prawnicze LexisNexis.

Stefanicki, R. (2011). Koncepcja zupełnej harmonizacji prawa ochrony konsumenta (na przykładzie dyrektywy o nieuczciwych praktykach handlowych). *Państwo i Prawo*, 6, 51–63.

Szymielewicz, K. i Iwańska, K. (2019). *Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem*. Warszawa: Fundacja Panoptykon. Pozyskano z: https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf (25.09.2020).

Szymielewicz, K. (2018). Profilowanie w marketingu, *ABI Expert,* 1.

Thaler, Richard H. i Sunstein. Cass R. (2008). *Nudge: Improving decisions about health, wealth, and happiness.* Yale University Press.

Underwood, S. (2019). Can you locate your location data? *Communications of the ACM, 62*, 9. https://doi.org/10.1145/3344291.

VDA. (2014). *Data Protection Principles for Connected Vehicles*. Berlin: Verband der Automobilindustrie. Pozyskano z: https://www.pdpjournals.com/docs/99009.pdf.

Voss, W.G. i Houser, K.A. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal*, *56*, 2. https://doi.org/10.1111/ablj.12139.