



**Anna
Nowak**

Personalizacja oparta na sztucznej inteligencji a ochrona praw konsumentów Zagadnienia wybrane

ANNA NOWAK

PERSONALIZACJA OPARTA
NA SZTUCZNEJ INTELIGENCJI
A OCHRONA PRAW KONSUMENTÓW
ZAGADNIENIA WYBRANE



Warszawa 2022

Wydawnictwo powstało w ramach serii „Biblioteka UOKiK”. Niniejsza publikacja zwyciężyła w konkursie Prezesa Urzędu Ochrony Konkurencji i Konsumentów na najlepszą pracę magisterską poświęconą ochronie konsumentów w edycji 2021/2022.

Wszelkie opinie wyrażone w niniejszym opracowaniu są osobistymi opiniami autora i nie mogą być utożsamiane ze stanowiskiem Urzędu Ochrony Konkurencji i Konsumentów.

Copyright @ 2022 Anna Nowak. Wszelkie prawa zastrzeżone.

Praca magisterska napisana pod kierunkiem naukowym dr hab. Moniki Namysłowskiej, prof. UŁ

ISBN 978-83-64681-37-0

Urząd Ochrony Konkurencji i Konsumentów
pl. Powstańców Warszawy 1, 00-950 Warszawa
www.uokik.gov.pl

Skład i druk:
Drukarnia Piotra Włodarskiego
ul. Ksawerów 21
02-656 Warszawa
www.wlodarski.pl

SPIS TREŚCI

Wprowadzenie.....	9
Rozdział I Charakterystyka personalizacji opartej na sztucznej inteligencji i jej oddziaływanie na konsumentów	11
1. Uwagi wprowadzające	11
2. Personalizacja stosowana wobec konsumentów	13
2.1. Definicja personalizacji	13
2.2. Rodzaje personalizacji	14
2.2.1. Reklama spersonalizowana.....	14
2.2.2. Personalizacja warunków umownych.....	15
2.3. Pojęcia związane z personalizacją	16
2.3.1. Profilowanie	16
2.3.2. Targetowanie oraz mikrotargetowanie	18
3. Sztuczna inteligencja wykorzystywana na potrzeby personalizacji	18
3.1. Definicja sztucznej inteligencji oraz jej rodzaje	19
3.2. Metoda działania sztucznej inteligencji w procesie personalizacji....	20
4. Oddziaływanie personalizacji opartej na sztucznej inteligencji na konsumentów.....	22
4.1. Korzyści wynikające z personalizacji opartej na sztucznej inteligencji.....	22
4.1.1. Zindywidualizowanie treści i usług kierowanych do konsumentów.....	22
4.1.2. Bezpłatny dostęp do treści za sprawą monetyzacji danych konsumentów.....	23
4.2. Zagrożenia wynikające z personalizacji opartej na sztucznej inteligencji	24

4.2.1. Manipulowanie zachowaniem konsumenta przez wykorzystanie mechanizmów wykrywania emocji	24
4.2.2. Utrata kontroli nad przekazanymi danymi	26
4.2.3. Nadużywanie danych osobowych jako formy zapłaty za towar lub usługę.....	29
4.2.4. Dyskryminacja konsumentów będąca wynikiem profilowania .	30
4.2.5. Ograniczanie dostępu do informacji przez bańki filtrujące.	32
5. Wnioski częściowe	34
Rozdział II RODO jako instrument prawny ochrony konsumenta przed personalizacją opartą na sztucznej inteligencji.....	35
1. Uwagi wprowadzające	35
2. Dane osobowe wykorzystywane w procesie profilowania	36
3. Zasady profilowania określone w RODO jako podstawy personalizacji..	37
3.1. Definicja profilowania zwykłego zgodnie z art. 4 pkt 4 RODO	37
3.2. Definicja profilowania szczególnego zgodnie z art. 22 RODO	38
3.2.1. Przestanka całkowitego zautomatyzowania procesu profilowania	39
3.2.2. Przestanka wywoływania skutków prawnych lub wpływania na sytuację osoby w podobnie istotny sposób	40
3.2.2.1. Przestanka wywoływania skutków prawnych.....	40
3.2.2.2. Przestanka wpływania na sytuację osoby w podobnie istotny sposób	40
3.2.3. Dopuszczalność wykorzystywania profilowania określonego w art. 22 RODO	42
4. Podstawy przetwarzania istotne z punktu widzenia personalizacji opartej na sztucznej inteligencji.....	44
4.1. Zasady przetwarzania danych zgodnie z art. 5 RODO	44
4.2. Przestanki legalizujące przetwarzanie danych osobowych w celu personalizacji treści	46

4.2.1. Przestanka niezbędności do wykonania umowy	46
4.2.2. Przestanka uzasadnionego interesu administratora	47
4.2.3. Przestanka zgody osoby, której dane dotyczą.....	48
5. Prawa konsumentów i obowiązki przedsiębiorców dotyczące procesu profilowania jako element ochrony przed nadmierną personalizacją...	50
5.1. Prawa konsumentów jako podmiotów danych	50
5.1.1. Prawo do ludzkiej interwencji.....	50
5.1.2. Prawo do sprzeciwu	51
5.1.3. Prawo do usunięcia danych	52
5.1.4. Prawo do sprostowania danych	52
5.2. Obowiązki przedsiębiorców jako administratorów danych	53
5.2.1. Obowiązek informacyjny	53
5.2.2. Ocena skutków dla ochrony danych	56
6. Wnioski częściowe	57
Rozdział III Personalizacja oparta na sztucznej inteligencji jako nieuczciwa praktyka handlowa	59
1. Uwagi wprowadzające	59
2. Pojęcie nieuczciwej praktyki handlowej	59
3. Zakres stosowania dyrektywy	61
4. Wpływ personalizacji opartej na sztucznej inteligencji na pojęcie przeciętnego i wrażliwego konsumenta	61
4.1. Pojęcia przeciętnego i wrażliwego konsumenta jako punkt odniesienia dla oceny nieuczciwości praktyki handlowej	62
4.2. Zasadność pojęcia przeciętnego konsumenta w obliczu personalizacji opartej na sztucznej inteligencji.....	64
4.3. Pojęcie konsumenta wrażliwego z uwagi na brak umiejętności cyfrowych	65
5. Personalizacja oparta na sztucznej inteligencji w świetle czarnej listy nieuczciwych praktyk handlowych	67

6. Personalizacja oparta na sztucznej inteligencji w świetle małych klauzul generalnych.....	68
6.1. Personalizacja jako praktyka handlowa wprowadzająca w błąd ...	69
6.1.1. Wprowadzające w błąd działanie polegające na personalizacji cenowej	69
6.1.1.1. Działanie wprowadzające w błąd.....	69
6.1.1.2. Możliwość zakwalifikowania personalizacji cenowej jako działania wprowadzającego w błąd.....	69
6.1.2. Wprowadzające w błąd zaniechanie polegające na pomijaniu istotnych obowiązków informacyjnych wobec konsumenta..	70
6.1.2.1. Zaniechanie wprowadzające w błąd	70
6.1.2.2. Ochrona konsumenta oparta na prawie do informacji	72
6.1.2.3. Naruszenie obowiązków informacyjnych wobec konsumenta	75
6.2. Profilowanie i personalizacja jako agresywne praktyki handlowe..	76
6.2.1. Agresywna praktyka handlowa.....	76
6.2.2. Agresywna praktyka handlowa polegająca na wykorzystywaniu słabości konsumentów w celu personalizacji reklam..	77
7. Personalizacja oparta na sztucznej inteligencji w świetle dużej klauzuli generalnej nieuczciwej praktyki handlowej.....	79
8. Wnioski częściowe	80
Rozdział IV Przyszłość ochrony konsumentów wobec stosowania personalizacji.....	81
1. Uwagi wprowadzające	81
2. Strategia UE w zakresie sztucznej inteligencji i jej znaczenie w kontekście personalizacji.....	82
2.1. Sztuczna inteligencja w dokumentach unijnych	82
2.2. Projekt rozporządzenia w sprawie sztucznej inteligencji	84

3. Nowe obowiązki platform internetowych wobec konsumentów w związku z personalizacją opartą na sztucznej inteligencji	84
3.1. Projekt Kodeksu Usług Cyfrowych	84
3.1.1. Zapewnienie przejrzystości spersonalizowanych reklam.....	85
3.1.2. Dodatkowe informacje o systemach rekomendujących	86
3.2. Projekt Kodeksu Rynków Cyfrowych	86
4. Zmiana uregulowania plików <i>cookie</i> wykorzystywanych do celów personalizacji opartej na sztucznej inteligencji	87
4.1. Obecna regulacja plików <i>cookie</i>	87
4.1.1. Charakterystyka plików <i>cookie</i> i ich rodzaje	87
4.1.2. Techniczne sposoby blokowania <i>cookies</i> przez konsumentów.....	88
4.1.3. Problematyka wstępnego ładowania plików <i>cookie</i>	89
4.1.4. Pliki <i>cookie</i> traktowane jako dane osobowe	90
4.1.5. Dwoistość obecnego uregulowania zagadnienia plików <i>cookie</i>	90
4.2. Projektowana regulacja plików <i>cookie</i> w rozporządzeniu <i>ePrivacy</i>	91
4.2.1. Przestanki legalizujące przechowywanie informacji na urządzeniach końcowych	92
4.2.2. Rozwiązanie problemu nieświadomości udzielanych zgód ..	93
4.2.2.1. Obowiązek informacyjny przed umieszczeniem plików <i>cookie</i> na urządzeniu	93
4.2.2.2. Zgoda spełniająca przesłanki art. 7 RODO	94
4.2.2.3. Możliwość udzielania zgód przy pomocy ustawień przeglądarki.....	95
4.2.2.4. Okresowe przypomnienia o udzieleniu zgody	95
4.2.3. Dopuszczalność <i>cookies walls</i>	96

5. Nowelizacja dyrektywy 2011/83/UE za sprawą Nowego Ładu dla konsumentów	98
6. Wnioski częściowe	98
Wnioski końcowe.....	100
Bibliografia.....	104

Wprowadzenie

Konsumenci poruszający się w przestrzeni internetowej coraz częściej mogą odnosić wrażenie, że przedsiębiorcy czytają w ich myślach. Takie możliwości daje personalizacja. Szeroki dostęp do informacji doprowadził do sytuacji, w której ich przyswajanie przez konsumentów stało się trudniejsze, a wyświetlanie reklam internetowych - mniej efektywne. Tradycyjne kampanie reklamowe w coraz mniejszym stopniu przyczyniają się do powiększenia sprzedaży¹. W związku z tym przedsiębiorcy zmieniają sposoby docierania do konsumentów. Wykorzystują m.in. personalizację wspomaganą najczęściej technologiami opartymi na sztucznej inteligencji. Celem jej zastosowania zwykle jest chęć zminimalizowania wydatków marketingowych przy jednoczesnej maksymalizacji zysków, np. przez predykcję preferencji zakupowych, a także tworzenie ofert uwzględniających możliwości finansowe danego konsumenta.

Konstruowanie i wykorzystywanie profili osób fizycznych w celu personalizacji przekazu w krótkim czasie stało się prężnie działającą sferą gospodarki, wartą obecnie około 50 mld dolarów². Powstały także wyspecjalizowane podmioty pośredniczące w handlu danymi, tzw. brokerzy danych, posiadające praktycznie nieograniczone możliwości łączenia i porównywania wielu rodzajów danych z różnych źródeł³. O wysokim stopniu komercjalizacji danych osobowych na cele personalizacji świadczy istnienie giełd reklam, na których odbywają się milisekundowe wirtualne aukcje o to, którą reklamę wyświetlić konkretnemu konsumentowi odwiedzającemu stronę internetową (ang. *real time bidding*, RTB). Konsument jest tym samym coraz częściej obecny w dwóch nowych rolach - użytkownika Internetu oraz podmiotu danych, co z jednej strony poszerza zakres dostępnych dla niego praw i gwarancji, ale z drugiej strony naraża go na charakterystyczne dla tych ról ryzyka.

Nadmierne wykorzystywanie technik profilowania i personalizacji doprowadziło do intensywnego powstawania nowych, nieznanych dotąd problemów z pogranicza dziedziny prawa i nowych technologii, dotyczących m.in.: sfery danych osobowych, prywatności oraz ograniczenia praw konsumentów do rzetelnych, niezmanipulowanych informacji. Okazuje się, że konsumenci nie do końca radzą sobie z prawidłowym identyfikowaniem faktu personalizacji *online*, głównie z powodu braku odpowiedniej świadomości technologicznej⁴. Statystycznie bardziej narażona na zagrożenia strona transakcji jest zatem dodatkowo osłabiana przez niektóre techniki oparte na sztucznej inteligencji, a brak przejrzystej informacji na temat personalizacji jedynie wzmacnia asymetrię informacyjną. Niestety podmioty z branży internetowej, mimo narastających od kilku lat problemów, nie są zdolne do samoregulacji. Internet oraz stosowana w ramach niego personalizacja mają charakter transgraniczny. Aby za-

1 Por. P. Wójcik, *Psychometria konsumentów*, Lublin 2017, s. 131.

2 A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Warszawa 2019, s. 46.

3 K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem*, 2019, s. 22.

4 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*. Request for Specific Services 2016 85 02 for the implementation of Framework Contract EAH/2013/CP/04, 2018, s. 263.

pewnieć jednakowo wysoki poziom ochrony konsumentów we wszystkich państwach członkowskich, Unia Europejska powinna wykazać aktywną rolę w tworzeniu regulacji z zakresu personalizacji. Już teraz jest to integralny element przestrzeni internetowej, którego znaczenie w kolejnych latach niewątpliwie będzie rosnać. Wraz z częstszym wykorzystaniem personalizacji będą też przybierać na sile związane z nią problemy. O istotności tego zagadnienia i pilnej potrzebie jego uregulowania świadczy również liczba toczących się obecnie procesów legislacyjnych na szczeblu unijnym, które dotyczą omawianej w tej pracy materii.

Niniejsza praca poświęcona jest aspektom prawnym procesu personalizacji opartej na sztucznej inteligencji. Główny problem badawczy to odpowiedź na pytanie, czy obecne przepisy z zakresu ochrony danych osobowych, prywatności elektronicznej i ochrony konsumenta normują kwestię zagrożeń wynikających z profilowania i personalizacji opartych na sztucznej inteligencji. Dokonam oceny, czy powyższe przepisy odpowiadają potrzebom konsumentów i zapewniają im wystarczającą ochronę.

Pierwszy rozdział pracy wyjaśnia istotę działania personalizacji oraz wskazuje praktyczne konsekwencje jej wykorzystania. Scharakteryzuję w nim dwa główne rodzaje personalizacji, tj. personalizację reklam oraz warunków umownych, i wskażę pojęcia pokrewne. Jako że personalizacja jest najczęściej wspomagana technologiami opartymi na sztucznej inteligencji, wyjaśnienia będzie wymagać sposób jej działania. Zasygnalizowane zostaną także najistotniejsze, w mojej opinii, korzyści oraz zagrożenia dla konsumentów związane z profilowaniem oraz z będącą jego skutkiem personalizacją.

Rozdział drugi poświęcony jest analizie procesu profilowania, który poprzedza etap personalizacji. W ramach niego odpowiem m.in. na pytanie, w jaki sposób dane osobowe są wykorzystywane w procesie profilowania oraz jaka podstawa prawna powinna być użyta w przypadku zbierania danych na potrzeby personalizacji. Omówienie praw konsumentów i obowiązków administratorów dotyczących procesu profilowania stanie się asumptem do zastanowienia się, czy ochrona konsumenta przed nadmiernym profilowaniem wynikająca z ogólnego rozporządzenia o ochronie danych jest wystarczająco skuteczna.

Trzeci rozdział pracy stara się przybliżyć kwestię personalizacji jako nieuczciwej praktyki handlowej. W tym celu wybrane praktyki handlowe z zakresu profilowania i personalizacji zostaną poddane analizie przy wykorzystaniu instrumentów prawnych dyrektywy o nieuczciwych praktykach handlowych, tj.: czarnej listy nieuczciwych praktyk handlowych, małych klauzul generalnych oraz dużej klauzuli generalnej. W ramach rozdziału rozważę również, czy, a jeśli tak, to jakim zmianom w kontekście personalizacji, uległo pojęcie przeciętnego i wrażliwego konsumenta.

Czwarty rozdział pracy dotyczy natomiast projektowanych obecnie na szczeblu unijnym sposobów ochrony konsumentów przed nadmierną personalizacją. Przeanalizuję w nim wybrane projekty aktów prawnych, ze szczególnym uwzględnieniem kwestii plików *cookie* zawartej w projekcie rozporządzenia *ePrivacy*.

Praca magisterska uwzględnia stan prawny na 11.06.2021 r.

Rozdział 1.

Charakterystyka personalizacji opartej na sztucznej inteligencji i jej oddziaływanie na konsumentów

1. Uwagi wprowadzające

Personalizacja oparta na sztucznej inteligencji wykorzystuje dane o aktywności internetowej konsumentów. Ilość tworzonych obecnie w ciągu dwóch dni informacji jest porównywalna z sumą wszystkich danych wyprodukowanych łącznie w 2003 roku⁵. W 2018 r. globalna liczba danych przekroczyła 33 zettabajty, natomiast szacuje się, że do 2025 r. osiągnie ona poziom 175 zettabajtów⁶. Proces ten może okazać się jeszcze szybszy z uwagi na powszechną digitalizację, na którą znaczny wpływ wywiera pandemia COVID-19. Przedsiębiorcy i konsumenci coraz powszechniej korzystają m.in. z możliwości handlu elektronicznego. Rynek *e-commerce* w Polsce w 2019 r. powiększył się o ponad 18% w porównaniu do roku poprzedniego⁷.

Użytkownicy Internetu w zdecydowanej większości przypadków są zarazem konsumentami, czyli grupą wyróżnianą ze względu na swoją słabość finansową, organizacyjną i informacyjną w relacjach z przedsiębiorcami⁸. Prawo Unii Europejskiej nie wytworzyło jednolitej definicji konsumenta. Na podstawie dyrektywy 2011/83/UE⁹ o prawach konsumenta i dyrektywy 2005/29/WE¹⁰ o nieuczciwych praktykach handlowych można skonstruować definicję konsumenta jako osoby fizycznej, która działa w celu niezwiązanym z jej działalnością handlową, gospodarczą, rzemieślniczą ani wykonywaniem wolnego zawodu. W orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej wytworzony został również przeciętny model konsumenta wyedukowanego, aktywnego i dostatecznie poinformowanego, nawet jeśli konkretni konsumenci tych cech spełniać nie będą¹¹. Na marginesie powyższych rozważań trzeba wspomnieć o zauważalnej tendencji do odchodzenia od pojęcia konsumenta na rzecz opisywa-

5 A. Mednis, *Prawo ochrony danych osobowych...*, s. 44.

6 Pozyskano z: <https://www.europarl.europa.eu/news/pl/headlines/society/20200918STO87404> sztuczna-inteligencja-szanse-i-zagrozenia. Dostęp: 11.06.2021 r.

7 R. Grygierek, *Rynek e-commerce* (w:) P. Kolenda (red.) *Raport Strategiczny Internet 2019/2020*, IAB Polska, 2020, s. 13.

8 T. Czech, *Komentarz do art. 1, Prawa konsumenta. Komentarz*, wyd. II, Warszawa 2020, s. 18-24.

9 *Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25.10.2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EEG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EEG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady*, Dz.Urz.UE L 304 z dnia 22.11.2011 r., s. 64.

10 *Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11.05.2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EEG, 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 („Dyrektywa o nieuczciwych praktykach handlowych”)*, Dz.Urz.UE L 149 z dnia 11.06.2005 r., s. 22.

11 T. Czech, *Komentarz do art. 1, Prawa konsumenta. Komentarz...*, s. 18-24.

nia adresata przepisów prawa ochrony konsumenta jako użytkownika (ang. *user*)¹². Uważam, że takie rozszerzanie podmiotowego zakresu obowiązywania prawa konsumenckiego, ze względu na zbliżenie się tej dziedziny do technologii cyfrowych, jest słusznym kierunkiem.

Konsumenci podlegają szczególnej ochronie, m.in. na podstawie: art. 4 ust. 2 lit. f TFUE¹³, art. 12 TFUE oraz art. 38 *Karty praw podstawowych Unii Europejskiej*¹⁴. Zakres tej ochrony obejmuje także zagrożenia związane z nadmierną personalizacją i profilowaniem w sieci internetowej. Personalizacja oparta na sztucznej inteligencji (ang. *AI, artificial intelligence*) najczęściej będzie nierozzerwalnie połączona z procesem profilowania. Przy rozpatrywaniu zagadnienia ochrony konsumenta przed nadmierną personalizacją konieczne będzie zatem odniesienie się zarówno do reżimu prawa konsumenckiego, jak i ochrony danych osobowych.

Obecnie aktami prawnymi zawierającymi rozwiązania zmierzające do ochrony konsumentów przed zagrożeniami wynikającymi z personalizacji są: rozporządzenie 2016/679¹⁵, dyrektywa 2002/58/WE o prywatności i łączności elektronicznej¹⁶ oraz dyrektywa 2005/29/WE o nieuczciwych praktykach handlowych. Ogólne rozporządzenie o ochronie danych odpowiada za zapewnienie prawidłowości i przejrzystości procesu profilowania prowadzącego do personalizacji. Dyrektywa 2002/58/WE normuje m.in. kwestię dopuszczalności przechowywania na urządzeniach konsumentów plików *cookie* śledzących aktywność internetową. Z kolei dyrektywa 2005/29/WE zapewnia ochronę konsumentów przed negatywnymi efektami nadmiernej personalizacji w postaci braku wystarczającej świadomości podejmowanych decyzji oraz zniekształcania procesów podejmowania decyzji.

Praktyka pokazała jednak, że konsumenci są na tych polach niedostatecznie wspierani, a samoregulacja dokonywana przez podmioty z branży internetowej nie jest wystarczająca do zapewnienia ochrony ich podstawowych praw. Potrzeba naprawy tej sytuacji została ukazana w unijnej polityce konsumenckiej na lata 2020-2025¹⁷, gdzie zaakcentowano, że sztuczna inteligencja oraz profilowanie, oprócz licznych korzyści, niosą ze sobą także ryzyko naruszenia praw konsumentów. Postuluje się podjęcie działań w postaci m.in. nałożenia na platformy internetowe nowych obowiązków informacyjnych oraz ograniczeń w stosowaniu profilowania w celach *scoringu* kredytowego, co znalazło odzwierciedlenie odpowiednio w projekcie Kodeksu Usług Cyfrowych oraz projekcie rozporządzenia o sztucznej inteligencji. Mają one za zadanie stworzenie bezpieczniejszej przestrzeni cyfrowej dla konsumentów przy równoczesnym umożliwieniu im czerpania korzyści wynikających z transformacji cyfrowej.

12 M. Brożyna, *Konsumenckie prawo do odwołania umowy*, Warszawa 2021, s. 53-62.

13 *Traktat o funkcjonowaniu Unii Europejskiej*, Dz.Urz.UE C 202 z dnia 7.06.2016 r., s. 1.

14 *Karta praw podstawowych Unii Europejskiej*, Dz.Urz.UE C 202 z dnia 7.06.2016 r., s. 389.

15 *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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 z dnia 4.05.2016 r., s. 1 (dalej: RODO, ogólne rozporządzenie o ochronie danych).

16 *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej*, Dz.Urz.UE C 201 z dnia 31.07.2002 r., s. 37 (dalej: dyrektywa o prywatności i łączności elektronicznej, dyrektywa 2002/58/WE).

17 Komunikat Komisji do Parlamentu Europejskiego i Rady, *Nowy program na rzecz konsumentów. Poprawa odporności konsumentów na potrzeby trwałej odbudowy*, COM(2020) 696 final, 2020.

2. Personalizacja stosowana wobec konsumentów

2.1. Definicja personalizacji

Personalizacja nie jest pojęciem zdefiniowanym prawnie, choć występuje w niektórych dokumentach unijnych organów¹⁸. Można ją scharakteryzować jako wyświetlanie dóbr, usług i zdarzeń dostosowanych do potrzeb¹⁹, które odbywa się przy pomocy intensywnego gromadzenia danych i budowania na ich podstawie wiedzy²⁰. Z perspektywy konsumentów personalizacja najczęściej jest utożsamiana z towarami lub usługami dostosowywanymi przed zakupem lub stworzonymi na podstawie danych osobowych²¹. W praktyce oznacza to np. dopasowane do indywidualnych zainteresowań i potrzeb reklamy internetowe, rekomendacje w aplikacjach streamingowych oraz spersonalizowane pod względem ceny oferty usług.

Najprostsza forma personalizacji polega na wykorzystaniu podstawowych informacji o osobie, takich jak imię lub miejsce zamieszkania, w celu wywołania wrażenia, że wyświetlana reklama, oferta, e-mail lub komunikat są stworzone bezpośrednio dla danego konsumenta²². Inne formy personalizacji nie polegają już jedynie na wywoływaniu wrażenia indywidualnego dopasowania, a na faktycznym wykorzystywaniu informacji w celu tworzenia dla konsumentów odpowiednio spersonalizowanego przekazu. W ramach tak rozumianej personalizacji przekazu przedsiębiorcy mogą automatycznie reagować na podejmowaną przez konsumentów aktywność przez dopasowywanie treści oraz oferowanych opcji. Dzięki personalizacji przekaz może być dostarczany w momentach, gdy osoba jest na niego najbardziej podatna.

Na tej podstawie możliwe staje się personalizowanie przekazu na wszystkich etapach kontaktu konsumenta z przedsiębiorcą. Przedsiębiorca może wpłynąć na zachowanie konsumenta już w chwili wyświetlenia mu odpowiednio dopasowanej reklamy lub oferty. W tym celu tworzone są ściśle dopasowane rekomendacje zakupowe oparte na potrzebach i pragnieniach konsumentów. Personalizacja może ujawnić się ponadto na etapie ustalania warunków umownych, np. w postaci dostosowywania ceny usługi. Na wysokość tak dostosowanej do konsumenta ceny może mieć wpływ to, czy utrzymanie zainteresowania danego klienta w dłuższej perspektywie jest opłacalne, jakimi cechami charakteryzuje się określony konsument oraz jaka jest jego skłonność do zapłaty określonej ceny. Najczęściej spotykana jest obecnie personalizacja etapu przedumownego w postaci spersonalizowanych reklam. Z kolei personalizacja warunków umownych w praktyce wciąż jest jeszcze dość rzadko używana przez przedsiębiorców.

18 Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, 2019, s. 16.

19 K. Flis, *Personalizacja, rekomendacja, prosumpcja – trzy wymiary dialogu organizacji i konsumenta*, Handel Wewnętrzny 2015, nr 1 (354), s. 94.

20 A. Jabłowska, M. Kuziemski, A. Nowak, H. Micklitz, P. Pałka, G. Sartor, *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 2018, nr 11, s. 59.

21 Pozyskano z: <https://www.3ds.com/newsroom/press-releases/ces-2020-survey-cite-research-dassault-systemes-consumers-want-personalized-products-wont-wait-them-and-expect-cost-benefit-their-data>. Dostęp: 11.06.2021 r.

22 N.S. Sahni, S.C. Wheeler, P.K. Chintagunta, *Personalization in Email Marketing: The Role of Non-Informative Advertising Content*, Marketing Science 2016, nr 37 (2), s. 236-258.

2.2. Rodzaje personalizacji

Wyróżniamy dwa rodzaje personalizacji: personalizację jawną, która polega na samodzielnym unikaniu przez użytkowników źródeł informacji niezgodnych z ich zainteresowaniami i światopoglądem, oraz personalizację niejawną, która jest dokonywana przez algorytmy filtrujące i nie zawsze opiera się na świadomym wyborze użytkownika Internetu²³. Konsument poprzez przeglądanie treści wywiera wpływ na to, które informacje w przyszłości zostaną mu wyświetlone oraz jaki będzie ich priorytet. Serwisy społecznościowe filtrują informacje tak, by były one jak najbardziej dopasowane do konkretnej osoby i odpowiadały jej zainteresowaniom²⁴. Niniejsza praca będzie się koncentrować na personalizacji niejawnej, a w szczególności na jej dwóch formach: reklamie spersonalizowanej oraz personalizacji warunków umownych.

2.2.1. Reklama spersonalizowana

Spersonalizowana reklama opiera się na określonych cechach, zainteresowaniach i preferencjach danego konsumenta. Możliwe jest dopasowywanie reklamy m.in. pod względem: wyników wyszukiwania, odwiedzonych witryn, czynników demograficznych, położenia geograficznego, zachowania konkretnej osoby w mediach społecznościowych i publikowanych przez nią treści lub informacji pozyskanych przez aplikacje z urządzeń mobilnych²⁵.

Szerszego omówienia wymaga również pojęcie reklamy behawioralnej oraz reklamy kontekstowej, które stanowią dwie odrębne formy reklam spersonalizowanych. Reklama kontekstowa jest jedną z najprostszych i najmniej kontrowersyjnych form reklam ukierunkowanych, która polega na analizowaniu stron pod względem treści, tworzeniu ich profilu tematycznego oraz dostosowywaniu na tej podstawie treści reklam na takiej stronie wyświetlanych²⁶. Przykładem może być wyświetlenie reklamy kocięj karmy na blogu dotyczącym zwierząt. Znacznie więcej wątpliwości wzbudza dopuszczalność niezwykle rozpowszechnionej obecnie reklamy behawioralnej. Opiera się ona na obserwacji zachowań użytkowników oraz ich analizie w celu stworzenia profilu i dostarczenia reklam pasujących do wywnioskowanych zainteresowań, cech i preferencji konsumentów²⁷. Dzięki niej możliwe jest np. wyświetlenie reklamy okularów przeciwsłonecznych osobie, która wcześniej wyszukiwała w Internecie informacji o wyjazdach wakacyjnych. Głównym celem tak inwazyjnej formy reklamy jest zwiększenie tzw. konwersji, czyli stosunku sprzedaży do liczby wyświetleń reklam lub wizyt na określonej stronie.

Obecnie rynek reklamy internetowej, w tym reklamy spersonalizowanej, można określić jako duopol cyfrowy dwóch przedsiębiorstw - Google i Facebooka - które według wyliczeń Europejskiego Obserwatorium Audiowizualnego w 2016 r. odpowia-

23 F.J. Zuiderveen Borgesius, D. Trilling, J. Möller, B. Bodó, C. De Vreese, N. Helberger, *Should we worry about filter bubbles?* Internet Policy Review, nr 5(1), 2016, s. 7.

24 V. Vīķe-Freiberga, H. Däubler-Gmelin, B. Hammersley, L.M. Poiares Pessoa Maduro, *A free and pluralistic media to sustain European democracy*, High Level Group on Media Freedom and Pluralism 2013, s. 27.

25 K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta...*, s. 45.

26 J. Ożegalska-Trybalska, *Internetowa reklama kontekstowa* (w:) M. Namysłowska (red.), *Reklama. Aspekty prawne*, Warszawa 2012, s. 469.

27 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam behawioralnych*, 2010, s. 5.

dały nawet za 85% wzrostu na rynku reklamy cyfrowej²⁸. W 2020 r. spersonalizowane reklamy wygenerowały niemal 98% przychodu Facebooka²⁹. Jednak sposoby przekazywania spersonalizowanych reklam wykraczają już w dużym stopniu poza witryny internetowe. Rozwój nowych technologii doprowadził do powstania m.in. telewizji adresowalnej, dzięki której osoby w sąsiednich domach na tym samym kanale mogą oglądać różne reklamy dopasowane do ich preferencji³⁰. W niedalekiej przyszłości kolejną platformą do udostępniania spersonalizowanych reklam mogą stać się pojazdy autonomiczne, ze względu na szeroki zakres pozyskiwanych przez nie danych oraz możliwość bezpiecznego przeniesienia uwagi kierowcy na inne niż obserwacja otoczenia czynności³¹. Rekomendacje te mogłyby być przekazywane przez asystenta głosowego, wyświetlane na kokpicie, a nawet na przedniej szybie pojazdu.

2.2.2. Personalizacja warunków umownych

Do najczęściej modyfikowanych w wyniku personalizacji elementów umowy należy cena, choć nie jest wykluczone personalizowanie także innych warunków umownych. Konsumenci mogą zapłacić za tę samą usługę lub produkt różne ceny, co będzie zależało np. od posiadanych przez te osoby cech osobowościowych, ich przewidywanych możliwości finansowych lub też momentu, w którym zdecydują się dokonać zakupu. Dzięki temu konsumentowi korzystającemu podczas zakupów internetowych z droższego sprzętu zostanie wyświetlona wyższa cena biletu lotniczego. Podobnie wyższa niż przeciętnie cena może być zaoferowana osobie, która od dłuższego czasu przegląda określone oferty lotów. Wykorzystywana jest wiedza o skłonności danego konsumenta do zapłaty określonej ceny³². Historycznie personalizacja cen wymagała ingerencji człowieka, który bez pomocy algorytmów negocjował warunki umowne z konsumentem³³.

Najbardziej zaawansowane wykorzystanie tego rodzaju personalizacji stosuje obecnie branża ubezpieczeniowa, która coraz częściej oferuje możliwość spersonalizowania stawki ubezpieczenia OC w oparciu o analizę cech ubezpieczonego, np. stylu jazdy³⁴. W takim przypadku może zostać oceniona m.in. szybkość i płynność jazdy oraz częstotliwość jazdy po zmroku danego kierowcy.

Praktyka personalizacji cen może przybrać postać dyskryminacji cenowej, w ramach której przedsiębiorca stosuje różne ceny dla różnych grup konsumentów za te same

28 Rezolucja Parlamentu Europejskiego z dnia 3.05.2018 r. w sprawie pluralizmu mediów i wolności mediów w Unii Europejskiej, 2017/2209(INI). Dz.Urz. C 41 z 6.02.2020, s. 64-75.

29 Pozyskano z: <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx>. Dostęp: 11.06.2021 r.

30 Experian, *Addressable TV. Harness the power of audience data for one-to-one targeting*, 2016, s. 9.

31 A. Nowak, M. Węglowska, M. Gapsa, *Profilowanie na podstawie danych osobowych konsumentów przetwarzanych przez pojazd autonomiczny*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2020, nr 7(9), s. 54-55.

32 Z. Xu, A. Dukes, *Personalization, Customer Data Aggregation, and The Role of List Price*, 2020, s. 2. Pozyskano z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777081. Dostęp: 11.06.2021 r.

33 The Council of Economic Advisers, *Big data and differential pricing*, 2015, s. 12. Pozyskano z: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. Dostęp: 11.06.2021 r.

34 Pozyskano z: <https://payhowyudrive.pl/>. Dostęp: 11.06.2021 r.

towary bądź usługi³⁵. Dyrektywa 2006/123/WE o usługach³⁶ zakazuje dyskryminacji cenowej na podstawie kryterium obywatelstwa i miejsca zamieszkania. Nie wyklucza to jednak możliwości uzasadnienia stosowanych różnic obiektywnymi kryteriami. W tym kontekście można zastanawiać się, czy oferowanie wyższych cen zamożniejszym osobom nosi znamiona dyskryminacji cenowej, czy też jest uzasadnione ich wyższymi możliwościami finansowymi.

Personalizacji cen nie należy mylić z dynamicznym ustalaniem cen. Opiera się ono bowiem na globalnej analizie warunków panujących w danej chwili na rynku, a nie analizie zachowań konkretnego konsumenta. W wyniku zastosowania dynamicznego ustalania cen ceny produktów zyskujących w danym okresie na popularności wśród konsumentów będą zatem wyższe. Coraz częstszą formą dynamicznego ustalania cen są algorytmy cenowe, które automatycznie dostosowują ceny oferowane przez jednego przedsiębiorcę do cen jego rynkowego konkurenta. Niewątpliwie algorytmy te powodują wiele poważnych problemów z punktu widzenia prawa konkurencji, ale ich niekontrolowane użycie pośrednio wywiera też skutki na sytuację konsumentów. Na przykład w marcu 2020 r., na początku rozprzestrzeniania się pandemii COVID-19, z uwagi na duże zainteresowanie konsumentów algorytm cenowy podniósł cenę opakowania ryżu z 10 dolarów do rekordowych 60 dolarów³⁷.

2.3. Pojęcia związane z personalizacją

W praktyce personalizacja nie ma wypracowanej jednolitej definicji i jest wykorzystywana do różnorodnych celów. W związku z tym istnieją również pojęcia, które swoim zakresem pokrywają się z pojęciem personalizacji w sposób częściowy lub niemal całkowicie.

2.3.1. Profilowanie

Profilowanie na gruncie RODO jest jedną z kategorii operacji wykonywanych na danych osobowych³⁸ i stanowi formę ich przetwarzania. W uproszczeniu można określić je jako ocenę osoby, jej charakterystycznych cech i zachowania dokonywaną na podstawie analizy jej wcześniejszego zachowania oraz zachowania innych podobnych do niej osób³⁹. Profilowanie może przybrać formę bezpośrednią, opartą na danych osoby profilowanej, oraz pośrednią, podczas której wnioski na temat danej jednostki są tworzone na podstawie danych o innych, podobnych grupach ludzi⁴⁰. To właśnie

35 O. Bar-Gill, *Algorithmic price discrimination. When demand is a function of both preferences and (mis)perceptions*, University of Chicago Law Review 2018, nr 86, s. 217-254.

36 Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym, Dz.Urz.UE L 376 z 27.12.2006 r., s. 36.

37 Pozyskano z: <https://themarkup.org/ask-the-markup/2020/04/28/why-am-i-paying-60-for-that-bag-of-rice-on-amazon-com>. Dostęp: 11.06.2021 r.

38 P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 (w:) P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017, s. 130-132.

39 A. Mednis, *Prawo ochrony danych osobowych...*, s. 16.

40 A. Mednis, *Prawo ochrony danych osobowych...*, s. 28.

ta druga forma profilowania obarczona jest większym ryzykiem przypisania osobie błędnie wywnioskowanych cech⁴¹.

Profilowanie można podzielić na trzy zasadnicze etapy: zbieranie danych, ich eksploatację w celu odkrycia wzajemnych korelacji oraz wnioskowanie na ich podstawie co do profilu osoby fizycznej⁴². Proces ten może być dodatkowo zakończony podjęciem wobec tak sprofilowanej osoby określonej decyzji⁴³.

Do celów profilowania wykorzystywanych jest wiele różnorodnych danych pochodzących z aktywności internetowej użytkowników. Dane związane z aktywnością można podzielić na: dane dostarczone, dane zaobserwowane oraz dane wywnioskowane⁴⁴. Dane dostarczone są wynikiem samodzielnej aktywności użytkownika, np. przy rejestrowaniu konta w portalu społecznościowym. Jest to zazwyczaj niewielki procent informacji wykorzystywanych w procesie profilowania. Znacznie więcej spostrzeżeń pochodzi z danych zaobserwowanych przekazywanych w związku z korzystaniem z aplikacji, urządzeń lub platform internetowych⁴⁵. Przykładem są różnego typu udostępnienia, reakcje na określone treści oraz współrzędne GPS użytkownika. W katalogu tym mieszczą się też dane zbierane za pośrednictwem osób trzecich, np. informacje o odwiedzonych stronach oraz zakupionych produktach. Ostatnia forma to dane wywnioskowane, czyli tworzone przez administratora na podstawie danych zaobserwowanych i dostarczonych⁴⁶, np. wnioskowanie o stanie zdrowia danej osoby na podstawie historii wyszukiwania oraz lokalizacji wskazującej na częste odwiedzanie placówek medycznych. Dane wywnioskowane stwarzają największe ryzyko dla prywatności konsumentów⁴⁷. Za A. Mednisem należy przyjąć, że dane wywnioskowane składające się na profil, o ile zostaną przypisane do konkretnej osoby, mogą być zakwalifikowane jako dane osobowe bez względu na fakt, czy są one prawdziwe⁴⁸.

Rodzaj wykorzystanych do profilowania danych wiąże się z kwestią zakwalifikowania wytworzonego na ich podstawie profilu jako jawnego lub predykcyjnego. Profil jest zestawem wiadomości charakteryzujących kategorię osób, który ma zostać zastosowany w odniesieniu do danej osoby⁴⁹. Profile formalne są oparte na danych dostarczonych, a profile predykcyjne opierają się na długoterminowej obserwacji zachowań użytkowników⁵⁰, a więc danych zaobserwowanych i wywnioskowanych.

Wzajemna relacja pojęcia personalizacji i profilowania, w tym profilowania określonego w art. 22 RODO, jest niejednoznaczna i zależna od konkretnej sytuacji. Wydaje się, że najczęściej profilowanie będzie wchodziło w zakres pojęcia personalizacji

41 B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 (w:) M. Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 89.

42 M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu i sprzedaży*, Warszawa 2019, s. 84-85.

43 A. Mednis, *Prawo ochrony danych osobowych...*, s. 27.

44 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679*, 2018, s. 8.

45 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 8.

46 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 8.

47 Z. Dávida, *Consumer Rights and Personalised Advertising: Risk of Exploiting Consumer Vulnerabilities*, Socrates 2020, nr 1 (16), s. 79.

48 A. Mednis, *Prawo ochrony danych osobowych...*, s. 191.

49 Rekomendacja CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, 2010, s. 3.

50 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 7.

jako jeden z jej początkowych etapów. Wyświetlanie konsumentowi wyższej ceny produktu na skutek analizy rodzaju używanego do przeglądania stron internetowych urządzenia będzie zarówno profilowaniem w rozumieniu art. 22 RODO, jak i formą personalizacji oferty skierowanej do konsumenta. Niemniej jednak profilowanie ma znacznie szersze pole zastosowań, które nie zawsze będą powiązane z personalizacją, np. w przypadku wykorzystania profilowania w celu prognozowania ryzyka wystąpienia określonej choroby co do zasady nie będziemy mieli do czynienia z personalizacją. Odmienne sytuacja będzie się kształtować, gdy wiedza o zwiększonym ryzyku zachorowania na określoną chorobę zostanie wykorzystana w innych celach, np. rekomendowania suplementów diety.

2.3.2. Targetowanie oraz mikrotargetowanie

Z problematyką personalizacji związane są także terminy targetowania (ang. *targeting*) oraz mikrotargetowania (tzw. targetowanie niszowe, ang. *niche targeting*). Pojęcie targetowania można dostrzec w dokumentach z zakresu ochrony danych osobowych i definiowane jest ono jako próba odwołania się do osoby lub grupy lub wywarcia na nich jakiegoś wpływu, na przykład w celu marketingowym lub politycznym⁵¹. Praktyka ta polega na wybieraniu osób będących zamierzonymi odbiorcami określonych treści (tzw. grupa docelowa) i kierowaniu do tak określonej grupy treści na podstawie parametrów lub kryteriów⁵². Jest to możliwe dzięki prowadzeniu segregacji użytkowników z uwagi na różnorodne kategorie społeczne, kulturowe, religijne i ekonomiczne⁵³. Niektórzy autorzy wyróżniają dodatkowo pojęcie mikrotargetingu, które jest bardziej inwazyjne od targetowania. Oparte jest ono na precyzyjnym doborze przekazu do wąskiej grupy odbiorców⁵⁴.

Różnica między personalizacją a targetowaniem i mikrotargetowaniem polega na tym, że w przypadku personalizacji dostawca dostosowuje treść przekazu do konkretnej grupy odbiorców, np. dla rodzin z małymi dziećmi gazetka promocyjna zostanie spersonalizowana w ten sposób, że będzie zawierać produkty, które wzbudzą zainteresowanie rodziców. Z kolei w przypadku targetowania dostawca treści określa docelową grupę osób, do których przygotowany przez niego przekaz powinien trafić, np. decyduje, że gazetka promocyjna z przewagą produktów dla dzieci trafi do osób posiadających małe dzieci, mieszkających w dużych miastach. Efekt w postaci dostarczenia osobom zainteresowanym gazetkami z produktami dla dzieci pozostaje taki sam w obu przypadkach. Na potrzeby niniejszej pracy, ze względu na subtelne różnice między pojęciami targetowania i mikrotargetowania oraz personalizacji, pojęcia te będą traktowane synonimicznie.

3. Sztuczna inteligencja wykorzystywana na potrzeby personalizacji

Narzędzia oparte na sztucznej inteligencji w ostatnich latach przeżywają gwałtowny rozkwit. Są już na tyle istotnym elementem życia konsumentów, że znalazły odzwier-

51 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting of social media users*, Version 2.0, 2021, s. 4.

52 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 4.

53 Komitet Ministrów Rady Europy, Deklaracja z dnia 13.02.2019 r. w sprawie możliwości manipulacyjnych procesów algorytmicznych, 2019, s. 1.

54 O. Barbu, *Advertising, Microtargeting and Social Media*, *Procedia - Social and Behavioral Sciences* 2014, nr 163, s. 46.

ciedlenie w unijnej polityce konsumenckiej na lata 2020-2025. Większość działań marketingowych przedsiębiorców obecnie jest częściowo lub całkowicie zautomatyzowana, a za proces profilowania i będącą jego efektem personalizację treści odpowiedzialna jest coraz częściej sztuczna inteligencja.

3.1. Definicja sztucznej inteligencji oraz jej rodzaje

Sztuczna inteligencja nie ma jednej, powszechnie uznanej definicji. W zależności od sposobu jej wykorzystywania definicje mogą się między sobą różnić. Jako jedną z bardziej uniwersalnych definicji można wskazać tę, sformułowaną przez Grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji, która określa sztuczną inteligencję jako oprogramowania komputerowe, działające w wymiarze fizycznym lub cyfrowym poprzez postrzeganie otoczenia dzięki gromadzeniu danych, ich interpretacji, rozumowaniu na podstawie wiedzy lub przetwarzaniu informacji pochodzących z danych oraz podejmowaniu jak najlepszych decyzji w celu osiągnięcia założonego efektu⁵⁵. W praktyce legislacyjnej pojawia się wiele rozbieżności co do sposobu normowania terminu sztucznej inteligencji. Przykładem może być projekt rozporządzenia o sztucznej inteligencji⁵⁶, w którym zamiast definicją sztucznej inteligencji posłużono się definicją systemu SI. Zgodnie z nim jest to oprogramowanie, które zostało opracowane przy użyciu m.in. metod uczenia maszynowego lub *deep learningu* oraz może - dla danego zestawu celów określonych przez człowieka - generować wyniki takie jak: treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję⁵⁷.

Z uwagi na zakres niniejszej pracy odpowiednią definicją sztucznej inteligencji wykorzystywanej w celu personalizacji oraz związanego z tym procesu profilowania jest definicja sformułowana przez A. Kaplana oraz M. Haenleina, tj.: „zdolność systemu do poprawnej interpretacji zewnętrznych danych, aby uczyć się z takich danych i wykorzystywać tę wiedzę do osiągnięcia określonych celów dzięki adaptacji”⁵⁸. Definicja ta odnosi się bowiem w przeważającym stopniu do systemów cyfrowych oraz kładzie nacisk na aspekt interpretacji danych i wykorzystywania wytworzonych w ten sposób wniosków. Wnioskowanie jest istotnym elementem szeroko rozumianej personalizacji, gdyż na nim opiera się metoda jej działania - w celu znalezienia przydatnych powiązań analizie poddawane są ogromne wolumeny danych o aktywności konsumentów⁵⁹.

Pojęcie sztucznej inteligencji jest szerokim zbiorem, obejmującym m.in. podkategorię uczenia maszynowego (ang. *machine learning*). Uczenie maszynowe jest jednym ze sposobów służących ulepszeniu i przyspieszeniu procesu znajdowania rozwiązania⁶⁰. Systemy uczenia maszynowego, niezależnie od ich twórców, potrafią ulepszać

55 Grupa ekspertów wysokiego szczebla ds. SI, *Definicja SI: główne funkcje i dyscypliny naukowe*, 2019, s. 16.

56 Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final, (dalej: projekt rozporządzenia o sztucznej inteligencji).

57 Artykuł 4 ust. 1 projektu rozporządzenia o sztucznej inteligencji.

58 A. Kaplan, M. Haenlein, *Siri, Siri, in my hand, Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, Business Horizons 2019, nr 62, s. 15-25.

59 O. Ben-Shahar, *Data Pollution*, Journal of Legal Analysis 2019, nr 11, s. 114.

60 FIGI Security, Infrastructure and Trust Working Group, *Big data, machine learning, consumer protection and privacy*, 2020, s. 12.

swoje działanie dzięki rosnącemu doświadczeniu lub coraz większej ilości dostarczanych danych, które są poddawane analizie⁶¹. Mechanizmy te z powodzeniem są stosowane w systemach rekomendacji produktów i treści oraz w przypadku targetowania reklam opartego na identyfikacji osób z podobnymi cechami (ang. *look-alike evaluation*⁶²). Dzięki temu można przewidywać, czego i kiedy będzie potrzebował dany klient, a także jakie jest prawdopodobieństwo dokonania przez niego kolejnego zakupu⁶³.

W kategorii uczenia maszynowego można z kolei wyróżnić podkategorię nazywaną uczeniem głębokim (ang. *deep learning*). Wykorzystuje ona sieć neuronową, by samodzielnie weryfikować swoją poprawność, co pozwala na niemal całkowitą eliminację udziału człowieka⁶⁴. Uczenie głębokie jest wykorzystywane m.in. do przetwarzania języka naturalnego (ang. *natural language processing*, NLP). Polega ono na umożliwieniu maszynom wydobywania informacji i znaczeń z ludzkiego języka w celu podejmowania w oparciu o nie decyzji⁶⁵. NLP jest wykorzystywane w przypadku inteligentnych korektorów, wirtualnych asystentów, chatbotów oraz filtrowania spamu. Zaawansowane NLP pozwalają na analizę ludzkiego języka pod kątem kontekstu wypowiedzi oraz jej pozytywnego lub negatywnego wydźwięku⁶⁶.

Wszystkie wymienione wyżej dziedziny i podkategorie są częścią pojęcia sztucznej inteligencji i z powodzeniem są stosowane do osiągnięcia celu, jakim jest personalizacja przekazu. Algorytmiczna analiza w pierwszej kolejności ma za zadanie stworzenie szczegółowego profilu konsumenta⁶⁷, a następnie skierowanie do tak sprofilowanej osoby odpowiednio dobranych treści i cen. Im więcej różnorodnych danych zostanie dostarczonych algorytmom sztucznej inteligencji, tym personalizacja będzie bardziej dokładna i poprawna. Mimo możliwości osiągnięcia personalizacji na wiele sposobów to wybór konkretnej techniki sztucznej inteligencji może mieć duże znaczenie z punktu widzenia skuteczności personalizacji – działania reklamowe oparte na technice *deep learning* mogą być do 50% bardziej skuteczne niż klasyczne formy *machine learning*⁶⁸.

3.2. Metoda działania sztucznej inteligencji w procesie personalizacji

Dostępne obecnie narzędzia służące do monitorowania i analizowania aktywności konsumentów obejmują: pliki *cookie*, piksele śledzące, odciski palców przeglądark, sygnały nawigacyjne, adresy IP, współrzędne GPS i wiele innych⁶⁹. Za ich pomocą są pozyskiwane różnorodne dane dotyczące aktywności przeglądania sieci, np. in-

61 Pozyskano z: <https://www.elementsofai.com/>. Dostęp: 11.06.2021 r.

62 Pozyskano z: <https://patents.google.com/patent/US10380501B2/en>. Dostęp: 11.06.2021 r.

63 M.A. Zieliński, A. Czerniak, S. Dąbek, J. Żylińska (red.), *Iloraz sztucznej inteligencji. Potencjał AI w polskiej gospodarce*, Warszawa 2018, s. 16.

64 Pozyskano z: <https://www.elementsofai.com/>. Dostęp: 11.06.2021 r.

65 M. Biéri, F. Vallet, I. Corbara, P. Faget, B. Guley, E. Hary, J. Hirtz (w:) B. Pailhès (red.), *On the record. Exploring the ethical, technical and legal issues of voice assistants*, Commission Nationale de l'Informatique et des Libertés 2020, s. 19.

66 V. Bashyakarla, S. Hankey, A. Macintyre, R. Rennó, G. Wright, *Personal Data: Political Persuasion Inside the Influence Industry. How it works*, Tactical Tech's Data and Politics team 2019, s. 64.

67 Fundacja Panoptykon, raport *Kto (naprawdę) Cię namierzył? Facebook w polskiej kampanii wyborczej*. Pozyskano z: <https://panoptykon.org/ktocienamierzyl-raport>. Dostęp: 11.06.2021 r.

68 Ł. Abgarowicz (w:) *Perspektywy rozwojowe reklamy online w Polsce*, IAB Polska 2018, s. 24.

69 Zob. V. Bashyakarla, S. Hankey, A. Macintyre, R. Rennó, G. Wright, *Personal Data: Political Persuasion...*, s. 54-55.

formacje o odwiedzonych stronach i miejscach, dokonanych zakupach, informacje o ruchach myszy i otwartych oknach. Używane w celu przeglądania sieci urządzenia mogą się również stać źródłem wielu istotnych danych, np. o: używanym systemie operacyjnym, identyfikatorach pochodzących z gier, kont i aplikacji, pobliskich nadajnikach sieci komórkowej, a nawet przetrzymywanych na nich zdjęciach i kontaktach⁷⁰. Zyskującą na znaczeniu kategorią urządzeń zbierających dane o konsumentach są urządzenia *smart home* i inteligentne liczniki. Każde z takich urządzeń podłączonych do lokalnej sieci jest w stanie zbierać i przysyłać dane o tym, co dzieje się w domu, jakie są zwyczaje jego domowników, styl życia, godziny snu, zainteresowania. Urządzenia te są w stanie komunikować się ze sobą, co budzi kolejne problemy związane z prywatnością⁷¹. Z jednej strony informacje te w połączeniu z innymi danymi posiadanymi przez agencje marketingowe pozwalają na zastosowanie jeszcze bardziej spersonalizowanych reklam⁷². Z drugiej strony, w przypadku urządzeń *smart home*, ryzyko błędnej personalizacji jest duże, gdyż z urządzeń tych korzysta zazwyczaj kilku domowników.

Samo zgromadzenie dużej ilości danych nie jest wystarczające. Dane uzyskują bowiem swoją wartość przez ich właściwy dobór oraz możliwość ich wykorzystania⁷³. Podstawowym sposobem wykorzystywania danych w przypadku personalizacji jest poddanie ich analizie przez algorytmy sztucznej inteligencji. Analizy przeprowadzane na dużych zbiorach zgromadzonych danych zwykło nazywać się pojęciem *Big Data*⁷⁴. Ich celem jest eksploracja i wykorzystywanie wzajemnych korelacji między danymi w celu konstruowania modeli predykcyjnych⁷⁵. Analizy *Big Data* wpłynęły na szybszy rozwój nowych technologii, np.: autonomicznych pojazdów, idei *smart cities*, inteligentnego przewidywania chorób i przestępstw. W dziedzinie marketingu analizy te są wykorzystywane do przewidywania osobistych preferencji i zachowań konsumentów oraz decydowania o zastosowaniu spersonalizowanych rabatów, ofert specjalnych i reklam behawioralnych⁷⁶.

Algorytmy przekształcają dane wejściowe na określone atrybuty służące do kierowania przekazu⁷⁷, a więc tworzą profil danej osoby (tzw. *data mining*). Każdy użytkownik ma swój własny zestaw atrybutów, na podstawie których reklamodawcy mogą dokonywać personalizacji wyników wyszukiwania, kształtować preferencje użytkowników oraz poddawać ich działaniom opartym na marketingu behawioralnym⁷⁸. Im więcej różnorodnych danych uda się zebrać, tym większa szansa na znalezienie korelacji o większym stopniu dokładności.

70 K. Szymielewicz, W. Adamska, *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?* 2017, s. 10-11.

71 Rezolucja Parlamentu Europejskiego z dnia 16.02.2017 r. zawierające zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, Dz.Urz.UE C 252 z dnia 18.07.2018 r., s. 25.

72 M. Biéri, F. Vallet, I. Corbara, P. Faget, B. Guley, E. Hary, J. Hirtz (w:) B. Pailhès (red.), *On the record...*, s. 27.

73 M. Kibil (w:) M. Gawroński (red.), *RODO Przewodnik ze wzorami*, Warszawa 2018, s. 244.

74 M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 391-394.

75 C. Devins, T. Felin, S. Kauffman, R. Koppl, *The Law and Big Data*, 27 Cornell J. L. & Public Policy 357 (2017), s. 363-365.

76 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 45.

77 A. Andreou, G. Venkatadri, O. Goga, K.P. Gummadi, P. Loiseau, A. Mislove, *Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations*, Network and Distributed Systems Security (NDSS) Symposium 2018, s. 3.

78 Komitet Ministrów Rady Europy, Deklaracja z dnia 13.02.2019 r. w sprawie możliwości manipulacyjnych procesów algorytmicznych, 2019, s. 1.

Algorytmy powinny charakteryzować się poprawnością, efektywnością i skończonością. Poprawny algorytm jest uniwersalny, rozumiały i znajduje rozwiązanie dla postawionego przed nim zadania. Efektywność polega na jak najmniejszym stopniu złożoności algorytmu, natomiast o skończoności algorytmu można mówić w sytuacji, gdy gwarantuje on znalezienie rozwiązania w skończonej liczbie kroków⁷⁹.

Wnioski płynące z analizy danych są formułowane z określonym prawdopodobieństwem, które wynika z zastosowanych modeli statystycznych⁸⁰. Zawsze istnieje więc ryzyko uzyskania nieprawidłowego wniosku, za które mogą być odpowiedzialne na przykład: zła jakość danych, masowy charakter przetwarzania lub połączenie danych z różnych źródeł, które zwielokrotnia błędy tkwiące w zbiorach źródłowych⁸¹. Biorąc jednak pod uwagę fakt, że na podstawie 68 „polubień” na Facebooku badacze są w stanie określić m.in.: kolor skóry, orientację seksualną oraz preferencje polityczne jego użytkownika z prawdopodobieństwem wahającym się od 85% do 95%⁸², można stwierdzić, że skuteczność modeli statystycznych już dziś jest bardzo wysoka.

4. Oddziaływanie personalizacji opartej na sztucznej inteligencji na konsumentów

4.1. Korzyści wynikające z personalizacji opartej na sztucznej inteligencji

Personalizacja bez wątpienia na stałe wpisała się już w obraz cyfrowej rzeczywistości konsumentów i przedsiębiorców. Z uwagi na przyrost liczby przedsiębiorców działających w branży *e-commerce*, ale też większą chęć konsumentów do zakupów *online*, konieczność korzystania z systemów algorytmicznych opierających swoje działanie na personalizacji treści z roku na rok będzie coraz większa⁸³. Obie grupy mogą czerpać z zastosowywania tych metod pewne korzyści.

4.1.1. Zindywidualizowanie treści i usług kierowanych do konsumentów

Na wczesnym etapie rozwoju Internetu dostęp do globalnego rynku i możliwości uzyskiwania, weryfikowania i porównywania informacji o produktach i ich cenach wzmocnił siłę rynkową konsumenta w stosunku do przedsiębiorców⁸⁴. Obecnie rynek internetowy stał się jednak zbyt duży do komfortowego korzystania z niego przez konsumentów. Tempo przyrostu treści internetowych, w tym informacji kształtujących świadomość społeczną i polityczną, w znacznym stopniu ogranicza zdolność konsumenta do podejmowania świadomych decyzji zakupowych i światopoglądowych. Przeladowanie informacyjne jest łagodzone dzięki personalizacji.

Platformy społecznościowe stosują algorytmiczne filtrowanie wyświetlanych wiadomości w oparciu o wywnioskowane przez algorytm oraz wybrane przez użytkowników

79 A. Mednis, *Prawo ochrony danych osobowych...*, s. 34.

80 A. Mednis, *Prawo ochrony danych osobowych...*, s. 16.

81 M. Rojszczak, *Ochrona prywatności...*, s. 397-402.

82 A. Mednis, *Prawo ochrony danych osobowych...*, s. 31.

83 E. Sadowska, M. Pogorzelska, K. Balewski, *Display* (w:) P. Kolenda (red.), *Raport Strategiczny Internet 2019/2020*, IAB Polska 2020, s. 21.

84 G. Sartor, *New aspects and challenges in consumer protection. Digital services and artificial intelligence*, Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2020, s. 10.

dziedziny⁸⁵. Dzięki temu konsument jest w stanie wybrać najlepiej dopasowane do niego rozwiązanie. Personalizacja jest narzędziem, które ułatwia kontakt z osobami dzielącymi podobne zainteresowania i przekonania⁸⁶. Rekomendacje zakupowe oraz spersonalizowane reklamy i oferty dają także możliwość usprawnienia procesu wyszukiwania interesującej kategorii produktów i usług oraz sfinalizowania zakupu w krótszym czasie⁸⁷. Zastosowanie personalizacji w dziedzinie reklam internetowych sprawia natomiast, że wyświetlane na stronach internetowych banery są mniej uciążliwe⁸⁸. Spersonalizowana przestrzeń internetowa staje się tym samym bardziej interesująca i nie przytłacza konsumentów.

Z kolei profilowanie prowadzące do personalizacji warunków cenowych usługi sprawia, że oferty są konstruowane w sposób bardziej zindywidualizowany i przejrzysty dla konsumentów⁸⁹. Przykład może stanowić branża ubezpieczeniowa, gdzie wykorzystanie profilowania w celu różnicowania cen składek ubezpieczeniowych jest coraz powszechniejsze i pozwala na bardziej precyzyjne oszacowanie ryzyka ubezpieczeniowego i efektywny podział kapitału⁹⁰. Dzięki temu oferta ubezpieczenia dla osoby dbającej o swoje zdrowie w wyniku zastosowania profilowania może być korzystniejsza pod kątem finansowym niż oferta przedstawiona nałogowemu palaczowi. Ryzyko kolizji w przypadku osoby prowadzącej samochód zgodnie z przepisami ruchu drogowego jest mniejsze, a zatem składka ubezpieczenia OC potencjalnie będzie niższa. Świadome ograniczenie przez konsumentów swojej prywatności może więc przynosić im zauważalne korzyści finansowe, na co większość z nich jest skłonna się zgodzić⁹¹. Co więcej, przeświadczenie o tym, że oferta została przygotowana specjalnie z myślą o danym konsumentcie pozytywnie wpływa na odbiór przedsiębiorcy przez konsumentów⁹². Konsumentci doceniają znaczenie personalizacji, w szczególności w dziedzinie zdrowia i bezpieczeństwa osobistego, choć równocześnie podziwiają oni obawy co do sposobu gromadzenia ich danych i zarządzania nimi⁹³. Są oni skłonni zapłacić za spersonalizowaną usługę lub produkt średnio o 25% więcej, ale w zamian za udostępnienie swoich danych w tym celu oczekują rekompensaty na podobnym poziomie⁹⁴. Co ciekawe, duża część konsumentów nie dostrzega żadnych istotnych korzyści z personalizacji⁹⁵.

4.1.2. Bezpłatny dostęp do treści za sprawą monetyzacji danych konsumentów

Nadawanie usługom i produktom indywidualnego charakteru jest opłacalne również dla przedsiębiorców. Pozwala na wyróżnienie przekazu przedsiębiorcy spośród wielu

85 Motyw 62, 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.

86 K. Hosanagar, D. Fleder, D. Lee, A. Buja, *Will the Global Village Fracture into Tribes? Recommender Systems and their Effects on Consumer Fragmentation*, Management Science 2014, nr 60 (4), s. 805–823.

87 A. Mednis, *Prawo ochrony danych osobowych...*, s. 8.

88 W. Wang, L. Yang, Y. Chen, Q. Zhang, *A privacy-aware framework for targeted advertising*, Computer Networks 2015, nr 79, s. 17.

89 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 5.

90 PwC, *Insurance 2020: The digital prize - Taking customer connection to a new level*, 2020, s. 10.

91 PwC, *Insurance 2020: The digital prize - Taking customer connection to a new level*, 2020, s. 5.

92 KPMG.pl, *[Cyfrowy] klient nasz pan. Jak marki na polskim rynku zarządzają doświadczeniami klientów*, 2019, s. 13–14.

93 Pozyskano z: <https://www.3ds.com/...>

94 Pozyskano z: <https://www.3ds.com/...>

95 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 124–128.

innych komunikatów. Cieszy się dużą popularnością, na którą wpływają: stosunkowo niskie koszty monitoringu użytkowników w sieci, wysoka skuteczność predykcji⁹⁶ oraz elastyczne możliwości zastosowań tego narzędzia. To wszystko przekłada się na niższe koszty prowadzenia kampanii marketingowych, a zatem niższe ceny towarów dla konsumentów⁹⁷.

Oprócz zmniejszenia kosztów zbierane w celu profilowania dane osobowe potrafią wygenerować także osobne zyski uzyskane przez dalszą odsprzedaż danych innym podmiotom, takim jak: ubezpieczyciele, partie polityczne lub pracodawcy⁹⁸. Szacowano, że wartość danych osobowych przechowywanych w przestrzeni internetowej do 2020 r. osiągnie 1 bilion euro rocznie⁹⁹.

Monetyzacja zbieranych danych jest dodatkowo powiązana z szerszą możliwością udostępniania usług i treści w sposób „nieodpłatny” dla użytkowników. Ze względu na stosunek konsumentów do prawa do prywatności można podzielić ich na: osoby, które nie mają świadomości zagrożeń związanych z udostępnianiem przez siebie danych, osoby pragmatyczne, które mają świadomość zagrożeń, ale udostępniają dane w zamian za otrzymywane korzyści, oraz osoby świadome zagrożeń, ale niezwracające zbyt dużej uwagi na swoją prywatność¹⁰⁰. Dla wielu pragmatycznych konsumentów barter swoich danych osobowych w zamian za możliwość nieodpłatnego korzystania z usług i przeglądania treści jest uznawany za sprawiedliwy. Według takich osób korzyści przeważają nad stratami, które mogą wiązać się z udostępnieniem swoich danych¹⁰¹. Bardzo możliwe, że w przyszłości takie ograniczenie prywatności będzie szeroko akceptowaną regułą. W mojej opinii obecnie korzyści wynikające z udostępnienia danych osobowych nie są na tyle duże, by rezygnować z kontroli nad prywatnością.

4.2. Zagrożenia wynikające z personalizacji opartej na sztucznej inteligencji

Choć niewątpliwie personalizacja ma szerokie zastosowanie i niesie ze sobą określone korzyści, to niebezpieczeństwa z niej wynikające są równie istotne. Zaawansowane narzędzia analityczne negatywnie wpływają na równowagę ekonomiczną i informacyjną między przedsiębiorcami i konsumentami¹⁰². Pozornie korzystne funkcje personalizacji, takie jak: dostosowywanie reklam, rekomendowanie treści lub oferowanie bezpłatnych treści w zamian za dane osobowe, mogą wiązać się też z poważnymi zagrożeniami dla konsumentów.

4.2.1. Manipulowanie zachowaniem konsumenta przez wykorzystanie mechanizmów wykrywania emocji

Przełomowe wydarzenia w życiu ludzi mogą istotnie zaburzać ich zdolność racjonalnego myślenia. Tę przejściową wrażliwość i potencjalnie większą podatność na wpły-

96 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 4.

97 A. Mednis, *Prawo ochrony danych osobowych...*, s. 27.

98 K. Szymielewicz, W. Adamska, *Śledzenie i profilowanie w sieci: W czym problem?*..., s. 3.

99 Pozyskano z: <https://www.ft.com/cms/s/0/5fd7d8a8-28e5-11e2-b92c-00144feabdc0.html>. Dostęp: 11.06.2021 r.

100 A. Mednis, *Prawo ochrony danych osobowych...*, s. 92.

101 E. Milczarek, *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w internecie*, Warszawa 2020, s. 81.

102 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 46.

wy zewnętrzne starają się wykorzystywać reklamodawcy przez podświadome wpływanie na emocje oraz działania podejmowane przez ludzi¹⁰³. Ich celem jest dotarcie do osób w momentach, w których są najbardziej wrażliwi na określony przekaz.

Przy pomocy algorytmów identyfikujących zainteresowania poszczególnych konsumentów można wykryć ich potencjalne słabości, np. zły stan emocjonalny lub fizjologiczny¹⁰⁴. W oparciu o tę wiedzę możliwe jest wyświetlanie oddziałujących na konsumentów reklam oraz dostosowywanie cen. Osoba, która straciła pracę i ma problemy finansowe, może być bardziej podatna na reklamy oferujące pożyczki na wysoki procent. Z kolei dla kogoś, kto zmaga się z otyłością, reklama planu żywieniowego może okazać się atrakcyjna bez względu na cenę promowanej usługi. Targetowane reklamy mogą zostać wykorzystane, żeby dotrzeć do zadłużonych osób posiadających nieruchomości i zachęcić je do ich sprzedaży poniżej ceny rynkowej¹⁰⁵. Warto przytoczyć przykład pandemii COVID-19, która stworzyła nowe problemy społeczne i gospodarcze. Konsumenci niejednokrotnie podejmują irracjonalne decyzje zakupowe spowodowane strachem i niepewnością¹⁰⁶.

Z punktu widzenia wykorzystywania emocji w personalizowaniu przekazu marketingowego warto zwrócić uwagę, że algorytmy potrafią analizować również cechy osobowości konsumentów, zgodnie z tzw. modelem wielkiej piątki (ang. *Big Five*)¹⁰⁷. W ten sposób, w zależności od stopnia: neurotyczności, ekstrawersji, otwartości na nowe doświadczenia, ugodowości oraz sumienności, reklamodawcy mogą przygotowywać odpowiednio dobrany przekaz, odwołujący się na przykład do skłonności konkretnego konsumenta do zachowań kompulsywnych.

Należy zaznaczyć, że największe firmy na rynku reklamy internetowej zabraniają kierowania reklam, które wykorzystują wiedzę o niektórych osobistych trudnościach konsumentów. Facebook zakazuje reklam zawierających treści dotyczące m.in. statusu finansowego i schorzeń¹⁰⁸. Z kolei Google nie dopuszcza reklam, które odwołują się do kwestii: zdrowotnych, osobistych niepowodzeń, traumatycznych przeżyć¹⁰⁹. Przeglądając się bliżej stosowanym przez nich regulaminom reklamowym, można dostrzec sporo wyjątków, które łagodzą wymienione powyżej zakazy. Warto w tym kontekście wspomnieć o informacjach, które wyciekły w 2017 r. z biura Facebooka w Australii. Okazało się wtedy, że Facebook pozwala na wykorzystywanie stanu emocjonalnego nawet 14-letnich użytkowników w celu profilowania reklam. Możliwe było wykorzystywanie atrybutów takich jak: „niepewny swojej wartości”, „zestresowany” i „przechodzący kryzys życiowy”¹¹⁰.

103 Komitet Ministrów Rady Europy, Deklaracja z dnia 13.02.2019 r. w sprawie możliwości manipulacyjnych procesów algorytmicznych, 2019, s. 2.

104 A. Jabłonowska, M. Kuziemski, A. Nowak, H. Micklitz, P. Pałka, G. Sartor, *Consumer Law and Artificial Intelligences...*, s. 60.

105 Pozyskano z: <http://jakrobicmarketing.pl/jak-znalezc-zadluzonego-wlasciciela-mieszkania-ktory-chce-je-sprzedac-mozliwosci-ultraprecyzyjnego-targetowania-reklamy-na-facebook/>. Dostęp: 11.06.2021 r.

106 Pozyskano z: https://ec.europa.eu/info/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#sweep2020. Dostęp: 11.06.2021 r.

107 A. Porat, L.J. Strahilevitz, *Personalizing default rules and disclosure with big data*, Michigan Law Review 2014, nr 112, s. 1437.

108 Pozyskano z: <https://www.facebook.com/business/help/711488016082996?id=986554971804174&helpref=search&sr=20&query=personalizacja%20reklam>. Dostęp: 11.06.2021 r.

109 Pozyskano z: <https://support.google.com/adspolicy/answer/143465#547>. Dostęp: 11.06.2021 r.

110 K. Szymielewicz, W. Adamska, *Śledzenie i profilowanie w sieci: W czym problem?*, s. 17.

Z kolei Google pozwala reklamodawcom kierować przekaz marketingowy do użytkowników, którzy są w przetomowych momentach ich życia ze względu na np.: zawarcie związku małżeńskiego, zakup domu lub moment przejścia na emeryturę¹¹¹. Różnicowanie dopuszczalności kierowania reklam w zależności od faktu, czy konsument doświadcza nieprzyjemnego albo szczęśliwego wydarzenia, wydaje się nieuzasadnione. Ograniczenie zdolności do racjonalnego podejmowania decyzji może wystąpić w obu przypadkach.

4.2.2. Utrata kontroli nad przekazanymi danymi

Personalizacja przekazu jest związana w sposób nierozzerwalny z dużą ilością danych generowanych za pośrednictwem Internetu i zbieranych przez różnorodnych pośredników. Wiąże się to z ryzykiem utraty możliwości efektywnego zarządzania udostępnionymi danymi oraz potencjalnym naruszeniem prawa do prywatności przez ingerencję w uprawnienie do decydowania o zakresie informacji osobistych, które udostępnia się innym osobom¹¹².

Jak wynika z sondażu Eurobarometru przeprowadzonego w 2016 r., 72% ankietowanych konsumentów niepokoiło się procederem zbierania ich danych osobowych, przy czym aż 56% ankietowanych przyznało, że nie zwraca uwagi na regulaminy działania platform internetowych¹¹³. Z uwagi na postępujący proces digitalizacji, przyspieszony w dużej mierze za sprawą epidemii COVID-19, można wysunąć tezę, że konsumenci są obecnie jeszcze bardziej zaniepokojeni ochroną swoich danych osobowych. Ponadto, ze względu na wprowadzony przez RODO obowiązek informacyjny, większa liczba konsumentów zyskała świadomość na temat skali przetwarzania ich danych osobowych¹¹⁴. Do tej pory był to dla niektórych osób proces zupełnie niewidoczny.

W dalszym ciągu zdecydowana większość konsumentów nie zdaje sobie sprawy z ilości podmiotów zewnętrznych, którym przekazywane są ich dane za pomocą jednorazowo udzielonej zgody. Uniemożliwia to realną kontrolę nad ich wykorzystywaniem i utrudnia podmiotom danych korzystanie z przysługujących im praw. Niekiedy konsumenci nie są nawet proszeni o zgodę, gdyż ich dane zbierane są z przestrzeni ogólnodostępnej na podstawie innych przesłanek przetwarzania¹¹⁵. Nawet jeśli użytkownikowi uda się dotrzeć do właściwego podmiotu, próba uzyskania dostępu do danych tworzących jego profil najczęściej kończy się odmową. Brokerzy danych posługują się przy tym argumentacją, że dane użytkownika są zanonimizowane lub w ogóle nie są danymi osobowymi, gdyż nie identyfikują osoby fizycznej¹¹⁶. Takie wyjaśnienie należy uznać za nietrafne. Przyjmuje się, że dane osobowe są zanonimizowane, gdy są przetworzone w takim stopniu, który uniemożliwia ich ponowne

111 Pozyskano z: <https://support.google.com/google-ads/answer/6383030?hl=pl>. Dostęp: 11.06.2021 r.

112 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość, prywatność - aspekty prawne*, Warszawa 2020, s. 6-11.

113 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Platformy internetowe i jednolity rynek cyfrowy. Szanse i wyzwania dla Europy*, COM/2016/0288 final, 2016, s. 11.

114 Europejski Inspektor Ochrony Danych, *Opinia 3/2018, EDPS Opinion on online manipulation and personal data*, 2018, s. 7.

115 V. Bashyakarla, S. Hankey, A. Macintyre, R. Rennó, G. Wright, *Personal Data: Political Persuasion...*, s. 66.

116 K. Iwańska, *To track or not to track? Towards privacy-friendly and sustainable online advertising*, Panoptykon Foundation 2020, s. 15.

przypisanie do konkretnych osób¹¹⁷. Choć jest to skuteczny sposób na ochronę danych w wielu dziedzinach wykorzystujących sztuczną inteligencję, to w przypadku branży reklam behawioralnych taka anonimizacja jest niecelowa ze względu na zakładany skutek dokonywanej analizy - możliwości przypisania ich do konkretnego użytkownika i wyświetlenia na tej podstawie spersonalizowanej reklamy. Twierdzenie bowiem, że osoby są niemożliwe do zidentyfikowania, podczas gdy celem przetwarzania jest identyfikacja, zawiera w sobie wewnętrzną sprzeczność¹¹⁸.

Najczęściej wykorzystywanym sposobem ochrony danych jest ich pseudonimizacja, którą RODO w art. 4 pkt 5 definiuje jako przetwarzanie danych osobowych w taki sposób, że nie można ich już przypisać konkretnej osobie bez wykorzystania dodatkowych informacji. Informacje te są przechowywane oddzielnie i w sposób zapewniający, że dane osobowe nie zostaną przypisane do osoby fizycznej¹¹⁹. W przypadku użytkowników platform internetowych najczęściej nadaje się im odpowiednie ID, które umożliwia odszyfrowanie danych osobowych. Pomimo zastosowania pseudonimizacji dane składające się na profil użytkownika w dalszym ciągu stanowią dane osobowe¹²⁰. Gdy dane umożliwiają identyfikację lub ponowną identyfikację osoby, wciąż mają zastosowanie zasady ochrony danych osobowych¹²¹.

Trzeba zauważyć, że dane osobowe prowadzące bezpośrednio do identyfikacji użytkownika nie są w personalizacji reklam przydatne w takim stopniu jak dane, które wskazują na cechy osobowości i zainteresowania danej osoby. Ważniejszym od imienia i nazwiska źródłem rozpoznawania użytkownika Internetu są jego indywidualne identyfikatory reklamowe, na podstawie których podmioty z branży reklamowej są w stanie wymieniać się informacjami o danym użytkowniku oraz łączyć zebrane z różnych źródeł dane w jeden spójny profil osobowy¹²². Platformy internetowe najczęściej nie działają bowiem w odosobnieniu i kooperują w tworzeniu profilu użytkownika. Powszechna jest na przykład praktyka stosowania konta jednej platformy do rejestracji i logowania się na innych stronach internetowych. Choć jest to duże ułatwienie dla użytkowników, to może pociągać za sobą dość niejasne zasady wymiany danych osobowych między witrynami¹²³. Przekazywane jednemu administratorowi dane są łączone ze znacznie większymi i bardziej kompleksowymi zbiorami danych pozyskiwanymi z różnych źródeł. Wiele pozornie nieistotnych danych w wyniku połączenia ich ze sobą może ujawniać wrażliwe cechy danej osoby.

Trzeba zwrócić też uwagę na nadużywanie możliwości przekazywania danych osobowych osobom trzecim, tzw. „zaufanym partnerom”. Użytkownicy najczęściej tracą kontrolę nad przetwarzaniem danych przez kolejne podmioty występujące w ta-

117 D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 203-208.

118 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 4/2007 w sprawie pojęcia danych osobowych*, 2007, s. 16.

119 Consultative Committee of The Convention for The Protection of Individuals with regard to Automatic Processing of Personal Data, Rada Europy, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 2017, s. 2.

120 C. Castelluccia, A. Narayanan, *Privacy considerations of online behavioural tracking*, European Network and Information Security Agency 2012, s. 11.

121 Consultative Committee of The Convention for The Protection of Individuals with regard to Automatic Processing of Personal Data, Rada Europy, *Guidelines on the protection of individuals...*, s. 5.

122 K. Iwańska, *To track or not to track?*..., s. 8-10.

123 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Platformy internetowe i jednolity rynek cyfrowy...*, s. 11-12.

kim łańcuchu zgody¹²⁴. Kontrola przetwarzania kończy się zazwyczaj na pierwszym ogniwie w łańcuchu zgody, a sposób wykorzystania danych przez osoby trzecie nie jest już dla użytkowników oczywisty. Z dużym prawdopodobieństwem dane zostaną przekazane kolejnemu podmiotowi, który może nawet dokonać zmiany pierwotnego przeznaczenia danych deklarowanego przez administratora¹²⁵, co jest kolejnym niepokojącym problemem związanym z przetwarzaniem danych osobowych.

Istotnym zagrożeniem jest również praktyka nieuzasadnionego zbierania zbyt dużej ilości danych, wbrew zasadzie minimalizacji¹²⁶. Ma to miejsce w niektórych aplikacjach mobilnych. Często po ich uruchomieniu żądają one dostępu do danych w sposób oczywisty zbędnych do zapewnienia poprawnego działania aplikacji. Jako przykład można podać aplikację TikTok, która przyznawała sobie dostęp do schowków użytkowników smartfonów bez ich wiedzy¹²⁷. Ponadto zgoda na przetwarzanie danych osobowych udzielana przez użytkowników platform ma charakter iluzoryczny i najczęściej nie spełnia wymagań stawianych przez RODO¹²⁸. Podobnie w przypadku wyrażania zgód na stosowanie plików *cookie* - zapytania w formie banerów na stronach internetowych najczęściej są akceptowane przez użytkowników odruchowo, bez zapoznania się z zakresem informacji o przetwarzaniu danych, aby jak najszybciej uzyskać dostęp do treści strony internetowej¹²⁹. Istotnym problemem jest też stosowanie przez administratorów tzw. *dark patterns*, czyli elementów interfejsów zaprojektowanych tak, by skłaniać konsumentów do wybierania ustawień prywatności najkorzystniejszej dla firm zajmujących się komercjalizacją danych¹³⁰. Taką praktyką jest np. całkowicie nieuzasadniona fragmentaryzacja celów przetwarzania z jednoczesnym brakiem możliwości ich łącznego odznaczenia¹³¹. Manipuluje się również kolorystyką elementów na banerach.

Wymienione powyżej problemy dotyczące kontroli nad danymi wynikają ze zbyt małej przejrzystości procesów przetwarzania i braku świadomości po stronie podmiotów danych, ale też zbyt dużej presji przedsiębiorców na udostępnianie przez konsumentów danych osobowych¹³². W interesie administratorów danych powinna być odpowiedź na te problemy poprzez skuteczniejsze informowanie konsumentów o tym, jakie dane osobowe są gromadzone i w jaki sposób są one udostępniane i wykorzystywane oraz zwiększenie stopnia zaufania użytkowników do podejmowanych przez nie procesów¹³³.

124 V. Bashyakarla, S. Hankey, A. Macintyre, R. Rennó, G. Wright, *Personal Data: Political Persuasion...*, s. 58.

125 Europejski Inspektor Ochrony Danych, Opinia 3/2018, *EDPS Opinion on online manipulation...*, s. 15-16.

126 K. Iwańska, *To track or not to track?*..., s. 13-14.

127 Pozyskano z: <https://www.cyberdefence24.pl/tiktok-przechowuja-dane-ze-schowka-bez-wiedzy-uzytkownikow>. Dostęp: 11.06.2021 r.

128 K. Iwańska, *To track or not to track?*..., s. 12-13.

129 M. Rojszczak, *Ochrona prywatności...*, s. 252-256.

130 Forbrukerrådet, *Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*, 2018, s. 7.

131 K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta...*, s. 7-8.

132 A. Mednis, *Prawo ochrony danych osobowych...*, s. 45.

133 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Platformy internetowe i jednolity rynek cyfrowy...*, s. 12.

4.2.3. Nadużywanie danych osobowych jako formy zapłaty za towar lub usługę

Jeszcze do niedawna Facebook reklamował rejestrację w swoim serwisie społecznościowym hasłem „To jest (i zawsze będzie) darmowe!”, jednak hasło to stało w sprzeczności z rzeczywistym modelem biznesowym Facebooka, co potwierdził włoski urząd antymonopolowy Autorità Garante della Concorrenza e del Mercato's, nakładając w 2018 r. na Facebook karę w wysokości 10 mln euro¹³⁴. W sytuacji, gdy platforma opiera swoje działanie na monetyzacji danych osobowych, czyli generowaniu przychodów z posiadanych danych¹³⁵, prezentowanie rejestracji jako darmowej zostało uznane za nieuczciwą praktykę handlową mogącą wprowadzać konsumentów w błąd. Skłaniało to bowiem użytkowników do podjęcia decyzji co do transakcji, której w przeciwnym razie by nie podjęli. Organ przyjął przy tym, że ekonomiczna wartość danych osobowych użytkowników Facebooka jest wystarczająca, by warunkować powstanie relacji konsumenckiej¹³⁶.

Powszechność Internetu i możliwość analizy coraz większych zbiorów danych wpłynęła na postrzeganie danych osobowych, które nie są już efektem ubocznym transakcji głównej, ale stanowią podstawową strategię biznesową dla dużej części usług *online*. Dane osobowe są bowiem cennym surowcem dla branży marketingowej i coraz częściej stają się głównym źródłem dochodu dla platform internetowych i aplikacji¹³⁷. Przedsiębiorcy nie wymagają od użytkowników opłat pieniężnych, co nie oznacza, że oferowane przez nich treści i usługi mają charakter bezpłatny. W zamian za możliwość dostępu i korzystania z oferowanych funkcjonalności użytkownicy wyrażają zgodę na przetwarzanie danych osobowych w celu personalizacji reklam lub też ich dalszej odsprzedaży¹³⁸. Dane osobowe, preferencje użytkowników i inne generowane przez nich treści mają tym samym istotną wartość ekonomiczną¹³⁹, a zgoda na ich przetwarzanie, wyrażona w sposób mniej lub bardziej świadomy, stanowi formę wynagrodzenia za korzystanie z usług *online*. Konsument i jego dane osobowe stają się w ten sposób produktami, za który inny podmiot chętnie zapłaci¹⁴⁰. Powstaje jednak pytanie, czy tak sformułowane wynagrodzenie można uznać za ekwiwalentne dla konsumenta, który udostępnia niekiedy istotne dane dużej liczbie podmiotów, w zamian za potencjalne, niewielkie ułatwienia lub dostęp do określonej usługi?

Pozyskanie jak największej liczby zgód na przetwarzanie danych leży w interesie podmiotów monetyzujących dane. W związku z tym podmioty mogą uciekać się do nieuzasadnionego nadużywania podstawy prawnej niezbędności do wykonania umowy zamiast właściwej podstawy, jaką jest zgoda podmiotu danych. Należy bowiem zauważyć, że faktyczna niezbędność do wykonania umowy będzie zachodzić stosunkowo

134 Decyzja nr 27432 AGCM z dnia 29.11.2018 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>. Dostęp: 11.06.2021 r.

135 A. Mednis, *Prawo ochrony danych osobowych...*, s. 66.

136 M. Kulesza, *Odpłatny charakter „darmowych” usług Facebooka. Teza z wyroku Regionalnego Sądu Administracyjnego Lazio (Rzym) z 10 stycznia 2020 r. w sprawie Facebook, sygn. 261/20*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2020, nr 4(9), s. 102.

137 K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta...*, s. 4-5.

138 Europejska Rada Ochrony Danych, *Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)...*, s. 5.

139 Dokument Roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29 w sprawie nieuczciwych praktyk handlowych*. SWD/2016/0163 final, 2016, s. 30.

140 A. De Franceschi, M. Lehmann, *Data as Tradeable Commodity and New Measures for their Protection*, *The Italian Law Journal* 2015, nr 1, s. 53-55.

rzadko. Przesłanka ta nie obejmuje sytuacji, w której przetwarzanie jest przydatne dla celów biznesowych administratora lub służy zwiększeniu zaangażowania użytkownika w daną usługę, ale nie jest w sposób obiektywny niezbędne do wykonania umowy¹⁴¹.

Ponadto, aby przekonać konsumentów do wyrażenia zgody na przetwarzanie danych osobowych w celu dostarczania spersonalizowanych reklam, platformy internetowe często posługują się argumentacją, że reklamy behawioralne pośrednio finansują darmowe świadczenie usługi. Badania pokazują jednak, że reklama behawioralna wcale nie generuje dla właścicieli powierzchni reklamowej w Internecie znacznie większych przychodów niż reklamy kontekstowe, które są o wiele mniej inwazyjne dla konsumentów i nie wymagają zbierania od nich ogromnych ilości danych osobowych¹⁴². Argument o wspieraniu darmowych treści ma sprawić, że konsument z większą przychylnością spojrzy na prośbę o wyrażenie zgody na personalizację reklam.

Można zaobserwować niepokojącą tendencję, że pomimo rosnących obaw o swoją prywatność konsumenci powszechnie udostępniają swoje dane osobowe w zamian za udogodnienia i zniżki, co można określić mianem „paradoksu prywatności”¹⁴³. Unia Europejska zauważyła, że coraz częściej dane osobowe stają się formą zapłaty za treści cyfrowe i usługi świadczone *online*, co znalazło odzwierciedlenie w dyrektywie 2019/770¹⁴⁴ w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych. Zgodnie z motywem 24 dyrektywa zapewnia konsumentom prawo do umownych środków ochrony prawnej w przypadku, gdy podanie danych osobowych następuje do celów innych niż jedynie dostarczenie treści cyfrowych lub usługi cyfrowej lub innych niż spełnienie wymogów prawnych. Konsument ma m.in. prawo do rozwiązania umowy, także w przypadku nieistotnej niezgodności z umową. Dyrektywa nie ma natomiast zastosowania, gdy konsument ogląda reklamy wyłącznie w celu uzyskania dostępu do treści cyfrowych lub usługi cyfrowej¹⁴⁵.

Kwestia umów, na podstawie których konsument dostarcza lub zobowiązuje się dostarczyć dane osobowe, została uregulowana również za sprawą „Nowego Ładu dla konsumentów” w dyrektywie 2011/83/UE. Tym samym w przypadku zapłaty w formie danych osobowych będzie obowiązywać m.in. prawo do odstąpienia od umowy.

4.2.4. Dyskryminacja konsumentów będąca wynikiem profilowania

Przypadki świadomej lub niezamierzonej dyskryminacji algorytmicznej zdarzają się stosunkowo często i są dość szeroko udokumentowane, np.: firma zajmująca się szkoleniami *online* oferowała wyższe ceny osobom z azjatyckim pochodzeniem¹⁴⁶; portal rezerwacyjny proponował wyższe ceny hoteli osobom, które korzystały z MacBooków, zakładając, że świadczy to o wyższym statusie majątkowym tych osób¹⁴⁷; algorytm

141 Europejska Rada Ochrony Danych, *Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)...*, s. 9.

142 K. Iwańska, *To track or not to track?*..., s. 17.

143 O. Ben-Shahar, *Data Pollution*..., s. 107.

144 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych, Dz. Urz. UE L 136 z dnia 22.05.2019 r., s. 1.

145 Motyw 25 dyrektywy 2019/770 w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych.

146 F. J. Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making*, The Directorate General of Democracy, Rada Europy, Strasburg 2018, s. 16.

147 Pozyskano z: <https://edition.cnn.com/2012/06/26/tech/web/orbitz-mac-users/index.html>. Dostęp: 11.06.2021 r.

używany przez Amazon wyłączał możliwość bezpłatnej dostawy w dzielnicach zamieszkałych przez mniejszości etniczne¹⁴⁸.

Wyróżnia się kilka źródeł dyskryminacji algorytmicznej. Może mieć ona związek z użyciem zbyt wąskiego lub zbyt ogólnego kryterium klasyfikacji, przez co inne czynniki, istotne z punktu widzenia podejmowanej decyzji, nie zostaną wzięte pod uwagę. Przykładem jest próba klasyfikacji, czy zawrzeć z kimś umowę ubezpieczenia mieszkania na podstawie kryterium zamieszkiwania w „dobrej” okolicy, przy czym jedynym brany pod uwagę czynnikiem jest odsetek popełnianych w tej okolicy przestępstw. Może się jednak okazać, że okolica ze stosunkowo dużym odsetkiem popełnianych przestępstw pod względem częstotliwości kradzieży lub włamań nie wyróżnia się na tle średniej, a zatem podane kryterium nie powinno mieć w tym przypadku decydującego znaczenia. Wyniki dostarczane przez sztuczną inteligencję nie powinny być pozbawiane kontekstu poprzez uwzględnianie jedynie niektórych okoliczności dotyczących danych¹⁴⁹.

Innym źródłem dyskryminacji są założenia przyświecające samym twórcom algorytmu. Na przykład amerykański serwis Lenddo dokonujący ocen zdolności kredytowej dla banków bierze pod uwagę takie czynniki jak rodzaj słuchanej muzyki i problemy w spłatach kredytów znajomych osoby ocenianej¹⁵⁰. Choć wydaje się, że poddanie decyzji do rozstrzygnięcia sztucznej inteligencji powinno być bezstronne, to algorytmy w dalszym ciągu są w stanie powielać uprzedzenia tworzących je ludzi¹⁵¹. Podmioty stosujące algorytmy do profilowania osób fizycznych mogą więc świadomie lub nieświadomie implementować do nich kryteria dyskryminujące. Na przykład reklamy odzieży dla osób niepełnosprawnych notorycznie są blokowane przez algorytmy Facebooka, które w założeniu zostały stworzone w celu ochrony tej społeczności przed podrobionymi produktami¹⁵².

Istnieje również prawdopodobieństwo, że algorytm zacznie dyskryminować wskutek źle przeprowadzonego procesu „uczenia” lub złej jakości, charakteru i pochodzenia danych szkoleniowych zapewnionych algorytmowi. Dane mogą się charakteryzować: małą różnorodnością, zbyt dużą liczbą historycznych uprzedzeń, nadreprezentacją lub niedostateczną reprezentacją pewnej grupy względem innej. W takiej sytuacji algorytm podczas podejmowania decyzji odtworzy dyskryminacyjny charakter danych¹⁵³. Niektóre z tak wytworzonych przez algorytm powiązań i predykcji okażą się niepoprawne i przypadkowe. Na przykład zamieszkiwanie w określonej dzielnicy nie zawsze wskazuje na status społeczny danej osoby.

Efektami dyskryminacyjnych działań mogą być: podjęcie decyzji o niezawieraniu umowy z określonymi osobami, wykluczenie osób z grupy mającej dostęp do oferty lub zaproponowanie niektórym osobom wyższej ceny produktów lub usług. W konkretnych przypadkach ukryta dyskryminacja może zadecydować o tym, że komuś z uwagi na niski

148 D. Pedreschi, I. Miliou, *Artificial Intelligence (AI): new developments and innovations applied to e-commerce. Challenges to the functioning of the Internal Market*, Departament Tematyczny ds. Polityki Gospodarczej, Naukowej i Jakości Życia, 2020, s. 13.

149 Consultative Committee of The Convention for The Protection of Individuals with regard to Automatic Processing of Personal Data, Rada Europy, *Guidelines on the protection of individuals...*, s. 5.

150 A. Mednis, *Prawo ochrony danych osobowych...*, s. 69.

151 Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*, COM(2020) 65 final, s. 13.

152 Pozyskano z: <https://www.nytimes.com/2021/02/11/style/disabled-fashion-facebook-discrimination.html?fbclid=IwAR2WoFFm0tTVG2jlv9uRcnJTD6fHCss5UFRuK50OfXclaxSI462lqOcGjC4>. Dostęp: 11.06.2021 r.

153 F. J. Zuiderveen Borgesius, *Discrimination, artificial intelligence...*, s. 11.

scoring kredytowy nie zostanie udzielony kredyt¹⁵⁴, ktoś nie zostanie przyjęty do pracy¹⁵⁵ lub jego składka ubezpieczeniowa będzie zdecydowanie wyższa niż przeciętna¹⁵⁶.

Niekiedy odróżnienie personalizacji o charakterze dyskryminacyjnym od pożądanego personalizacji jest trudne¹⁵⁷. Na przykład personalizacja cen ma na celu wyświetlanie konsumentom maksymalnych cen, które są skłonni zapłacić za dany produkt lub usługę, i z pewnością prowadzi do pogłębiania się nierówności istniejących w społeczeństwie. Powstaje jednak pytanie - skoro ceny są dostosowywane do możliwości finansowych konkretnego konsumenta, to czy w dalszym ciągu mamy do czynienia z dyskryminacją? Kolejnym utrudnieniem jest fakt, że pozornie neutralne dane mogą pełnić rolę zastępczą dla cech szczególnie chronionych, takich jak: rasa, religia i orientacja seksualna. Na przykład z danych o wykonywaniu przez kogoś zawodu związanego z opieką nad dziećmi, który charakteryzuje się dość znaczną feminizacją, z dużym prawdopodobieństwem można wyciągnąć wniosek o tym, że dane dotyczą kobiety. Profilowanie może zatem opierać się na czynnikach, które niekiedy pozostają poza zakresem przepisów dotyczących dyskryminacji, ale w dalszym ciągu można uznać je za nieetyczne¹⁵⁸.

Większość przypadków dyskryminacji algorytmicznej ma charakter pośredni - przyjęte kryteria z pozoru zapewniają neutralność, ale dyskryminacyjny skutek ujawnia się w przyszłości. W tym kontekście za szczególnie niebezpieczny należy uznać efekt czarnej skrzynki (ang. *black box*), czyli niewytłumaczalności działania systemów sztucznej inteligencji¹⁵⁹. W złożonych, samoulepszających się algorytmach ich twórcy zazwyczaj ustalają nadrzędny cel algorytmu oraz dane wejściowe, jednak rozszyfrowanie poszczególnych kryteriów kierujących procesem podejmowania decyzji jest znacznie trudniejsze. W tej sytuacji weryfikacja, czy i na jakiej podstawie doszło do dyskryminacji, może być niedostępna. W związku z tym postuluje się, by wszelkie algorytmy używane do profilowania, zwłaszcza w obszarach wrażliwych, charakteryzowały się przejrzystością, zapewniały informacje o użytym przez nie rozumowaniu i umożliwiały przeprowadzenie ich audytu¹⁶⁰.

4.2.5. Ograniczanie dostępu do informacji przez bańki filtrujące

Dla coraz większej grupy konsumentów Internet stanowi centrum aktywności życiowej, a zarazem główne źródło informacji o otaczającym ich świecie¹⁶¹. W Polsce odsetek osób korzystających z Internetu w celu czytania wiadomości, gazet lub czasopism w 2020 r. wyniósł nieco ponad 78%¹⁶². Z kolei korzystanie z serwisów społecz-

154 Pozyskano z: <https://www.bbc.com/news/business-50432634>. Dostęp: 11.06.2021 r.

155 Pozyskano z: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>. Dostęp: 11.06.2021 r.

156 Pozyskano z: <https://caselaw.findlaw.com/us-5th-circuit/1292810.html>. Dostęp: 11.06.2021 r.

157 O. Ben-Shahar, *Data Pollution...*, s. 115.

158 Zalecenie CM/Rec (2020) 1 Komitetu Ministrów Rady Europy dla państw członkowskich z dnia 8.04.2020 r. w sprawie wpływu systemów algorytmicznych na prawa człowieka, s. 7.

159 Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji...*, s. 14.

160 Rezolucja z dnia 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL), s. 5.

161 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Zwalczanie dezinformacji w internecie: podejście europejskie*, COM/2018/236 final, s. 2.

162 Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, *Społeczeństwo informacyjne w Polsce w 2020 r.*, s. 143. Pozyskano z: <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne>. Dostęp: 11.06.2021 r.

nościowych zadeklarowało blisko 66% respondentów¹⁶³. Z dużym prawdopodobieństwem część z tych osób nie zdaje sobie sprawy, że treści internetowe, z którymi mają do czynienia, mogą być w różnym stopniu spersonalizowane.

Konsument poprzez przeglądanie treści wywiera wpływ na to, które informacje w przyszłości zostaną mu wyświetlone oraz jaki będzie ich priorytet. Serwisy społecznościowe filtrują informacje tak, by były one jak najbardziej dopasowane do konkretnej osoby i odpowiadały jej zainteresowaniom¹⁶⁴. Przeprowadzane eksperymenty dowodzą, że reagowanie na określone treści może wpłynąć na zwiększone wyświetlanie treści marketingowych oraz radykalizację treści dotyczących poglądów politycznych¹⁶⁵. Pozornie korzystne zjawisko niejawnej personalizacji treści może prowadzić do powstawania tzw. baniek filtrujących (ang. *filter bubble*)¹⁶⁶, które w sposób arbitralny ograniczają swobodny dostęp do różnorodnych informacji.

Bańki informacyjne można zdefiniować jako „osobiste i niepowtarzalne uniwersum informacyjne, w którym każdy z nas żyje *online*”¹⁶⁷. Spektrum informacji zawartych w bańce informacyjnej jest ściśle powiązane z osobą użytkownika¹⁶⁸, co w konsekwencji prowadzi do sytuacji, że takie samo hasło wpisane w wyszukiwarkę internetową przez dwie różne osoby z różnych adresów IP, kont lub lokalizacji może dać zupełnie odmienne wyniki¹⁶⁹. W pełni zautomatyzowane systemy rekomendujące mają za zadanie wyeksponować odbiorcom konkretne informacje, które są w ich kręgu zainteresowań. Niekoniecznie jest to skorelowane z tym, co zobaczyliby, gdyby przepływ informacji nie był spersonalizowany, np. informacje: ważne globalnie, niewygodne z punktu widzenia konkretnej osoby lub obrazujące inny punkt widzenia.

Serwisy społecznościowe, takie jak Facebook, zapewniają swoich użytkowników, że pokazują najistotniejsze, najbardziej wartościowe materiały i nadają priorytet lokalnym informacjom i zaufanym serwisom informacyjnym¹⁷⁰. Niemniej jednak sam proces filtrowania informacji jest niewidoczny dla użytkowników Internetu, a co za tym idzie, nie jest również możliwe skontrolowanie tego, co zostało celowo pominięte w wyniku zastosowanej personalizacji¹⁷¹.

Warto w tym miejscu wspomnieć o założeniach zawartych w propozycji projektu Kodeksu Usług Cyfrowych¹⁷² z 15 grudnia 2020 r., gdzie postuluje się wprowadzenie jasnych, przystępnych i łatwo zrozumiałych informacji o głównych parametrach systemów rekomendujących używanych przez platformy internetowe. Regulacje

163 Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, Społeczeństwo informacyjne w Polsce w 2020 r., s. 143...

164 V. Viķe-Freiberga, H. Däubler-Gmelin, B. Hammersley, L. M. Poiarés Pessoa Maduro, *A free and pluralistic media...*, s. 27.

165 B. Malinowski, *Jak Facebook zamyka nas w bańce informacyjnej. Algorytm filtrujący newsfeed a zjawisko filter bubble*, Zarządzanie mediami 2016, nr 1, s. 20.

166 Pojęcie to zostało użyte pierwszy raz przez Eli'ego Pariser'a w książce *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Press 2011.

167 B. Malinowski, *Jak Facebook zamyka...*, s. 19, za: E. Pariser.

168 E. Pariser, *Beware online "filter bubbles"*, 2011. Pozyskano z: https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles#t-241191. Dostęp: 11.06.2021 r.

169 Wpisane w wyszukiwarkę hasło „Egipt” u jednej z osób spowodowało wyświetlenie ofert wakacji, a u innej -informacji związanych z protestami toczącymi się w Egipcie. Pozyskano z: https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles#t-241191. Dostęp: 11.06.2021 r.

170 Pozyskano z: <https://www.facebook.com/help/1974897772766979>. Dostęp: 11.06.2021 r.

171 E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin Press 2011, s. 15.

172 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.

w zaproponowanym kształcie pozwoliłyby konsumentom zdecydować o niekorzystaniu z wyświetlania opartego na profilowaniu, co mogłoby w dużej mierze rozwiązać problem baniek filtrujących.

5. Wnioski częściowe

Personalizacja może mieć wiele zastosowań wykorzystywanych w kontakcie z konsumentami. Nie ogranicza się to jedynie do personalizacji reklam internetowych, choć niewątpliwie jest to jedna z najbardziej rozwiniętych obecnie gałęzi personalizacji. Jednocześnie nie sposób określić personalizacji jako zjawiska jednoznacznie pozytywnego lub negatywnego. Sztuczna inteligencja zapewniła technologie, dzięki którym można wykorzystywać informacje o konsumentach w celu uatrakcyjnienia ich przestrzeni internetowej i ułatwienia im dokonywania wyborów¹⁷³. Niemniej jednak pozytywne aspekty bardzo szybko uległy wypaczeniu i skutkowało to powstaniem nieznanych dotąd zagrożeń dla podstawowych praw i wolności jednostek. Jako że są to zagrożenia względnie nowe, to regulacje prawne nie odpowiadają na nie jeszcze w pełni, choć z pewnością są one w przestrzeni prawnej dostrzegane.

Obecne możliwości technologiczne na niespotykaną wcześniej skalę pozwalają w sposób niezauważony wkraczać w prywatność konsumentów. Procesy te są zazwyczaj nieprzejrzyste, a powszechna świadomość konsekwencji udostępniania dużej ilości danych osobowych zbyt wielu podmiotom jest wciąż niewielka. Korzyści będące efektem personalizacji nie równoważą obecnie skali wynikających z niej zagrożeń. Z uwagi na samą specyfikę personalizacji, która nie może istnieć bez profilowania, ochrona konsumenta, będącego jednocześnie najczęściej podmiotem danych osobowych, będzie podlegała obu tym reżimom. Co więcej, rozwiązania prawne z obu tych gałęzi zaczynają wzajemnie siebie wspierać i uzupełniać, czego dowodem jest wspomniany wcześniej wyrok Regionalnego Sądu Administracyjnego Lazio z 10 stycznia 2020 r. w sprawie Facebooka.

Aktem prawnym, który chroni użytkowników Internetu w sferze konsumenckiej, jest w głównej mierze dyrektywa 2005/29/WE o nieuczciwych praktykach handlowych. W ramach niej konsumenci mogą poszukiwać ochrony przed personalizacją opierającą się na manipulowaniu emocjami oraz wykorzystywaniu ich słabości. Choć personalizacja w celach politycznych i społecznych wykazuje pewne podobieństwa do nadużyć, o których mowa w prawie konsumenckim, to wykracza ona poza jego zakres¹⁷⁴. Z tego powodu problematyka wpływania na przekonania polityczne, choć niezwykle aktualna, zostanie pominięta w dalszych rozważaniach.

Z kolei z perspektywy podmiotu danych osobowych najważniejszym aktem prawnym normującym problematykę personalizacji i nieodłącznego procesu profilowania jest RODO. W oczekiwaniu na rozporządzenie *ePrivacy* to właśnie tam należy szukać ochrony podmiotów danych przed pozbawianiem ich kontroli nad danymi osobowymi oraz związaną z tym kwestią wykorzystania danych jako formy zapłaty. Z tego też względu regulacja ogólnego rozporządzenia o ochronie danych stanowi punkt wyjścia dla dalszych rozważań.

173 G. Sarton, *New aspects and challenges in consumer protection...*, s. 6.

174 Europejski Inspektor Ochrony Danych, *Opinia 3/2018, EDPS Opinion on online manipulation...*, s. 17.

Rozdział 2.

RODO jako instrument prawny ochrony konsumenta przed personalizacją opartą na sztucznej inteligencji

1. Uwagi wprowadzające

Nieodłącznym elementem personalizacji jest profilowanie, które łączy się z koniecznością przetwarzania dużych ilości danych, w tym danych osobowych. Związane jest to z zagrożeniami, m.in.: nieprzejrzystością algorytmów, zbieraniem danych bez wiedzy osób, których dane dotyczą, oraz dyskryminacyjnym charakterem profilowania¹⁷⁵.

Profilowanie w RODO zostało omówione dwukrotnie: w art. 4 pkt 4 RODO oraz w art. 22 RODO. W art. 4 pkt 4 RODO mamy do czynienia z najszerszą definicją profilowania, które obejmuje również przetwarzanie częściowo zautomatyzowane. Takie profilowanie co do zasady traktowane jest jak każdy inny rodzaj przetwarzania danych osobowych. W związku z tym zastosowanie mają zasady ogólne RODO dotyczące przetwarzania¹⁷⁶. Na potrzeby niniejszej pracy ten rodzaj profilowania został określony profilowaniem zwykłym. Z kolei art. 22 RODO odnosi się jedynie do profilowania całkowicie zautomatyzowanego, co nazwane zostało profilowaniem szczególnym.

Ochrona danych osobowych niewątpliwie powinna uwzględniać interesy osób nieświadomych zagrożeń związanych z wykorzystaniem danych w celu personalizacji oraz tych, które są szczególnie narażone na nadmierne profilowanie z uwagi na swój duży ślad cyfrowy. Jako że każdy konsument w przypadku internetowej personalizacji jest jednocześnie podmiotem danych osobowych, regulacje RODO zachowują swoją aktualność. W tym rozdziale ocenię, czy regulacja RODO zapewnia skuteczne mechanizmy ochronne w stosunku do konsumentów poddawanych personalizacji.

Z powodu obszerności zagadnienia poza zakresem niniejszej pracy znajduje się problem właściwego określenia administratorów danych i zakresu ich odpowiedzialności. W procesie personalizacji uczestniczy bowiem wiele podmiotów, m.in.: wynajmujący powierzchnię reklamową, dostawcy profili osobowościowych, reklamodawcy wykorzystujący profile w celu tworzenia konkretnych kampanii marketingowych, a także tzw. zaufani partnerzy, którym administratorzy przekazują dane osobowe. W tym miejscu trzeba jednak poprzestać na stwierdzeniu, że taka rozpiętość potencjalnych administratorów danych również może negatywnie wpływać na utrzymanie kontroli nad danymi osobowymi oraz realizację praw konsumentów.

¹⁷⁵ M. Kibil (w:) M. Gawroński (red.), *RODO Przewodnik ze wzorami*, Warszawa 2018, s. 244.

¹⁷⁶ Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 9.

2. Dane osobowe wykorzystywane w procesie profilowania

Z uwagi na stale rozwijające się techniki śledzenia konsumentów oraz szerokie spektrum pozyskiwanych spostrzeżeń profilowanie na potrzeby personalizacji najczęściej będzie opierać się właśnie na danych osobowych, czyli informacjach dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Jest to niezależne od tego, czy dane osobowe zostały użyte do zbudowania profilu, czy też powstały dopiero na skutek połączenia wielu danych niebędących wcześniej danymi osobowymi. O ile informacja o zakupie dużej ilości słodyczy sama w sobie nie ma charakteru danej osobowej, to wyciągnięty z takiej informacji wniosek, że dany konsument ma zwiększone ryzyko otyłości, jest już daną osobową, w dodatku o charakterze wrażliwym¹⁷⁷.

Już w samej definicji danych osobowych zawartej w art. 4 pkt 1 RODO jako przykład wymienione są m.in.: dane o lokalizacji, identyfikatory internetowe, takie jak pliki *cookies* i adresy IP, lub czynniki określające psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Danymi osobowymi mogą więc być informacje, które identyfikują osobę, ale też takie, które odnoszą się do jej cech, statusu osobistego lub rzeczowego¹⁷⁸. Powyższe wyliczenie w dużym stopniu pokrywa się z kategoriami danych osobowych, najczęściej pojawiającymi się w profilach behawioralnych konsumentów, które obejmują m.in.: adres, stan cywilny, poziom edukacji, uzyskiwane dochody, profil religijny i etniczny lub dane o lokalizacji¹⁷⁹. Do tego należy dodać wszelkie inne atrybuty, które zostały wywnioskowane z połączenia pozornie nieistotnych spostrzeżeń dotyczących użytkownika¹⁸⁰.

Choć w doktrynie postuluje się, by wszelka aktywność internetowa była automatycznie traktowana jako dana osobowa¹⁸¹, to przeważa stanowisko, że nie jest możliwe zakwalifikowanie określonej informacji jako danej osobowej w sposób uniwersalny. Kategoria ta zawsze będzie charakteryzowała się pewnym stopniem względności zależnym od tego, jakimi innymi informacjami i możliwościami dysponuje osoba, która weszła w ich posiadanie¹⁸². Przykład może stanowić adres IP, którego status jest dość niejednoznaczny. W świetle orzeczeń Trybunału Sprawiedliwości zarówno statyczny identyfikator IP¹⁸³, jak i IP dynamiczne¹⁸⁴ zostały uznane, w pewnych sytuacjach, za dane osobowe. W przypadku sprawy C-70/10 *Société belge des auteurs, compositeurs et éditeurs* Trybunał Sprawiedliwości uznał, że adres IP jest daną osobową dla dostawcy usługi dostępu do Internetu. Z kolei w sprawie C- 582/14 *Patrick Breyer* dotyczącej dynamicznego IP przyjęto, że adres IP ma charakter danych osobowych dla podmiotów mających możliwość połączenia go z dodatkowymi informacjami będącymi w posiadaniu np. dostawcy usługi dostępu do Internetu.

177 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 59.

178 P. Fajgielski, *Komentarz do art. 4, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 100-141.

179 K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta...*, s. 24-25.

180 D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, s. 200-203.

181 A. Mednis, *Prawo ochrony danych osobowych...*, s. 142.

182 P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 (w:) P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony...*, s. 172.

183 Wyrok TS z 24.11.2011 r. w sprawie C-70/10 *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, ECLI:EU:C:2011:771, pkt 51.

184 Wyrok TS z 19.10.2016 r. w sprawie C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, pkt 44-48.

A minori ad maius można potwierdzić, że dla branży reklamowej, która ma wiele innych specyficznych spostrzeżeń dotyczących danej osoby, adres IP będzie stanowił w większości przypadków daną osobową. Przy tak rozwiniętych metodach sprzedaży i łączenia ze sobą wiedzy o użytkownikach Internetu nawet potencjalna możliwość uzyskania w ten sposób danych osobowych jest, moim zdaniem, wystarczająca do uznania, że administrator powinien postępować z takimi informacjami jakby były one danymi osobowymi¹⁸⁵. Niezależnie od przyznanego adresowi IP statusu, nie wydaje się, by była to informacja szczególnie użyteczna w branży reklamowej z uwagi na specyfikę dynamicznego adresu IP, którym posługuje się większość użytkowników Internetu. Dynamiczne IP zmienia się bowiem przy każdym połączeniu z Internetem, a zatem możliwość identyfikacji osoby fizycznej na tej podstawie jest dość ograniczona.

Co ciekawe, z pozoru najbardziej oczywiste dane osobowe, takie jak imię i nazwisko lub numer PESEL, nie są w procesie profilowania na cele personalizacji szczególnie użyteczne¹⁸⁶. Znacznie ważniejszą rolę odgrywają indywidualne identyfikatory nadawane przez poszczególne podmioty z branży reklamowej, które w sposób bezpośredni są powiązane z określoną osobą. Podmioty te przekazują sobie wzajemnie informacje o nadanych konsumentom identyfikatorach i profilach w ramach tzw. *cookie syncing* w celu sprawdzenia, czy posiadają dane o konkretnym użytkowniku w swoich zasobach¹⁸⁷. Użycie takiego identyfikatora nie będzie jednak powodowało, że informacje zawarte w profilu osobowościowym staną się anonimowe.

3. Zasady profilowania określone w RODO jako podstawy personalizacji

3.1. Definicja profilowania zwykłego zgodnie z art. 4 pkt 4 RODO

Definicja profilowania zwykłego została określona w art. 4 pkt 4 RODO. Według niej 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. Funkcjami profilowania w tym znaczeniu są: identyfikacja, ocena zachowania i cech określonej osoby oraz przewidywanie jej zachowań¹⁸⁸.

Dokonując analizy art. 4 ust. 4 RODO, trzeba wyróżnić trzy przesłanki profilowania zwykłego:

- a. dotyczy danych osobowych,
- b. stanowi dowolną formę zautomatyzowanego przetwarzania,
- c. na jego podstawie powinna być dokonywana ocena czynników osobowych osoby fizycznej¹⁸⁹.

185 Por. A. Mednis, *Prawo ochrony danych osobowych...*, s. 144-145.

186 K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta...*, s. 16.

187 Pozyskano z: <https://adtechexplained.com/cookie-syncing-explained/>. Dostęp: 11.06.2021 r.

188 A. Mednis, *Prawo ochrony danych osobowych...*, s. 29.

189 M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu...*, s. 83.

Profilowanie może przybrać postać: nieautomatyzowaną, częściowo zautomatyzowaną oraz całkowicie zautomatyzowaną¹⁹⁰. Nieautomatyzowane profilowanie oparte jest na ludzkim działaniu¹⁹¹ i nie będzie wchodzić w zakres definicji art. 4 pkt 4 RODO¹⁹². Z kolei profilowanie częściowo zautomatyzowane pozbawione zostaje czynnika ludzkiego głównie w obszarze analiz danych¹⁹³. Treść art. 4 pkt 4 RODO wskazuje na dowolną formę zautomatyzowanego przetwarzania, co potwierdza, że profilowanie zautomatyzowane może łączyć się z pewnymi formami ludzkiej interwencji¹⁹⁴. Ostatnia, całkowicie zautomatyzowana forma profilowania jest oparta wyłącznie na algorytmach, które nie tylko dokonują analizy danych, ale też wyciągają z nich odpowiednie wnioski, kategoryzują je i wykorzystują do określonego celu¹⁹⁵. Profilowaniem w tym znaczeniu nie będzie zatem proces, w którym człowiek będzie miał możliwość nadzoru nad wynikiem profilowania¹⁹⁶, np. przez konieczność weryfikacji zaproponowanej przez algorytm rekomendacji cenowej dla danego klienta. Profilowanie całkowicie zautomatyzowane zostało opisane w art. 22 RODO.

W przypadku ostatniej przesłanki profilowania zwykłego, jaką jest ocena czynników osobowych osoby fizycznej, należy podkreślić, że zawarte w tym przepisie wyliczenie czynników nie jest wyczerpujące¹⁹⁷. Dokonanie takiej oceny ma na celu ułatwienie w zakwalifikowaniu danego konsumenta do jakiejś kategorii¹⁹⁸. Uważa się jednak, że prosta kategoryzacja danych bez wnioskowania o nowych informacjach nie będzie profilowaniem w rozumieniu RODO¹⁹⁹.

Personalizacja ma szerokie spektrum zastosowania - poczynając od reklam behawioralnych, zindywidualizowanych promocji, a kończąc na dostosowanych cenach produktów i usług oraz innych warunkach umownych. Odnosząc wymienione powyżej przesłanki profilowania do procesu personalizacji, można stwierdzić, że wiele form personalizacji będzie zarazem wyczerpywało definicję profilowania zwykłego z art. 4 pkt 4 ogólnego rozporządzenia o ochronie danych.

3.2. Definicja profilowania szczególnego zgodnie z art. 22 RODO

Niekiedy profilowanie jest wykorzystywane do podejmowania decyzji wobec danej osoby, co zostało określone w art. 22 RODO²⁰⁰. Podleganie takiemu profilowaniu szczególnemu podlega restrykcyjnym ograniczeniom. Ma to minimalizować ryzyko

190 Por. J. Niklas, *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji*, Polskie Towarzystwo Prawa Antydyskryminacyjnego 2015, s. 3. Pozyskano z: http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekście_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf. Dostęp: 11.06.2021 r.

191 Por. B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, *Komentarz do art. 4 (w:) M. Sakowska-Baryła (red.), Ogólne rozporządzenie...*, s. 88-89.

192 M. Kibil (w:) M. Gawroński (red.), *RODO Przewodnik ze wzorami*, Warszawa 2018, s. 248.

193 J. Niklas, *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji...*, s. 3.

194 D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, s. 200-203.

195 J. Niklas, *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji...*, s. 3.

196 M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu...*, s. 87.

197 D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, *Komentarz do art. 4 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, Warszawa 2018, s. 200-203.

198 M. Kibil (w:) M. Gawroński (red.), *RODO Przewodnik ze wzorami*, Warszawa 2018, s. 250.

199 M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu...*, s. 88.

200 P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 (w:) P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony...*, s. 129-132.

niebezpieczeństwa dla praw jednostki wynikające z rozwoju nowych technologii²⁰¹. Na marginesie należy wspomnieć, że obok profilowania szczególnego w art. 22 RODO wymieniono też zautomatyzowane podejmowanie decyzji, które jest kategorią szerszą od profilowania i niekoniecznie musi być z nim związane.

Mogą bowiem zaistnieć sytuacje, w których podjęcie decyzji nastąpi bez dokonywania oceny czynników osobowych danej osoby fizycznej, np. w przypadku przyznania kuponów rabatowych w aplikacji do sklepów ze względu na fakt, że algorytm na podstawie geolokalizacji wykrył, że dana osoba je minęła²⁰². Jednak podobna decyzja może zostać podjęta na skutek całkowicie zautomatyzowanego profilowania, jeśli algorytm przyznający kupony rabatowe kierowałby się np. stopniem zamożności danej osoby lub faktem posiadania przez taką osobę małych dzieci, co zostałoby wywnioskowane z dokonywanych przez taką osobę zakupów. Niekiedy, wraz ze zmianą sposobu wykorzystania danych, działanie oparte jedynie na procesie zautomatyzowanego podejmowania decyzji może przekształcić się w działanie oparte na profilowaniu²⁰³. Ze względu na brak dokonywania oceny czynników osobowych zautomatyzowane podejmowanie decyzji pozostaje na uboczu rozważań dotyczących personalizacji.

3.2.1. Przesłanka całkowitego zautomatyzowania procesu profilowania

Według art. 22 RODO osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Pierwszą przesłanką profilowania określonego w art. 22 RODO jest całkowite zautomatyzowanie. W przeciwieństwie do art. 4 pkt 4 RODO art. 22 RODO zakłada bowiem pełną automatyzację przetwarzania, co oznacza zdolność do podejmowania decyzji z wykorzystaniem rozwiązań technicznych bez interwencji ludzkiej²⁰⁴. Również proces profilowania poprzedzający podjęcie decyzji musi spełniać przesłankę pełnej automatyzacji²⁰⁵. Przy ocenie udziału człowieka w podejmowaniu decyzji należy brać pod uwagę jej realny wpływ na proces decyzyjny²⁰⁶. Chodzi w tym przypadku o możliwość zmiany lub całkowitego odrzucenia zaproponowanej przez algorytm rekomendacji. W przypadku personalizacji przekazu większość działań jest całkowicie zautomatyzowana. Zarówno tworzenie profili użytkowników, proces ich sprzedaży na giełdach reklamowych, jak i ostateczna decyzja co do wyświetlenia konsumentowi danej reklamy, treści lub ceny jest dokonywana poprzez zastosowanie algorytmu sztucznej inteligencji. Ingerencja ludzka kończy się zazwyczaj w momencie określenia atrybutów służących do targetowania konsumentów.

201 P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 22 (w:) P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony...*, s. 423-424.

202 M. Kibił (w:) M. Gawroński (red.), *RODO Przewodnik ze wzorami*, Warszawa 2018, s. 255.

203 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 8-9.

204 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 8.

205 A. Mednis, *Prawo ochrony danych osobowych...*, s. 179.

206 M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020, s. 127.

3.2.2. Przesłanka wywoływania skutków prawnych lub wpływania na sytuację osoby w podobnie istotny sposób

Poza pierwszą przesłanką całkowitego zautomatyzowania profilowania konieczne do spełnienia są również alternatywnie: wywarcie skutków prawnych w stosunku do osoby objętej decyzją lub też wywarcie na niej podobnego istotnego wpływu. Obie te przesłanki zostały wyjaśnione przez Grupę Roboczą Art. 29 ds. Ochrony Danych w wytycznych dotyczących zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679.

3.2.2.1. Przesłanka wywoływania skutków prawnych

Odnosząc się do wywoływania skutków prawnych przez decyzję opartą wyłącznie na zautomatyzowanym profilowaniu, Grupa Robocza Art. 29 ds. Ochrony Danych określiła, że taka decyzja ma wpływ na status prawny danej osoby, ich prawa przewidziane w przepisach lub na prawa przysługujące jej na mocy umowy²⁰⁷. Za wpływ prawny uznane będą na przykład: zawarcie umowy, jej zmiana, rozwiązanie lub anulowanie. W doktrynie wyrażane jest stanowisko, że treść art. 22 RODO przesądza o tym, że pod uwagę brane są jedynie negatywne skutki prawne dla konsumenta²⁰⁸.

Przykładem decyzji, która w sposób ewidentny wpływa na sytuację prawną danej osoby, jest decyzja o udzieleniu lub odmowie udzielenia kredytu albo decyzja o zawarciu lub odmowie zawarcia umowy ubezpieczenia. W doktrynie przyjmuje się, że personalizacja cen wywiera wpływ na sytuację prawną konsumenta²⁰⁹. Można też wskazać na profilowanie pomocy dla osób bezrobotnych, co uskuteczniłoby przez powiatowe urzędy pracy w Polsce do 2019 r. Profilowanie prowadziło do tego, że zakwalifikowanie osób do konkretnej kategorii pozbawiało ich możliwości skorzystania z niektórych instrumentów aktywizacji zawodowej, co niewątpliwie różnicowało sytuację prawną bezrobotnych²¹⁰. Można wyciągnąć wniosek, że decyzja będzie wywierać skutek prawny, jeżeli będzie wpływać na prawa konsumenta zawarte m.in. w ustawie o ochronie konkurencji i konsumentów²¹¹, np. prawo do rzetelnej, prawdziwej i pełnej informacji. Za takim stanowiskiem przemawia też pogląd, że skutek prawny może pojawić się na etapie kontraktowania lub wykonania umowy²¹².

3.2.2.2. Przesłanka wpływania na sytuację osoby w podobnie istotny sposób

O wiele bardziej niejednoznaczną przesłanką jest „wpływ na sytuację osoby w podobnie istotny sposób”. Chodzi o wpływ na sytuację danej osoby, jej zachowanie lub podejmowane przez nią wybory. Przesłankę tę będzie spełniał wpływ długotrwa-

207 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 24.

208 D. Lubasz, *Big brother is watching you. Profilowanie i zautomatyzowane podejmowanie decyzji w kontekście zasad legalności i przejrzystości* (w:) R. Wojciechowski, H. Wolska (red.), *Rok RODO*, Warszawa 2019, s. 119-124.

209 R. Steppe, *Online price discrimination and personal data: A General Data Protection Regulation perspectives*, *Computer Law & Security Review* 2017, nr 33, s. 784.

210 Pozyskano z: <https://www.gov.pl/web/rodzina/koniec-z-profilowaniem-pomocy-dla-bezrobotnych>. Dostęp: 11.06.2021 r.

211 *Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów*, Dz.U. z 2007 r. Nr 50, poz. 331.

212 D. Lubasz, *Big brother is watching you...*, s. 119-124.

ty lub taki, który prowadzi do dyskryminacji osób fizycznych²¹³. Jednocześnie nie każde różnicowanie warunków sprzedaży lub świadczenia usług będzie świadczyło o dyskryminacji. Istotność wpływu zaistnieje np., gdy decyzja dotyczy sytuacji finansowej danej osoby, dostępu do świadczeń zdrowotnych i edukacyjnych lub utraty szansy na zatrudnienie²¹⁴. W przypadku personalizacji dokonywanej w celach reklamowych spełnienie tej przesłanki jest niejednoznaczne. W doktrynie prezentowane jest stanowisko, że wyświetlanie użytkownikowi reklam behawioralnych nie wpływa w sposób istotny na jego sytuację, jeśli nie prowadzi do jego dyskryminacji lub nierównego traktowania²¹⁵. Grupa Robocza Artykułu 29 ds. Ochrony Danych także wychodzi z założenia, że w typowych sytuacjach, gdy profile tworzone są w oparciu o najpopularniejsze cechy osobowościowe, takie jak wiek i miejsce zamieszkania, decyzja o skierowaniu do danej osoby spersonalizowanej oferty nie będzie wywierała podobnie istotnego wpływu na osoby fizyczne. Zaznacza przy tym, że w indywidualnych przypadkach wpływ może okazać się istotny ze względu na stopień inwazyjności procesu profilowania, oczekiwania i wolę zainteresowanych osób, sposób dostarczenia materiału reklamowego lub wykorzystywania wiedzy o czynnikach zwiększających podatność osób, których dane dotyczą²¹⁶. Przykładem wykorzystywania wiedzy o konsumentach w celu manipulacji i zarazem inwazyjnego sposobu dostarczenia reklamy jest kierowanie reklam wysokooprocentowanych pożyczek do osób przechodzących trudności finansowe²¹⁷. Podobnie istotny skutek będzie mieć negatywny wpływ na sytuację rodzinną lub zawodową oraz pogorszenie stanu zdrowia z powodu np. zakupu w wyniku reklamy ryzykownych środków na odchudzanie²¹⁸. Zawarcie na skutek reklamy umów wiąże się dla takich osób z poważnymi konsekwencjami majątkowymi, osobistymi i zdrowotnymi. Można zatem uznać, że kierowanie reklam behawioralnych zakończonych ostatecznie skutecznym zawarciem umowy będzie spełniało przesłankę „istotnego wpływania w podobny sposób”²¹⁹. Nie jest to jednak, moim zdaniem, warunek *sine qua non* uznania reklam behawioralnych za profilowanie w rozumieniu art. 22 RODO. Nie każda reklama ma bowiem na celu nakłonienie do zawarcia umowy, czego przykładem jest np. targetowanie polityczne i społeczne. Tego rodzaju targetowanie z pewnością wywołuje podobny istotny wpływ na osobę profilowaną. W moim przekonaniu przesłanka istotnego wpływu powinna być rozumiana szerzej i spełniona zostaje m.in. w przypadku przesyłania wiadomości handlowych i reklam behawioralnych ingerujących w prawo do prywatności oraz różnicowaniu kuponów promocyjnych w zależności od profilu konsumenta²²⁰. Nie jest zatem konieczne uzależnianie istotnego wpływania w podobny sposób od osiągnięcia skutku w postaci zawarcia umowy. Podobnie stwierdziła Grupa Robocza art. 29 ds. Ochrony Danych, uznając, że już samo wyświetlanie reklam zakładów *online* w stosunku do osób znajdujących się w trudnej sytuacji finansowej może wchodzić w zakres art. 22

213 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 24.

214 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 24.

215 A. Mednis, *Prawo ochrony danych osobowych...*, s. 177.

216 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 25.

217 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 25.

218 M. Sakowska-Baryła, *Komentarz do art. 22 (w:) M. Sakowska-Baryła (red.), Ogólne rozporządzenie...*, s. 272.

219 P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 22 (w:) P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony...*, s. 434.

220 M. Czerniawski, *Komentarz do art. 22 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, s. 561-573.

RODO²²¹. Również zróżnicowanie cen w Internecie można uznać za wywierające istotny wpływ, jeśli prowadzi to do cen na tyle wysokich, że mają one charakter blokujący dostęp do pewnych towarów lub usług.

Z pewnością niejednoznaczność przestanki istotnego wpływu stanowi duże pole do nadużyć ze strony administratorów danych. Przy obecnych inwazyjnych metodach śledzenia konsumentów w sieci oraz coraz częstszemu opieraniu się reklamodawców na ich emocjach i obawach, a nie potrzebach, granice między zautomatyzowanym profilowaniem zwykłym, a zautomatyzowanym profilowaniem z artykułu 22 RODO zacierają się. Administratorzy często zakładają bezpodstawnie, że dokonywane przez nich profilowanie nie podlega restrykcjom z artykułu 22 RODO, gdyż nie wywołuje w stosunku do użytkowników istotnego wpływu podobnego do skutków prawnych. Niemniej jednak przy wykorzystywaniu do profilowania sztucznej inteligencji nie są oni w stanie określić jednoznacznie momentu, w którym decyzja nabierze dla danego konsumenta istotnego wpływu. W związku z tym proces profilowania powinien być traktowany przez administratorów z ostrożnością. W przypadku braku możliwości potwierdzenia, że decyzje skierowane do konsumentów nie będą wywierać na nie podobnego istotnego wpływu, zasadne byłoby stosowanie przez nich ograniczeń wynikających z artykułu 22 RODO.

3.2.3. Dopuszczalność wykorzystywania profilowania określonego w art. 22 RODO

W doktrynie dywaguje się, czy treść art. 22 ust 1 RODO oznacza zakaz, który łagodzony jest wyjątkami określonymi w ust. 2²²², czy też jest to raczej istotne uprawnienie osoby fizycznej, które nie ma charakteru zakazowego²²³. Niezależnie od przyjętej koncepcji osoby fizyczne są niejako automatycznie objęte ochroną przed tego typu przetwarzaniem²²⁴. Komisja początkowo była gotowa wprowadzić całkowity zakaz indywidualnych rozstrzygnięć opartych na automatycznym procesie przetwarzania danych osobowych, jednak zwyciężyło podejście lobbowane przez firmy technologiczne i administratorów danych. Tym samym powstała kompromisowa regulacja RODO²²⁵.

Profilowanie w rozumieniu art. 22 RODO jest co do zasady dopuszczalne w przypadku wystąpienia jednej z trzech sytuacji:

- a. jeżeli decyzja jest niezbędna do zawarcia lub wykonania umowy,
- b. jeżeli decyzja jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, lub
- c. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Wyjątek stanowią dane szczególnie wrażliwe określone w art. 9 ust. 1 RODO, które zgodnie z art. 22 ust. 4 RODO mogą być użyte do profilowania tylko w przypadku

221 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 26.

222 P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 22 (w:) P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony...*, s. 423-438.

223 M. Sakowska-Baryła, *Komentarz do art. 22 (w:) M. Sakowska-Baryła (red.), Ogólne rozporządzenie...*, s. 268- 269.

224 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 22.

225 M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, Europejski Przegląd Sądowy 2017, nr 5 (141), s. 40.

wystąpienia przestanki zgody lub gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym. W tej kwestii uwidacznia się jednak zasadniczy problem związany z wykorzystaniem do profilowania sztucznej inteligencji. Połączenie zwykłych danych osobowych może doprowadzić do powstania danych wywnioskowanych o charakterze szczególnie wrażliwym, które wykraczają poza dane podane dobrowolnie administratorowi²²⁶. Jeśli proces profilowania został oparty na przesłance niezbędności do zawarcia lub wykonania umowy, to pojawia się pytanie, czy tego rodzaju profilowanie nie staje się niedopuszczalne?

Ograniczenie z art. 9 RODO będzie stosowane, jeśli dane zostaną faktycznie wykorzystane do wnioskowania o szczególnych kategoriach danych. Sama możliwość połączenia danych i wytworzenia danych szczególnie wrażliwych nie jest wystarczająca²²⁷. Według Grupy Roboczej Art. 29 ds. Ochrony Danych zakresem tego ograniczenia objęte są również wrażliwe dane wywiedzione lub wywnioskowane z profilowania²²⁸. W praktyce kontrola algorytmu pod tym względem może okazać się niemożliwa i profilowanie oparte na przesłance niezbędności do zawarcia lub wykonania umowy może wykorzystywać informacje o charakterze szczególnie wrażliwym. W doktrynie można spotkać także stanowisko przeciwne, oparte na założeniu, że ograniczenie z art. 22 ust. 4 RODO nie dotyczy danych wywnioskowanych z profilowania²²⁹.

Warto wskazać na motyw 71 RODO, w którym zakazano stosowania profilowania w rozumieniu art. 22 RODO w odniesieniu do szczególnej grupy, jaką są dzieci. Według Grupy Roboczej Art. 29 ds. Ochrony Danych z uwagi na nieumieszczenie zakazu bezpośrednio w przepisie należy traktować je w większym stopniu jako zalecenia²³⁰. Tak elastyczne uregulowanie profilowania w stosunku do dzieci, w świetle powszechnego korzystania przez tę grupę z Internetu, budzi poważne wątpliwości. Wyraźnie odradza się stosowanie profilowania w celach marketingowych, związanych np. z reklamą behawioralną, na której wpływ są naturalnie bardziej podatne dzieci. Jeśli administrator zdecyduje się na taki proceder, to dzieci powinny podlegać szczególnej ochronie, gdyż są one mniej świadome ryzyka z tym związanego²³¹. Niestety, nie określono, na czym te szczególne środki ochrony miałyby polegać. Podobne zapatrywanie wyraziła Grupa Robocza Art. 29 ds. Ochrony Danych w opinii w sprawie internetowych reklam behawioralnych, stwierdzając, że dostawcy sieci reklamowych nie powinni proponować kategorii zainteresowań, które mogłyby być stosowane w celu kierowania reklam behawioralnych w stosunku do dzieci²³². Niezależnie od powyższego profilowanie dzieci w celach marketingowych jest dość powszechnie stosowane. Po części może być to spowodowane ograniczeniami technicznymi związanymi z weryfikacją rzeczywistego wieku odbiorców. Wydaje się, że rozpowszechnienie zagrożeń związanych z reklamą behawioralną opartą na profilowaniu przemawia za objęciem nieco bardziej restrykcyjną ochroną najmłodszej grupy konsumentów. Choć wywa-

226 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 17.

227 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 33.

228 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 17.

229 A. Mednis, *Prawo ochrony danych osobowych...*, s. 182.

230 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 33.

231 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 33.

232 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 18.

zenie efektywności mechanizmów sprawdzania wieku i ochrony prywatności jest niezwykle trudnym zadaniem, Grupa Robocza Art. 29 ds. Ochrony Danych oczekuje od administratorów, że będą podejmować rozsądne wysiłki w celu sprawdzenia, czy użytkownik osiągnął odpowiedni wiek, by wyrazić zgodę cyfrową, nie doprowadzając jednocześnie do nadmiernego przetwarzania danych²³³.

Dla porządku należy wspomnieć, że niektóre branże objęte są jeszcze surowszymi przepisami dotyczącymi zautomatyzowanego podejmowania decyzji, w tym profilowania. W przypadku branży ubezpieczeniowej ustawa o działalności ubezpieczeniowej i reasekuracyjnej²³⁴ określa zamknięty katalog danych, na których można oprzeć decyzje dotyczące oceny ryzyka ubezpieczeniowego bez konieczności uzyskiwania zgody osoby profilowanej²³⁵. W konsekwencji analityka ubezpieczeniowa oparta na sztucznej inteligencji i profilowaniu nie rozwija się w sposób dynamiczny. Bez względu jednak na wymienione tu odrębności profilowanie szczególne będzie musiało spełnić również podstawowe zasady przetwarzania określone w RODO.

4. Podstawy przetwarzania istotne z punktu widzenia personalizacji opartej na sztucznej inteligencji

4.1. Zasady przetwarzania danych zgodnie z art. 5 RODO

Wśród zasad przetwarzania za szczególnie ważne w kontekście personalizacji w celach marketingowych należy uznać: zasadę przejrzystości, zasadę ograniczenia celu oraz minimalizacji danych.

Z uwagi na szerokie wykorzystanie sztucznej inteligencji w procesie personalizacji największym zagrożeniem dla konsumentów, a zarazem poważnym wyzwaniem dla administratorów danych jest kwestia przejrzystości przetwarzania określona w art. 5 ust. 1 lit. a RODO. Procesy oparte na algorytmach trudno w sposób jasny i zrozumiały przełożyć na informacje dla konsumentów. Potęgowane jest to przez problem czarnych skrzynek oraz ochrony tajemnicy przedsiębiorstwa, które powodują jeszcze większą nieprzejrzystość algorytmów, a w konsekwencji – niepodważalność podejmowanych przez nie decyzji. Niemniej jednak administratorzy danych powinni czynić zadość tej zasadzie poprzez rzetelne realizowanie obowiązku informacyjnego, w tym szczególnego obowiązku informacyjnego związanego z zastosowaniem procesu profilowania. Dodatkowo obowiązek informacyjny z RODO będzie stanowił realizację prawa konsumentów do rzetelnej, prawdziwej i pełnej informacji wyrażonego w art. 24 ust. 2 pkt 2 ustawy o ochronie konkurencji i konsumentów. Innym elementem zasady przejrzystości jest audyt dostępnych dla użytkowników interfejsów i wyskakujących okienek (ang. *pop-upów*) w celu upewnienia się, że sposób prezentowania w nich informacji jest zrozumiały dla konsumenta.

Z kolei zasada ograniczenia celu przetwarzania wyrażona w art. 5 ust. 1 lit. b RODO ma fundamentalne znaczenie z uwagi na stale rosnącą w siłę działalność brokerów danych. Niekiedy legalność zebranych w ten sposób danych budzi wątpliwości,

233 Europejska Rada Ochrony Danych, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, 2020, s. 27.

234 Ustawa z dnia 11.09.2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, Dz.U. z 2015 r., poz. 1844. 235 A. Mednis, *Prawo ochrony danych osobowych...*, s. 209-210.

a kupno danych osobowych od brokerów częstokroć skutkuje nieuprawnioną zmianą celu przetwarzania. W 2017 r. taka sytuacja miała miejsce w przypadku brokera danych Experian, który zakupił dane osobowe od witryny internetowej *Emma's diary*, zawierającej porady dla przyszłych mam. Sprzedaż obejmowała ponad milion rekordów nielegalnie zabranych danych użytkowników, zawierających m.in.: nazwiska rodziców, adresy, liczbę posiadanych dzieci oraz daty ich narodzin, które zostały następnie wykorzystane w kampanii wyborczej Partii Pracy w Wielkiej Brytanii²³⁶. Podobnie oczywista niezgodność z zasadą ograniczenia celu będzie zachodzić w przypadku wykorzystania przez sklep internetowy danych o systemie operacyjnym używanym przez konsumenta w celu różnicowania wysokości przyznanego mu rabatu bez poinformowania o tym klientów²³⁷.

Należy podkreślić konieczność wyraźnego określania celów przetwarzania, co zapewni jednocześnie transparentność i przewidywalność przetwarzania oraz możliwość jego kontroli przez konsumenta. W ten sposób konsumenci są w stanie dokonywać świadomego wyboru, czy chcą powierzyć swoje dane firmie, która wykorzystuje je w bardzo szerokim zakresie²³⁸. Cele powinny zostać określone w sposób kompleksowy. Jednocześnie Grupa Robocza Art. 29 ds. Ochrony Danych wskazuje, że czasami zbyt szczegółowy opis może przynieść efekty przeciwne do zamierzonych²³⁹. W praktyce administratorzy najczęściej określają cele dość ogólnie, ukrywając profilowanie, np. pod sformułowaniem „poprawa doświadczeń użytkownika”²⁴⁰.

Wyświetlanie spersonalizowanych reklam na podstawie zainteresowań użytkowników oraz tworzenie profilu użytkownika powinny być określone jako odrębne cele przetwarzania. Użycie danych zebranych w jednym z tych celów na potrzeby drugiego celu jest sprzeczne z zasadą ograniczenia celu przetwarzania. Nie wolno również wzbogacać informacji zebranych dla celów reklam behawioralnych innymi informacjami²⁴¹. Przetwarzanie danych poza celem, w którym zostały one pierwotnie zebrane, według art. 6 ust. 4 RODO jest dopuszczalne tylko w ściśle określonych przypadkach. Należy brać pod uwagę m.in.: związek między pierwotnym celem i celem dalszego przetwarzania; kontekst, w którym zbierano dane; charakter danych; wpływ dalszego przetwarzania na osoby, których dane dotyczą; a także zabezpieczenia przyjęte przez administratora²⁴².

Niemniej jednak nie sposób nie zaznaczyć uwag wysuwanych przez branżę nowych technologii, zgodnie z którymi zasada ograniczenia celu może być poważnym utrudnieniem możliwości prowadzenia procesu uczenia algorytmu. Dane osobowe stanowią bowiem dane treningowe, które są niezbędne dla doskonalenia usług i produktów²⁴³.

236 Uzasadnienie kary nałożonej przez Information Commissioner's Office (ICO) na właściciela witryny internetowej *Emma's Diary*. Pozyskano z: <https://ico.org.uk/media/action-weve-taken/mpns/2259583/lifecycle-marketing-mother-and-baby-ltd-mpn-8-august-2018.pdf>. Dostęp: 11.06.2021 r.

237 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 23.

238 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 17.

239 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 16.

240 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security 2019, s. 4.

241 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 21.

242 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 12.

243 A. Krasuski, *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021, s. 312-322.

Ostatnią już zasadą, na jaką warto zwrócić szczególną uwagę, jest zasada minimalizacji danych określona w art. 5 ust. 1 lit. c RODO. Śledzenie aktywności użytkowników jest obecnie tak głębokie, że uzyskiwane za jego pomocą dane niekiedy są zbędne dla celów personalizacji, co jest niezgodne z zasadą minimalizacji danych, a także wymogami w zakresie ograniczenia przechowywania zawartych w art. 5 ust. 1 lit. e RODO²⁴⁴. Choć agregowanie takich danych w przypadku algorytmów sztucznej inteligencji może przyczyniać się do ich doskonalenia, to wnioskuje się, by przechowywanie ograniczało się do niezbędnego minimum²⁴⁵. Konflikt zasady minimalizacji oraz algorytmów sztucznej inteligencji opartych na analizie dużych zbiorów danych jest zauważalny w literaturze²⁴⁶. W przypadku tego typu algorytmów dane uzyskują bowiem znaczenie dopiero po dokonaniu analizy i ustaleniu powiązań między nimi. Tym samym początkowo zbiór danych faktycznie jest nadmierny.

4.2. Przesłanki legalizujące przetwarzanie danych osobowych w celu personalizacji treści

Personalizacja treści oraz profilowanie zwykle, które nie wykorzystuje szczególnych kategorii danych osobowych, zasadniczo może być oparte na każdej podstawie prawnej wymienionej w RODO, a więc na podstawie:

- a. zgody,
- b. niezbędności do wykonania umowy,
- c. niezbędności do celów wynikających z prawnie uzasadnionych interesów,
- d. niezbędności do wypełnienia obowiązku prawnego ciążącego na administratorze,
- e. niezbędności do ochrony żywotnych interesów,
- f. niezbędności do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Natomiast w przypadku profilowania wypełniającego przesłanki art. 22 RODO przesłanki przetwarzania zostały ograniczone. Z uwagi na ścisły związek personalizacji i profilowania z nowymi technologiami nie zawsze będzie możliwe jednoznaczne określenie właściwej podstawy przetwarzania²⁴⁷. Najistotniejsze znaczenie będą miały trzy pierwsze przesłanki - i to właśnie one zostały omówione szerzej w niniejszej pracy.

4.2.1. Przesłanka niezbędności do wykonania umowy

Przesłanka niezbędności do wykonania umowy w przypadku personalizacji przekazu będzie zachodziła rzadko. Będą to sytuacje, w których personalizacja i profilowanie są nieodłączną częścią usługi, np. w przypadku oferowania usługi ubezpieczenia pojazdu uzależnionej od analizy bezpieczeństwa jazdy kierowcy. W razie braku

244 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 12.

245 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 13.

246 M. Rojszczak, *Ochrona prywatności...*, s. 423-425.

247 D. Lubasz, *Big brother is watching you...*, s. 125-130.

przetwarzania danych dotyczących stylu jazdy konkretna usługa spersonalizowanego ubezpieczenia nie mogłaby zostać zrealizowana²⁴⁸. Personalizacja treści może także stanowić uzasadnienie niezbędności do wykonania umowy pod warunkiem ustalenia, że personalizacja stanowi nieodłączny i oczekiwany element usług *online*, co będzie zależeć od: charakteru usługi, oczekiwań przeciętnej osoby ustalonych na podstawie warunków świadczenia usługi oraz sposobu jej reklamowania²⁴⁹. Z tego względu platforma handlowa chcąc wyświetlać spersonalizowane sugestie dotyczące produktów nie może oprzeć się na przesłance niezbędności do wykonania umowy.

Niezbędność nie obejmuje przetwarzania, które jest jedynie przydatne do wykonania usługi. Nie chodzi tu też o niezbędność do celów biznesowych administratora danych²⁵⁰, polegających np. na zbieraniu danych osobowych zamiast pobierania faktycznej opłaty za oferowane usługi. Podobnie zanegowano konieczność przetwarzania danych do celów reklamy behawioralnej tylko dlatego, że reklama taka pośrednio finansuje świadczenie usługi²⁵¹.

Postanowienia umowne, które jedynie w sposób pozorny uzależniają świadczenie usługi od dokonania pewnych czynności przetwarzania, nie będą spełniały przesłanki niezbędności²⁵². W przypadku dokonania zakupu w sklepie internetowym możliwość wywiązania się z umowy nie będzie zależeć od stworzenia profilu preferencji konsumenta, nawet w przypadku zawarcia w umowie informacji o możliwości stosowania profilowania²⁵³. Nie będzie również niezbędne do wykonania umowy zbieranie danych w celu poprawy jakości usługi lub opracowania nowych funkcji usługi²⁵⁴.

4.2.2. Przesłanka uzasadnionego interesu administratora

Administratorzy często określają uzasadnione interesy związane z personalizacją w dość kontrowersyjny sposób, np. jako poznanie preferencji konsumentów w celu personalizacji ofert lub zwiększenie sprzedaży swoich produktów²⁵⁵. Przesłanki dopuszczalności przetwarzania opartego na uzasadnionym interesie zostały sformułowane w wyroku Trybunału Sprawiedliwości w sprawie C-40/17 *Fashion ID*²⁵⁶. Po pierwsze, konieczna jest realizacja uzasadnionych interesów przez administratora danych lub osobę trzecią, której dane są ujawniane. Po drugie, przetwarzanie danych osobowych musi odbywać się na potrzeby uzasadnionych interesów. Kluczowa w tym względzie jest przesłanka niezbędności przetwarzania do realizacji interesów, która

248 Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)..., s. 4.

249 Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)..., s. 16.

250 Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)..., s. 9.

251 Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)..., s. 15.

252 Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)..., s. 9.

253 Grupa Robocza Artykułu 29 ds. Ochrony Danych, Wytyczne dotyczące zautomatyzowanego podejmowania decyzji..., s. 15.

254 Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b)..., s. 15.

255 R. Steppe, *Online price discrimination and personal data...*, s. 780.

256 Wyrok TS z 29.07.2019 r. w sprawie C-40/17 *Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629, pkt 95.

powinna być interpretowana wąsko²⁵⁷. Po trzecie, w procesie ważenia interesów należy wykazać brak pierwszeństwa praw i wolności osoby objętej ochroną danych. W trakcie procesu ważenia interesów pod uwagę brana jest obecność dodatkowych zabezpieczeń, m.in. prawa do sprzeciwu²⁵⁸.

Administrator powinien, zgodnie z zasadą legalizmu, wziąć pod uwagę interesy osoby, której dane dotyczą, i sprawdzić, czy w wyniku personalizacji przekazu jego działania nie będą wiązały się z nadmierną ingerencją w prawo prywatności²⁵⁹. Według wytycznych Grupy Roboczej art. 29 ds. Ochrony Danych w trakcie tej analizy administrator powinien wziąć pod uwagę: poziom szczegółowości profilu, jego wszechstronność; skutki, jakie profilowanie wywrze na osobie, której dane dotyczą; a także zabezpieczenia prawidłowości procesu profilowania²⁶⁰. W literaturze zwraca się uwagę na aspekt łączenia profili, wykorzystywania wiedzy o podatnościach osób, których dotyczą dane, oraz uwzględniania oczekiwań zainteresowanych osób²⁶¹.

Po uwzględnieniu powyższych przesłanek można dojść do wniosku, że inwazyjne profilowanie i śledzenie osoby, przy wykorzystaniu różnych źródeł, urządzeń i brokerów informacji w celach marketingowych lub reklamowych, nie powinno być prowadzone na podstawie uzasadnionego interesu²⁶². Tym samym personalizacja treści oparta na monitorowaniu zachowania osób w sieci przy użyciu technologii śledzenia, w tym plików *cookies*, może być oparta wyłącznie na przestance zgody²⁶³. Za dopuszczalne należy uznać jednak śledzenie aktywności użytkownika na potrzeby własne właściciela strony internetowej²⁶⁴.

4.2.3. Przestanka zgody osoby, której dane dotyczą

Przestanka zgody jest wyrazem daleko posuniętej autonomii osoby fizycznej²⁶⁵ i powinna być podstawową przestanką legalizującą personalizację i profilowanie. Grupa Art. 29 ds. Ochrony Danych podkreśla, że zgoda *opt-in* jest wymagana m.in. do śledzenia i profilowania na potrzeby marketingu bezpośredniego, reklam behawioralnych lub reklam opartych na lokalizacji²⁶⁶. Zgoda musi być wyrażona przed rozpoczęciem przetwarzania²⁶⁷. Zaleca się dodatkowo jej odnawianie w określonych odstępach czasu²⁶⁸. Trzeba jednak podkreślić, że nawet jeśli przetwarzanie danych osobowych opiera się na zgodzie osoby, której dane dotyczą, nie uzasadnia to targetowania nieproporcjonalnego lub niesprawiedliwego²⁶⁹.

257 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 17.

258 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 18.

259 D. Lubasz, *Big brother is watching you...*, s. 124-125.

260 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 16.

261 D. Lubasz, *Big brother is watching you...*, s. 124-130.

262 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 16.

263 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 24.

264 K. Szymielewicz, W. Adamska, *Śledzenie i profilowanie w sieci: W czym problem?...*, s. 22.

265 D. Lubasz, *Big brother is watching you...*, s. 124-130.

266 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 46.

267 M. Czerniawski, *Komentarz do art. 22 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, s. 561-573.

268 Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017, s. 20.

269 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 18.

Zgoda powinna spełniać warunki określone w art. 4 pkt 11 i 7 RODO, a więc być dobrowolna, konkretna, świadoma, jednoznaczna i być wyrażona przez oświadczenie lub wyraźne potwierdzenie działania. W przypadku profilowania spełniającego przesłanki z art. 22 RODO zgoda powinna być ponadto wyraźna, co oznacza np. wymóg uzyskania potwierdzenia w formie pisemnej lub dokumentowej²⁷⁰. Oceniając dobrowolność zgody, należy wziąć pod uwagę fakt, czy zgoda jest zawarta w pakiecie jako niepodlegająca negocjacji część warunków umownych²⁷¹. Taka konstrukcja nie spełnia bowiem przesłanki dobrowolności zgody. Jeśli usługa obejmuje wiele operacji przetwarzania w więcej niż jednym celu, konsumenci powinni mieć zapewnioną swobodę wyboru celu, który akceptują. Niedopuszczalne jest łączenie celów przetwarzania w pakiety oparte na jednej, zbiorowej zgodzie²⁷².

Co istotne, z uwagi na powszechny proceder wykorzystywania danych poza wstępnie ustalonymi celami pierwotna zgoda nie może legitymizować dalszych celów przetwarzania²⁷³. Należy zagwarantować konsumentowi możliwość odmowy lub wycofania zgody bez żadnych negatywnych konsekwencji, np. bez obniżenia wartości usługi ze szkodą dla konsumenta²⁷⁴. Zgoda nie będzie ważna, jeżeli administrator zastosuje wstępnie zaznaczone pola wyboru lub uzna za jednoznaczne ze zgodą milczenie, brak aktywności ze strony użytkownika, a także kontynuowanie usługi²⁷⁵. Z tego powodu nie można uznać za prawidłowe wyrażenia zgody poprzez przewinięcie w dół strony internetowej²⁷⁶. Przed wyrażeniem zgody podmioty powinny zostać należycie poinformowane, m.in.: o celach przetwarzania, rodzaju zbieranych danych oraz możliwościach ich dalszego przekazania podmiotom trzecim, tak by wyrażona przez nich zgoda wynikała ze świadomej decyzji²⁷⁷. Przy przekazywaniu informacji powinno używać się jasnego i prostego języka zrozumiałego dla przeciętnego człowieka²⁷⁸.

Niestety w praktyce istnieje poważny problem z aspektem świadomości wyrażenia zgody. Z jednej strony konsumenci nie czytają wyświetlanych im *pop-upów* dotyczących przetwarzania danych osobowych i klikają przypadkowe elementy powodujące ich zniknięcie. Z drugiej strony administratorzy nie starają się zachęcać użytkowników do ich czytania, gdyż konstruują nieprzejrzyste i skomplikowane banery oparte na *dark patterns*. Administratorzy manipulują bowiem kolorystyką i rozmieszczeniem przycisków odpowiedzialnych za wyrażenie zgody w ten sposób, by użytkownicy podświadomie lub przez przypadek klikali na przyciski wyrażające zgodę na przetwarzanie²⁷⁹. Jak pokazują badania, nawet niewielkie zmiany w architekturze banerów są w stanie wpłynąć na decyzje podejmowane przez konsumentów²⁸⁰. Wybory dokonywane przez konsumentów w warunkach wstępnie zaznaczonych pól okazują się zdecydowanie bardziej korzystne dla administratorów od banerów opartych na domyślnej prywatności²⁸¹.

270 Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017, s. 18-19.

271 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 18.

272 Europejska Rada Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody...*, s. 12.

273 Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017, s. 12.

274 Europejska Rada Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody...*, s. 8.

275 Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017, s. 16.

276 Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017, s. 17.

277 D. Lubasz, *Big brother is watching you...*, s. 124-130.

278 Europejska Rada Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody...*, s. 16.

279 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 4.

280 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 1.

281 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 9.

Ponadto jednorazowe niewyrażenie zgody na przetwarzanie najczęściej nie będzie powodowało, że administrator przestanie próbować uzyskać ją przy kolejnych okazjach²⁸². W ten sposób użytkownicy otrzymują jedynie złudne poczucie wyboru²⁸³. Prędzej czy później użytkownik, chcąc szybko przejść do treści strony, wyrazi zgodę na przetwarzanie swoich danych. Z tego powodu niezwykle ważne jest, by zgoda uzyskiwana przez administratorów charakteryzowała się świadomością i swobodą.

5. Prawa konsumentów i obowiązki przedsiębiorców dotyczące procesu profilowania jako element ochrony przed nadmierną personalizacją

RODO daje do dyspozycji konsumentom prawa i gwarancje, które można wykorzystać do ochrony przed nadmierną personalizacją oraz związanym z nią procesem profilowania. Z kolei administratorzy, w związku z wykorzystywaniem procesu profilowania i personalizacji, są obciążeni dodatkowymi obowiązkami, głównie z zakresu zapewnienia przejrzystości i bezpieczeństwa.

5.1. Prawa konsumentów jako podmiotów danych

5.1.1. Prawo do ludzkiej interwencji

Zautomatyzowana decyzyjność oparta na sztucznej inteligencji i samodoskonalących się algorytmach z założenia nie podlega jakiegokolwiek kontroli człowieka²⁸⁴. Potencjalna niedokładność lub stronniczość algorytmów wiąże się także z większym ryzykiem dla praw i wolności obywateli²⁸⁵. W związku z tym unijny prawodawca, oprócz ogólnej zasady stanowiącej o tym, że przetwarzanie danych musi również odbywać się w sposób rzetelny i przejrzysty, przewidział pewne formy weryfikacji podejmowanych w ramach profilowania decyzji.

Zgodnie z art. 22 ust. 3 RODO, jeżeli automatyczne podejmowanie decyzji jest niezbędne do zawarcia lub wykonania umowy lub odbywa się na podstawie zgody, administrator jest zobowiązany do wdrożenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Obejmuje to w szczególności prawo konsumenta do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Zapewniono tym samym możliwość swoistego odwołania się od podjętej automatycznie decyzji do wyższej instancji, jaką ma być w tym przypadku człowiek. Osoba rozpatrująca takie odwołanie powinna dokonać oceny wszystkich danych oraz dodatkowych informacji przedstawionych przez osobę, której dotyczy decyzja²⁸⁶. Oprócz tego administratorzy są obowiązani do regularnego sprawdzania algorytmów pod kątem ich ewentualnej stronniczości, nieprawidłowości lub nadmiernego opierania się na ko-

282 Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017, s. 17.

283 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0. Structural asymmetries in digital consumer markets*, 2021, s. 33.

284 M. Kibil (w:) M. Gawroński (red.), *RODO Przewodnik ze wzorami*, Warszawa 2018, s. 244.

285 Rekomendacja CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, 2010, s. 1.

286 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 31.

relacjach statystycznych²⁸⁷. Prawo do ludzkiej interwencji bezsprzecznie wzmacnia pozycję konsumenta wobec profilowania i pozwala na kwestionowanie decyzji, które mają na niego istotny wpływ. Dostawcom rozwiązań z zakresu sztucznej inteligencji powinno zależeć na zapewnieniu przyjaznego i wartościowego dla konsumentów prawa do ludzkiej interwencji, gdyż tego typu weryfikacja zwiększa pośrednio zaufanie do samych procesów algorytmicznych.

5.1.2. Prawo do sprzeciwu

Prawo do sprzeciwu wynikające z art. 21 ust. 1 i 2 RODO nie dotyczy wyłącznie profilowania. Przysługuje w przypadku, gdy podstawą prawną jest realizacja zadania wykonywanego w interesie publicznym lub uzasadniony interes administratora danych, a osoba wnosząca sprzeciw znajduje się w słabszej sytuacji, którą sprzeciw równoważy²⁸⁸. W przypadku wyrażenia zgody uprawnienie do sprzeciwu jest zastąpio- ne dalej idącym prawem do wycofania zgody, które nie może być zakwestionowane przez administratora²⁸⁹. Wyrażenie sprzeciwu, w przeciwieństwie do wycofania zgody, nie jest automatycznie jednoznaczne z koniecznością zaprzestania profilowania i usunięcia danych.

Rozpatrując sprzeciw, administrator dokonuje ważenia podstaw do przetwarzania danych z interesami, prawami i wolnościami osoby, której dane dotyczą²⁹⁰. Oprócz testu równowagi interesów administrator powinien ocenić stopień niezbędności przetwarzania danych, w tym profilowania dla osiągnięcia zakładanego celu²⁹¹. Szczególna sytuacja konsumenta może polegać na tym, że ponosi on negatywne konsekwencje, związane np. z groźbą naruszenia sfery jego prywatności osobistej, zawodowej lub społecznej, a przy tym przetwarzanie danych w konkretnej sytuacji nie jest bezwzględnie konieczne²⁹². Dopiero po uznaniu, że interesy wnoszącego sprzeciw konsumenta są ważniejsze od podstaw przetwarzania administratora, konieczne będą zaprzestanie przetwarzania oraz usunięcie zebranych danych na podstawie art. 17 ust. 1 lit. c RODO.

Zgodnie z art. 21 ust. 2 i 3 RODO bezwzględnie skuteczny jest natomiast sprzeciw dotyczący przetwarzania w celu marketingu bezpośredniego²⁹³. Jest to niezwykle istotny przepis z punktu widzenia działań marketingowych opartych na reklamach spersonalizowanych. Osoba wnosząca sprzeciw nie ma w tym przypadku obowiązku uzasadniania swojej decyzji, a administrator nie ma możliwości dalszego przetwarzania danych po zgłoszeniu sprzeciwu. Przepis ten jest skuteczny niezależnie od podstawy prawnej wykorzystywanej do uzasadnienia przetwarzania, choć w praktyce najczęstszą podstawą jest uzasadniony interes administratora²⁹⁴ polegający na zwiększeniu zainteresowania jego towarami poprzez kierowanie reklam targetowanych lub finansowanie świadczenia usług przez sprzedaż powierzchni reklamowej lub danych osobowych. Pozostawiając na marginesie kwestie dopuszczalności stosowania

287 M. Sakowska-Baryła, *Komentarz do art. 22 (w:) M. Sakowska-Baryła (red.), Ogólne rozporządzenie...*, s. 274.

288 P. Fajgielski, *Komentarz do art. 22, Ogólne rozporządzenie o ochronie danych...*, s. 294.

289 P. Fajgielski, *Komentarz do art. 22, Ogólne rozporządzenie o ochronie danych...*, s. 294.

290 M. Czerniawski, *Komentarz do art. 21 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, s. 554-561.

291 A. Mednis, *Prawo ochrony danych osobowych...*, s. 183.

292 P. Fajgielski, *Komentarz do art. 22, Ogólne rozporządzenie o ochronie danych...*, s. 294.

293 M. Ciechomska, *Prawne aspekty profilowania...*, s. 41.

294 A. Mednis, *Prawo ochrony danych osobowych...*, s. 184.

tej podstawy prawnej w przedstawionych powyżej celach²⁹⁵, należy zaznaczyć, że administrator, chcąc korzystać z podstawy uzasadnionego interesu administratora, musi ułatwić osobie fizycznej wyrażenie uprzedniego sprzeciwu wobec wykorzystania jego aktywności do celu targetowania i profilowania²⁹⁶. Niestety, obowiązek ten jest skutecznie obchodzony przez administratorów. Mimo tego, że przy okazji pierwszej komunikacji z osobą, której dane dotyczą, administrator musi poinformować w sposób jasny o prawie do wniesienia sprzeciwu, a samo złożenie sprzeciwu powinno być dostępne również drogą elektroniczną, to konsumenci rzadko korzystają z tego prawa. Problem stanowi w głównej mierze konstrukcja *pop-up*ów dotyczących celów przetwarzania. Administratorzy nie przewidują bowiem możliwości jednoczesnego odznaczenia wszystkich okienek dotyczących uzasadnionego interesu administratora, a co za tym idzie, użytkownik chcący zgłosić sprzeciw musi w sposób manualny odznaczać kilkanaście, a czasem nawet kilkadziesiąt domyślnie zaznaczonych okienek. Praktyka obrotu zweryfikowała, że ochrona przed przetwarzaniem w celu marketingu bezpośredniego skonstruowana na podstawie mechanizmu *opt-out* jest wypaczana przez administratorów danych.

5.1.3. Prawo do usunięcia danych

Zgodnie z art. 17 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, m.in. jeżeli osoba cofnęła zgodę, na której opiera się przetwarzanie, lub wniosła skuteczny sprzeciw wobec przetwarzania. Co do zasady, administrator sam powinien zaprzestać przetwarzania danych osobowych w przypadku wystąpienia którejkolwiek z wyżej opisanych sytuacji. Niemniej jednak, jeżeli z jakiegoś powodu administrator nie dopełnił tego obowiązku, możliwe jest wysunięcie żądania usunięcia danych osobowych na podstawie art. 17 RODO²⁹⁷.

Zapewnienie prawa do usunięcia danych w sytuacji wykorzystywania samodoskonalącej się sztucznej inteligencji może powodować pewne konflikty²⁹⁸. Aby uznać, że administrator wywiązał się ze swojego obowiązku, powinien usunąć dane z modelu trenującego algorytm, co niekiedy, ze względu na ich objętość, może okazać się czasochłonne, kosztowne lub nieskuteczne²⁹⁹. Co istotne z punktu widzenia profilowania, administrator powinien usunąć dane wejściowe, jak i dane wynikowe³⁰⁰. Natomiast nie jest konieczne usuwanie danych użytych przez algorytm w celu zbudowania modelu, o ile są one anonimowe.

5.1.4. Prawo do sprostowania danych

Rozpatrując gwarancje dotyczące procesu personalizacji i profilowania, szczególną uwagę należy zwrócić na art. 16 RODO dotyczący prawa do sprostowania danych.

²⁹⁵ Szerzej w pkt 4.2 niniejszego rozdziału.

²⁹⁶ Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 18.

²⁹⁷ P. Fajgielski, *Komentarz do art. 17, Ogólne rozporządzenie o ochronie danych...*, s. 267-278.

²⁹⁸ E. F. Villaronga, P. Kieseberg, T. Li, *Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten*, *Computer Law & Security Review: The International Journal of Technology Law and Practice* 2017, s. 2.

²⁹⁹ A. Krasuski, *Status prawny sztucznego agenta...*, s. 350-353.

³⁰⁰ A. Mednis, *Prawo ochrony danych osobowych...*, s. 276.

Uzupełnia on prawo do zakwestionowania decyzji przysługujące na podstawie art. 22 ust. 3 RODO, które nie dotyczy wszystkich form profilowania. Prawo do sprostowania danych uprawnia do żądania od administratora sprostowania danych osobowych, które są nieprawidłowe. Dotyczy zarówno danych wejściowych służących do tworzenia profilu, jak i danych wyjściowych, czyli wyniku profilowania³⁰¹. Konsumenci mogą tym samym zakwestionować prawidłowość wykorzystanych do profilowania danych oraz słuszność zakwalifikowania ich do danej grupy lub kategorii³⁰².

Uprawnieniu do sprostowania danych odpowiada zasada prawidłowości danych wyrażona w art. 5 ust. 1 lit. d RODO. Według niej administratorzy powinni zapewniać prawidłowość, bezstronność i reprezentatywność danych na wszystkich etapach procesu profilowania, w tym przy: zbieraniu danych, ich analizowaniu, tworzeniu profilu danego konsumenta oraz wykorzystywaniu profilu do podjęcia decyzji wywierającej wpływ na daną osobę fizyczną³⁰³. Prawo do sprostowania danych daje możliwość monitorowania aktualności danych i poprawienia ich jakości.

Wydaje się jednak, że prawo do sprostowania danych ma w przypadku personalizacji i profilowania pewne ograniczenia. O ile weryfikacja decyzji o ustaleniu składki ubezpieczeniowej opartej na profilowaniu oraz użytych w celu jej podjęcia danych jest możliwa, o tyle sprostowanie wyniku profilowania w postaci wyświetlenia niewłaściwej reklamy behawioralnej *ex post* jest niemożliwe³⁰⁴. Możliwe jest jedynie wpłynięcie na reklamy wyświetlane w przyszłości. Kolejnym ciekawym aspektem tego prawa jest konieczność wykazania przez osobę żądającą sprostowania, że dane są nieprawidłowe³⁰⁵. Powstaje zatem pytanie, w jaki sposób osoba będąca profilowaną powinna wykazać, że przypisany jej w celu marketingowym profil behawioralny jest nieprawidłowy. Czy wystarczy samo zapewnienie osoby żądającej sprostowania, że dane osobowe będące częścią profilu są nieprawidłowe?

5.2. Obowiązki przedsiębiorców jako administratorów danych

5.2.1. Obowiązek informacyjny

Profilowanie w przeważającej części przypadków jest niewidoczne dla osoby, której dane dotyczą. Ponadto konsumenci są zróżnicowani z uwagi na poziom zrozumienia tego skomplikowanego pod względem technicznym procesu³⁰⁶. Niezbędne jest zapewnianie zrozumiałej, zwięzłej i przejrzystej dla przeciętnego konsumenta informacji o ryzykach związanych z przetwarzaniem, skutkach wiążących się z przekazaniem danych administratorowi oraz przysługujących uprawnieniach³⁰⁷. Z tego powodu tak ważne w przypadku profilowania jest czynienie zadość zasadzie transparentności

301 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 20.

302 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 20.

303 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 13.

304 A. Mednis, *Prawo ochrony danych osobowych...*, s. 132.

305 P. Fajgielski, *Komentarz do art. 17, Ogólne rozporządzenie o ochronie danych...*, s. 263.

306 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 10.

307 D. Lubasz, *Big brother is watching you...*, s. 130-132.

przetwarzania wyrażonej w art. 5 ust. 1 lit. a RODO. Podstawowym narzędziem służącym realizacji tej zasady jest obowiązek informacyjny.

Obowiązek informacyjny określony w art. 13 i 14 RODO stanowi szczególnie ważną gwarancję dla podmiotów danych poddawanych personalizacji i profilowaniu. Z perspektywy administratora stanowi on z kolei element składający się na zasadę przejrzystości przetwarzania. Pozwala m.in. na zidentyfikowanie administratora, odbiorców danych osobowych oraz celów i podstaw prawnych przetwarzania danych osobowych. W przypadku pozyskania danych z innych źródeł niż od osoby, której dane dotyczą, w ramach obowiązku informacyjnego podane zostanie również źródło pochodzenia danych osobowych.

Najczęściej obowiązek informacyjny sformułowany jest w formie polityki prywatności. Dokumenty te powinny mobilizować przedsiębiorców do przestrzegania ustanowionych w nich zasad, a dla konsumentów być źródłem przydatnych informacji o przetwarzaniu danych przez administratora i przysługujących im w związku z tym praw. W praktyce polityki prywatności niejednokrotnie stanowią skopiowany z innych stron, niezrozumiały oraz zbyt długi dokument, który jest ignorowany przez konsumentów³⁰⁸.

W szczególności ważne jest odpowiednie poinformowanie o celach przetwarzania. Słusznie wskazuje się, że użycie przy określaniu celu słowa „reklama”, gdy w rzeczywistości chodzi o reklamę spersonalizowaną, nie stanowi należytego wykonania obowiązku informacyjnego³⁰⁹. Za niejednoznaczne i niespełniające kryterium konkretności należy uznać cele takie jak poprawa doświadczeń użytkowników lub cele marketingowe³¹⁰. Ponadto, by dopełnić obowiązku przejrzystości, informacje powinny być przekazywane interaktywnie, a niekiedy z zastosowaniem kolejnych warstw powiadomień³¹¹.

Na podstawie art. 13 ust. 2 lit. f i art. 14 ust. 2 lit. g RODO administrator, oprócz typowych informacji dotyczących przetwarzania, jest zobowiązany do poinformowania o stosowaniu profilowania w rozumieniu art. 22 RODO, podania istotnych informacji na temat zasad zautomatyzowanego podejmowania decyzji, a także poinformowania o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. W tym samym zakresie podmiotowi danych przysługuje na podstawie art. 15 ust. 1 lit. h RODO prawo dostępu do tych informacji. Ponadto na podstawie art. 15 ust. 3 RODO na żądanie podmiotu danych administrator udostępnia dane wykorzystane do stworzenia profilu, informacje o samym profilu i kategoriach, do których zakwalifikowano daną osobę³¹².

Administrator powinien, w celu zagwarantowania zasady rzetelności przetwarzania, wytłumaczyć proces, któremu poddawany jest podmiot danych, oraz wskazać jego potencjalne skutki³¹³. Prawo do wyjaśnienia w doktrynie zostało określone jako opis procesu, w którym określony zestaw danych wejściowych doprowadził do konkretnie-

308 C. Castelluccia, A. Narayanan, *Privacy considerations of online behavioural tracking...*, s. 20.

309 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 26.

310 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 15-16.

311 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 27.

312 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 19.

313 M. Czerniawski, *Komentarz do art. 22 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, s. 561-573.

go wniosku³¹⁴. Informacje te są konieczne, by konsument podlegał decyzjom, które rozumie i jest w stanie kontrolować³¹⁵. Pojęcie istotnych informacji należy rozumieć szeroko, jako informację o stosowaniu narzędzi analitycznych i śledzących oraz tworzeniu profili osobowych przez portale społecznościowe³¹⁶. Choć Grupa Robocza Art. 29 ds. Ochrony Danych zaznacza, że niezależnie od typu profilowania podmiotowi danych należą się informacje o fakcie i zasadach jego stosowania³¹⁷, to w przypadku profilowania niewypełniającego przesłanek z art. 22 RODO udzielanie informacji wymaganych przez art. 13 ust. 2 lit. f i art. 14 ust. 2 lit. g RODO jest uważane jedynie za dobrą praktykę³¹⁸. Niemniej jednak w doktrynie sugeruje się, że w celu zachowania rzetelności i przejrzystości przetwarzania w niektórych sytuacjach podawanie powyższych informacji jest wymagane niezależnie od tego, czy w ramach profilowania podejmowana jest decyzja w rozumieniu art. 22 RODO³¹⁹.

Niestety systemy sztucznej inteligencji niekiedy utrudniają wypełnienie obowiązku informacyjnego w sposób prawidłowy, a tym samym także wypełnienie zasady przejrzystości przetwarzania. Problem wiąże się z techniczną stroną algorytmów profilowania, których zmienne nie zawsze są łatwe do wyjaśnienia w sposób zrozumiały dla podmiotów danych³²⁰. W przypadku samodoskonalącej się sztucznej inteligencji zmienne, którymi kieruje się algorytm, nie będą znane także samym twórcom³²¹. Innym źródłem ograniczenia prawa do informacji o profilowaniu jest korzystanie z oprogramowania chronionego przez tajemnicę handlową lub prawa autorskie do algorytmów³²². Z punktu widzenia zasady przejrzystości obowiązek ten nie oznacza z pewnością konieczności udostępniania całości algorytmu, a jedynie wyjaśnienia, jakie czynniki zadecydowały o podjęciu konkretnej decyzji.

Może to obejmować np. kategorie danych wykorzystanych do profilowania wraz z podaniem powodów, dla których są one uznane za istotne, sposób tworzenia profili oraz ich późniejsze wykorzystywanie do podjęcia decyzji³²³. To pozwala podmiotom danych na ocenę, czy w ich sytuacji system podjął właściwą decyzję³²⁴. Postuluje się, by w celu zadośćuczynienia obowiązkowi informacyjnemu tworzyć dodatkowe algorytmy, których celem będzie identyfikowanie czynników wziętych pod uwagę przy podejmowaniu decyzji³²⁵. Z kolei w celu przedstawienia przewidywanych konsekwencji profilowania rekomenduje się opieranie się na autentycznych i konkretnych przykładach³²⁶.

314 F. Doshi-Velez, M. Kortz, *Accountability of AI Under the Law: The Role of Explanation*, Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper 2017, s. 2-3.

315 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013, s. 45.

316 M. Ciechomska, *Prawne aspekty profilowania...*, s. 41.

317 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 18-19.

318 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 28.

319 A. Mednis, *Prawo ochrony danych osobowych...*, s. 263.

320 FIGI Security, Infrastructure and Trust Working Group, *Big data, machine learning...*, s. 35.

321 A. Krasuski, *Status prawny sztucznego agenta...*, s. 338-350.

322 M. Ciechomska, *Prawne aspekty profilowania...*, s. 42.

323 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 36.

324 M. Ciechomska, *Prawne aspekty profilowania...*, s. 42.

325 A. Krasuski, *Status prawny sztucznego agenta...*, s. 338-350.

326 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 30.

W doktrynie zwraca się również uwagę na rolę obowiązku informacyjnego w przypadku różnicowania cen produktów i usług³²⁷. Dla konsumenta istotne znaczenie ma informacja o tym, czy zaproponowana w wyniku profilowania cena jest wyższa lub niższa niż przeciętna. Postulaty te zostały częściowo zrealizowane w nowym obowiązku informacyjnym wprowadzonym za sprawą „Nowego Ładu dla konsumentów” do dyrektywy 2011/83/UE w art. 6 ust. 1 lit. ea. W dalszym ciągu konsument nie zyskał jednak narzędzi do zweryfikowania, czy aby na pewno identyczne kryteria zastosowane w stosunku do innej osoby spowodowały wyświetlenie identycznej ceny³²⁸. Póki konsument nie będzie miał prawa do porównania swojej sytuacji z sytuacją innych konsumentów, może jedynie mieć nadzieję, że uzyskane od administratora wyjaśnienie jest zgodne z prawdą.

5.2.2. Ocena skutków dla ochrony danych

Ocena skutków dla ochrony danych (ang. *Data Protection Impact Assessment*, DPIA) to proces pozwalający opisać przetwarzanie, ocenić jego niezbędność i proporcjonalność oraz pomóc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych przez jego ocenę i ustalenie odpowiednich środków zaradczych³²⁹. Proces DPIA należy przeprowadzić przed rozpoczęciem przetwarzania i dokonywać jego cyklicznej aktualizacji³³⁰. Składa się on z trzech etapów:

- a. oceny, czy przetwarzanie wiąże się z dużym ryzykiem naruszenia praw lub wolności osób fizycznych,
- b. dokonania oceny skutków przetwarzania dla danych osobowych,
- c. uprzednich konsultacji z organem nadzorczym, o ile ujawniono istnienie wysokiego ryzyka szczegółowego³³¹.

Ocena jest obowiązkowa tylko wtedy, gdy proces przetwarzania wiąże się z dużym ryzykiem naruszenia praw lub wolności osób fizycznych. Według art. 35 ust. 3 lit. a RODO administrator ma wymóg przeprowadzenia oceny skutków dla ochrony danych w przypadku prowadzenia systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną. Oznacza to, że w tym przypadku pierwszy etap oceny skutków dla ochrony danych automatycznie uznajemy za spełniony - profilowanie wiąże się z dużym ryzykiem naruszenia praw lub wolności osób fizycznych. Jako że nie użyto w tym przypadku słowa „wyłącznie”, można założyć, że obowiązek oceny dotyczy także profilowania zautomatyzowanego częściowo³³².

327 A. Mednis, *Prawo ochrony danych osobowych...*, s. 132.

328 A. Mednis, *Prawo ochrony danych osobowych...*, s. 132.

329 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679*, 2017, s. 4.

330 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące oceny skutków...*, s. 17.

331 A. Mednis, *Prawo ochrony danych osobowych...*, s. 291.

332 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji...*, s. 34.

Warto w tym kontekście zwrócić uwagę na przesłankę systematyczności i kompletności, którą powinna cechować się ocena czynników osobowych. Jest to pojęcie w znacznym stopniu uznaniowe, co nie wpływa pozytywnie na zakres zastosowania art. 35 ust. 3 lit. a RODO. Jeżeli przesłanka systematyczności i kompletności nie zostanie spełniona, administrator zgodnie z pierwszym etapem ocenia, czy przetwarzanie wiąże się z dużym ryzykiem naruszenia praw lub wolności osób fizycznych³³³. Obowiązkowy charakter oceny skutków przetwarzania w tym przypadku będzie zatem uzależniony od wyników pierwszego etapu. Istotnym kryterium decydującym o tym, że przetwarzanie może charakteryzować się dużym ryzykiem, jest m.in. dokonywanie oceny lub punktacji³³⁴. Kryterium to spełniają przedsiębiorstwa tworzące profile behawioralne oparte na wykorzystaniu lub nawigacji na swoich stronach internetowych³³⁵, ale nie jest to przesądzające o zaistnieniu wysokiego ryzyka. Grupa Robocza art. 29 ds. Ochrony Danych uważa bowiem, że dla strony internetowej wyświetlającej reklamy behawioralne oparte na analizie aktywności internautów na tej stronie nie będzie wymagane przeprowadzenie procesu DPIA, choć kryterium oceny lub punktacji wystąpi. Nieco odmienna teza została sformułowana w wytycznych 8/2020 dotyczących kierowania reklam do użytkowników mediów społecznościowych. Grupa Robocza art. 29 ds. Ochrony Danych uznała, że w niektórych przypadkach charakter reklamowanego produktu lub usługi, treść komunikatu lub sposób, w jaki reklama zostanie dostarczona, mogą mieć wpływ na wrażliwe osoby³³⁶. Aby zweryfikować istnienie wysokiego ryzyka dla praw i wolności osób fizycznych, w tym przypadku należy wziąć pod uwagę: cel kampanii reklamowej, stopień jej ingerencji oraz to, czy kierowanie wiąże się z przetwarzaniem zaobserwowanych lub wywnioskowanych danych osobowych.

Ocena skutków przetwarzania w przypadku personalizacji profilowania będzie polegała m.in. na opisie: planowanej operacji profilowania i celów przetwarzania, oceny niezbędności oraz proporcjonalności profilowania, a także oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą³³⁷. Ocena będzie zawierać również opis środków zapobiegających istniejącemu ryzyku, m.in.: prawa do ludzkiej interwencji, obowiązku informacyjnego, prawa do sprzeciwu. Gdyby wprowadzone środki zaradcze okazały się niewystarczające, należy zaprzestać przetwarzania³³⁸.

6. Wnioski częściowe

Rolą prawa ochrony danych jest próba pogodzenia dwóch przeciwstawnych interesów – ochrony prawa do prywatności po stronie konsumentów oraz potrzeby reklamodawców, by jak najskuteczniej dotrzeć do przyszłych klientów. Argumentem przedsiębiorców jest fakt, że zbyt restrykcyjna ochrona danych osobowych może spowodować spadek ich konkurencyjności w dziedzinie sztucznej inteligencji³³⁹. Postuluje

333 K. Witkowska-Nowakowska, *Komentarz do art. 35 (w:) E. Bielak-Jomaa, D. Lubasz (red.), RODO...*, s. 728-756.

334 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące oceny skutków...*, s. 10.

335 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące oceny skutków...*, s. 10.

336 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 30.

337 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące oceny skutków...*, s. 20.

338 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 31.

339 M. Humerick, *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, Santa Clara High Technology L. J. 2018, nr 34, s. 396.

się, że prywatność nie jest celem samym w sobie i przyszłość ochrony danych musi ewoluować na rzecz bardziej elastycznego podejścia opartego na pewnej dostępności danych osobowych³⁴⁰. Jednymi z wysuwanych propozycji są przyjęcie, że podstawowe dane osobowe, takie jak: imię, nazwisko, adres e-mailowy, numer telefonu, nie są objęte ochroną, a także wzmocnienie kar za ich nieodpowiednie wykorzystywanie³⁴¹.

Z kolei konsumenci wraz z rozwojem technik personalizacji i śledzenia są narażeni na nowe zagrożenia związane z nieprzejrzystością i zbyt dużym skomplikowaniem tych procesów. Pogłębia się tym samym problem utraty kontroli nad prywatnością w erze cyfrowej. Wiele przedsiębiorców dokonało tzw. złośliwego wdrożenia RODO i ich praktyki agresywnego wymuszania zgód na użytkownikach balansują na granicy legalności³⁴². Model, w którym obecnie odbywa się zbieranie zgód na przetwarzanie danych osobowych z punktu widzenia konsumentów, nie zapewnia wystarczającej ochrony.

RODO daje konsumentom wiele narzędzi do egzekwowania swojej prywatności. Narzędzia te nie są jednak moim zdaniem skutecznie wdrażane i wykorzystywane przez administratorów, co jest warunkiem koniecznym do osiągnięcia wysokiego poziomu ochrony konsumentów. Konsumenci nie korzystają z praw przysługujących im na podstawie działu III RODO, gdyż nie są świadomi skali zbierania i wykorzystywania ich danych osobowych³⁴³. Administratorzy powinni odpowiedzieć na te problemy poprzez skuteczniejsze i bardziej odformalizowane informowanie użytkowników o tym, jakie dane osobowe są gromadzone, w jaki sposób są wykorzystywane i komu są one udostępniane³⁴⁴. To właśnie zasada transparentności przetwarzania danych będzie stale zyskiwała na znaczeniu. Uważam, że przepisy dotyczące szczególnych gwarancji w przypadku profilowania powinny być interpretowane w jak najszerszym zakresie, tak aby profilowanie zwykle stało się dla konsumentów bardziej widoczne i zrozumiałe.

340 A. Mednis, *Prawo ochrony danych osobowych...*, s. 338.

341 W. Iszkowski, *O „nieciągłościach” ochrony danych osobowych* (w:) A. Mednis (red.), *Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016, s. 33-47.

342 K. Szymielewicz, W. Adamska, *Śledzenie i profilowanie w sieci: W czym problem?...*, s. 29.

343 A. Krasuski, *Status prawny sztucznego agenta...*, s. 338-350.

344 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Platformy internetowe i jednolity rynek cyfrowy...*, s. 11-12.

Rozdział III.

Personalizacja oparta na sztucznej inteligencji jako nieuczciwa praktyka handlowa

1. Uwagi wprowadzające

Konsumenci codziennie muszą podejmować ogromną liczbę decyzji dotyczących transakcji. Przedsiębiorcy chcą wpływać na te decyzje m.in. poprzez zastosowanie praktyk opartych na personalizacji. Wiele z nich, np.: zaniechania informacyjne, dyskryminacyjna personalizacja cenowa oraz reklama behawioralna o charakterze manipulacyjnym i wprowadzającym w błąd, budzi wątpliwości natury etycznej i prawnej. Niektóre z tych praktyk mogą przyczyniać się także do ograniczania zdolności poznawczych konsumentów i utrudniania dokonywania decyzji transakcyjnych³⁴⁵. W takiej sytuacji praktyki oparte na personalizacji mogą zostać zakwalifikowane jako nieuczciwe praktyki handlowe w rozumieniu dyrektywy 2005/29/WE o nieuczciwych praktykach handlowych (dalej: dyrektywa, dyrektywa 2005/29/WE). Dyrektywa jest bowiem wystarczająco kompleksowa, żeby objąć szybko zmieniające się w erze cyfrowej produkty oraz metody ich marketingu i sprzedaży³⁴⁶. Konsumentom zapewnia się na jej podstawie ochronę przed konsekwencjami związanymi z zawieraniem umów w warunkach manipulacji oraz niedostatecznej informacji³⁴⁷.

2. Pojęcie nieuczciwej praktyki handlowej

Praktyka handlowa, zgodnie z art. 2 lit. d dyrektywy 2005/29/WE, oznacza każde działanie przedsiębiorcy, jego zaniechanie, sposób postępowania, oświadczenie lub komunikat handlowy, w tym reklamę i marketing, które są bezpośrednio związane z promocją, ze sprzedażą lub z dostawą produktów do konsumentów. Może przybrać formę działania faktycznego, np. spersonalizowanej reklamy *online*, lub prawnego, np. dostosowywania warunków umownych w wyniku profilowania konsumentów³⁴⁸. Są one bezpośrednio związane z promocją lub ze sprzedażą produktu. Z orzecznictwa Trybunału Sprawiedliwości wynika, że jednorazowość działania lub zaniechania przedsiębiorcy oraz skierowanie go tylko do jednego konsumenta nie wykluczają

345 G. Sarton, *Artificial Intelligence: Challenges for EU Citizens and Consumers*, Policy Department for Economic, Scientific and Quality of Life Policies 2019, s. 5.

346 Dokument roboczy Służb Komisji, *Wytoczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 6.

347 R. Stefanicki, *Koncepcja zupełnej harmonizacji prawa ochrony konsumenta (na przykładzie dyrektywy o nieuczciwych praktykach handlowych)*, Państwo i Prawo 2011, nr 6, s. 57.

348 E. Rutkowska-Tomaszewska, *Nieuczciwe praktyki na rynku bankowych usług konsumenckich*, Warszawa 2011, s. 43-46.

stwierdzenia stosowania nieuczciwej praktyki³⁴⁹. Dotyczy to także działań opartych na personalizacji, które z zasady cechują się dużym stopniem zindywidualizowania i mogą być wykorzystywane w stosunku do niewielkiej grupy konsumentów, a nawet konkretnego konsumenta.

Ocena praktyki handlowej pod kątem nieuczciwości została oparta na trzypoziomym systemie - klauzuli generalnej, tzw. małych klauzulach generalnych, które obejmują dwa rodzaje najczęściej występujących nieuczciwych praktyk handlowych, oraz zamkniętym katalogu praktyk bezwzględnie zakazanych w każdych okolicznościach, czyli tzw. czarnej liście zawartej w załączniku I do dyrektywy. W pierwszej kolejności należy stwierdzić, czy praktyka nie jest jedną z nieuczciwych praktyk handlowych wymienionych na czarnej liście³⁵⁰. Jeśli tak, nie jest konieczne ocenianie konkretnego przypadku w świetle małych klauzul generalnych lub klauzuli generalnej. W przypadku stwierdzenia, że praktyka mieści się w wykazie określonym w załączniku I, trzeba zbadać, czy nie spełnia przesłanek jednej z małych klauzul generalnych, tj. agresywnej praktyki handlowej lub praktyki wprowadzającej w błąd³⁵¹. Co istotne, w świetle orzecznictwa Trybunału Sprawiedliwości zakwalifikowanie określonej praktyki handlowej jako wprowadzającej w błąd lub agresywnej nie wymaga odwoływania się do przesłanek określonych w klauzuli generalnej³⁵², która jest analizowana jako ostatnia. Ma ona zastosowanie do wszelkich niestypizowanych nieuczciwych praktyk handlowych, które nie mieszczą się w kategoriach czarnej listy oraz nazwanych praktyk handlowych³⁵³.

Dyrektywa jest swoistym mechanizmem bezpieczeństwa w przypadkach, które nie są regulowane w innych aktach prawnych³⁵⁴. Z tego powodu mogłaby stanowić doskonały instrument ochrony przed nieuczciwymi praktykami związanymi z personalizacją, które wciąż czekają na bezpośrednie uregulowanie³⁵⁵. Wskazuje się, że dyrektywa może być narzędziem wykorzystywanym do oceny nowych praktyk internetowych, w tym reklam *online*³⁵⁶. Niemniej jednak, zgodnie z art. 3 dyrektywy, w przypadku kolizji z innymi przepisami regulującymi szczególne aspekty nieuczciwych praktyk handlowych, dyrektywa ustępuje im pierwszeństwa. Do takich szczególnych aspektów należą m.in. wymogi informacyjne i zasady dotyczące sposobu prezentowania informacji konsumentom³⁵⁷. W wytycznych dotyczących stosowania dyrektywy 2005/29/WE zaznaczono jednak, że może być ona stosowana do praktyk handlowych, które są uregulowane w innych ogólnych bądź sektorowych przepisach unijnych³⁵⁸.

349 Wyrok TS z 16.04.2015 r. w sprawie C-388/13 *Nemzeti Fogyasztóvédelmi Hatóság v. UPC Magyarország Kft*, ECLI:EU:C:2015:225, pkt 41-42.

350 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 60.

351 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 60.

352 Wyrok TS z 19.09.2013 r. w sprawie C-435/11 *CHS Tour Services GmbH v. Team4 Travel GmbH*, ECLI:EU:C:2013:574, pkt 45.

353 M. Namysłowska, *Dziesięć lat dyrektywy 2005/29/WE o nieuczciwych praktykach handlowych*, Europejski Przegląd Sądowy 2016, nr 3, s. 5.

354 Komunikat Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie stosowania dyrektywy o nieuczciwych praktykach handlowych. *Osiągnięcie wysokiego poziomu ochrony konsumentów. Budowanie zaufania do rynku wewnętrznego*, COM(2013) 138 final, s. 2.

355 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 95.

356 Komunikat Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie stosowania dyrektywy o nieuczciwych praktykach handlowych..., s. 6.

357 Motyw 10 dyrektywy 2005/29/WE.

358 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 16.

3. Zakres stosowania dyrektywy

Dyrektywa 2005/29/WE chroni konsumentów przed nieuczciwymi praktykami handlowymi, które wywierają wpływ na podejmowane przez nich decyzje dotyczące transakcji³⁵⁹. Zwrot „decyzja dotycząca transakcji” obejmuje nie tylko decyzję o zakupie, ale też decyzje przygotowawcze bezpośrednio z nią związane³⁶⁰, co znajduje potwierdzenie w art. 3 ust. 1 dyrektywy. W kontekście praktyki personalizacji działaniem poprzedzającym zakup jest decyzja o kliknięciu i przejściu na odpowiednią stronę internetową w następstwie oferty handlowej³⁶¹. Dyrektywa ma zastosowanie również w przypadku, w którym nieuczciwa praktyka nie będzie skutkować przystąpieniem przez konsumenta do transakcji lub umowy. Wystarczające jest samo poświęcenie większej ilości czasu np. na realizację procesu rezerwacji³⁶². W związku z powyższym należy przyjąć, że internetowe reklamy behawioralne wchodzą w zakres stosowania dyrektywy jako praktyki reklamowe³⁶³.

Zgodnie z motywem 6 dyrektywy nie ma ona zastosowania do praktyk związanych z reklamą, takich jak stosowanie zachęt, które mogą w sposób zgodny z prawem oddziaływać na postrzeganie produktów przez konsumentów i wpływać na ich zachowanie, nie zakłócając ich zdolności do podejmowania świadomej decyzji. W przypadku personalizacji granica między dopuszczalnym wpływem na konsumenta a wpływem zniekształcającym zdolność do podejmowania decyzji jest niejednoznaczna. Trudno określić, jak profilowanie i personalizacja wpływają na decyzje kontraktowe konsumenta i czy prowadzą do zaburzenia procesu decyzyjnego. Ocena tego, czy praktyka handlowa jest nieuczciwa, musi odbywać się każdorazowo na podstawie analizy indywidualnego przypadku³⁶⁴.

4. Wpływ personalizacji opartej na sztucznej inteligencji na pojęcie przeciętnego i wrażliwego konsumenta

Według danych GUS w 2020 r. w Polsce dostęp do Internetu w domu miało aż 90% gospodarstw domowych³⁶⁵. Co najmniej raz w tygodniu korzystało z niego 81% osób w wieku od 16 do 74 lat. Widoczna jest tendencja wzrostowa, gdyż w poprzednim roku było to tylko 78% osób³⁶⁶. Z jednej strony część konsumentów jest już świadoma technik behawioralnych i podejmowane przez siebie decyzje zakupowe uważa za rozsądne i przemyślane. Z drugiej strony umiejętności cyfrowe dużej grupy konsumentów wciąż są na niskim poziomie. Konieczna jest zatem analiza tego, jak nowe technologie, w tym personalizacja, wpływają na pojęcie przeciętnego i wrażliwego konsumenta.

359 M. Sieradzka, *Komentarz do ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym*. Komentarz, Warszawa 2008, s. 297.

360 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 41.

361 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 42.

362 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 45.

363 J. Laux, S. Wachter, B. Mittelstadt, *Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice*, *Common Market Law Review* 2021, nr 58, s. 719-750.

364 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 6.

365 Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, *Spółeczeństwo informacyjne w Polsce w 2020 r.*, s. 131...

366 Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, *Spółeczeństwo informacyjne w Polsce w 2020 r.*, s. 137...

4.1. Pojęcia przeciętnego i wrażliwego konsumenta jako punkt odniesienia dla oceny nieuczciwości praktyki handlowej

Dyrektywa 2005/29/WE przewiduje trzy modele konsumentów: konsumenta przeciętnego, przeciętnego członka grupy konsumentów, do których praktyka handlowa jest skierowana, oraz konsumenta wrażliwego³⁶⁷. Modele te są wykorzystywane do oceny praktyk handlowych pod kątem ich nieuczciwości.

Motyw 18 dyrektywy 2005/29/WE stanowi, że przy ocenie nieuczciwości praktyk handlowych konieczne jest zbadanie wpływu praktyki na przeciętnego konsumenta. Pojęcie to wywodzi się z orzecznictwa Trybunału Sprawiedliwości. Zgodnie z nim przeciętny konsument to konsument dostatecznie dobrze poinformowany, dostatecznie spostrzegawczy i ostrożny³⁶⁸. Przy interpretacji pojęcia przeciętnego konsumenta należy uwzględnić art. 114 TFUE, który przewiduje wysoki poziom ochrony konsumentów³⁶⁹. Można założyć, że model przeciętnego konsumenta nie zawsze będzie odpowiadał rzeczywistości, zwłaszcza w przypadku konsumentów poruszających się w Internecie i mających do czynienia z praktykami opartymi na sztucznej inteligencji.

Konsument jest grupą zróżnicowaną, dlatego istnieje potrzeba uwzględniania ich sytuacji, czynników społecznych, językowych i kulturowych, które mogą różnić się w poszczególnych państwach członkowskich. W związku z powyższym nie można zakładać, że test przeciętnego konsumenta jest testem statystycznym, o czym wprost stanowi motyw 18 dyrektywy. W doktrynie podkreśla się, że na wzorzec przeciętnego konsumenta, a w szczególności na poziom jego uwagi w danej sytuacji, mogą wpływać m.in. cena oraz rodzaj produktu³⁷⁰. Na przykład w przypadku oferty pożyczki konsument powinien wykazać się większą uważnością niż w przypadku reklamy odzieży. Od przeciętnego konsumenta można oczekiwać tylko pewnego stopnia wiedzy, która nie musi być kompletna i profesjonalna³⁷¹. Nie należy zakładać w sposób automatyczny, że przeciętny konsument zawsze ma możliwość uzyskania niezbędnych informacji i podjęcia na ich podstawie korzystnej dla siebie decyzji³⁷², gdyż niekiedy konieczne jest odstępstwo od tak skonstruowanego wzorca.

Zgodnie z motywem 18 dyrektywy, jeżeli praktyka jest skierowana do szczególnej grupy konsumentów, ocena powinna następować z perspektywy przeciętnego członka takiej grupy. Jest to drugi model przeciętnego konsumenta, który został określony w dyrektywie. Na przykład w przypadku reklam zabawek dla dzieci grupą docelową są dzieci - i to z ich perspektywy trzeba dokonywać oceny nieuczciwości danej praktyki. Tym samym model przeciętnego konsumenta konstruowany będzie z uwzględnieniem cech tejże grupy.

367 J. Laux, S. Wachter, B. Mittelstadt, *Neutralizing online behavioural advertising...*, s. 719-750.

368 Wyrok TS z 16.07.1998 r. w sprawie C-210/96 *Gut Springenheide i Tusky v. Oberkreisdirektor des Kreises Steinfurt - Amt für Lebensmittelüberwachung*, ECLI:EU:C:1998:369, pkt 31; motyw 18 dyrektywy 2005/29/WE.

369 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 47.

370 A. Wiewiórowska-Domagalska, A. Kunkiel-Kryńska (w:) K. Osajda (red.) *Prawo konsumenckie. Komentarz*, Tom VII, Warszawa 2019, s. 259.

371 M. Sieradzka, *Wzorzec przeciętnego konsumenta jako punkt odniesienia przy dokonywaniu oceny nieuczciwości praktyki rynkowej. Glosa do wyroku SN z dnia 4 marca 2014 r. III SK 34/13*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 6(3), s. 128.

372 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 47.

Konsument może posiadać cechy, które będą czyniły go tzw. konsumentem wrażliwym, szczególnie podatnym na nieuczciwe praktyki handlowe. Konsument ten wymaga szczególnej ochrony³⁷³, która jest zapewniana przez art. 5 ust. 3 dyrektywy 2005/29/WE. Zgodnie z nim praktyki handlowe, które mogą w sposób istotny zniekształcić zachowanie gospodarcze wyłącznie dającej się jednoznacznie zidentyfikować grupy konsumentów szczególnie podatnej na tę praktykę lub na produkt, którego ona dotyczy, oceniane są z perspektywy przeciętnego członka tej grupy.

Co istotne, grupa konsumentów, do której skierowana jest dana praktyka, musi dać się jednoznacznie zidentyfikować, a sama praktyka handlowa musi być skierowana wyłącznie do konsumentów wrażliwych. W moim przekonaniu przesłanka wyłączności została użyta w dyrektywie dość niefortunnie i nie powinna być interpretowana restrykcyjnie. Ocena tego, czy praktyka skierowana jest wyłącznie do grupy konsumentów wrażliwych, czy do ogółu konsumentów, może sprawiać kłopoty³⁷⁴. Wyłączenie szerszego zakresu ochrony z powodu takich wątpliwości byłoby bardzo niekorzystne z punktu widzenia konsumentów i powodowałoby, że w większości przypadków art. 5 ust. 3 nie miałby zastosowania. Dodatkowo nie jest do końca klarowne, dla kogo grupa musi być jasna do zidentyfikowania³⁷⁵. Trudności może również przysparzać próba określenia, w stosunku do jakich praktyk handlowych konsumenci wrażliwi są bardziej podatni, gdyż wrażliwość nie powoduje *per se* bezbronności konsumenta w każdym aspekcie. Aby zastosować szczególny wariant ochrony przewidziany w art. 5 ust. 3, przedsiębiorca musi mieć także racjonalną możliwość przewidzenia wrażliwości, którą cechuje się dana grupa konsumentów.

Podatny na zagrożenia może stać się konsument w związku ze swoją charakterystyką społeczno-demograficzną, behawioralną, sytuacją osobistą lub sytuacją na rynku³⁷⁶. Dyrektywa wprost wymienia wiek, niepełnosprawność fizyczną lub umysłową jako cechy czyniące konsumentów szczególnie podatnymi na praktykę handlową. Charakter tego katalogu jest poddawany dyskusjom w doktrynie³⁷⁷. Z uwagi na literalną treść motywu 19 dyrektywy należy jednak przychylić się do stanowiska o otwartym charakterze tego katalogu³⁷⁸. W literaturze jako inne cechy stanowiące o wrażliwości wskazuje się np. na: rasę, dochód, płeć i wykształcenie³⁷⁹, stan zdrowia, umiejętności cyfrowe oraz umiejętność rozumowania matematycznego³⁸⁰.

Warto zwrócić uwagę, że wrażliwość konsumentów może być postrzegana na trzech płaszczyznach: ograniczonej zdolności radzenia sobie z praktykami handlowymi, wyższym stopniu narażenia pewnych konsumentów na określone praktyki oraz donio-

373 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 7.

374 B. Duivenvoorde, *The Protection of Vulnerable Consumers under the Unfair Commercial Practices Directive*, *Journal of European Consumer and Market Law* 2013, nr 2, s. 71.

375 B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 71.

376 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 53.

377 Por. B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 71; M. Namysłowska, A. Jabłonska, *Prawo konsumenckie wobec personalizacji - nowe wyzwanie dla prawa konsumenckiego* (w:) L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. 107; A. Jabłonska, K. Klafkowska-Waśniowska, A. Kunkiel-Kryńska, R. Mańko, M. Namysłowska, P. Tereszkievicz, *Cnoty a prawo konsumenckie. Artykuł sprawozdawczy z XV konferencji Międzynarodowego Stowarzyszenia Prawa Konsumentckiego (International Association of Consumer Law - IACL)*, *Państwo i Prawo* 2016, nr 4, s. 88-89.

378 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 53; Komunikat Komisji do Parlamentu Europejskiego i Rady, *Nowy program na rzecz konsumentów...*, s. 20.

379 B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 78.

380 Komunikat Komisji do Parlamentu Europejskiego i Rady, *Nowy program na rzecz konsumentów...*, s. 20.

nością konsekwencji, jakie wynikają z danej praktyki dla różnych konsumentów³⁸¹. Niektórzy autorzy przyjmują, że dyrektywa o nieuczciwych praktykach handlowych normuje jedynie pierwszy rodzaj wrażliwości konsumentów, bowiem w dwóch ostatnich płaszczyznach konsumenci nie mają zmniejszonej zdolności do radzenia sobie z nieuczciwymi praktykami³⁸². Zgodnie z tym stanowiskiem, mimo że osoby korzystające z Internetu w oczywisty sposób są bardziej narażone na personalizację, nie oznacza to, że mają mniejszą zdolność do radzenia sobie z takimi praktykami. Innymi słowy, dyrektywa skupia się na wewnętrznych elementach wrażliwości konsumenta, pozostawiając na uboczu elementy zewnętrzne³⁸³.

Podsumowując, co do zasady ocena nieuczciwych praktyk handlowych jest przeprowadzana z uwzględnieniem modelu przeciętnego konsumenta, czyli uważnego i dostatecznie poinformowanego uczestnika obrotu. Model przeciętnego konsumenta może ulec modyfikacji w przypadku skierowania praktyki handlowej do określonej grupy konsumentów. Niemniej jednak w celu ochrony konsumentów, których cechy czynią ich szczególnie podatnymi na nieuczciwe praktyki handlowe, dyrektywa pozwala odstąpić od powyższych zasad. Jeśli praktyka handlowa skierowana jest do takiej grupy, to nieuczciwość praktyki należy ocenić z perspektywy jej przeciętnego członka. Dyrektywa 2005/29/WE posługuje się pojęciem konsumenta wrażliwego, w opozycji do konsumenta przeciętnego, lecz nie zawsze wpasowanie konsumentów w jedną z tych kategorii jest jednoznaczne³⁸⁴. W prawie konsumenckim obserwuje się nieustanne napięcie pomiędzy tymi pojęciami³⁸⁵.

4.2. Zasadność pojęcia przeciętnego konsumenta w obliczu personalizacji opartej na sztucznej inteligencji

Ogólny model przeciętnego konsumenta wypracowany przez Trybunał Sprawiedliwości oraz sądy państw członkowskich może nie sprawdzić się w sferze cyfrowej. Konsumenci nie mają narzędzi i umiejętności do zachowania odpowiedniej uwagi i ostrożności w relacjach z przedsiębiorcami, którzy wykorzystują techniki z zakresu sztucznej inteligencji. Wciąż istnieje znikoma świadomość tego, w jaki sposób dane osobowe są zbierane i wykorzystywane do personalizacji³⁸⁶, a jeszcze mniejszy jest stopień kontroli konsumentów nad tymi danymi. Założenie, że konsument poruszający się w przestrzeni internetowej wykazuje się uwagą, ostrożnością i dostatecznie dobrym poinformowaniem, jest nieelastyczne i nie przystaje do rzeczywistości. Z tych względów trzeba zrewidować model przeciętnego konsumenta w odniesieniu do grupy konsumentów poddawanych spersonalizowanym praktykom handlowym w Internecie³⁸⁷.

Zgadzam się z przedstawionym w doktrynie postulatem, że wymagania dla przeciętnego konsumenta w środowisku cyfrowym powinny zostać zmniejszone stosownie do zwiększonej złożoności technicznej i organizacyjnej przestrzeni internetowej oraz

381 B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 73.

382 B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 73.

383 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 9.

384 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 3.

385 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 8.

386 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 91.

387 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 7.

zmienionego charakteru produktów poddanych personalizacji³⁸⁸. Rozpatrując dostosowanie modelu przeciętnego konsumenta do przestrzeni internetowej, należałoby odstąpić przede wszystkim od założenia, że konsument jest dostatecznie dobrze poinformowany. Odstąpienie od przesłanki ostrożności lub uważności mogłoby być uznane za zbyt daleko idące. Niektórzy argumentują bowiem, że świadomość stopnia skomplikowania przestrzeni internetowej oraz odbywających się tam procesów może prowadzić do zwiększonej spostrzegawczości konsumentów³⁸⁹. Dostrzec należy, że zróżnicowanie wiedzy technologicznej konsumentów jest obecnie na tyle duże, że stanowi to element utrudniający skonstruowanie tak ogólnego modelu przeciętnego konsumenta, z jakim mamy do czynienia obecnie. Ponadto warto zwrócić uwagę na fakt, że w przypadku obszernych profili osobowościowych uwzględniających wiele cech i zmiennych zastosowanie modelu przeciętnego konsumenta może okazać się niemożliwe³⁹⁰. Na przykład spersonalizowana cena zostanie dostosowana do dokładnie tego poziomu, który jest w stanie zapłacić dany konsument. Reklama spersonalizowana z kolei będzie uwzględniać niepowtarzalny zestaw cech danego konsumenta. Konsument poddany personalizacji przestaje być tym samym konsumentem przeciętnym.

4.3. Pojęcie konsumenta wrażliwego z uwagi na brak umiejętności cyfrowych

Modyfikacji powinno ulec również pojęcie konsumenta szczególnie podatnego na nieuczciwe praktyki handlowe. Dyrektywa o nieuczciwych praktykach handlowych wprost wymienia jedynie trzy przesłanki mogące powodować zwiększoną podatność na praktyki handlowe stosowane przez przedsiębiorców. Są to: wiek, niepełnosprawność oraz łatwowierność. Według mnie przesłanką, która obecnie wpływa w dużym stopniu na wrażliwość europejskich konsumentów, jest niedostateczny poziom umiejętności cyfrowych³⁹¹, w tym brak znajomości technik opartych na personalizacji. Konsument w związku ze swoją wrażliwością powinni uzyskać wyższy poziom ochrony niż przeciętny, dobrze poinformowany, uważny i ostrożny konsument³⁹².

Stopień zaawansowania umiejętności technologicznych konsumentów wyraźnie wpływa na ich pewność siebie oraz podatność na manipulacje³⁹³. Można stwierdzić, że generalnie umiejętności cyfrowe osób młodszych są na wyższym poziomie, gdyż od najmłodszych lat Internet jest integralną częścią ich życia. Starsi konsumenci swój pierwszy kontakt z Internetem mieli znacznie później, co wpływa na ich stopień umiejętności cyfrowych³⁹⁴. Trudniej im porównywać oferty, a spersonalizowane treści oraz nieprzejrzyste praktyki zbierania danych uniemożliwiają im dokonanie świadomego wyboru. Konsument w podeszłym wieku mogą mieć wydłużony czas

388 N. Helberger, *Profiling and targeting consumers in the Internet of Things - A new challenge for consumer law*, SSRN Electronic Journal 2016, s. 21.

389 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 21.

390 A. Nowak, M. Węglowska, M. Gapsa, *Profilowanie na podstawie danych osobowych...*, s. 59.

391 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 24.

392 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 52.

393 F. Lupiáñez-Villanueva, G. Gaskell, P. Tornese, J. Vila, Y. Gómez, A. Allen, G. Veltri, C. Codagnone, *Behavioural study on the transparency of online platforms*, European Commission, 2018, s. 117.

394 F. Lupiáñez-Villanueva, G. Gaskell, P. Tornese, J. Vila, Y. Gómez, A. Allen, G. Veltri, C. Codagnone, *Behavioural study...*, s. 118.

przetwarzania informacji i mniejszą zdolność do pozostawania uważnymi i czujnymi przez dłuższy czas³⁹⁵.

Kolejną grupą konsumentów, która może być szczególnie podatna na praktyki oparte na personalizacji, są dzieci. Pod pojęciem tym należy rozumieć także młodzież, która co prawda ma zdolności decyzyjne porównywalne do zdolności dorosłych, lecz wciąż ma niewystarczające doświadczenie i samokontrolę³⁹⁶.

Brak umiejętności radzenia sobie z technikami personalizacji nie musi być jednak powiązany z wiekiem konsumentów. Niektóre badania wykazują, że starsi konsumenci niekoniecznie są oszukiwani w Internecie częściej niż młodszy konsumenci³⁹⁷. W obliczu personalizacji opartej na sztucznej inteligencji zasadniczo każdy konsument może okazać się podatny na manipulacyjne techniki behawioralne³⁹⁸.

Komisja Europejska, po przeprowadzeniu badań dotyczących podatności konsumentów na zagrożenia, doszła do wniosku, że konsumenci czują się względnie dobrze poinformowani o cenach, czytają informacje w Internecie i nie polegają wyłącznie na informacjach z reklam³⁹⁹. Konsumenci postrzegają siebie jako raczej ostrożnych w podejmowaniu decyzji⁴⁰⁰. Niemniej jednak w przypadku bardziej złożonych technik reklamowych opartych na analizie behawioralnej konsumenci nie byli już tak samo pewni w odpowiedziach i nie potrafili wybrać obiektywnie najlepszej oferty. Jak wskazują badania, konsumenci uważają, że zła sytuacja finansowa jest czynnikiem wpływającym na ich wrażliwość bardziej niż obecna sytuacja dotycząca zatrudnienia, wiek, a także problemy zdrowotne⁴⁰¹. W związku z tymi cechami konsument może trudniej przyswajać informacje, wybierać nieodpowiednie produkty, przez co jest bardziej podatny na określone praktyki marketingowe⁴⁰². Konsument poddany personalizacji może być zatem scharakteryzowany jako łatwowierny i bezbronny⁴⁰³.

Ze względu na szeroką analizę behawioralną każdy konsument poruszający się w sferze cyfrowej stał się w pewnych aspektach konsumentem wrażliwym⁴⁰⁴. Tym samym przyjęte w dyrektywie 2005/29/WE założenie o przeciętnym konsumencie jako regule, a konsumentem wrażliwym jako wyjątku, uległo diametralnej zmianie⁴⁰⁵. Sam fakt posiadania przez przedsiębiorców profili osobowościowych konsumentów sprawia, że są oni bardziej podatni na nieuczciwe praktyki handlowe⁴⁰⁶. Dzięki personalizacji przedsiębiorcy z łatwością mogą ustalić grupę osób w trudnej sytuacji finansowej, którym można zaoferować wysokooprocentowane pożyczki. Z kolei osobom cierpiącym z powodu uzależnień w sposób podprogowy można podsuwać odpowiednie oferty i reklamy powodujące jeszcze większe uzależnienie. Są to okoliczności, które w przypadku tradycyjnych technik marketingowych nie mogłyby zostać wykorzystane, gdyż

395 B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 76.

396 B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 76.

397 B. Duivenvoorde, *The Protection of Vulnerable Consumers...*, s. 77.

398 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 24.

399 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 49.

400 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 49.

401 Komisja Europejska, *Consumer Condition Scoreboard. Consumers at Home in the Single Market*, 2019, s. 56.

402 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 53.

403 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 22.

404 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 11; Z. Dávila, *Consumer Rights and Personalised Advertising...*, s. 81.

405 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 10.

406 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 17-18.

konsumenci nie dzielą się powszechnie tego typu informacjami. Dzięki śledzeniu działań konsumentów w sieci znalezienie ich słabości nie sprawia przedsiębiorcom trudności technicznych i finansowych. Jednocześnie trudno jednoznacznie określić moment, w którym przeciętny konsument poddawany procesom manipulacyjnej personalizacji stanie się konsumentem wrażliwym⁴⁰⁷. W związku ze wskazanymi powyżej trudnościami postuluje się, by zamiast określania kolejnych grup wrażliwych konsumentów przyjąć ogólną cechę wrażliwości, jaką jest podatność cyfrowa, co będzie oznaczało stan podatności będący wynikiem automatyzacji handlu oraz specyficzną architekturą rynków cyfrowych⁴⁰⁸.

Jeżeli praktyka skierowana jest do konsumentów przynależących do grupy szczególnie podatnej na oddziaływanie praktyki lub produktu, należy uwzględnić to przy ocenie nieuczciwości praktyki handlowej. Możliwości zapewniane przez profilowanie i personalizację powinny pomagać przedsiębiorcom wyznaczać grupę konsumentów, z jaką mają do czynienia, np. osobami borykającymi się z problemami finansowymi. To od przedsiębiorcy zależy, czy zdobytą wiedzę o słabościach konsumenta wykorzysta do manipulowania, czy do dostosowania używanej przez siebie praktyki w taki sposób, by ułatwić konsumentowi podjęcie świadomej decyzji dotyczącej umowy. Modelowo przedsiębiorcy powinni spożytkować szerszą wiedzę o słabościach konsumenta do kierowania w stosunku do nich odpowiednio skonstruowanych reklam i warunków umownych, niwelując przy tym ryzyko zarzutu stosowania nieuczciwych praktyk handlowych. Z większą wiedzą na temat konsumentów powinna się również wiązać większa odpowiedzialność⁴⁰⁹.

Szczególną uwagę należy zwrócić także na przesłankę racjonalnej możliwości przewidzenia przez przedsiębiorcę wrażliwości, którą cechuje się dana grupa konsumentów. Odpowiednia interpretacja tej przesłanki może mieć kluczowe znaczenie w przypadku personalizacji opartej na sztucznej inteligencji. Przy tak zaawansowanym śledzeniu konsumentów w sieci i rozbudowanym profilowaniu przedsiębiorcy korzystający z reklam behawioralnych i spersonalizowanych warunków umownych będą mieli możliwość w sposób racjonalny przewidzieć, że ich praktyka handlowa będzie skierowana do wrażliwej grupy konsumentów. Uważam, że szeroka wiedza o cechach konsumentów uzyskiwana poprzez wykorzystywanie technik sztucznej inteligencji będzie tym samym w pewnym stopniu ułatwiać wykazywanie, że określona praktyka powinna być oceniana z perspektywy konsumenta wrażliwego.

5. Personalizacja oparta na sztucznej inteligencji w świetle czarnej listy nieuczciwych praktyk handlowych

Niewiele spośród praktyk opartych na personalizacji może zostać zakwalifikowana jako jedna z praktyk z tzw. czarnej listy. Moim zdaniem spersonalizowana reklama odwołująca się do pragnień dziecka może wypełniać dyspozycję pkt 28 załącznika I do dyrektywy. Agresywna praktyka handlowa zakazana w pkt 28 polega na wywieraniu bezpośredniej presji na dzieciach, by kupiły dany produkt lub przekonały do

407 N. Helberger, F. Zuiderveen Borgesius, A. Reyna, *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, Common Market Law Review 2017, nr 54, s. 1458.

408 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 5.
409 C. Busch, *Implementing Personalized Law: Personalized Disclosures in Consumer Law and Privacy Law*, University of Chicago Law Review 2019, nr 86, s. 328.

zakupu rodziców. Przepis ten nie oznacza całkowitego zakazu reklamy skierowanej do dzieci.

U dzieci obserwuje się trudności w rozpoznawaniu wpływu spersonalizowanych reklam internetowych i opieraniu się mu, gdyż nie dostrzegają intencji stojących za zaprezentowaną w ten sposób reklamą⁴¹⁰. Wywarcie na dziecku bezpośredniej presji dotyczącej zakupu danego produktu, dzięki tworzeniu rozbudowanych profili marketingowych, jest o wiele prostsze niż dotychczas. Tym samym jeszcze wyraźniej warto podkreślić postulat zaprzestania profilowania dzieci oraz wyświetlania im dopasowanych reklam, mimo że nie są to działania wprost zakazane na gruncie RODO. W doktrynie prezentowane są też węższe interpretacje pojęcia bezpośredniej presji⁴¹¹. Decydująca będzie analiza konkretnego przypadku, uwzględniająca m.in. językowy sposób sformułowania reklamy behawioralnej, a niekiedy okoliczności, w których doszło do wyświetlenia reklamy⁴¹².

Można również rozważyć nowe nieuczciwe praktyki handlowe wprowadzające w błąd w każdych okolicznościach, dodane do załącznika I przez dyrektywę 2019/2161⁴¹³, zwanej też dyrektywą Omnibus. Punkt 23c zabrania zamieszczania lub zlecenia innej osobie prawnej lub fizycznej zamieszczania nieprawdziwych opinii konsumentów lub rekomendacji. Przepis obejmuje także zniekształcanie opinii konsumentów lub rekomendacji użytkowników Internetu w celu promowania produktów. Owo zniekształcanie z powodzeniem może nastąpić w wyniku zastosowania personalizacji opartej na sztucznej inteligencji – konkretnemu konsumentowi można bowiem wyświetlić spersonalizowane rekomendacje dotyczące danego produktu. Innymi słowy, każdy konsument miałby dostęp do odmiennego zakresu rekomendacji. Sztuczna inteligencja może być wykorzystywana także do egzekwowania wspomnianego zakazu poprzez wykrywanie fałszywych opinii⁴¹⁴.

W doktrynie podkreśla się potrzebę dostosowania czarnej listy do praktyki nadmiernej personalizacji o charakterze manipulacyjnym. Postuluje się m.in. zakazanie praktyki wykorzystywania w spersonalizowanych reklamach osobistych słabości konsumentów oraz wykorzystywania profili osobowościowych konsumentów w celu wywierania na nich presji emocjonalnej skłaniającej do zakupu⁴¹⁵.

6. Personalizacja oparta na sztucznej inteligencji w świetle małych klauzul generalnych

Jako że tylko nieliczne przejawy personalizacji mogą zostać zakwalifikowane w świetle czarnej listy nieuczciwych praktyk handlowych jako nieuczciwe w każdych okolicznościach, należy zbadać, czy zastosowanie mogą znaleźć małe klauzule generalne. Dyrektywa 2005/29/WE wymienia dwie formy nazwanych nieuczciwych praktyk

410 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 55.

411 A. Wiewiórowska-Domagalska, A. Kunkiel-Kryńska (w:) K. Osajda (red.) *Prawo konsumenckie...*, s. 338-353.

412 A. Wiewiórowska-Domagalska, A. Kunkiel-Kryńska (w:) K. Osajda (red.) *Prawo konsumenckie...*, s. 338-353.

413 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2161 z dnia 27 listopada 2019 r. zmieniająca dyrektywę Rady 93/13/EEG i dyrektywę 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 328 z dnia 18.12.2019 r., s. 7 (dalej: dyrektywa Omnibus).

414 G. Zhe Jin, *Artificial intelligence and consumer privacy*, National Bureau of Economic Research Working Paper Series 2018, s. 13.

415 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 145.

handlowych - praktyki handlowe wprowadzające w błąd, które dzielą się na działania i zaniechania, oraz agresywne praktyki handlowe. Na tle ogólnej problematyki personalizacji opartej na sztucznej inteligencji scharakteryzuję wybrane nieuczciwe praktyki handlowe, tj. naruszanie przepisów dotyczących obowiązków informacyjnych oraz personalizację cenową jako praktyki wprowadzające w błąd, a także reklamę behawioralną ukierunkowaną na emocje i słabości konsumenta jako agresywną praktykę handlową⁴¹⁶.

6.1. Personalizacja jako praktyka handlowa wprowadzająca w błąd

6.1.1. Wprowadzające w błąd działanie polegające na personalizacji cenowej

W wyniku rozpowszechnienia profilowania coraz częściej można spotkać się z praktyką dostosowywania cen do sytuacji finansowej i osobistej konkretnego konsumenta. Po raz pierwszy praktyka personalizacji cenowej została wykorzystana w 2000 r. przez Amazon do różnicowania cen płyt DVD dla nowych nabywców i stałych klientów⁴¹⁷. W określonych sytuacjach personalizacja cenowa może zostać zakwalifikowana jako działanie wprowadzające w błąd.

6.1.1.1. Działanie wprowadzające w błąd

Zgodnie z art. 6 ust. 1 dyrektywy 2005/29/WE z wprowadzającym w błąd działaniem mamy do czynienia, gdy praktyka zawiera fałszywe informacje i w związku z tym jest niezgodna z prawdą lub w jakikolwiek sposób, w tym przez wszystkie okoliczności jej prezentacji, wprowadza lub może wprowadzić w błąd przeciętnego konsumenta i która powoduje lub może spowodować podjęcie przez konsumenta decyzji dotyczącej transakcji, której inaczej by nie podjął. Zakazane są więc działania wprowadzające w błąd, które mogą zmylić przeciętnego konsumenta m.in. co do: głównych cech produktu, zakresu obowiązków przedsiębiorców lub sposobu obliczania ceny⁴¹⁸. Przekazanie informacji w sposób wprowadzający w błąd prowadzi do mylnego wyobrażenia konsumenta o produkcie i upośledzenia procesu podejmowania decyzji. Przy ocenie praktyki nie ma znaczenia fakt, czy informacje są zgodne z rzeczywistością w odniesieniu do jednego lub do większej liczby elementów. Wprowadzenie w błąd może nastąpić w wyniku różnych działań marketingowych, w tym reklam za pośrednictwem których przekazywane są konsumentowi nieprawdziwe lub prawdziwe informacje. Z kolei art. 6 ust. 2 dyrektywy 2005/29/WE dotyczy procesu wprowadzania produktu na rynek oraz nieprzestrzegania kodeksów postępowania.

6.1.1.2. Możliwość zakwalifikowania personalizacji cenowej jako działania wprowadzającego w błąd

Dzięki personalizacji cenowej możliwe jest zaproponowanie wyższej ceny osobie, której może szczególnie zależeć na zakupie danej rzeczy lub takiej, która może zapłacić więcej. W idealnej sytuacji konsumenci płaciliby za produkty tyle, ile maksy-

416 G. Sarton, *Artificial Intelligence: Challenges for EU Citizens and Consumers...*, s. 6.

417 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 43.

418 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 64.

malnie byliby w stanie zaoferować. Personalizacja pozwala przedsiębiorcom zbliżyć się do tej granicy.

Co do zasady przedsiębiorcy mają dowolność w zakresie określania cen pobieranych za ich produkty⁴¹⁹. Niemniej jednak, według art. 6 ust. 1 lit. d dyrektywy 2005/29/WE konsumenci powinni być odpowiednio poinformowani o łącznych kosztach i sposobie ich obliczania⁴²⁰. Z tego względu w pewnych okolicznościach praktyki personalizacji cenowej mogą spełnić kryteria definicji nieuczciwych praktyk wprowadzających w błąd.

W kontekście personalizacji cen uwarunkowanej stopniem zamożności konsumenta Komisja Europejska w wytycznych dotyczących stosowania dyrektywy 2005/29/WE z 2016 r. poprzestaje na stwierdzeniu, że praktyka ta nie jest obecnie zbyt rozpowszechniona wśród przedsiębiorców. Wydaje się jednak, że w ciągu ostatnich 5 lat praktyki personalizacji cenowej przestały być marginalnym zjawiskiem⁴²¹, choć wciąż nie są równie popularne jak spersonalizowane reklamy. W sytuacji gdy prezentowana jest określona cena, konsument ma prawo przewidywać, że będzie ona kształtowana niezależnie od jego osobistych cech i sytuacji finansowej. Wprowadzenie w błąd może polegać w tym przypadku na zniekształceniu procesu decyzyjnego poprzez wytworzenie mylnego wrażenia co do sposobu wyliczenia ceny w danej transakcji. Gdyby konsument wiedział, że zaproponowana mu cena uwzględnia także jego sytuację finansową lub skłonność do zapłaty wyższej ceny, mógłby nie podjąć takiej decyzji.

Na tle powyższych rozważań powstaje również pytanie, czy podwyższanie ceny na podstawie wiedzy o tym, że dany konsument musi dokonać określonego zakupu, powinno być w dalszym ciągu dopuszczalne. Z pewnością nie jest to zjawisko korzystne dla konsumentów. Mimo to uważam, że taka praktyka może funkcjonować na rynku pod warunkiem klarownego poinformowania konsumenta nie tylko o fakcie spersonalizowania ceny, ale też powodów, dla których cena została indywidualnie dopasowana. Postulat ten częściowo został zrealizowany przez wprowadzenie do dyrektywy 2011/83/UE o prawach konsumenta nowego obowiązku informacyjnego z zakresu personalizacji cen, który polega na poinformowaniu konsumenta o indywidualnym dostosowaniu ceny w oparciu o zautomatyzowane podejmowanie decyzji.

6.1.2. Wprowadzające w błąd zaniechanie polegające na pomijaniu istotnych obowiązków informacyjnych wobec konsumenta

Personalizacja wiąże się z koniecznością wypełniania wielu obowiązków informacyjnych względem konsumentów. Niedopełnienie niektórych z nich może skutkować zarzutem zaniechania wprowadzającego w błąd.

6.1.2.1. Zaniechanie wprowadzające w błąd

Zgodnie z art. 7 dyrektywy 2005/29/WE za zaniechanie wprowadzające w błąd uważa się praktykę pomijania istotnych informacji potrzebnych przeciętnemu konsumentowi, stosownie do okoliczności, do podjęcia świadomej decyzji dotyczącej transak-

419 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 163.

420 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 163.
421 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 43-44.

cji, która powoduje lub może powodować podjęcie przez przeciętnego konsumenta decyzji dotyczącej transakcji, której inaczej by nie podjął. Ocena dokonywana jest z uwzględnieniem okoliczności danego przypadku. Zaniechaniem wprowadzającym w błąd jest także zatajanie lub przekazywanie istotnych informacji w sposób niejasny, niezrozumiały, dwuznaczny lub z opóźnieniem oraz nieujawnianie komercyjnego celu praktyki, jeżeli nie wynika on jasno z kontekstu. Dochodzi tym samym do pozbawienia konsumenta możliwości dokonania świadomego wyboru przez pominięcie istotnych informacji⁴²². Zgodnie z motywem 15 w przypadku gdy prawo Unii Europejskiej określa wymogi informacyjne dotyczące komunikatów handlowych, reklamy i marketingu, dana informacja jest uznawana za istotną w ramach niniejszej dyrektywy. Wymogi informacyjne stanowiące istotne informacje zawiera wykaz zamieszczony w załączniku II do dyrektywy. Katalog ten nie jest wyczerpujący i może być uzupełniany niekiedy bardziej szczegółowymi wymogami informacyjnymi ustanowionymi w przepisach branżowych⁴²³. Każda z informacji, do której podania zobowiązany jest przedsiębiorca na podstawie dyrektywy 2011/83/UE o prawach konsumenta, może zostać uznana za istotny obowiązek informacyjny względem konsumenta⁴²⁴.

Artykuł 7 ust. 4 dyrektywy 2005/29/WE wyznacza dodatkowo zamknięty katalog informacji uważanych za istotne w przypadku zaproszenia do dokonania zakupu. Przez pojęcie zaproszenia do dokonania zakupu rozumie się komunikat handlowy określający cechy produktu oraz jego cenę, w sposób właściwy dla użytego środka komunikacji⁴²⁵. Zaproszenie do dokonania zakupu jest pojęciem węższym niż reklama, w przypadku której cena nie musi być określona. Zaproszenia do dokonania zakupu nie stanowi przy tym reklama zapraszająca konsumenta do odwiedzenia strony internetowej w celu uzyskania oferty⁴²⁶. Szczególną uwagę należy zwrócić na nową, istotną z punktu widzenia dyrektywy o nieuczciwych praktykach handlowych, informację określoną w art. 7 ust. 4a, która została wprowadzona za sprawą tzw. dyrektywy Omnibus. Analogiczny obowiązek informacyjny został dodany do dyrektywy 2011/83/UE o prawach konsumenta w art. 6a ust. 1 lit. a. W przypadku platform umożliwiających wyszukiwanie, z wyłączeniem wyszukiwarek internetowych, za istotne uważa się ogólne informacje dotyczące głównych parametrów decydujących o plasowaniu produktów przedstawianych konsumentowi w wyniku wyszukiwania oraz względne znaczenie tych parametrów w porównaniu z innymi parametrami. Innymi słowy, platformy oferujące np. oferty podróży, zakwaterowania i wypoczynku powinny informować w przejrzysty sposób o parametrach wpływających na plasowanie określonych ofert. Zgodnie z motywem 22 dyrektywy Omnibus parametry decydujące o plasowaniu to: wszelkie ogólne kryteria, procesy, specyficzne sygnały wbudowane w algorytmy stosowane w związku z plasowaniem. Tym samym, jeżeli przedsiębiorca przy prezentowaniu wyników wyszukiwania używałby technik personalizacji, które wpływałyby na kolejność wyświetlania ofert i produktów, konsument powinien zostać poinformowany o tym w zwięzły sposób i w łatwo dostępnym miejscu. Zaniechanie podania stosownej informacji może być zatem sankcjonowane na gruncie dyrektywy 2005/29/WE. Motyw 23 dyrektywy Omnibus wyjaśnia jednak, że opis powinien być

422 A. Wiewiórowska-Domagalska, A. Kunkiel-Kryńska (w:) K. Osajda (red.) *Prawo konsumenckie*..., s. 279-297.

423 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29*..., s. 21.

424 P. Księżak, *Skutki prawne naruszenia obowiązków informacyjnych przedsiębiorcy zamierzającego zawrzeć umowę z konsumentem* (w:) T. Skoczny, D. Karczewska, M. Namysłowska, *Ustawa o prawach konsumenta*, Warszawa 2015, s. 158.

425 Artykuł 2 lit. i dyrektywy 2005/29/WE.

426 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29*..., s. 59.

ogólny, a zatem konsument nie dowie się prawdopodobnie, z jakich powodów dokonano stosownej personalizacji.

Nie każde pominięcie istotnych informacji będzie skutkować uznaniem, że mamy do czynienia z praktyką wprowadzającą w błąd. Konieczne jest bowiem wykazanie, że prawdopodobnie doprowadzi ono przeciętnego konsumenta do podjęcia decyzji dotyczącej transakcji, której inaczej by nie podjął⁴²⁷.

6.1.2.2. Ochrona konsumenta oparta na prawie do informacji

W ramach unijnej koncepcji ochrony konsumenta jako słabszej strony umowy jednym z najważniejszych przysługujących mu praw jest prawo do informacji, które ma zagwarantować konsumentom autonomię decyzyjną⁴²⁸. Prawo do informacji ma za zadanie motywować konsumenta do podjęcia właściwej i najkorzystniejszej z jego punktu widzenia decyzji⁴²⁹.

Prawo do informacji należy interpretować szeroko, uwzględniając podstawowy obowiązek informacyjny, ale także prywatność informacyjną i możliwość decydowania przez konsumenta o sposobie wykorzystania dotyczących go danych⁴³⁰. Zapewnienie konsumentowi realnej ochrony przez informacje wymaga ciągłego podnoszenia jego świadomości na temat stosowanych wobec niego technologii i praktyk marketingowych⁴³¹. Istotą prawa do informacji jest nie tylko ochrona interesów majątkowych konsumenta, ale przede wszystkim zapewnienie możliwości wyboru i podjęcia przez niego świadomej decyzji⁴³².

Treść obowiązków informacyjnych zależy od stopnia złożoności umowy, a niekiedy od miejsca jej zawarcia⁴³³. Wynika to m.in. z ryzyka generowanego przez poszczególne umowy oraz ograniczeń technicznych niektórych kanałów sprzedaży. Na przykład zakres informacji wymagany w przypadku umowy zawieranej w Internecie będzie inny niż w przypadku umowy zawieranej w lokalu przedsiębiorstwa. Informacje powinny być przekazywane w przystępnej formie bez odwoływania się do fachowego i specjalistycznego języka oraz na tyle zrozumiale, by przeciętny konsument mógł podjąć decyzję z wystarczającym rozeznaniem⁴³⁴. Nawet jeżeli konsument posiadałby wyższą niż przeciętnie wiedzę, przedsiębiorca powinien dostarczyć mu rzetelnej i niewprowadzającej w błąd informacji⁴³⁵. Podkreśla się potrzebę ochrony konsumentów przez całe ich życie, a w konsekwencji możliwość zróżnicowania informacji

427 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 116.

428 S. Łazarewicz, *Konsument - pojęcie i jego europejski model* (w:) M. Królikowska-Olczak, B. Pachuca-Smulka (red.), *Ochrona konsumenta w prawie polskim i Unii Europejskiej*, Warszawa 2013, s. 33-37.

429 B. Pachuca-Smulka, *Prawo do informacji i edukacji podstawą ochrony interesów konsumenta* (w:) M. Królikowska-Olczak, B. Pachuca-Smulka (red.), *Ochrona konsumenta...*, s. 43-47.

430 B. Pachuca-Smulka, *Prawo do informacji i edukacji podstawą ochrony interesów konsumenta* (w:) M. Królikowska-Olczak, B. Pachuca-Smulka (red.), *Ochrona konsumenta...*, s. 62.

431 E. Macierzyńska-Franaszczuk, *Konsument, Internet i informacja* (w:) M. Fras, M. Jagielska, K. Podgórski, E. Sługocka-Krup (red.), *Prawa konsumenta w teorii i praktyce*, Warszawa 2018, s. 125-137.

432 P. Księżak, *Skutki prawne naruszenia obowiązków informacyjnych...*, s. 160.

433 E. Wojtaszek-Mik, *Informacja konsumencka w świetle orzecznictwa Europejskiego Trybunału Sprawiedliwości* (w:) K. Ślęzak (red.), *Studia i analizy Sądu Najwyższego. Tom VII*, Warszawa 2014, s. 337-364.

434 E. Wojtaszek-Mik, *Informacja konsumencka w świetle orzecznictwa Europejskiego Trybunału Sprawiedliwości* (w:) K. Ślęzak (red.), *Studia i analizy Sądu Najwyższego...*, s. 337-364.

435 E. Macierzyńska-Franaszczuk, *Konsument, Internet i informacja* (w:) M. Fras, M. Jagielska, K. Podgórski, E. Sługocka-Krup (red.), *Prawa konsumenta...*, s. 125-137.

z uwagi na takie przesłanki jak: wiek, doświadczenie i stopień świadomości⁴³⁶. Nie oznacza to jednak różnicowania poziomów ochrony konsumentów.

W związku z rozwojem praktyk handlowych w sferze cyfrowej w obszarze prawa do informacji pojawiły się problemy związane z prywatnością informacyjną, ilością i jakością przekazywanych konsumentowi informacji⁴³⁷, a także narastającą nierównowagą informacyjną pomiędzy konsumentami i przedsiębiorcami. Wynikają one m.in. z rozpowszechnienia się procesu analizy behawioralnej oraz o wiele łatwiejszego dostępu do danych. Dziś informacje są tworzone i analizowane przez algorytmy sztucznej inteligencji⁴³⁸. Przedsiębiorcy uzyskali praktycznie nieograniczoną wiedzę o konsumentach. Z kolei konsumenci mają dostęp tylko do wybranych informacji o produkcie i nie są w stanie ocenić, czy transakcja będzie dla nich korzystna⁴³⁹. Ryzyka związane z analizą behawioralną nie są dla konsumentów oczywiste. Z tego względu konsumentom należałoby przyznać gwarancję uzyskania pewnych informacji w szerszym zakresie, tak aby zniwelować niekorzystną asymetrię informacyjną⁴⁴⁰. Cel ten można osiągnąć m.in. przez: nałożenie na przedsiębiorców obowiązku stosowania ostrzeżeń; zobowiązanie stron do korzystania z pomocy wykwalifikowanych pośredników podczas zawierania umowy; standaryzację postanowień umów w taki sposób, by ułatwić ich porównywanie⁴⁴¹. Najczęściej jednak nakłada się na przedsiębiorców obowiązki informacyjne względem konsumenta. W zakresie profilowania i personalizacji treści wynikają one m.in. z: przepisów RODO (art. 13 i 14), z dyrektywy 2002/58/WE o prywatności i łączności elektronicznej⁴⁴² (art. 5 ust. 3) oraz z dyrektywy 2011/83/UE o prawach konsumenta (art. 6 ust. 1 lit. ea, art. 6a ust. 1 lit. a). Realizacja obowiązków informacyjnych podlega natomiast kontroli za sprawą dyrektywy 2005/29/WE.

Uważam, że model ochrony konsumenta przez informację przyjęty m.in. w RODO, dyrektywie o prywatności i łączności elektronicznej i dyrektywie 2011/83/UE o prawach konsumenta uległ częściowej dewaluacji. W doktrynie można spotkać się z argumentem, że zbyt duża ilość i precyzyjność przekazywanych informacji wpływa na nieskuteczność obowiązków informacyjnych⁴⁴³. Wątpliwości budzi też skuteczność udostępnienia złożonych informacji w sytuacji, gdy konsumenci nie są zaznajomieni nawet z podstawowymi pojęciami⁴⁴⁴, dotyczącymi m.in. możliwości śledzenia i pozyskiwania danych osobowych w sieci, oraz mechanizmami działania personalizacji⁴⁴⁵. Obowiązek informacyjny ma sens tylko wtedy, gdy konsument na podstawie poda-

436 E. Macierzyńska-Franaszczuk, *Konsument, Internet i informacja* (w:) M. Fras, M. Jagielska, K. Podgórski, E. Sługocka-Krup (red.), *Prawa konsumenta...*, s. 125-137.

437 B. Pachuca-Smulka, *Prawo do informacji i edukacji podstawą ochrony interesów konsumenta* (w:) M. Królikowska-Olczak, B. Pachuca-Smulka (red.), *Ochrona konsumenta...*, s. 38.

438 B. Pachuca-Smulka, *Prawo do informacji i edukacji podstawą ochrony interesów konsumenta* (w:) M. Królikowska-Olczak, B. Pachuca-Smulka (red.), *Ochrona konsumenta...*, s. 42-43.

439 K. Południak-Gierz, *Wady oświadczenia woli w umowach zawieranych na internetowym rynku konsumenckim*, Warszawa 2020, s. 151-154.

440 B. Pachuca-Smulka, *Prawo do informacji i edukacji podstawą ochrony interesów konsumenta* (w:) M. Królikowska-Olczak, B. Pachuca-Smulka (red.), *Ochrona konsumenta...*, s. 43-47.

441 K. Południak-Gierz, *Wady oświadczenia woli w umowach...*, s. 151-154.

442 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz.Urz.UE. C 201 z dnia 31.07.2002 r., s. 37 (dalej: dyrektywa o prywatności i łączności elektronicznej).

443 O. Ben-Shahar, *Data Pollution...*, s. 130-131.

444 A. Jabłonowska, K. Klafkowska-Waśniowska, A. Kunkiel-Kryńska, R. Mańko, M. Namysłowska, P. Tereszkievicz, *Cnoty a prawo konsumenckie...*, s. 88.

445 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 31.

nych mu informacji jest w stanie podjąć świadomą decyzję⁴⁴⁶. W przypadku natłoku informacyjnego, z którym konsumenci mają do czynienia w przestrzeni internetowej, możliwość ta jest znacząco ograniczona. Konsumenci na rynkach cyfrowych są coraz bardziej zmęczeni koniecznością udzielania zgód⁴⁴⁷. Przekazywane informacje są nieprzejrzyste i bardzo rozbudowane, dlatego konsumenci ich nie czytają⁴⁴⁸. Dodatkowo niektóre z informacji w stosunku do różnych grup konsumentów są zbędne, np. w stosunku do osób głuchoniemych podawanie danych kontaktowych w postaci numeru telefonu jest zbędne⁴⁴⁹. Skuteczność ochrony przez informacje w dobie nowych technologii należy tym samym ocenić krytycznie.

W moim przekonaniu standard informacji udzielanej konsumentowi w erze cyfrowej powinien ulec gruntownej zmianie. Priorytetem Unii Europejskiej nie powinno być ciągłe zwiększanie ilości przekazywanych informacji, ale też działania na rzecz poprawy ich jakości i jednolitości. Na przykład bardziej złożone informacje mogłyby być przekazywane w sposób graficzny, gdyż badania wykazują, że jest on bardziej skuteczny od formy tekstowej⁴⁵⁰.

Ponadto usprawnienia wymaga kontrola jakości przekazywanych przez przedsiębiorców informacji w Internecie. Uważam, że w realizacji tych celów pomóc może sformułowanie przez unijne organy klarownych wytycznych dotyczących dopuszczalnych sposobów wykonywania przez przedsiębiorców poszczególnych obowiązków informacyjnych oraz dobrych praktyk w tym zakresie. Należy rozważyć możliwość wprowadzenia obowiązku przeprowadzania przez przedsiębiorców testów przejrzystości informacji kierowanych do konsumentów (ang. *reader testing*)⁴⁵¹, a także personalizację treści obowiązków informacyjnych w celu ich dostosowania do różnych grup konsumentów⁴⁵². Skoro nowe technologie oparte na personalizacji sprawdzają się w przypadku reklam behawioralnych, to z powodzeniem można wykorzystać je do projektowania spersonalizowanych treści obowiązków informacyjnych. Wyeliminowanie zbędnych informacji powinno złagodzić efekt przeciążenia informacyjnego obserwowany wśród konsumentów⁴⁵³. Zróżnicowanie informacyjne budzi jednak obawy ze względu na ryzyko dokonania złej oceny, a w konsekwencji dostarczenia konsumentowi zbyt ograniczonych informacji⁴⁵⁴.

446 B. Pachuca-Smulska, *Prawo do informacji i edukacji podstawą ochrony interesów konsumenta* (w:) M. Królikowska-Olczak, B. Pachuca-Smulska (red.), *Ochrona konsumenta...*, s. 43-47.

447 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 1.

448 F. Lupiáñez-Villanueva, G. Gaskell, P. Tornese, J. Vila, Y. Gómez, A. Allen, G. Veltri, C. Codagnone, *Behavioural study...*, s. 54.

449 J. Luzak, *Tailor-made Consumer Protection: Personalisation's Impact on the Granularity of Consumer Information* (w:) M. C. Compagnucci, H. Haapio, M. Hagan, M. Doherty (red.), *Legal Design: Integrating Business, Design and Legal Thinking with Technology*, Edward Elgar Publishing Ltd. 2021. Pozyskano z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3696483. Dostęp: 11.06.2021 r.

450 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 42.

451 A. Jabłonowska, K. Klafkowska-Waśniowska, A. Kunkiel-Kryńska, R. Mańko, M. Namysłowska, P. Tereszkiewicz, *Cnoty a prawo konsumenckie...*, s. 92.

452 N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, *EU consumer protection 2.0...*, s. 42; J. Luzak, *Tailor-made Consumer Protection...*

453 K. Południak-Gierz, *Personalization of Information Duties Challenges for Big Data Approach*, *European Review of Private Law* 2018, nr 3, s. 303.

454 J. Luzak, *Tailor-made Consumer Protection...*

6.1.2.3. Naruszenie obowiązków informacyjnych wobec konsumenta

Obowiązki informacyjne wynikające z RODO lub dyrektywy 2002/58/WE mogą zostać uznane za istotne informacje, pomimo niewymienienia ich w załączniku II dyrektywy. Według wytycznych Komisji Europejskiej nie każde naruszenie przez przedsiębiorcę powyższych przepisów będzie równoznaczne z tym, że praktyka jest sprzeczna z dyrektywą w sprawie nieuczciwych praktyk handlowych⁴⁵⁵. Nie zawsze będzie skutkowało wypaczeniem procesu decyzyjnego konsumenta w takim stopniu, by uznać to za nieuczciwą praktykę handlową. Nieprzestrzeganie przepisów dotyczących ochrony danych powinno rzutować na ogólną ocenę nieuczciwości praktyk handlowych, gdy celem nieprawidłowo przetwarzanych danych konsumentów są: marketing bezpośredni, profilowanie lub wyceny indywidualizowane⁴⁵⁶.

Przedsiębiorcy niejednokrotnie korzystają z *dark patterns*, ustawień domyślnych lub przekazują informacje celowo w sposób skomplikowany, co może być uznawane za zaniechanie wprowadzające konsumentów w błąd⁴⁵⁷. Nie tylko bowiem treści informacji, ale także sposób ich prezentacji mogą mieć znaczący wpływ na działania konsumentów⁴⁵⁸. Aby zaniechanie było zakwalifikowane jako nieuczciwe, należałoby wykazać, że istnieje możliwość, że doprowadzi ono przeciętnego konsumenta do podjęcia decyzji dotyczącej transakcji, której inaczej by nie podjął. Szanse uprawdopodobnienia, że gdyby konsument np. był prawidłowo poinformowany o możliwości niewyrażania zgody na przetwarzanie danych, to podjąłby inną decyzję dotyczącą transakcji, są niewielkie. W doktrynie prezentowana jest jednak odmienna teza zakładająca szeroką interpretację pojęcia decyzji dotyczącej transakcji⁴⁵⁹. Zgodnie z nią możliwe jest zakwalifikowanie wyrażenia zgody na przetwarzanie danych osobowych do celów reklamy spersonalizowanej jako decyzji w sprawie transakcji.

Inaczej można ocenić sytuację, gdy przedsiębiorca poinformował konsumenta, że przetwarza dane osobowe w celu wykonania umowy, ale pominął fakt, że przetwarzanie danych będzie obejmowało również udostępnianie ich podmiotom trzecim w celach komercyjnych⁴⁶⁰. Takie zaniechanie podania informacji będzie zarówno naruszeniem obowiązków administratora danych, jak i formą zaniechania wprowadzającego konsumenta w błąd⁴⁶¹. Z tej perspektywy warto przeanalizować drugą część art. 7 ust. 2 dyrektywy 2005/29/WE. Sprecyzowano w nim, że zaniechaniem wprowadzającym w błąd może być nieujawnienie komercyjnego celu praktyki, jeżeli nie wynika ono jasno z kontekstu i jeżeli powoduje lub może spowodować podjęcie przez przeciętnego konsumenta decyzji dotyczącej transakcji, której inaczej by nie podjął. Dotychczas przepis ten wiązany był głównie z reklamą ukrytą, choć obecnie można rozważyć możliwość jego zastosowania w kontekście procederu zbierania danych w celach ich dalszej odsprzedaży w ramach *cookie walls*. Jeżeli przedsiębiorca nie poinformuje, że dane, które konsument musi podać, żeby uzyskać dostęp do usługi będą wykorzystywane do celów handlowych, wówczas z uwagi na naruszenie prawa

455 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 30.

456 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 30.

457 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 64.

458 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 64.

459 N. Helberger, F. Zuiderveen Borgesius, A. Reyna, *The perfect match?*..., s. 1449-1451.

460 M. Nisevic, *A study on the personal data processing and the UCPD focused on Italy, Germany and the UK*, Maastricht Journal of European and Comparative Law 2021, nr 28(1), s. 13-14.

461 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 10.

do uzyskania informacji może to zostać uznane za wprowadzające w błąd pominięcie istotnych informacji⁴⁶².

Decyzja o przekazaniu danych w zamian za bezpłatny dostęp do treści może zostać uznana za świadomą, jedynie w przypadku nielicznych osób, które znają wartość danych osobowych i mają bogate doświadczenie w świecie cyfrowym⁴⁶³. Niemniej jednak w świetle przyjętego przez orzecznictwo modelu przeciętnego konsumenta, który jest wystarczająco dobrze poinformowany i aktywnie poszukuje informacji, zakwalifikowanie tejże praktyki jako zaniechania wprowadzającego w błąd może okazać się niemożliwe.

Na podstawie definicji zaniechania wprowadzającego w błąd można ocenić także zapewnianie konsumentów o bezpłatnym charakterze usługi w sytuacji, gdy ich dane osobowe będą przez przedsiębiorcę monetyzowane. Oferowanie takich usług jako „bezpłatnych” bez informowania konsumentów, w jaki sposób ich dane osobowe będą używane, w pewnych okolicznościach może zostać uznane za praktykę wprowadzającą w błąd⁴⁶⁴. W tym kontekście warto przytoczyć wyrok Regionalnego Sądu Administracyjnego Łazio z 10 stycznia 2020 r. w sprawie Facebooka, sygn. C-261/20. Sąd uznał, że praktyka podkreślania darmowego charakteru platformy bez jednoczesnego wyraźnego informowania o tym, że przedsiębiorca będzie traktował dane osobowe jako wynagrodzenie, stanowi praktykę wprowadzającą w błąd. Istotny dla rozstrzygnięcia okazał się także fakt, że większość przychodów platformy osiąganych jest właśnie w procesie monetyzacji danych jej użytkowników⁴⁶⁵. Wyrok jest przełomowy, gdyż potraktowano dane osobowe jako zasoby podlegające negocjacjom i przedmiot obrotu między dostawcą platformy i konsumentem⁴⁶⁶. Dzięki temu możliwe było wykorzystanie dyrektywy o nieuczciwych praktykach handlowych w celu ochrony konsumentów.

Zaniechaniem wprowadzającym w błąd może stać się również naruszenie nowego obowiązku informacyjnego wprowadzonego do dyrektywy 2011/83/UE o prawach konsumenta dotyczącego zastosowania personalizacji cenowej. Na podstawie art. 6 ust.1 lit. ea dyrektywy przedsiębiorcy będą zobowiązani do informowania konsumentów o dostosowaniu ceny w wyniku zautomatyzowanego podejmowania decyzji. Konsumenty najczęściej nie kwestionują domyślnych cen wyświetlanych przez przedsiębiorców, ale uważam, że informacja o zastosowaniu personalizacji cenowej może diametralnie zmienić zachowanie konsumenta dotyczące transakcji. W przypadku niewywiązania się z opisywanego powyżej obowiązku przedsiębiorcy będą narażali się zatem na zarzut zaniechania wprowadzającego w błąd.

6.2. Profilowanie i personalizacja jako agresywne praktyki handlowe

6.2.1. Agresywna praktyka handlowa

Zgodnie z art. 8 dyrektywy 2005/29/WE z agresywną praktyką handlową mamy do czynienia, jeżeli w konkretnym przypadku, biorąc pod uwagę wszystkie cechy i oko-

462 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 30.

463 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 11.

464 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 107-108.

465 M. Kulesza, *Odplatny charakter „darmowych” usług Facebooka...*, s. 102.

466 M. Kulesza, *Odplatny charakter „darmowych” usług Facebooka...*, s. 102.

liczności, przez nękanie, przymus, w tym z użyciem siły fizycznej lub bezprawny nacisk, w znaczny sposób ogranicza lub może ograniczyć swobodę wyboru przeciętnego konsumenta lub jego zachowanie względem produktu i tym samym powoduje lub może spowodować podjęcie przez niego decyzji dotyczącej transakcji, której inaczej by nie podjął. Przy ocenie danej praktyki, zgodnie z art. 9 dyrektywy 2005/29/WE, 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 i podjęcia swobodnej decyzji⁴⁶⁷. Nie ma przy tym znaczenia, czy dana okoliczność będzie miała charakter pozytywny, czy negatywny. Mogą one obejmować zachowania na etapie marketingu, ale też praktyki, które występują w trakcie realizacji umowy lub po transakcji.

Najczęściej wykorzystywana przez przedsiębiorców postać agresywnych praktyk handlowych to bezprawny nacisk. Według art. 2 lit. j dyrektywy 2005/29/WE oznacza on wykorzystywanie przewagi przedsiębiorcy względem konsumenta w celu wywarcia na niego presji, czego efektem ma być ograniczenie zdolności konsumenta do podjęcia świadomej decyzji. Dla zakwalifikowania praktyki jako agresywnej wystarczające jest wykazanie, że praktyka potencjalnie może ograniczyć możliwość wyboru przeciętnego konsumenta⁴⁶⁸.

6.2.2. Agresywna praktyka handlowa polegająca na wykorzystywaniu słabości konsumentów w celu personalizacji reklam

W świetle przepisów o agresywnych praktykach handlowych można rozpatrywać praktykę internetowych reklam behawioralnych opartych na wykorzystaniu sztucznej inteligencji, które ograniczają swobodę wyboru konsumenta i wpływają na jego decyzyjność⁴⁶⁹. Pogłębiona analiza danych pochodzących od konsumentów może skutkować ujawnieniem ich słabości, lęków oraz aktualnego stanu emocjonalnego. Za pomocą technik śledzenia działań w sieci można zidentyfikować np. konsumentów cierpiących na depresję, zmagających się z żałobą, ale też takich, którzy znaleźli nową pracę lub są w nowym związku i ich zdolności poznawcze są częściowo zaburzone. Wiedza ta służy niekiedy przedsiębiorcom do kierowania spersonalizowanych reklam. Nadużywanie elementów emocjonalnych i sugestywnych w reklamach behawioralnych prowadzi do wywołania silnej presji na konsumentach i podejmowania przez nich irracjonalnych działań, co można oceniać z perspektywy przepisów o agresywnych praktykach handlowych. Znajomość wymagań, potrzeb, upodobań i gustów konsumenta niekiedy może przybrać charakter manipulacyjny i oddziaływać na psychikę konsumenta w taki sposób, że nie będzie zdolny podjąć świadomej decyzji co do zakupu⁴⁷⁰. Informacje o samym produkcie odgrywają wtedy znaczenie marginalne.

Sposób przekazania agresywnej reklamy nie będzie miał przy tym znaczenia. Uważa się, że skoro za agresywną praktykę można uznać informowanie konsumenta o ofer-

467 Dokument roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29...*, s. 94.
468 K. Lis-Zarrias, *Ochrona konsumenta przed agresywnymi praktykami rynkowymi w świetle pytań prejudycjalnych SN w sprawie C-628/17 Orange Polska S.A.*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2018, nr 6(7), s. 143.

469 Z. Dāvida, *Consumer Rights and Personalised Advertising...*, s. 82.

470 M. Modrzejewska, *Umowy w sferze marketingu i reklamy* (w:) M. Stec (red.), *Prawo umów handlowych...*, s. 613-614.

cie drogą telefoniczną lub e-mailową, to tym bardziej może być nią informacja wyświetlana bezpośrednio na urządzeniach konsumenta⁴⁷¹.

Żeby zakwalifikować reklamę behawioralną jako agresywną praktykę handlową, należy wykazać, że wykorzystuje słabości lub określony stan emocjonalny konsumenta. Reklama behawioralna oparta na kryterium zainteresowania konsumenta określonym tematem nie będzie spełniała automatycznie kryterium agresywności. Niemniej jednak ta sama reklama w połączeniu z wykorzystaniem wiedzy o problemie konsumenta, np. dotyczącym kompulsywnych zakupów, może stanowić agresywną praktykę handlową.

Wykorzystana przez przedsiębiorcę okoliczność musi być na tyle poważna, by spowodować u konsumenta problem z podjęciem racjonalnej decyzji. Konieczne jest wykazanie, że konsument nie miał zamiaru zawierania umowy, ale użyta strategia marketingowa wymusiła na nim zmianę decyzji⁴⁷². Zróżnicowanie dopuszczalnej reklamy behawioralnej oraz techniki marketingowej, której skuteczność oparta jest na manipulacji, w praktyce nie jest zadaniem prostym⁴⁷³. W każdym przypadku należy sprecyzować rzeczywisty potencjał perswazyjny określonej reklamy oraz stopień ograniczenia autonomii konsumenta⁴⁷⁴. Nie sposób ustalić w sposób generalny granicy, po przekroczeniu której perswazja będzie uznawana za nadmierną i wypaczającą proces decyzyjny konsumenta. W doktrynie ustalenie tejże granicy upatruje się za jedno z głównych wyzwań dla prawa konsumenckiego w kontekście profilowania i personalizacji w Internecie⁴⁷⁵.

Przy dokonywaniu oceny danej praktyki brany pod uwagę będzie m.in. czas. Na przykład zgodnie z wyrokiem Wyższego Sądu Okręgowego we Frankfurcie nad Menem⁴⁷⁶ praktyka kierowania reklamy nagrobków do rodziny niedawno zmarłej osoby stanowi agresywną praktykę handlową⁴⁷⁷. Stanowisko sądu z powodzeniem odnosi się do praktyki reklam behawioralnych *online*. Stała dostępność Internetu zapewnia przedsiębiorcom możliwość dotarcia do konsumentów o dowolnej porze dnia oraz momentach, w których jest on szczególnie wrażliwy, co może mieć znaczenie dla oceny agresywności danej praktyki⁴⁷⁸.

Należy ponadto wziąć pod uwagę ilość zebranych o konsumentach informacji, to, czy miał on świadomość zastosowania technik perswazyjnych i czy mógł się tym technikom sprzeciwić przez wyłączenie profilowania i personalizacji reklam⁴⁷⁹. Na ocenę praktyki będzie również wpływać stopień skuteczności używanych przez przedsiębiorców algorytmów personalizujących reklamy, a przede wszystkim indywidualne cechy konsumenta⁴⁸⁰.

W przypadku reklamy behawioralnej opartej na sztucznej inteligencji można mieć dodatkowo wątpliwość, czy przedsiębiorca jest w stanie kontrolować proces targetowania na tyle, by móc zapobiec wyświetleniu konsumentowi agresywnej reklamy. W większości przypadków w dalszym ciągu to przedsiębiorca decyduje o tym, jakie kryteria targetowania wybierze. Warto zaznaczyć, że pewne ramy dla reklam be-

471 K. Potudniak-Gierz, *Wady oświadczenia woli w umowach...*, s. 314-318.

472 K. Potudniak-Gierz, *Wady oświadczenia woli w umowach...*, s. 314-318.

473 K. Potudniak-Gierz, *Wady oświadczenia woli w umowach...*, s. 314-318.

474 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 20.

475 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 16.

476 Wyrok Wyższego Sądu Okręgowego we Frankfurcie nad Menem z dnia 29.01.2009 r., sprawa nr 6 U 90/08. Pozyskano z: <https://openjur.de/u/30714.html>. Dostęp: 11.06.2021 r.

477 K. Potudniak-Gierz, *Wady oświadczenia woli w umowach...*, s. 311-314.

478 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 18.

479 N. Helberger, *Profiling and targeting consumers in the Internet of Things...*, s. 19.

480 K. Potudniak-Gierz, *Wady oświadczenia woli w umowach...*, s. 314-318.

hawioralnych są ustalane w drodze samoregulacji przez platformy internetowe⁴⁸¹. Przykładem może być Google Ads, które nie zezwala na reklamy spersonalizowane odnoszące się do problemów osobistych, zdrowia, statusu społecznego⁴⁸².

7. Personalizacja oparta na sztucznej inteligencji w świetle dużej klauzuli generalnej nieuczciwej praktyki handlowej

Dyrektywa o nieuczciwych praktykach handlowych została oparta na modelu pełnej harmonizacji, co oznacza, że państwa członkowskie nie mogą przyjąć bardziej restrykcyjnych środków, nawet gdyby miało to zapewnić jeszcze wyższy poziom ochrony konsumentów niż ten przewidziany przez dyrektywę⁴⁸³. Niemniej jednak w przypadku pojawienia się innych, niestypizowanych dotąd nieuczciwych praktyk handlowych, zastosowanie będzie miała generalna klauzula, która uelastycznia dyrektywę i odgrywa rolę uzupełniającą wobec nieuczciwych praktyk nazwanych⁴⁸⁴. Klauzula generalna zawiera zazwyczaj nieodokreślone pojęcia odnoszące się do systemu ocen i norm pozaprawnych⁴⁸⁵. Dzięki jej zastosowaniu dyrektywa nie ulega zbyt szybkiej dezaktualizacji.

Artykuł 5 ust. 1 dyrektywy 2005/29/WE przewiduje ogólny zakaz nieuczciwych praktyk handlowych. Za nieuczciwą uważa się praktykę, która jest sprzeczna z wymogami staranności zawodowej, a zarazem w sposób istotny zniekształca lub może zniekształcić zachowanie przeciętnego konsumenta lub określonej grupy konsumentów. Wymienione powyżej przesłanki muszą być spełnione łącznie. Motyw 7 dyrektywy przewiduje, że przy stosowaniu jej przepisów, a zwłaszcza klauzuli generalnej, należy w pełni uwzględnić okoliczności konkretnego przypadku.

Staranność zawodową definiuje art. 2 lit. h dyrektywy o nieuczciwych praktykach handlowych jako standard dotyczący szczególnej wiedzy i staranności, których można w racjonalny sposób oczekiwać od przedsiębiorcy w jego relacjach z konsumentami, zgodnie z uczciwymi praktykami handlowymi i ogólną zasadą dobrej wiary w zakresie jego działalności. Jest to fachowość, której oczekuje się od przedsiębiorcy danego rodzaju. Przyjęta miara staranności nie jest statyczna i będzie zależeć m.in. od stopnia złożoności umowy oraz zagrożenia interesu konsumenta wynikającego z jej charakteru, a w przypadku reklam - od stopnia ich spersonalizowania. Prawidłowe wypełnienie obowiązków informacyjnych względem konsumenta może stanowić dowód dochowania staranności zawodowej⁴⁸⁶.

Z kolei przesłanka istotnego zniekształcenia zachowania gospodarczego konsumenta, zdefiniowana w art. 2 lit. e dyrektywy 2005/29/WE, ma miejsce w przypadku wykorzystania praktyki handlowej w celu ograniczenia zdolności konsumenta do podjęcia świadomej decyzji. Zniekształcenie musi być na tyle istotne, aby wpłynąć na swobodę decyzyjną konsumenta i skłonić go do podjęcia decyzji dotyczącej transakcji, któ-

481 A. Nowak, M. Węglowska, M. Gapsa, *Profilowanie na podstawie danych osobowych...*, s. 57.

482 Pozyskano z: <https://support.google.com/adspolicy/answer/143465?hl=pl>. Dostęp: 11.06.2021 r.

483 Wyrok TS z 23.04.2009 r. w sprawach połączonych C-261/07 i C-299/07 *VTB-VAB NV v. Total Belgium NV oraz Galatea BVBA v. Sanoma Magazines Belgium NV*, ECLI:EU:C:2009:244, pkt 52.

484 M. Sieradzka, *Komentarz do ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym...*, s. 313-322.

485 M. Strzelecki, *Klauzula generalna nieuczciwej praktyki rynkowej*, Przegląd Prawa Handlowego 2008, nr 11, s. 39.

486 Wyrok TS z 7.09.2016 r. w sprawie C-310/15 *Vincent Deroo-Blanquart v. Sony Europe Limited*, ECLI:EU:C:2016:633, pkt 37.

rej inaczej by nie podjął⁴⁸⁷. Wpływ na ograniczenie tej zdolności będzie zależeć m.in. od rodzaju nieuczciwych praktyk handlowych stosowanych przez przedsiębiorcę⁴⁸⁸.

Nie zawsze uda się zakwalifikować nieuczciwe praktyki handlowe oparte na personalizacji jako praktyki handlowe wprowadzające w błąd lub agresywne. W świetle przedstawionych powyżej przesłanek uważam, że klauzula generalna może mieć w pewnych okolicznościach zastosowanie do nieuczciwych praktyk handlowych opartych na personalizacji, które nie mogą być objęte ochroną wynikającą z czarnej listy oraz małych klauzul generalnych.

8. Wnioski częściowe

W mojej opinii dyrektywa o nieuczciwych praktykach handlowych nie jest wystarczająco elastyczna, by sprostać wszystkim problemom, jakie stawia przed konsumentami personalizacja oparta na sztucznej inteligencji. Techniki marketingowe oparte na personalizacji tylko częściowo mogą zostać objęte zakresem przewidzianym w niej ochroną.

Czarna lista nieuczciwych praktyk handlowych ma jedynie szczątkowe zastosowanie wobec personalizacji opartej na sztucznej inteligencji. Z kolei małe klauzule generalne w założeniu mogłyby być wykorzystane do oceny praktyki personalizacji cen, niedopełnienia obowiązków informacyjnych wynikających z RODO i dyrektywy o prywatności i łączności elektronicznej oraz reklam behawioralnych odwołujących się do słabości i stanu emocjonalnego konsumenta. Możliwe jest również ocenianie innych, niestypizowanych praktyk opartych na personalizacji w świetle dużej klauzuli generalnej. Każdy przypadek będzie jednak wymagać indywidualnej analizy i wykazania, że praktyka w istotny sposób wpłynęła lub mogła wpłynąć na proces decyzyjny konsumenta. Zasadniczym problemem przy ocenie nieuczciwości praktyk handlowych jest niedostosowanie pojęcia przeciętnego konsumenta oraz konsumenta wrażliwego do ery cyfrowej i praktyk handlowych opartych na personalizacji. Przedstawiłam propozycje zmian tych pojęć, które ułatwiłyby stosowanie dyrektywy. Zakwestionowałam także skuteczność modelu ochrony konsumentów przez informację, na której w głównej mierze opiera się europejskie prawo konsumenckie, w tym dyrektywa o nieuczciwych praktykach handlowych. Postrzeganie konsumentów jako jednorodnej grupy, wobec której trzeba spełnić obowiązek informacyjny, powinno zostać zastąpione podejściem spersonalizowanym.

Na marginesie należy nadmienić, że w Nowym programie na konsumentów na lata 2020-2025 zapowiedziano aktualizację wytycznych dotyczących dyrektywy w sprawie nieuczciwych praktyk handlowych⁴⁸⁹. Po dokonaniu stosowanej weryfikacji do 2022 r. Komisja planuje zbadać konieczność przyjęcia dodatkowych przepisów w celu zapewnienia równego poziomu sprawiedliwości w Internecie, co potencjalnie może wpłynąć na ochronę konsumentów przed nieuczciwymi praktykami wynikającymi z personalizacji opartej na sztucznej inteligencji. Wyrażam nadzieję, że choć obecnie w dyrektywie widocznych jest wiele ograniczeń skutkujących trudnością stosowania przepisów w odniesieniu do technik opartych na personalizacji, to w przyszłości ma ona potencjał do stania się podstawą ochrony konsumentów poddawanych procesom personalizacji.

487 M. Sieradzka, *Komentarz do ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym...*, s. 298-307.

488 E. Rutkowska-Tomaszewska, *Nieuczciwe praktyki na rynku bankowych usług konsumenckich...*, s. 46-55.

489 Komunikat Komisji do Parlamentu Europejskiego i Rady, *Nowy program na rzecz konsumentów...*, s. 13.

Rozdział IV.

Przyszłość ochrony konsumentów wobec stosowania personalizacji

1. Uwagi wprowadzające

Jednym z priorytetów Unii Europejskiej na lata 2019-2024 jest wprowadzenie Europy w erę cyfrową. W ramach tej wizji podejmowanych jest wiele działań legislacyjnych z zakresu: sztucznej inteligencji, danych osobowych i nieosobowych, cyberbezpieczeństwa, poprawy dostępu do Internetu i umiejętności cyfrowych oraz regulacji platform internetowych⁴⁹⁰. Część z tych obszarów w sposób bezpośredni lub pośredni dotyka materii personalizacji opartej na sztucznej inteligencji.

Sztuczna inteligencja umożliwia używanie w stosunku do konsumentów pogłębionej personalizacji. Z tego powodu należy przyjrzeć się projektowanym w tej dziedzinie aktom prawnym, które będą oddziaływać na dopuszczalność wykorzystania sztucznej inteligencji w procesie personalizacji. W ostatnich latach powstało wiele dokumentów dotyczących sztucznej inteligencji, m.in. związanych ze sferą etyczną jej wykorzystywania, odpowiedzialnością za ewentualne szkody, dyskryminacją i nieprzejrzystością algorytmów. Zwieńczeniem tych prac było opublikowanie w kwietniu 2021 r. projektu pierwszego rozporządzenia w sprawie sztucznej inteligencji⁴⁹¹.

Działania Unii Europejskiej koncentrowały się również na uregulowaniu funkcjonowania platform cyfrowych, m.in. w sferze spersonalizowanych reklam, co pozwoliłoby na lepszą ochronę konsumentów oraz ich praw podstawowych w Internecie. Na poziomie Unii Europejskiej projektowane są dwa akty prawne z tego zakresu - Kodeks Usług Cyfrowych (ang. *Digital Services Act*)⁴⁹² oraz Kodeks Rynków Cyfrowych (ang. *Digital Markets Act*)⁴⁹³, gdzie ustanowione zostaną zasady dotyczące przejrzystości spersonalizowanych reklam oraz systemów rekomendujących wykorzystywanych przez platformy internetowe.

Również w zakresie problematyki ochrony danych osobowych projektowane są zmiany wpływające na zakres stosowania personalizacji. Trzeba podkreślić, że działania Unii Europejskiej w zakresie danych nie zakończyły się z chwilą uchwalenia RODO. W ramach strategii jednolitego rynku cyfrowego zaproponowanej przez Komisję Europejską w 2015 r. postulowano usunięcie barier w świadczeniu i dostępie do in-

490 Pozyskano z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pl. Dostęp: 11.06.2021 r.

491 Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021) 206 final (dalej: rozporządzenie w sprawie sztucznej inteligencji).

492 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 (dalej: Kodeks Usług Cyfrowych).

493 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final (dalej: Kodeks Rynków Cyfrowych).

nowacyjnych usług cyfrowych przy jednoczesnym zapewnieniu wysokiego poziomu ochrony konsumentów i ich danych. Jednym z aktów prawnych składających się na strategię jest rozporządzenie w sprawie prywatności i łączności elektronicznej⁴⁹⁴, które ma zapewniać prywatność treści komunikacyjnych i metadanych m.in. przez ustalenie nowych zasad dotyczących akceptowania lub odrzucania plików *cookie*. Regulacje zawarte w rozporządzeniu *ePrivacy* mogą wpłynąć na ograniczenie śledzenia aktywności konsumentów w Internecie, a co za tym idzie - także dostępność personalizacji.

Projekt rozporządzenia przedstawiony w 2017 roku przez Komisję Europejską napotkał duży opór ze strony niektórych państw członkowskich oraz podmiotów zajmujących się reklamą internetową⁴⁹⁵, które miałyby podlegać tej regulacji. Podmioty z branży reklamowej stworzyły kampanię pod hasłem „Like a bad movie”, która ma przekonywać o negatywnych skutkach rozporządzenia *ePrivacy* dla konsumentów, np. przeciążenia konsumentów pytaniami o wyrażenie zgody na przetwarzanie lub zanik bezpłatnych treści cyfrowych. Między innymi z tego powodu prace nad rozporządzeniem wciąż nie zostały ukończone, a samo rozporządzenie doczekało się kilkunastu zmienionych wersji. Kolejny ważny krok w procedurze uchwalania tego aktu nastąpił 10 lutego 2021 r., gdy państwa członkowskie uzgodniły porozumienie w sprawie mandatu negocjacyjnego Rady UE w sprawie rozporządzenia *ePrivacy*.

Ostatnim aktem prawnym przyczyniającym się do unormowania personalizacji, który zostanie omówiony w ramach tego rozdziału, jest zmieniona za sprawą pakietu „Nowy ład dla konsumentów” dyrektywa 2011/83/UE. Ma ona na celu m.in. zagwarantowanie konsumentom przejrzystych warunków zakupów w Internecie, również w kontekście stosowanej wobec nich personalizacji cenowej.

2. Strategia UE w zakresie sztucznej inteligencji i jej znaczenie w kontekście personalizacji

2.1. Sztuczna inteligencja w dokumentach unijnych

Unia Europejska stoi na stanowisku, że sztuczna inteligencja powinna być przede wszystkim wiarygodna, oparta na zaufaniu i skoncentrowana na człowieku⁴⁹⁶. Wśród kluczowych wymagań dla systemów sztucznej inteligencji wymienia się m.in. zapewnienie ludzkiej wolnej woli i nadzoru, prywatności, przejrzystości, różnorodności, niedyskryminacji oraz sprawiedliwości⁴⁹⁷. Algorytmy muszą być zgodne m.in. z prawami podstawowymi i ochroną danych osobowych⁴⁹⁸. Podkreśla się konieczność wykorzystywania niedyskryminujących zbiorów danych i pomagania konsumentom

494 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP 2017/0003(COD) (dalej: rozporządzenie *ePrivacy*).

495 Pozyskano z: <https://www.likeabadmovie.eu/>. Dostęp: 11.06.2021 r.

496 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka*, COM/2019/168 final, s. 1.

497 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Budowanie zaufania...*, s. 3.

498 Rezolucja Parlamentu Europejskiego z dnia 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 39.

w dostępie do różnorodnych treści i usług⁴⁹⁹. Postuluje się też wprowadzenie wytycznych dotyczących przejrzystości i rozliczalności w odniesieniu do zautomatyzowanych procesów podejmowania decyzji⁵⁰⁰. Konsumenci w przypadku interakcji z takimi procesami muszą mieć zapewnione prawo do otrzymywania terminowej, zwięzłej, łatwo zrozumiałej i przystępnej informacji o fakcie zastosowania sztucznej inteligencji oraz o sposobie żądania skorygowania ewentualnych błędów wynikających z podjętych w ten sposób decyzji⁵⁰¹. Niezwykle ważne jest też zapewnienie możliwości odmowy, ograniczenia lub wyłączenia personalizacji opartej na sztucznej inteligencji⁵⁰².

Podkreśla się fakt, że choć usługi oparte na sztucznej inteligencji mają ogromny potencjał w zakresie zapewnienia korzyści konsumentom, to należy stworzyć odpowiednie przepisy w celu zminimalizowania ryzyka dyskryminacji, nieprzejrzystości oraz niezrozumiałego objaśnienia algorytmów⁵⁰³. Personalizacja oparta na sztucznej inteligencji powinna wspierać wybory konsumentów i poszerzać ich możliwości, a nie zmniejszać ludzką autonomię i powodować manipulację⁵⁰⁴.

Ważnym krokiem w uregulowaniu sztucznej inteligencji było opublikowanie w 2020 r. *Białej księgi w sprawie sztucznej inteligencji*. Określono tam m.in. potrzebę zwiększania powszechnej wiedzy oraz umiejętności w zakresie sztucznej inteligencji, aby przygotować konsumentów do coraz częstszeo kontaktu z nią⁵⁰⁵, m.in. w postaci personalizacji internetowej. Podkreślono, że obecne, rygorystyczne ramy prawne, zapewniające m.in. ochronę konsumentów, danych osobowych i prywatności, będą miały nadal zastosowanie do sztucznej inteligencji, chociaż konieczne mogą być ich aktualizacje⁵⁰⁶.

Personalizacja oparta na sztucznej inteligencji pośrednio znalazła odzwierciedlenie także w dokumencie „Nowy program na rzecz konsumentów. Poprawa odporności konsumentów na potrzeby trwałej odbudowy” na lata 2020-2025. Zauważono, że konsumenci w sferze cyfrowej są narażeni na ukryte mechanizmy gromadzenia danych, które w połączeniu z analizą zachowań opartą na sztucznej inteligencji mogą być wykorzystywane do manipulacyjnych praktyk handlowych⁵⁰⁷, w tym również personalizacji internetowej. Z tego powodu konieczne jest wdrożenie dodatkowych wymagań z zakresu przejrzystości w celu rozwiązania problemu asymetrii informacyjnej⁵⁰⁸.

499 Rezolucja Parlamentu Europejskiego z dnia 20. 10. 2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 40.

500 Rezolucja Parlamentu Europejskiego z dnia 20. 10. 2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 41.

501 Rezolucja Parlamentu Europejskiego z dnia 20. 10. 2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 42-43.

502 Rezolucja Parlamentu Europejskiego z dnia 20. 10. 2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 44.

503 Rezolucja Parlamentu Europejskiego z dnia 20. 10. 2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 38.

504 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Budowanie zaufania...*, s. 4.

505 Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji...*, s. 7.

506 Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji...*, s. 19-20.

507 Komunikat Komisji do Parlamentu Europejskiego i Rady, *Nowy program na rzecz konsumentów...*, s. 12.

508 Komunikat Komisji do Parlamentu Europejskiego i Rady, *Nowy program na rzecz konsumentów...*, s. 23.

2.2. Projekt rozporządzenia w sprawie sztucznej inteligencji

W kwietniu 2021 r. został opublikowany projekt rozporządzenia w sprawie sztucznej inteligencji, który wprowadza czteropoziomowy system klasyfikacji SI oparty na ocenie ryzyka. Przewiduje on m.in. listę zabronionych praktyk opartych na sztucznej inteligencji oraz wykaz systemów sztucznej inteligencji, które zostały zidentyfikowane jako powodujące wysokie ryzyko. W ramach pierwszej kategorii w art. 5 ust. 1 zakazano opartych na sztucznej inteligencji praktyk, które mogą powodować manipulację osobami lub wyzyskiwać wrażliwości określonych grup w celu zniekształcenia ich zachowania. Jednocześnie określono, że inne niż wymienione praktyki manipulacyjne oparte na systemach sztucznej inteligencji mogą zostać objęte istniejącymi już przepisami z zakresu ochrony danych, ochrony konsumentów lub usług cyfrowych⁵⁰⁹. Personalizacja reklam oraz warunków umownych skierowanych do konsumentów została zatem wyłączona z zakresu zakazanych praktyk ujętych w rozporządzeniu. W ramach drugiej kategorii w zamkniętym katalogu praktyk powodujących wysokie ryzyko ujęto jedynie szczególną formę profilowania i personalizacji warunków umownych, jaką jest wykorzystywanie sztucznej inteligencji do oceny zdolności kredytowej⁵¹⁰.

Rozporządzenie w sprawie sztucznej inteligencji w tym kształcie w niewielkim stopniu odnosi się do problematyki personalizacji stosowanej wobec konsumentów. Wydaje się, że w przypadku mniej poważnych z punktu widzenia ryzyka decyzji, dotyczących np. spersonalizowanych reklam *online*, również powinno się zapewnić odpowiedni poziom wyjaśnialności, tak aby chronić konsumentów przed manipulacjami⁵¹¹. Pozostaje oczekiwać, że wymogi dotyczące przejrzystości personalizacji zostaną określone bezpośrednio w prawie konsumenckim lub - tak jak zasugerowano w motywie 81 komentowanego rozporządzenia - dostawcy takich systemów dobrowolnie wdrożą wymogi mające zastosowanie do systemów wysokiego ryzyka.

3. Nowe obowiązki platform internetowych wobec konsumentów w związku z personalizacją opartą na sztucznej inteligencji

Z uwagi na postępującą w szybkim tempie transformację cyfrową, coraz częstsze opieranie modeli biznesowych platform internetowych na reklamach behawioralnych oraz powstające w związku z tym nowe zagrożenia dla ich użytkowników Unia Europejska podjęła kroki zmierzające do uregulowania funkcjonowania platform internetowych, co będzie wpływać także na stosowaną przez nie personalizację w postaci ukierunkowanych reklam. 15 grudnia 2020 r. Komisja Europejska opublikowała pierwsze projekty dwóch aktów prawnych dotyczących rynku cyfrowego.

3.1. Projekt Kodeksu Usług Cyfrowych

Przepisy Kodeksu Usług Cyfrowych mają za zadanie przywrócić równowagę między użytkownikami, platformami internetowymi oraz organami publicznymi. Dzięki nim

509 Strona 13 projektu rozporządzenia o sztucznej inteligencji.

510 Punkt 5 lit. b załącznika III, Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. High-risk AI systems referred to in article 6(2), COM(2021) 206 final.

511 D. Pedreschi, I. Miliou, *Artificial Intelligence (AI): new developments...*, s. 26.

nadzór nad działaniami platform internetowych zostanie poszerzony, a prawa podstawowe konsumentów w Internecie będą objęte skuteczniejszą ochroną.

3.1.1. Zapewnienie przejrzystości spersonalizowanych reklam

Konsumenti mają uzasadnione podstawy, aby oczekiwać od platform internetowych uczciwych warunków dostępu oraz przejrzystości. Podkreśla się zwłaszcza potrzebę przejrzystości warunków umownych dotyczących możliwości i zakresu udostępniania danych podmiotom trzecim⁵¹². W propozycji Kodeksu Usług Cyfrowych częściowo uregulowano kwestię reklam internetowych. W tym zakresie projekt w art. 24 przewiduje, że platformy internetowe, które wyświetlają reklamy na swoich interfejsach internetowych, powinny zapewnić usługobiorcom możliwość jednoznacznego zidentyfikowania, czy wyświetlane informacje są reklamą, a jeśli tak, to jaki podmiot za nią odpowiada.

W kontekście poprawy przejrzystości reklam spersonalizowanych zaproponowano obowiązek podawania miarodajnych informacji o głównych parametrach wykorzystywanych do określenia odbiorcy, któremu wyświetlana jest reklama. Praktyka ta jest już obecnie stosowana przez Facebook i właśnie na tym przykładzie można zakwestionować skuteczność przedstawionego przez Kodeks Usług Cyfrowych rozwiązania. Facebook w banerze „Dlaczego widzę tę reklamę?” informuje bowiem, że oprócz wyświetlanych tam parametrów mogą występować też inne czynniki, które nie zostały w tym miejscu wyszczególnione. Badania wykazują, że mimo większej liczby atrybutów wybranych jednocześnie przez reklamodawców, wyjaśnienia często informują tylko o jednym z nich⁵¹³. Faworyzowane są ponadto parametry bardziej popularne, takie jak kryterium: wieku, lokalizacji i płci. Co więcej, kryterium lokalizacji jest umieszczane w wyjaśnieniach nawet wtedy, gdy reklamodawca nie wybrał tego atrybutu⁵¹⁴. Przyznawanie pierwszeństwa popularnym kryteriom może sprawić, że z perspektywy konsumenta każda taka informacja będzie niemal identyczna, a co za tym idzie – pozbawiona realnej wartości informacyjnej.

Ze względu na specyfikę reklamy behawioralnej istotne znaczenie mają użyte przez reklamodawców kryteria niszowe dotyczące zainteresowań konkretnych użytkowników oraz ich danych wrażliwych, a nie popularne parametry wieku i lokalizacji, które w znikomym stopniu wpływają na skuteczność reklamy spersonalizowanej. Informacja o tych parametrach mogłaby realnie zmniejszyć asymetrię informacyjną między konsumentami a reklamodawcami. Jeśli obowiązek informowania o głównych parametrach określających odbiorcę będzie interpretowany przez platformy podobnie jak w przypadku Facebooka, reklamodawcy mogą zacząć świadomie umieszczać niszowe atrybuty obok tych najpopularniejszych. Mimo iluzorycznej kontroli danej konsumentom pozwoli to ukryć przed nimi prawdziwy powód targetowania. Ponadto należy zwrócić uwagę, że niejasne pozostaje, czy obowiązek podawania informacji dotyczy tylko parametrów manualnie wybranych przez reklamodawcę, czy również tych okre-

512 Rezolucja Parlamentu Europejskiego z dnia 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 21.

513 A. Andreou, G. Venkatadri, O. Goga, K.P. Gummadi, P. Loiseau, A. Mislove, *Investigating Ad Transparency Mechanisms in Social Media...*, s. 9.

514 A. Andreou, G. Venkatadri, O. Goga, K.P. Gummadi, P. Loiseau, A. Mislove, *Investigating Ad Transparency Mechanisms in Social Media...*, s. 10.

ślonych samoistnie przez algorytmy i systemy rekomendacji. Dopiero stosowanie takiego obowiązku w praktyce pozwoli na weryfikację, czy jest on przestrzegany przez platformy internetowe w rzetelny sposób.

Dodatkowo tzw. bardzo duże platformy internetowe, do których można zaliczyć np. Google i Facebooka, będą miały obowiązek udostępniać biblioteki reklam, w których możliwe będzie sprawdzenie treści reklamy, osoby odpowiedzialnej za reklamę, okresu jej wyświetlania, parametrów targetowania - o ile takie targetowanie zostało użyte - oraz całkowitą liczbę odbiorców usługi, do których dotarła reklama⁵¹⁵. Taki obowiązek ma ułatwić nadzór nad zagrożeniami związanymi z technikami manipulacji i dezinformacji⁵¹⁶. Obecnie takie repozytoria reklam funkcjonują na Facebooku w odniesieniu do reklam politycznych i dotyczących kwestii społecznych.

3.1.2. Dodatkowe informacje o systemach rekomendujących

Coraz częstsze wykorzystanie systemów rekomendujących opartych na algorytmicznym sugerowaniu i filtrowaniu informacji rodzi niebezpieczeństwa w postaci manipulowania zachowaniami użytkowników platform oraz wirusowego rozpowszechniania informacji⁵¹⁷. Z tego względu projekt Kodeksu Usług Cyfrowych przewiduje dodatkowe obowiązki informacyjne dla bardzo dużych platform internetowych. Zgodnie z art. 29 Kodeksu Usług Cyfrowych platformy te będą zobowiązane do umieszczenia w swoich regulaminach głównych parametrów, którymi kierują się wykorzystywane przez nie systemy rekomendujące. Informacje te powinny być przedstawione w sposób jasny i zrozumiały dla odbiorców.

Oprócz tego platformy będą obowiązane do pozostawienia swoim użytkownikom przynajmniej jednej opcji segregacji treści, która nie będzie opierała się na profilowaniu. Ten obowiązek wydaje się kluczowym rozwiązaniem, które pomoże chronić konsumentów przed nadmierną personalizacją. Choć konsumenci potrzebują pomocy w filtrowaniu istotnych dla siebie informacji, to możliwość przeglądania informacji jako anonimowy użytkownik jest równie istotna⁵¹⁸. Podobne zapatrywanie przyjął Parlament Europejski w przyjętej przez siebie rezolucji⁵¹⁹, stwierdzając, że Kodeks Usług Cyfrowych powinien przewidywać prawo do anonimowego korzystania z usług cyfrowych wszędzie tam, gdzie jest to technicznie możliwe. Konsumenci powinni mieć wybór, czy chcą być poddawani personalizacji nakierowanej najczęściej na wywołanie w nich nieuzasadnionej potrzeby zakupu produktu lub usługi, co może być szczególnie ważne dla konsumentów o większym stopniu wrażliwości i skłonności do działań kompulsywnych.

3.2. Projekt Kodeksu Rynków Cyfrowych

Kodeks Rynków Cyfrowych ma za zadanie uzupełniać unijne prawo konkurencji i przeciwdziałać nieuczciwym zachowaniom tzw. „strażników dostępu” (*ang. gatekeeper*).

515 Artykuł 30 projektu Kodeksu Usług Cyfrowych.

516 Motyw 63 projektu Kodeksu Usług Cyfrowych.

517 Motyw 62 projektu Kodeksu Usług Cyfrowych.

518 G. Sarton, *Artificial Intelligence: Challenges for EU Citizens and Consumers...*, s. 7.

519 Rezolucja Parlamentu Europejskiego z dnia 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego..., pkt 18.

s)⁵²⁰, czyli dużych dostawców podstawowych usług platformy o znacznej sile gospodarczej mających znaczący wpływ na rynek wewnętrzny. W zakres takich usług mogą wchodzić np.: usługi pośrednictwa internetowego, wyszukiwarki internetowe, systemy operacyjne, portale społecznościowe, usługi komunikacji interpersonalnej niewykorzystujące numerów, usługi przetwarzania w chmurze i usługi reklamy *online*⁵²¹.

Za szczególnie istotną w kontekście profilowania oraz personalizacji należy uznać propozycję z art. 5 pkt a) Kodeksu Rynków Cyfrowych, dotyczącą powstrzymania się od łączenia danych użytkowników końcowych z różnych źródeł, w tym z usług własnych *gatekeepera*, co obecnie daje im znaczącą przewagę i możliwość tworzenia kompleksowych zbiorów danych i profili użytkowników. Proponowany zakaz nie jest bezwzględny, gdyż użytkownikom pozostawiono możliwość swobodnej decyzji o wyrażeniu zgody na takie praktyki, przy czym zgoda powinna obejmować wszystkie możliwe źródła danych osobowych. Wysunięta przez Komisję Europejską propozycja potencjalnie ogranicza więc możliwości profilowania, a co za tym idzie - również personalizacji. Przede wszystkim daje jednak użytkownikom platform internetowych minimum kontroli nad tym, w jaki sposób przetwarzane są ich dane osobowe.

4. Zmiana uregulowania plików *cookie* wykorzystywanych do celów personalizacji opartej na sztucznej inteligencji

4.1. Obecna regulacja plików *cookie*

Aktem regulującym obecnie problematykę oprogramowania śledzącego aktywność konsumentów w internecie jest obowiązująca od niemal 20 lat dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. W przypadku tak pręźnie rozwijających się technologii *Big Data* i personalizacji dyrektywa sprzed 20 lat nie jest w stanie uwzględnić obecnych realiów i nowo powstałych zagrożeń. Zwraca się uwagę m.in. na szerokie rozpowszechnienie usług łączności elektronicznej, które dla konsumentów stanowią już pełnoprawny substytut tradycyjnych usług⁵²². Dyrektywa 2002/58/WE zostanie zastąpiona przez długo oczekiwane rozporządzenie *ePrivacy*. Projekt rozporządzenia określa m.in. zasady wykorzystywania plików *cookie* do kierowania spersonalizowanych reklam, co stanowi ważną część personalizacji opartej na sztucznej inteligencji.

4.1.1. Charakterystyka plików *cookie* i ich rodzaje

Pliki *cookie* to niewielkie informacje tekstowe wysyłane przez serwer do przeglądarki i zapisywane na urządzeniach końcowych użytkownika⁵²³. Niektóre z nich są jedynie tymczasowo przechowywane na urządzeniu i służą np. do obsługi koszyka towarów w sklepach internetowych (tymczasowe, sesyjne *cookies*). Inne pozostają na urządzeniu użytkownika, niezależnie od faktu zamknięcia przeglądarki, do czasu ich samodzielnego usunięcia przez użytkownika (*cookies* stałe)⁵²⁴. To właśnie ten rodzaj

520 J. Laux, S. Wachter, B. Mittelstadt, *Neutralizing online behavioural advertising...*, s. 719-750.

521 Motyw 13 projektu Kodeksu Rynków Cyfrowych.

522 Motyw 6 projektu rozporządzenia *ePrivacy*.

523 K. Grzybczyk, *Reklama behawioralna* (w:) P. Ślęzak (red.), *Prawo mediów*, Warszawa 2020, s. 184-186.

524 C. Castelluccia, A. Narayanan, *Privacy considerations of online behavioural tracking...*, s. 4.

cookies służy do wielopoziomowego śledzenia aktywności konsumenta, począwszy od ruchów myszki oraz kliknięć, po rejestrowanie czasu, który konsument poświęcił określonym treściom. Stałe cookies mają bowiem ustawiony bardzo długi okres ważności, przez co śledzenie użytkownika może odbywać się w sposób ciągły przez wiele miesięcy, a nawet lat⁵²⁵. Należy wspomnieć o użytecznych w personalizacji, ale niezwykle niebezpiecznych z punktu widzenia prywatności konsumentów tzw. wiecznych cookies (ang. *evercookie*, *zombie cookie*), które pomimo prób usunięcia ich z urządzenia są automatycznie odtwarzane⁵²⁶.

Pliki cookie można dzielić również na własne (ang. *first party cookies*), które są zamieszczane przez właściciela strony internetowej, i zewnętrzne (*third party cookies*) umieszczane na danej stronie z uwagi na wykorzystywane na niej usługi⁵²⁷, np. w przypadku umieszczenia przycisku „Lubię to” na stronie konieczne jest też umieszczenie zewnętrznego cookie Facebooka.

Stałe pliki cookie są obecnie jednym z najpopularniejszych narzędzi, które mogą służyć do monitorowania aktywności konsumentów odwiedzających strony internetowe, tworzenia profili przez wnioskowanie o zainteresowaniach tych osób oraz podejmowania wobec nich decyzji⁵²⁸. Na przykład dane zbierane przez śledzące cookies w połączeniu z informacjami wprowadzonymi przez konsumenta do formularzy kalkulacji pożyczki mogą służyć dostosowywaniu warunków umownych⁵²⁹. Liczba instalowanych na urządzeniach końcowych plików cookie wydaje się nadmierna, a ich akceptacja jest najczęściej wymuszana na konsumentach. Wraz z rozpowszechnieniem się technologii cookies śledzących konsumenci zaczęli stosować narzędzia chroniące ich prywatność i blokujące niechciane cookies, co niewątpliwie skłania branżę reklamową do poszukiwania skuteczniejszych metod śledzenia aktywności. Dodatkowo popularność plików cookie może zmniejszyć się ze względu na zapowiedzianą przez Google rezygnację z zewnętrznych cookies w 2022 r.⁵³⁰.

4.1.2. Techniczne sposoby blokowania cookies przez konsumentów

Istnieje niewiele technicznych rozwiązań, które pozwalałyby konsumentom na ochronę przed instalowaniem na ich urządzeniach końcowych plików cookie. Jednym ze sposobów jest używanie funkcji „Do Not Track” w przeglądarkach. Funkcja ta wysyła prośbę do odwiedzanych przez konsumenta stron internetowych, by nie zbierały i nie śledziły danych przeglądania⁵³¹. Z uwagi na brak możliwości skontrolowania przez konsumenta tego, czy dana strona zastosowała się do wysłanej prośby, skuteczność tej metody zależy w głównej mierze od dobrej woli twórców stron. Konsument

525 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 6.
526 J. Byrski, L. Sytniewski (w:) E. Traple (red.), *Ochrona gry komputerowej. Aktualne wyzwania prawne*, Warszawa 2015, s. 187-204.

527 X. Konarski, *Podstawy prawne korzystania z „ciasteczek” internetowych (cookies) jako przykład wzajemnej relacji przepisów RODO oraz przepisów o ochronie prywatności w sektorze łączności elektronicznej* (w:) G. Sibiga (red.), *Przepisy prawa uzupełniające RODO. Aktualne problemy prawnej ochrony danych osobowych 2018*, dodatek MoP 2018, nr 22, s. 33.

528 A. Krasuski, *Status prawny sztucznego agenta...*, s. 302-309.

529 The Data Protection Commission, *Report by the Data Protection Commission on the use of cookies and other tracking technologies*, 2020, s. 22.

530 Pozyskano z: <https://www.pcworld.pl/news/Google-rezygnuje-z-plikow-cookies-Firma-nie-bedzie-sledzic-uzytkownikow,425920.html>. Dostęp: 11.06.2021 r.

531 C. Castelluccia, A. Narayanan, *Privacy considerations of online behavioural tracking...*, s. 17.

może dodatkowo zdecydować się na instalację specjalnego oprogramowania, które będzie blokować *cookies* śledzące na stronach internetowych przy zachowaniu ich funkcjonalności. Skutecznym sposobem uniknięcia śledzenia aktywności w sieci internetowej jest także używanie przeglądarki internetowej w trybie „prywatnym”, co skutkuje usunięciem wszystkich utworzonych plików *cookie* po zamknięciu okna przeglądarki⁵³². To rozwiązanie będzie jednak wpływać na wygodę przeglądania stron internetowych, np. przez brak możliwości zapamiętywania haseł. Ostatecznie konsument może zdecydować się na zablokowanie plików *cookie* z poziomu ustawień przeglądarki, co jest równoznaczne z niedostępnością wielu użytecznych funkcji stron internetowych opartych na plikach *cookie*.

4.1.3. Problematyka wstępnego ładowania plików *cookie*

Z jednej strony konsumenci nie wiedzą, do czego tak naprawdę służą *cookies*, jak nimi zarządzać oraz usuwać. A z drugiej strony administratorzy stron internetowych wciąż dość swobodnie podchodzą do ciążących na nich obowiązków. Bez trudu można znaleźć strony internetowe niezawierające komunikatów dotyczących wyrażenia zgody na *cookies*, pomimo używania plików *cookie* śledzących aktywność użytkowników⁵³³, lub takie, które jedynie informują o używaniu śledzących plików *cookie* bez możliwości jakiegokolwiek interakcji⁵³⁴.

Jeszcze większym problemem dla administratorów jest sama organizacja procesu implementacji *cookies* pod względem technicznym⁵³⁵. Jako że możliwość instalacji *cookies* na urządzeniu końcowym musi być poprzedzona zgodą użytkownika, *cookies* nie mogą być instalowane zaraz po wejściu użytkownika na stronę. Do czasu wyrażenia zgody możliwość umieszczania na urządzeniach plików *cookie* powinna być zablokowana. Niemniej jednak wciąż istnieje dość niewielka świadomość, w jaki sposób poprawnie zbudować stronę internetową bez wstępnego ładowania *cookies*. Skutkuje to tym, że w wielu przypadkach decyzja o niewyrażeniu zgody na *cookies* śledzące nie będzie powodowała dla konsumenta żadnej zmiany – pliki *cookie* zostaną automatycznie umieszczone na jego urządzeniu w momencie odwiedzenia strony internetowej. W jednym z badań zanotowano, że aż 92% witryn ustawia co najmniej jeden plik *cookie* przed wyświetleniem jakiegokolwiek powiadomienia konsumentowi⁵³⁶. Doskonałym przykładem mogą być postępowania przeciwko Google oraz Amazon, które zostały ukarane przez francuski organ ochrony danych za instalowanie plików *cookie*, w tym plików o charakterze śledzącym, po wejściu na ich witryny bez konieczności podejmowania żadnych działań⁵³⁷. Pokazuje to, że weryfikacja momentu instalowania *cookies* najczęściej następuje dopiero w przypadku kontroli.

532 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 6-7.

533 The Data Protection Commission, *Report by the Data Protection Commission...*, 2020, s. 3.

534 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 3.

535 The Data Protection Commission, *Report by the Data Protection...*, s. 7.

536 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 12.

537 Pozyskano z: <https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland> oraz <https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core>. Dostęp: 11.06.2021 r.

4.1.4. Pliki cookie traktowane jako dane osobowe

Choć plik *cookie* sam w sobie nie jest daną osobową, to może się nią stać ze względu na swoją zawartość⁵³⁸. Uzasadnienie tego stanowiska można znaleźć w art. 4 pkt 1 RODO, który nie pozostawia wątpliwości, że identyfikatory internetowe mogą prowadzić bezpośrednio lub pośrednio do rozpoznania osoby fizycznej. W przypadku *cookies* śledzących wykorzystywanych do stosowania reklam behawioralnych możliwość identyfikacji jest niemal pewna ze względu na zapisywanie na danym urządzeniu tzw. *cookies* ID, które będzie umożliwiać łączenie informacji dotyczących konsumenta w celu wytworzenia jego profilu⁵³⁹. Podobnego zdania jest Grupa Robocza Art. 29 ds. Ochrony Danych, która zbieranie za pomocą plików *cookie* adresów IP i unikalnych identyfikatorów internetowych wymieniła jako jeden z powodów, dla których reklamy behawioralne oparte na plikach *cookie* będą wiązały się ze zbieraniem danych osobowych⁵⁴⁰. Samo „wyszczególnienie” osób, bez poznawania ich dokładnej tożsamości, jest wystarczające⁵⁴¹. Ponadto zwraca się uwagę, że zebrane m.in. za pomocą plików *cookie* informacje dotyczą cech lub zachowania danej osoby i mogą być wykorzystywane do wywierania na nią wpływu⁵⁴². Na przykład monitorowanie ruchu telefonu może ujawnić zmiany w chodzie, które mogą okazać się wczesnym symptomem depresji⁵⁴³. Taka informacja z kolei może posłużyć ubezpieczycielowi do odmowy udzielenia ubezpieczenia lub zwiększenia jego składki. Z łatwością można również połączyć zebrane informacje o aktywności internetowej konsumenta z danymi identyfikującymi go w sposób bezpośredni, podanymi np. w czasie rejestracji⁵⁴⁴.

Choć wciąż pojawiają się głosy, że pliki *cookie* identyfikują urządzenie, a nie osobę fizyczną, to należy zgodzić się, że pozwala to na możliwość wyodrębnienia informacji o danej osobie i traktowanie tych informacji jako unikalnych, nawet jeśli bezpośrednio zidentyfikowanie osoby fizycznej nie będzie możliwe⁵⁴⁵. Podobnie charakteru zawartych w plikach *cookie* danych nie zmienia zastosowanie pseudonimizacji⁵⁴⁶.

Często wątpliwości dotyczą analitycznych plików *cookie*, np. Google Analytics, które pozwalają na analizę danych statystycznych dotyczących strony. Administrator strony przy pomocy tych *cookies*, poza anonimowymi danymi statystycznymi, faktycznie nie będzie miał możliwości identyfikacji określonego użytkownika. Niemniej jednak zawartość tego samego pliku *cookie* dla Google daje zupełnie inne możliwości identyfikacji i z pewnością stanowi daną osobową.

4.1.5. Dwoistość obecnego uregulowania zagadnienia plików cookie

Zasady uzyskiwania zgody na pliki *cookie* zostały uregulowane w głównej mierze w dyrektywie o prywatności i łączności elektronicznej. Z art. 5 ust. 3 dyrektywy

538 J. Byrski, H. Hoser, *Social media oraz technologie umożliwiające śledzenie użytkowników Internetu a współ-administrowanie danymi osobowymi* (w:) X. Konarski (red.), *Prawo nowych technologii dane osobowe i cyberbezpieczeństwo, Internet i media, handel elektroniczny, prawo IT, technologie*, dodatek MoP 2019, nr 21, s. 6-14.

539 X. Konarski, *Podstawy prawne korzystania z „ciasteczek”*..., s. 33.

540 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam*..., s. 10.

541 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam*..., s. 10.

542 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam*..., s. 10.

543 C. Castelluccia, A. Narayanan, *Privacy considerations of online behavioural tracking*..., s. 12.

544 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam*..., s. 10.

545 X. Konarski, *Podstawy prawne korzystania z „ciasteczek”*..., s. 33.

546 X. Konarski, *Podstawy prawne korzystania z „ciasteczek”*..., s. 34.

2002/58/WE o prywatności i łączności elektronicznej wynika, że przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym jest dozwolone wyłącznie pod warunkiem wyrażenia zgody przez użytkownika oraz wcześniejszego udzielenia jasnych i wyczerpujących informacji. Przepis ten ma na celu ochronę przed ingerencją w urządzenia końcowe konsumentów, tj.: telefonów, tabletów i komputerów konsumentów, bez ich wiedzy⁵⁴⁷. Ingerencja ta polega na instalowaniu oprogramowania mającego na celu automatyczną identyfikację konsumenta, uzyskanie dostępu do danych zgromadzonych w jego urządzeniu lub śledzeniu podejmowanych przez niego działań w sieci⁵⁴⁸. Nie ma w tym przypadku znaczenia, czy pliki *cookie* zawierają dane osobowe⁵⁴⁹.

Artykuł 5 ust. 3 wprost stanowi także, że zgoda użytkownika końcowego powinna zostać wyrażona zgodnie z dyrektywą 95/46/WE⁵⁵⁰, zastąpioną obecnie przez RODO. Należy zatem uznać, że obecnie do uzyskania zgody abonenta lub użytkownika końcowego stosuje się przepisy RODO. Niemniej jednak dyrektywa o prywatności i łączności elektronicznej, jako *lex specialis*, ma pierwszeństwo przed RODO, które pozostaje aktem o większym stopniu ogólności⁵⁵¹.

Z powyżej wymienionych powodów możemy mówić o charakterystycznej dwoistości uregulowania plików *cookie*, które podlegają zarówno dyrektywie 2002/58/WE, jak i RODO, co moim zdaniem nie wpływa korzystnie na egzekwowanie przepisów w praktyce poszczególnych państw członkowskich.

4.2. Projektowana regulacja plików *cookie* w rozporządzeniu *ePrivacy*

Rozporządzenie *ePrivacy* ma polepszyć i ujednolicić poziom ochrony zapewniany obecnie przez dyrektywę o prywatności i łączności elektronicznej, a także uzupełniać RODO, zapewniając przy tym dodatkowe gwarancje poufności⁵⁵². Zakres obowiązywania rozporządzenia *ePrivacy* został sformułowany szeroko - podstawowym kryterium będzie fakt przebywania użytkownika końcowego w Unii Europejskiej⁵⁵³. Treść rozporządzenia z dużym prawdopodobieństwem ulegnie jednak zmianie w trakcie procesu legislacyjnego.

Implementacja dyrektywy 2002/58/WE w państwach członkowskich była niejednolita⁵⁵⁴. Jako że w Internecie granice między porządkami prawnymi poszczególnych państw nie są tak namacalne, ujednolicenie zasad dotyczących prywatności w Internecie w ramach rozporządzenia wpłynie korzystnie na egzekwowanie wyrażonych w nim praw konsumentów.

547 S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2018, s. 1182.

548 S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2018, s. 1182.

549 M. Rojszczak, *Ochrona prywatności...*, s. 199-200.

550 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Dz.Urz.UE L 281 z dnia 23.11.1995 r., s. 31.

551 Motyw 10 dyrektywy o prywatności i łączności elektronicznej.

552 Europejska Rada Ochrony Danych, *Oświadczenie 03/2021 w sprawie rozporządzenia o prywatności i łączności elektronicznej*, 2021, s. 1.

553 Artykuł 3 ust. 1 projektu rozporządzenia *ePrivacy*.

554 Pozyskano z: <https://prawo.gazetaprawna.pl/artykuly/1498889,kary-za-ciasteczka-google-amazon.html>. Dostęp: 11.06.2021 r.

Projekt przewiduje, że dane pochodzące z łączności elektronicznej powinny być traktowane jako poufne, a wszelkie ingerencje w te dane bez zgody użytkownika są zakazane, co ma zastosowanie także do procedury monitorowania przez podmioty trzecie odwiedzanych stron internetowych oraz interakcji międzyludzkich w celu tworzenia profili użytkowników⁵⁵⁵.

Oprócz plików *cookie* projekt rozporządzenia odnosi się wprost do: oprogramowania szpiegującego, ukrytych identyfikatorów, błędów internetowych oraz tzw. odcisku palca przeglądarki⁵⁵⁶. Ochrona obejmuje również metadane. Zwraca się uwagę na fakt, że metadane mogą ujawniać dane szczególnie chronione i pozwalać na wyciągnięcie wniosków dotyczących prywatnego życia osób, np.: zainteresowań, zwyczajów, relacji towarzyskich. Do metadanych rozporządzenie zalicza m.in. odwiedzane strony internetowe i lokalizację geograficzną. W przypadku metadanych zakazano możliwości ich wykorzystywania do określenia charakteru i cech użytkownika końcowego lub budowania indywidualnego profilu użytkownika końcowego bez wyrażenia przez niego zgody⁵⁵⁷. Dokonano tym samym zauważalnego ograniczenia przesłanek przetwarzania, gdyż w poprzednich wersjach projektu, obok przesłanki zgody, dopuszczano możliwość wykorzystania przesłanki uzasadnionego interesu.

Warto wspomnieć, że w porównaniu do poprzednich wersji rozporządzenia obecny projekt ograniczył zakres stosowania przepisów dotyczących marketingu bezpośredniego. Wprost wskazano bowiem, że rozporządzenie nie będzie miało zastosowania w przypadku wyświetlania reklam na odwiedzanych stronach internetowych⁵⁵⁸. W innym razie, przed wyświetleniem reklamy internetowej, należałoby uzyskać uprzednią zgodę użytkownika. Takie rozwiązanie z pozoru wydaje się niezwykle korzystne dla konsumentów, ale jego wprowadzenie mogłoby prowadzić do niepożądanych efektów w postaci szerszego stosowania przez przedsiębiorców *cookie walls* oraz pogłębienia problemu nieświadomości udzielanych przez konsumentów zgód.

4.2.1. Przesłanki legalizujące przechowywanie informacji na urządzeniach końcowych

Z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej wynika, że przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym jest dozwolone wyłącznie pod warunkiem wyrażenia zgody przez użytkownika oraz wcześniejszego udzielenia jasnych i wyczerpujących informacji. Niektóre z europejskich organów ochrony danych osobowych przyjmują restrykcyjne, lecz z całą pewnością korzystne dla konsumentów stanowisko, że skoro podstawą dla instalowania plików *cookie* jest zgoda, to podstawę prawną do przetwarzania danych osobowych może stanowić również jedynie zgoda⁵⁵⁹. Eliminują w ten sposób problem powszechnie nadużywanej podstawy prawnej uzasadnionego interesu administratora.

Na gruncie obecnie obowiązującej dyrektywy 2002/58/WE, z konieczności uzyskania zgody, wyłączone zostały pliki *cookie* ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta

555 Motyw 18 projektu rozporządzenia *ePrivacy*.

556 Motyw 20 projektu rozporządzenia *ePrivacy*.

557 Motyw 17aa projektu rozporządzenia *ePrivacy*.

558 Motyw 32 projektu rozporządzenia *ePrivacy*.

559 J. Byrski, H. Hoser, *Social media oraz technologie umożliwiające śledzenie...*, s. 6-14.

lub użytkownika, czyli tzw. *cookies* techniczne. W przypadku rozporządzenia *ePrivacy* katalog sytuacji, w których przechowywanie informacji na urządzeniach końcowych jest dopuszczalne bez konieczności wyrażania zgody, jest szerszy niż w dyrektywie 2002/58/WE. Taka możliwość zaistnieje m.in., gdy jest to konieczne wyłącznie w celu świadczenia usługi łączności elektronicznej, w przypadku niezbędności do świadczenia żądanej przez konsumenta usługi, pomiaru widowni, wykonania aktualizacji oprogramowania, zapobiegania oszustwom oraz wykrywania usterek technicznych. Celem tak szczegółowego wyliczenia jest zmniejszenie zjawiska powszechnego kierowania do konsumentów banerów z prośbą o wyrażenie zgody, w sytuacjach, w których pliki *cookie* są użyteczne i nie są wykorzystywane do identyfikowania osób.

Powstaje wątpliwość, czy tak szerokie określenie wyjątków nie będzie rodzić w praktyce pola do nadużyć. Ryzyko to minimalizuje z pewnością art. 8 ust. 1 lit. g, który stanowi, że wykorzystanie informacji zebranych bez zgody konsumenta do innych niż pierwotnie ustalonych celów jest dopuszczalne po spełnieniu dodatkowych warunków, dotyczących m.in. konieczności zaistnienia związku pomiędzy celami. Kluczowy jest fakt, że dalsze wykorzystywanie nie może polegać na budowaniu profilu behawioralnego konsumenta⁵⁶⁰. Projekt rozporządzenia nie reguluje dopuszczalności dalszego przetwarzania informacji pozyskanych na podstawie zgody. Można zatem przyjąć, że tak jak w przypadku rozporządzenia RODO, dalsze przetwarzanie w zakresie przekraczającym pierwotną zgodę nie jest możliwe bez uzyskania nowej zgody.

4.2.2. Rozwiązanie problemu nieświadomości udzielanych zgód

Z uwagi na coraz większe wykorzystywanie profilowania i personalizacji w strategiach biznesowych przedsiębiorców liczba komunikatów dotyczących zgód na pliki *cookie* śledzące rośnie. Wśród konsumentów obserwuje się coraz większe zmęczenie tymi banerami i zanikanie zakładanego efektu ostrzegawczego⁵⁶¹. Wyniki badań pokazują, że gdyby strony internetowe zbierały zgody w pełnej zgodności z RODO i stosowały zasady domyślnej prywatności, to mniej niż 0,1% użytkowników wyrażałoby zgodę na instalowanie zewnętrznych *cookies*⁵⁶². To uwiadamia, że konsumenci nie chcą dzielić się swoją prywatnością, a obecnie zgody są udzielane w większości z powodu pozbawienia konsumentów realnego wyboru. Rozporządzenie *ePrivacy* w założeniu ma poprawić obecną sytuację przeciążenia informacyjnego konsumentów i zapewnić większą kontrolę nad udzielanymi zgodami na śledzenie ich aktywności internetowej. Jeszcze raz trzeba bowiem podkreślić, że personalizacja jest nierozzerwalnie połączona ze śledzeniem podejmowanych przez konsumentów działań w sferze cyfrowej. Ograniczenie możliwości zbierania tych danych wpłynie także na możliwości stosowania wobec konsumentów personalizacji.

4.2.2.1. Obowiązek informacyjny przed umieszczeniem plików *cookie* na urządzeniu

Zgodnie z art. 8 ust. 2a projektu rozporządzenia *ePrivacy* przed udzieleniem zgody na umieszczenie plików *cookie* na urządzeniu konieczne będzie wyraźne i widoczne

⁵⁶⁰ Artykuł 8 ust. 1 lit. h projektu rozporządzenia *ePrivacy*.

⁵⁶¹ Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody...*, s. 19.

⁵⁶² C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 14.

powiadomienie użytkownika o sposobie zbierania informacji, celach ich zbierania, osobie odpowiedzialnej oraz o środkach, jakie użytkownik może podjąć w celu usunięcia plików *cookie*. W przypadku gromadzenia przez *cookies* danych osobowych konieczne będzie spełnienie obowiązku informacyjnego określonego w art. 13 RODO. Wydaje się, że w dalszym ciągu zastosowanie będzie miał wyrok Trybunału Sprawiedliwości w sprawie C-673/17 *Planet49*, według którego informacje obejmują także wskazanie okresu funkcjonowania plików *cookie* oraz określenie, czy osoby trzecie mogą uzyskać dostęp do takich plików⁵⁶³. Tym samym zakres przekazywanych użytkownikowi informacji uległ znacznemu poszerzeniu w porównaniu do dyrektywy 2002/58/WE.

Podkreśla się, że metody udostępniania informacji oraz wyrażania zgody lub odmowy na umieszczanie plików *cookie* powinny być przyjazne dla konsumentów i nie mogą opierać się na języku technicznym lub zakładać, że konsument posiada specjalne wykształcenie lub doświadczenie⁵⁶⁴. Chodzi o możliwie jak najbardziej przejrzyste poinformowanie, że w pamięci urządzenia umieszczona zostanie informacja, nad którą użytkownik nie będzie miał jednak kontroli⁵⁶⁵. W przypadku *cookies* śledzących konieczna wydaje się informacja o tym, że rejestrowane będą odwiedzane przez użytkownika strony internetowe, wyświetlane reklamy oraz kliknięcia⁵⁶⁶. Strona może też odsyłać do miejsca, w którym przedstawione będą rodzaje wykorzystywanych plików *cookie*⁵⁶⁷.

4.2.2.2. Zgoda spełniająca przesłanki art. 7 RODO

Projekt rozporządzenia *ePrivacy* nie zmienia założenia sformułowanego na gruncie dyrektywy 2002/58/WE - możliwość identyfikacji osoby fizycznej przez pliki *cookie* implikuje uznanie, że zgoda na przechowywanie informacji lub uzyskiwanie do nich dostępu musi spełniać kryteria zgody w rozumieniu przepisów art. 5 ust. 1 lit. a RODO⁵⁶⁸. Zastosowanie znajdzie też art. 7 RODO. Świadome wyrażenie zgody ma miejsce dopiero po podaniu użytkownikowi informacji m.in. o celach przechowywania i uzyskiwania dostępu do plików *cookie*. Zgoda musi być więc dobrowolna, przedstawiona w łatwej formie i możliwa do wycofania w każdym czasie w sposób prosty i bezpłatny. Nie można uznać za zgodę czynności przewijania strony internetowej lub pozostawiania na niej⁵⁶⁹, gdyż nie może być to równoznaczne z przejawem aktywności użytkownika. Co istotne, zgodnie z wyrokiem Trybunału Sprawiedliwości w sprawie C-673/17 *Planet49*⁵⁷⁰ zgoda nie jest ważna, jeżeli polega na zaakceptowaniu domyślnie zaznaczonego okienka wyboru, którego zaznaczenie użytkownik musi usunąć, aby odmówić udzielenia zgody.

563 Wyrok TS z 1.10.2019 r. w sprawie C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*, ECLI:EU:C:2019:801, pkt 82.

564 S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2018, s. 1185.

565 S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2018, s. 1185.

566 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 18.

567 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Dokument roboczy 2/2013 przedstawiający wytyczne w sprawie pozyskiwania zgody na zapisywanie plików cookie*, 2013, s. 4.

568 Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017, s. 5.

569 Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting...*, s. 21.

570 Wyrok TS z 1.10.2019 r. w sprawie C-673/17..., pkt 82.

4.2.2.3. Możliwość udzielania zgód przy pomocy ustawień przeglądarki

Projekt rozporządzenia *ePrivacy* dopuszcza, że zgoda może być wyrażona za pomocą ustawień przeglądarki internetowej i będzie miała pierwszeństwo przed ustawieniami oprogramowania. Ustawienie preferencji będzie mogło dotyczyć jednego celu lub większej liczby celów przetwarzania i powinno mieć zastosowanie do wszystkich odwiedzanych stron internetowych⁵⁷¹. Ten sposób wyrażenia zgody budzi wiele wątpliwości, gdyż zakłada, że konsumenci wiedzą, jak zmienić ustawienia dotyczące plików *cookie* w przeglądarkach⁵⁷². W praktyce taka znajomość jest znikoma⁵⁷³. Trzeba również zauważyć, że wyrażenie zgody na instalowanie plików *cookie* przez ustawienia przeglądarki nie spełnia przesłanek zgody wyrażonych w art. 7 RODO⁵⁷⁴, a w szczególności przesłanki jednoznaczności. Jednokrotny wybór dokonany przez konsumenta lub brak zmiany domyślnych ustawień wpływa na wszystkie zgody wyrażone w przyszłości bez wiedzy o okolicznościach konkretnego przetwarzania, co poddaje w wątpliwość prawidłowość wyrażonych w ustawieniach przeglądarek zgód. Tak skonstruowane domyślne ustawienia funkcjonują w przynajmniej kilku najpopularniejszych wyszukiwarkach. Uważam, że przy pierwszej instalacji przeglądarki konsumentom powinno umożliwiać się samodzielny wybór ustawień dotyczących plików *cookie*, co odzwierciedlałoby realną wolę konsumentów i wyeliminowałoby problem braku świadomości zgód udzielanych za pomocą ustawień przeglądarki.

Niestety projekt rozporządzenia nie dotyka też kwestii zapamiętywania ustawień na różnych urządzeniach należących do tego samego użytkownika⁵⁷⁵, co wydaje się ważnym elementem wpływającym na przeciążenie konsumentów koniecznością udzielania zgody. W motywie 20a zachęca się twórców oprogramowania do tworzenia takich funkcjonalności jak np. białe listy, na których konsument będzie mógł umieścić konkretnych dostawców, którym pozwala na instalację plików *cookie*, pomimo braku wyrażenia ogólnej zgody na pliki *cookie* w przeglądarce. Przy założeniu aktywnej roli konsumentów proponowane rozwiązanie może korzystnie wpłynąć na zwiększenie świadomości udzielanych przez konsumentów zgód, a co za tym idzie - częściowe ograniczenie personalizacji. Literalne brzmienie rozporządzenia wskazuje jednak na to, że wprowadzenie takich funkcjonalności jest jedynie zaleceniem. Europejska Rada Ochrony Danych podkreśla, że artykuł 4a powinien być bardziej restrykcyjny i zobowiązywać przeglądarki do projektowania przyjaznego i skutecznego mechanizmu uzyskiwania zgody⁵⁷⁶.

4.2.2.4. Okresowe przypomnienia o udzieleniu zgody

Postulat okresowego informowania konsumentów o prowadzonym wobec nich monitoringu nie jest nowy. W doktrynie rozważano wprowadzenie takiego rozwiązania z uwagi na możliwość nieuświadamiania sobie, jakich zgód udzielono kilka lat wstecz⁵⁷⁷. Choć powyższemu stanowisku nie można odmówić słuszności, to z uwagi na

⁵⁷¹ Motyw 20a projektu rozporządzenia *ePrivacy*.

⁵⁷² J. Byrski, H. Hoser, *Social media oraz technologie umożliwiające śledzenie...*, s. 6-14.

⁵⁷³ Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 158.

⁵⁷⁴ J. Byrski, H. Hoser, *Social media oraz technologie umożliwiające śledzenie...*, s. 6-14.

⁵⁷⁵ M. Czerniawski (w:) M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu...*, s. 335-336.

⁵⁷⁶ Europejska Rada Ochrony Danych, *Oświadczenie 03/2021 w sprawie rozporządzenia o prywatności i łączności elektronicznej*, 2021, s. 3.

⁵⁷⁷ Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 19.

obecne przytłoczenie konsumentów komunikatami rozwiązywanie mogłoby okazać się nieskuteczne. Grupa Robocza Art. 29 zaproponowała również alternatywne rozwiązanie. Na stronach internetowych, na których ma miejsce monitoring, umieszczany mógłby być stosowny symbol przypominający o monitorowaniu i możliwości wycofania zgody⁵⁷⁸.

Projekt rozporządzenia *ePrivacy* wprowadza pierwsze z proponowanych rozwiązań. Konieczne będzie okresowe przypominanie użytkownikom o możliwości wycofania uprzednio udzielonej zgody. Zakłada się, że odstęp pomiędzy przypomnieniami nie może być dłuższy niż 12 miesięcy. Na zasadzie mechanizmu *opt-up* wprowadzono także możliwość zrezygnowania z takich przypomnień⁵⁷⁹. Wprowadzenie okresowych przypomnień jest istotnym krokiem ku zapewnieniu konsumentom transparentności procesu śledzenia. Najważniejszym czynnikiem wpływającym na skuteczność takich powiadomień będzie jednak sposób ich implementacji w praktyce. W mojej opinii konieczne będzie doprecyzowanie tego obowiązku, tak aby nie stał się on kolejnym elementem pogłębiającym problem zbyt dużej liczby, a co za tym idzie - także nieświadomości udzielanych zgód.

4.2.3. Dopuszczalność *cookies walls*

Wiele stron internetowych swój model biznesowy opiera na zbieraniu danych o aktywności konsumentów i wyświetlaniu spersonalizowanych reklam. Oferują one treści bezpłatnie w zamian za akceptację plików *cookie*. W związku z tym popularną praktyką na takich stronach są tzw. *cookie walls*, na podstawie których odmawia się użytkownikom dostępu do stron, jeśli nie zostanie wyrażona zgoda na odczytywanie plików *cookie*. Z badań wynika, że nawet na stronach niewymagających zgody konsumenci często akceptują pliki *cookie* sądząc, że bez tego nie uzyskają do nich dostępu⁵⁸⁰. Konsumenci zaczynają więc oswajać się z takim wymogiem, co należy uznać za niekorzystną zmianę mającą przełożenie na upowszechnienie się procesów personalizacji i profilowania.

Legalność stosowania tego typu praktyki budzi poważne wątpliwości. Z jednej strony, zgodnie z motywem 25 dyrektywy o prywatności i łączności elektronicznej, możliwe jest uzależnienie dostępu do niektórych treści zamieszczonych na stronach internetowych od świadomej akceptacji zastosowania plików *cookie*, jeżeli służy ono prawnie dopuszczalnemu celowi. Z drugiej strony nie jest to, moim zdaniem, równoznaczne z uniemożliwianiem dostępu do całej witryny w postaci *cookie wall*, ponieważ narusza przesłankę dobrowolności zgody⁵⁸¹. Konsumenci mają uzasadnioną podstawę do przeciwstawiania się nieustannemu śledzeniu podczas korzystania z usług cyfrowych, co wynika m.in. z zagwarantowanych im praw podstawowych. W doktrynie pojawia się w związku z tym stanowisko, aby tworzyć dwie wersje portalu. W jednej z nich konsumenci akceptujący *cookies* mieliby szerszy dostęp do treści. W drugiej, niewymagającej zaakceptowania plików *cookie*, strona prezento-

578 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam...*, s. 24.

579 Artykuł 4a ust. 3 projektu rozporządzenia *ePrivacy*.

580 C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent...*, s. 12.

581 S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2018, s. 1190-1199.

wałaby ograniczone treści, ale wciąż byłaby dostępna dla konsumentów⁵⁸². Istnieje również możliwość wprowadzenia odpłatności w pieniądzu dla tych konsumentów, którzy nie godzą się na wykorzystanie *cookies* śledzących⁵⁸³.

Dodatkowo należy wspomnieć o najnowszych wytycznych Europejskiej Rady Ochrony Danych, w których stwierdza się, że aby spełniony został warunek dobrowolnej zgody, dostęp do usług i funkcji nie może być uzależniony od zgody użytkownika na przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym użytkownika⁵⁸⁴. Na przykład, jeśli aplikacja do edycji zdjęć wymaga włączenia GPS i wyrażenia zgody na użycie zebranych w ten sposób danych do celów reklamy behawioralnej, to odmowa dostępu do aplikacji w wyniku niewyrażenia zgody jest niedopuszczalna⁵⁸⁵.

Projekt rozporządzenie *ePrivacy* w dalszym ciągu dopuszcza uzależnianie dostępu do treści stron internetowych od wyrażenia zgody konsumenta na stosowanie plików *cookie*, gdy nie są one niezbędne do zawarcia umowy, a np. wykorzystywane w celu personalizacji reklam. Dobrowolność zgody będzie jednak podlegała kryterium istnienia alternatyw⁵⁸⁶. Konsument będzie musiał mieć możliwość porównania, na podstawie jasnych, precyzyjnych i przyjaznych informacji, oferty wymagającej wyrażenia zgody na pliki *cookie* z równoważną ofertą tego samego dostawcy, która takiej zgody nie wymaga⁵⁸⁷. Możliwe wydaje się też oferowanie zachęt, pod warunkiem niedyskryminowania osób, które zdecydują się na nieudzielenie zgody. W niektórych przypadkach uzależnienie dostępu do treści strony internetowej od zgody na stosowanie plików *cookie* będzie można nadal uznać za pozbawiające użytkownika rzeczywistego wyboru, np. w sytuacji posiadania przez usługodawcę pozycji dominującej⁵⁸⁸. Jest to implementacja stanowiska wyrażanego przez Europejską Radę Ochrony Danych w opinii z 2016 r.⁵⁸⁹. Pozytywnie trzeba ocenić fakt, że porównanie będzie następować z inną ofertą tego samego dostawcy, a nie innego dostawcy oferującego równoważne usługi na rynku, gdyż w innym przypadku swoboda wyboru zależałaby od działań innych uczestników rynku⁵⁹⁰. Niemniej jednak powstaje wątpliwość, w jaki sposób w praktyce owe porównanie usług miałyby wyglądać. Z punktu widzenia prawa konsumenckiego, a w szczególności klauzul abuzywnych, problematyczna może okazać się również kwestia uregulowania przez poszczególnych dostawców konsekwencji wycofania udzielonej w taki sposób zgody⁵⁹¹.

Proponowana regulacja jest zachowawcza i nie rozwiązuje w sposób jednoznaczny problemu stosowania *cookies* *walls*, ale z pewnością racjonalizuje jej użycie. W kontekście tej propozycji przepisu Europejska Rada Ochrony Danych w swoim oświadczeniu sygnalizuje, że potrzebne jest zbudowanie jasnych wytycznych dotyczących

582 Pozyskano z: <https://prawo.gazetaprawna.pl/artykuly/1498889,kary-za-ciasteczka-google-amazon.html>. Dostęp: 11.06.2021 r.

583 O. Ben-Shahar, *Data Pollution...*, s. 142.

584 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody...*, s. 12.

585 Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody...*, s. 8.

586 M. Gumularz (w:) M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu...*, s. 138-143.

587 Motyw 20aaaa projektu rozporządzenia *ePrivacy*.

588 Motyw 20aaaa projektu rozporządzenia *ePrivacy*.

589 Europejski Inspektor Ochrony Danych, *Opinion 5/2016 Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)*, 22.07.2016 r.

590 M. Gumularz (w:) M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu...*, s. 138-143.

591 M. Gumularz (w:) M. Gumularz, P. Kozik, *Ochrona danych osobowych w marketingu...*, s. 138-143.

ochrony przed nieuczciwymi praktykami *take it or leave it*⁵⁹², czyli stawianiem ultimatum w postaci zaakceptowania jednostronnie ustalonych warunków albo rezygnacji z oferowanych usług⁵⁹³.

5. Nowelizacja dyrektywy 2011/83/UE za sprawą Nowego Ładu dla konsumentów

Dyrektywa Omnibus wprowadziła do dyrektywy 2011/83/UE nowy obowiązek informacyjny dotyczący zastosowania wobec konsumenta personalizacji cenowej⁵⁹⁴. Obowiązek ten dotyczy umów zawieranych na odległość. Przed zawarciem umowy konsument będzie informowany o tym, czy ustalona wobec niego cena towaru lub usługi została indywidualnie dostosowana w oparciu o zautomatyzowane podejmowanie decyzji. Państwa członkowskie mają czas na implementację tego uregulowania do krajowych porządków prawnych do 28 listopada 2021 r.

Zakresem tego obowiązku nie jest objęte ustalanie cen w sposób dynamiczny, a więc zależny od popytu i podaży. Mimo że przepis literalnie stanowi jedynie o zautomatyzowanym podejmowaniu decyzji, można uznać, że obejmuje on również profilowanie szczególne z art. 22 RODO, co znajduje potwierdzenie w motywie 45 dyrektywy 2019/2161.

Wprowadzone rozwiązanie oceniam pozytywnie. Według motywu 45 dyrektywy 2019/2161 taka informacja pomoże konsumentom uwzględnić potencjalne ryzyko przy podejmowaniu decyzji o zakupie. Niemniej jednak trzeba zwrócić uwagę na stosunkowo wąski zakres wprowadzonego obowiązku. Konsument dowie się jedynie o tym, że wyświetlona mu cena została indywidualnie dostosowana. Znacznie ważniejsza jest informacja o kryteriach, które wpłynęły na zindywidualizowanie ceny, co miało zostać zawarte w obowiązku informacyjnym w kształcie proponowanym przez Parlament Europejski. Informacja na ten temat zapewniana jest przez szczególnie obowiązek informacyjny określony w art. 13 ust. 2 lit. f i art. 14 ust. 2 lit. g RODO jedynie częściowo. Warto przypomnieć, że w przypadku profilowania niewypełniającego przesłanek z art. 22 RODO udzielanie tych informacji jest uważane jedynie za dobrą praktykę. Jeśli dostosowanie cen produktu nie zostanie uznane przez administratora za decyzję mającą wpływ na sytuację prawną konsumenta lub wpływającą na niego w podobnie istotny sposób, konsument nie uzyska informacji o kryteriach profilowania. Kluczowe znaczenie będzie miał sposób wdrożenia nowego obowiązku przez przedsiębiorców, a w szczególności interpretacji przesłanki jasnego i zrozumiałego informowania⁵⁹⁵.

6. Wnioski częściowe

Z omówionych w tym rozdziale dokumentów i proponowanych aktów prawnych wynika wiele obiecujących rozwiązań dotyczących bezpośrednio lub pośrednio procesu

592 Europejska Rada Ochrony Danych, *Oświadczenie 03/2021 w sprawie rozporządzenia o prywatności i łączności elektronicznej*, 2021, s. 3.

593 Forbrukerrådet, *Deceived by design. How tech companies use dark patterns...*, s. 25.

594 Art. 6 ust. 1 lit. ea dyrektywy 2011/83/UE.

595 I. Małobęcka-Szwast, *Stosowanie spersonalizowanych cen w świetle nowelizacji dyrektywy 2011/83/UE o prawach konsumentów i rozporządzenia 2016/679 (RODO)*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2020, nr 7(9), s. 15.

personalizacji. W szczególności należy podkreślić to, jak wiele projektów uwzględnia potrzebę zwiększenia przejrzystości procesów opartych na sztucznej inteligencji. Konsumenci powinni mieć możliwość poznania szczegółowych kryteriów personalizacji, by zrozumieć ten proces i podjąć świadomą decyzję co do ich dalszego wykorzystywania. Dzięki przejrzystości mogą zwiększać swoje zaufanie do takich systemów. Z uwagi na dość wąski zakres rozporządzenia w sprawie sztucznej inteligencji największe znaczenie w tym względzie będą miały Kodeks Usług Cyfrowych oraz rozporządzenie *ePrivacy*. Rozporządzenie *ePrivacy* może pozytywnie wpłynąć na możliwość przeciwstawienia się nadmiernemu śledzeniu w przestrzeni internetowej. Uważam, że będzie ono stanowić immamentną część regulacji dotyczących personalizacji. Na kwestię przejrzystości wpłynie także nowy obowiązek informacyjny określony w dyrektywie 2011/83/UE.

W tym miejscu należy również wspomnieć, że Unia Europejska podejmuje działania w celu utworzenia unijnej tożsamości cyfrowej, zapewniającej m.in. kontrolę nad udostępnianymi danymi osobowymi i weryfikację wieku osób niepełnoletnich. Proponowany system nie powinien być wykorzystywany w celach komercyjnych ani do śledzenia użytkowników w witrynach internetowych⁵⁹⁶. Komisja Europejska przedstawiła niedawno projekt rozporządzenia w sprawie tożsamości cyfrowej⁵⁹⁷, który ustanawia ramy prawne dla takiego narzędzia.

Za sprawą projektowanych aktów prawnych personalizacja z pewnością zostanie częściowo zracjonalizowana, a przepisy pozytywnie wpłyną na równowagę sił między przedsiębiorcami a konsumentami. Większość z omówionych w tym rozdziale aktów prawnych jest na bardzo wczesnym etapie legislacyjnym, a zatem mają szansę wejść w życie dopiero za kilka lat. Pilna potrzeba odpowiedniej reakcji regulacyjnej w sferze personalizacji jest jednak widoczna już dziś.

⁵⁹⁶ Rezolucja Parlamentu Europejskiego z dnia 20.10.2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych, 2020/2022(INI), s. 10.

⁵⁹⁷ Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final).

Wnioski końcowe

Personalizacja oparta na sztucznej inteligencji jest zjawiskiem korzystnym dla konsumentów posiadających znaczne zdolności technologiczne oraz potrafiących efektywnie zadbać o ochronę swojej prywatności. Z kolei w przypadku mniej świadomych i zaangażowanych konsumentów personalizacja stała się nowym narzędziem do wykorzystywania przewagi informacyjnej⁵⁹⁸. Podmiotami, które w największym stopniu korzystają z tej nieustannej chęci do jak najszerszego personalizowania przekazu, są pośrednicy tacy jak Google i Facebook, którzy zbierają dane, oferują przestrzeń reklamową, szeroką bazę profili użytkowników oraz algorytmy targetujące. Nie sposób ukryć, że w ciągu najbliższych lat wykorzystanie danych konsumentów do personalizacji jedynie zyska na znaczeniu z uwagi na ciągły rozwój technologii i narzędzi służących pozyskiwaniu i analizie danych. Przewiduje się, że personalizacja wkroczy również do innych, bardziej tradycyjnych kanałów, takich jak telewizja⁵⁹⁹.

Przedsiębiorcy w coraz szerszym zakresie będą wykorzystywać personalizację warunków umownych, by unikać ryzykownych transakcji i maksymalizować zyski przez dopasowywanie cen do możliwości finansowych konsumentów. Dalszy rozwój i popularność spersonalizowanych reklam są nawet bardziej oczywiste, gdyż już teraz jest to podstawowe narzędzie marketingowe. Choć niektóre badania pokazują, że reklama kontekstowa jest tylko nieznacznie mniej skuteczna od reklamy behawioralnej⁶⁰⁰, to uważam, że powrót do tego modelu reklamowego nie jest już możliwy. Tym samym należy zaadaptować prawo do postępującej personalizacji przestrzeni internetowej i skupić się na minimalizowaniu ryzyka dyskryminacji, naruszenia prywatności i manipulacji, które ze sobą niesie dla konsumentów personalizacja.

Głównym celem niniejszej pracy była próba analizy, czy dostępne obecnie instrumenty prawne zapewniają wysoki poziom ochrony konsumentów przed personalizacją opartą na sztucznej inteligencji. W moim przekonaniu odpowiedź na to pytanie może być jedynie częściowo pozytywna.

W pierwszej kolejności trzeba zaznaczyć, że wszelkie metody samoregulacji przez branżę reklamową, jak dotąd, okazywały się nieskuteczne. Przedsiębiorcy nie mają wystarczających motywacji do szukania alternatyw, które byłyby neutralne dla prywatności konsumentów. Presja ze strony konsumentów nie jest bowiem wystarczająco silna⁶⁰¹, a wartość pozyskiwanych od nich danych - zbyt wysoka. Stąd konieczna wydaje się aktywna rola Unii Europejskiej we właściwym uregulowaniu praw konsumentów związanych z procesem personalizacji reklam i warunków umownych. Najistotniejsze akty prawne, które mogą być obecnie wykorzystywane do ochrony przed nadmierną personalizacją, to: ogólne rozporządzenie o ochronie danych, dyrektywa 2002/58/WE o prywatności i łączności elektronicznej oraz dyrektywa 2005/29/WE o nieuczciwych praktykach handlowych. W niewielkim zakresie na poziom ochrony konsumentów przed personalizacją wpłynie także znowelizowana dyrektywa 2011/83/UE. Analiza powyższych aktów prawnych wykazała, że personalizacja cen

598 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 249.

599 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 143.

600 K. Iwańska, *To track or not to track?...*, s. 16-17.

601 O. Ben-Shahar, *Data Pollution...*, s. 120.

jest obecnie lepiej uregulowana pod względem prawnym niż wszechobecna praktyka personalizacji reklam.

Ogólne rozporządzenie o ochronie danych osobowych w sposób kompleksowy normuje niezwykle ważny z perspektywy personalizacji proces profilowania. Akt ten przewiduje szerokie gwarancje dla podmiotów danych będących zarazem konsumentami, które pełnią funkcję prewencyjną względem personalizacji. Proces profilowania jest jednak na gruncie RODO ujęty w sposób dualistyczny i przyjmuje dwie odrębne formy, które różnią się między sobą zakresem przyznanej konsumentom ochrony. Ujednolicenie zakresu ochrony konsumentów w przypadku praktyki profilowania mogłoby wpłynąć pozytywnie na respektowanie praw konsumentów i ograniczyć kreatywne podejście do przepisów, które obecnie jest szeroko stosowane przez przedsiębiorców. Rozwiązanie problemu nadmiernej personalizacji o charakterze manipulacyjnym można osiągnąć poprzez wprowadzenie zakazu tworzenia profili na podstawie danych pozyskiwanych z różnych źródeł, a co za tym idzie - ograniczenie roli brokerów danych⁶⁰². To właśnie łączenie profili daje bowiem możliwość niezwykle głębokiej personalizacji konsumentów, niejednokrotnie w oparciu o ich słabości.

Ochrona prywatności w coraz większym stopniu zyskuje charakter kompromisowy i pragmatyczny. Konsumenti przyzwyczaili się do tego, że ich dane osobowe stanowią formę zapłaty i takie ustępstwa nie budzą w nich wewnętrznego oporu. Choć zgadzam się ze stwierdzeniem, że prawo do ochrony danych osobowych nie jest prawem absolutnym i powinno być analizowane w kontekście funkcji, jaką pełni w społeczeństwie⁶⁰³, to jednak charakter transakcji mającej za przedmiot prywatność konsumenta pozostawia obecnie wiele wątpliwości. Konsument, w przeciwieństwie do przedsiębiorcy, w większości przypadków nie jest świadom konsekwencji, które pociąga za sobą udostępnienie danych. Wątpliwe jest też to, czy korzyść, jaką uzyskuje w zamian za udostępnienie swoich danych osobowych administratorowi oraz wielu jego „zaufanym partnerom”, jest dostateczna.

Łączy się to również z przepisami dyrektywy o prywatności i łączności elektronicznej, które normują kwestie wyrażania zgody na pliki *cookie*. Dyrektywa ta być może zostanie zastąpiona w niedługim czasie przez rozporządzenie *ePrivacy*, ale nie należy oczekiwać, że będzie to akt przełomowy z punktu widzenia dopuszczalności personalizacji. Ambitne plany Unii Europejskiej zostały bowiem znacznie ograniczone w toku prac nad projektem rozporządzenia. Niemniej jednak uzależnienie dopuszczalności *cookie walls* od istnienia alternatywnych rozwiązań tego samego dostawcy należy ocenić pozytywnie. Duże nadzieje pokładam także w przedstawionym niedawno rozporządzeniu w sprawie tożsamości cyfrowej, które pomoże konsumentom efektywnie zarządzać dostępem do swoich danych⁶⁰⁴.

Rozporządzenie 2016/679 oraz dyrektywę 2002/58/WE o prywatności i łączności elektronicznej łączy jeden wspólny problem w egzekwowaniu przejrzystości informacji przekazywanych konsumentom. Oba te akty skumulowały w sobie wiele obowiązków informacyjnych, których skuteczność wydaje się obecnie wątpliwa. Konsumenti tylko teoretycznie są informowani o zbieraniu ich danych i wykorzystywaniu ich w celach

602 Pozyskano z: <https://panoptykon.org/sledzic-czy-nie-sledzic>. Dostęp: 11.06.2021 r.

603 Wyrok TS z dnia 9.11.2010 r. w sprawach połączonych C-92/09 i 93/09 *Volker und Markus Schecke GbR i Hartmut Eifert v. Land Hessen*, ECLI:EU:C:2010:662, pkt 48.

604 Pozyskano z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en. Dostęp: 11.06.2021 r.

personalizacji, a równie często są pozbawieni przez administratorów efektywnego wyboru i możliwości odrzucenia plików *cookie*⁶⁰⁵. Z niepokojem obserwuję również kolejne obowiązki informacyjne względem konsumentów, tworzone m.in. w rozporządzeniu *ePrivacy* i Kodeksie Usług Cyfrowych. Już dawno przekroczona została granica zdolności percepcyjnych konsumentów w przestrzeni internetowej. Tworzenie nowych obowiązków informacyjnych bez jednoczesnego egzekwowania ich jakości nie będzie skuteczną formą ochrony konsumentów. Niestety odpowiedzialne za egzekwowanie obowiązków informacyjnych organy stosunkowo rzadko podejmują prewencyjną kontrolę nad sposobem realizacji tych obowiązków, a ewentualne nieprawidłowości incydentalnie stają się przedmiotem skarg samych konsumentów. Rozwiązanie tego problemu widzę w częściowym ujednoliceniu wzorów informowania o wykorzystywaniu plików *cookie* i przetwarzaniu danych osobowych na stronach internetowych oraz wyraźnym określeniu, jakie praktyki *dark patterns* są uznawane za niedopuszczalne w świetle prawa. Dodatkowo w parze z jasną informacją na temat personalizacji przekazywaną przez przedsiębiorców powinna iść szeroko zakrojona edukacja konsumentów na temat: narzędzi wykorzystywanych do śledzenia aktywności internetowej, sposobu działania personalizacji oraz związanych z nią potencjalnych zagrożeń.

O ile powyżej przywoływane akty przede wszystkim stanowią prewencyjną ochronę konsumentów przed praktyką personalizacji, o tyle dyrektywa 2005/29/WE o nieuczciwych praktykach handlowych zapewnia konsumentom w głównej mierze ochronę *ex post*. Dyrektywa, ze względu na sposób przyjętej harmonizacji zupełnej, jest w mojej opinii zbyt nieelastyczna do sprostania wyzwaniu, jakim jest nadmierna personalizacja oparta na sztucznej inteligencji. Brak jest bowiem wyraźnych wytycznych, które pozwoliłyby na odpowiednią kwalifikację personalizacji jako nieuczciwej praktyki handlowej. Interpretacja rozszerzająca przepisów dyrektywy przez organy ochrony konsumentów oraz sądy państw członkowskich jest natomiast w dużym stopniu ograniczona. Choć obecne wytyczne dotyczące dyrektywy z 2016 r. dopuszczają kwalifikację personalizacji jako nieuczciwej praktyki handlowej, to w praktyce nawet klauzula generalna okazuje się problematyczna pod względem dowodowym. Poważną trudnością jest próba określenia modelu przeciętnego i wrażliwego konsumenta w kontekście personalizacji. Wypracowany w doktrynie i orzecznictwie model, który używany jest do oceny nieuczciwości danej praktyki, wydaje się bowiem nieodpowiedni dla konsumentów działających w przestrzeni internetowej i poddawanych personalizacji. W stosunku do tej grupy konsumentów wymagania powinny być odpowiednio złagodzone. Charakterystyka konsumenta wrażliwego w obliczu personalizacji również powinna ulec stosownej korekcie.

Pozytywnym aspektem jest fakt, że pojawiają się wyroki, które interpretują przepisy dyrektywy 2005/29/WE dość szeroko, uwzględniając przy tym ewentualne naruszenia prawa ochrony danych osobowych⁶⁰⁶. Prawo ochrony danych osobowych oraz prawo konsumenckie coraz częściej pełnią wobec siebie funkcję komplementarną i uzupełniającą, co dodatkowo wzmacnia pozycję konsumenta i realizację jego

605 Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market...*, s. 147.

606 Wyrok Regionalnego Sądu Administracyjnego Lazio (Rzym) z 10 stycznia 2020 r. w sprawie Facebook, sygn. 261/20.

praw⁶⁰⁷. Wiele kwestii związanych z ochroną danych staje się jednocześnie sprawami z zakresu prawa konsumenckiego⁶⁰⁸. Niemniej jednak należy podkreślić konieczność stworzenia na poziomie unijnym odpowiednich wytycznych, które zapobiegałyby w takich sytuacjach dwutorowości postępowania z zakresu ochrony danych osobowych oraz prawa konsumenckiego, a także wprowadzenie mechanizmów współpracy między organami⁶⁰⁹.

Zatem, choć istnieją obecnie pewne narzędzia prawne, które są nakierowane na ochronę konsumentów przed nadmierną personalizacją, to są one mało precyzyjne, niejednolite, a niekiedy również nieskutecznie egzekwowane. O tym, czy sytuacja związana z nadużywaniem personalizacji w kontaktach z konsumentami ulegnie poprawie, mogą zdecydować tworzone obecnie na szczeblu unijnym akty prawne, ale przede wszystkim edukacja konsumentów o dostępnych możliwościach przeciwstawiania się nieuczciwej personalizacji.

607 I. Małobęcka-Szwast, *Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów*, (w:) G. Sibiga (red.), *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych*, dodatek MoP 2020, nr 23, s. 7.

608 N. Helberger, F. Zuiderveen Borgesius, A. Reyna, *The perfect match?...*, s. 1428.

609 I. Małobęcka-Szwast, *Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów...*, s. 12-13.

Bibliografia

1. Abgarowicz Ł. (w:) *Perspektywy rozwojowe reklamy online w Polsce*, IAB Polska, 2018.
2. Andreou A., Venkatadri G., Goga O., Gummadi K.P., Loiseau P., Mislove A., *Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations*, Network and Distributed Systems Security (NDSS) Symposium 2018.
3. Bar-Gill O., *Algorithmic price discrimination. When demand is a function of both preferences and (mis)perceptions*, University of Chicago Law Review 2018, nr 86.
4. Barbu O., *Advertising, Microtargeting and Social Media*, Procedia - Social and Behavioral Sciences 2014, nr 163.
5. Bashyakarla V., Hankey S., Macintyre A., Rennó R., Wright G., *Personal Data: Political Persuasion. Inside the Influence Industry. How it works*, Tactical Tech's Data and Politics team 2019.
6. Ben-Shahar O., *Data Pollution*, Journal of Legal Analysis 2019, nr 11.
7. Biéri M., Vallet F., Corbara I., Faget P., Guley B., Hary E., Hirtz J. (w:) Pailhès B. (red.), *On the record. Exploring the ethical, technical and legal issues of voice assistants*, Commission Nationale de l'informatique et des Libertés 2020.
8. Brożyna M., *Konsumenckie prawo do odwołania umowy*, Warszawa 2021.
9. Busch C., *Implementing Personalized Law: Personalized Disclosures in Consumer Law and Privacy Law*, University of Chicago Law Review 2019, nr 86.
10. Byrski J., Sytniewski L. (w:) Traple E. (red.), *Ochrona gry komputerowej. Aktualne wyzwania prawne*, Warszawa 2015.
11. Byrski J., Hoser H., *Social media oraz technologie umożliwiające śledzenie użytkowników Internetu a współadministrowanie danymi osobowymi* (w:) Konarski X. (red.), *Prawo nowych technologii dane osobowe i cyberbezpieczeństwo, Internet i media, handel elektroniczny, prawo IT, technologie*, dodatek MoP 2019, nr 21.
12. Castelluccia C., Narayanan A., *Privacy considerations of online behavioural tracking*, European Network and Information Security Agency 2012.
13. Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, Europejski Przegląd Sądowy 2017, nr 5 (141).
14. Chałubińska-Jentkiewicz K., Nowikowska M., *Bezpieczeństwo, tożsamość, prywatność - aspekty prawne*, Warszawa 2020.
15. Czech T., *Prawa konsumenta. Komentarz, wyd. II*, Warszawa 2020.
16. Czerniawski M., *Komentarz do art. 21, art. 22* (w:) Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

17. Czerniawski M. (w:) Gumularz M., Kozik P., *Ochrona danych osobowych w marketingu i sprzedaży*, Warszawa 2019.
18. Dāvida Z., *Consumer Rights and Personalised Advertising: Risk of Exploiting Consumer Vulnerabilities*, Socrates 2020, nr 1 (16).
19. De Franceschi A., Lehmann M., *Data as Tradeable Commodity and New Measures for their Protection*, The Italian Law Journal 2015, nr 1.
20. Devins C., Felin T., Kauffman S., Koppl R., *The Law and Big Data*, 27 Cornell J.L. & Public Policy 357 (2017).
21. Doshi-Velez F., Kortz M., *Accountability of AI Under the Law: The Role of Explanation*, Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper 2017.
22. Duivenvoorde B., *The Protection of Vulnerable Consumers under the Unfair Commercial Practices Directive*, Journal of European Consumer and Market Law 2013, nr 2.
23. Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.
24. Fischer B., Górski M., Nerka A., Sakowska-Baryła M., Wygoda K., art. 4 (w:) Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.
25. Flis K., *Personalizacja, rekomendacja, prosumpcja - trzy wymiary dialogu organizacji i konsumenta*, Handel Wewnętrzny 2015, nr 1 (354).
26. Gumularz M., Kozik P., *Ochrona danych osobowych w marketingu i sprzedaży*, Warszawa 2019.
27. Grygierek R., *Rynek e-commerce* (w:) Kolenda P. (red.), *Raport Strategiczny Internet 2019/2020*, IAB Polska 2020.
28. Grzybczyk K., *Reklama behawioralna* (w:) Ślęzak P. (red.), *Prawo mediów*, Warszawa 2020.
29. Helberger N., *Profiling and targeting consumers in the Internet of Things - A new challenge for consumer law*, SSRN Electronic Journal 2016.
30. Helberger N., Zuiderveen Borgesius F., Reyna A., *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, Common Market Law Review 2017, nr 54.
31. Helberger N., Lynskey O., Micklitz W.H., Rott P., Sax M., Strycharz J., *EU consumer protection 2.0. Structural asymmetries in digital consumer markets*, 2021.
32. Hosanagar K., Fleder D., Lee D., Buja A., *Will the Global Village Fracture into Tribes? Recommender Systems and their Effects on Consumer Fragmentation*, Management Science 2014, nr 60 (4).
33. Humerick M., *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, Santa Clara High Technology L.J. 2018, nr 34.

34. Iszkowski W., *O „nieciągłościach” ochrony danych osobowych* (w:) Mednis A. (red.), *Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016.
35. Iwańska K., *To track or not to track? Towards privacy-friendly and sustainable online advertising*, Panoptykon Foundation, 2020.
36. Jabłonowska A., Kłafkowska-Waśniowska K., Kunkiel-Kryńska A., Mańko R., Namysłowska M., Tereszkiewicz P., *Cnoty a prawo konsumenckie. Artykuł sprawozdawczy z XV konferencji Międzynarodowego Stowarzyszenia Prawa Konsumenckiego (International Association of Consumer Law - IACL)*, Państwo i Prawo 2016, nr 4.
37. Jabłonowska A., Kuziemski M., Nowak A., Micklitz H., Pałka P., Sartor G., *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 2018, nr 11.
38. Kaplan A., Haenlein M., *Siri, Siri, in my hand, Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, *Business Horizons* 2019, nr 62.
39. Kibil M. (w:) Gawroński M., *RODO Przewodnik ze wzorami*, Warszawa 2018.
40. Konarski X., *Podstawy prawne korzystania z „ciasteczek” internetowych (cookies) jako przykład wzajemnej relacji przepisów RODO oraz przepisów o ochronie prywatności w sektorze łączności elektronicznej* (w:) Sibiga G. (red.), *Przepisy prawa uzupełniające RODO Aktualne problemy prawnej ochrony danych osobowych 2018*, dodatek MoP 2018, nr 22.
41. Krasuski A., *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021.
42. Księżak P., *Skutki prawne naruszenia obowiązków informacyjnych przedsiębiorcy zamierzającego zawrzeć umowę z konsumentem* (w:) Skoczny T., Karczeńska D., Namysłowska M., *Ustawa o prawach konsumenta*, Warszawa 2015.
43. Kulesza M., *Odpłatny charakter „darmowych” usług Facebooka. Teza z wyroku Regionalnego Sądu Administracyjnego Lazio (Rzym) z 10 stycznia 2020 r. w sprawie Facebook, sygn. 261/20, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2020*, nr 4(9).
44. Kusak M., Wiliński P., *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020.
45. Laux J., Wachter S., Mittelstadt B., *Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice*, *Common Market Law Review* 2021, nr 58.
46. Lis-Zarrias K., *Ochrona konsumenta przed agresywnymi praktykami rynkowymi w świetle pytań prejudycjalnych SN w sprawie C-628/17 Orange Polska S.A.*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2018, nr 6(7).

47. Litwiński P., Barta P., Kawecki M., *Komentarz do art. 4, art. 22 (w:) Litwiński P. (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017.
48. Lubasz D., Chomiczewski W., Czerniawski M., Drobek P., Góral U., Kuba M., Makowski P., Witkowska-Nowakowska K., *Komentarz do art. 4 (w:) Bielak-Jomaa E., Lubasz D. (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.
49. Lubasz D., *Big brother is watching you. Profilowanie i zautomatyzowane podejmowanie decyzji w kontekście zasad legalności i przejrzystości (w:) Wojciechowski R., Wolska H. (red.), Rok RODO*, Warszawa 2019.
50. Luzak J., *Tailor-made Consumer Protection: Personalisation's Impact on the Granularity of Consumer Information (w:) Compagnucci M. C., Haapio H., Hagan M., Doherty M. (red.), Legal Design: Integrating Business, Design and Legal Thinking with Technology*, Edward Elgar Publishing Ltd. 2021.
51. Lupiáñez-Villanueva F., Gaskell G., Tornese P., Vila J., Gómez Y., Allen A., Veltri G., Codagnone C., *Behavioural study on the transparency of online platforms*, European Commission 2018.
52. Łazarewicz S., *Konsument - pojęcie i jego europejski model (w:) Królikowska-Olczak M., Pachuca-Smulska B. (red.), Ochrona konsumenta w prawie polskim i Unii Europejskiej*, Warszawa 2013.
53. Macierzyńska-Franaszczyk M., *Konsument, Internet i informacja (w:) Fras M., Jagielska M., Podgórski K., Sługocka-Krup E. (red.), Prawa konsumenta w teorii i praktyce*, Warszawa 2018.
54. Malinowski B., *Jak Facebook zamyka nas w bańce informacyjnej. Algorytm filtrujący newsfeed a zjawisko filter bubble*, Zarządzanie mediami 2016, nr 1.
55. Małobęcka-Szwast I., *Stosowanie spersonalizowanych cen w świetle nowelizacji dyrektywy 2011/83/UE o prawach konsumentów i rozporządzenia 2016/679 (RODO)*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2020, nr 7(9).
56. Małobęcka-Szwast I., *Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów (w:) Sibiga G. (red.), Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych*, dodatek MoP 2020, nr 23.
57. Mednis A., *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Warszawa 2019.
58. Milczarek E., *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w Internecie*, Warszawa 2020.
59. Modrzejewska M., *Umowy w sferze marketingu i reklamy (w:) Stec M. (red.), Prawo umów handlowych. System prawa handlowego. Tom 5b*, Warszawa 2020.

60. Namysłowska M., *Dziesięć lat dyrektywy 2005/29/WE o nieuczciwych praktykach handlowych*, Europejski Przegląd Sądowy 2016, nr 3.
61. Namysłowska M., Jabłonowska A., *Prawo konsumenckie wobec personalizacji - nowe wyzwanie dla prawa konsumenckiego* (w:) Lai L., Świerczyński M. (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.
62. Niklas J., *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji*, Polskie Towarzystwo Prawa Antydyskryminacyjnego, 2015.
63. Nisevic M., *A study on the personal data processing and the UCPD focused on Italy, Germany and the UK*, Maastricht Journal of European and Comparative Law 2021, nr 28(1).
64. Nowak A., Węłowska M., Gapsa M., *Profilowanie na podstawie danych osobowych konsumentów przetwarzanych przez pojazd autonomiczny*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2020, nr 7(9).
65. Ożegalska-Trybalska J., *Internetowa reklama kontekstowa* (w:) Namysłowska M. (red.), *Reklama. Aspekty prawne*, Warszawa 2012.
66. Pachuca-Smulska B., *Prawo do informacji i edukacji podstawą ochrony interesów konsumenta* (w:) Królikowska-Olczak M., Pachuca-Smulska B. (red.), *Ochrona konsumenta w prawie polskim i Unii Europejskiej*, Warszawa 2013.
67. Pariser E., *The Filter Bubble: What The Internet Is Hiding From You*, Penguin Press 2011.
68. Pedreschi D., Miliou I., *Artificial Intelligence (AI): new developments and innovations applied to e-commerce. Challenges to the functioning of the Internal Market*, Departament Tematyczny ds. Polityki Gospodarczej, Naukowej i Jakości Życia, 2020.
69. Piątek S., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2018.
70. Południak-Gierz K., *Personalization of Information Duties Challenges for Big Data Approach*, European Review of Private Law 2018, nr 3.
71. Południak-Gierz K., *Wady oświadczenia woli w umowach zawieranych na internetowym rynku konsumenckim*, Warszawa 2020.
72. Porat A., Strahilevitz J.L., *Personalizing default rules and disclosure with big data*, Michigan Law Review 2014, nr 112.
73. Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.
74. Rutkowska-Tomaszewska E., *Nieuczciwe praktyki na rynku bankowych usług konsumenckich*, Warszawa 2011.
75. Sadowska E., Pogorzelska M., Balewski K., *Display* (w:) Kolenda P. (red.), *Raport Strategiczny Internet 2019/2020*, IAB Polska 2020.
76. Sahni S.N., Wheeler C.S., Chintagunta K.P., *Personalization in Email Marketing: The Role of Non-Informative Advertising Content*, Marketing Science 2016, nr 37 (2).

77. Sakowska-Baryła M., *Komentarz do art. 22 (w:) Sakowska-Baryła M. (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.
78. Sartor G., *New aspects and challenges in consumer protection. Digital services and artificial intelligence*, Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2020.
79. Sartor G., *Artificial Intelligence: Challenges for EU Citizens and Consumers*, Policy Department for Economic, Scientific and Quality of Life Policies 2019.
80. Sieradzka M., *Komentarz do ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz*, Warszawa 2008.
81. Sieradzka M., *Wzorzec przeciętnego konsumenta jako punkt odniesienia przy dokonywaniu oceny nieuczciwości praktyki rynkowej. Glosa do wyroku SN z dnia 4 marca 2014 r. III SK 34/13*, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 6(3).
82. Stefanicki R., *Koncepcja zupełnej harmonizacji prawa ochrony konsumenta (na przykładzie dyrektywy o nieuczciwych praktykach handlowych)*, Państwo i Prawo 2011, nr 6.
83. Steppe R., *Online price discrimination and personal data: A General Data Protection Regulation perspectives*, Computer Law & Security Review 2017, nr 33.
84. Strzelecki M., *Klauzula generalna nieuczciwej praktyki rynkowej*, Przegląd Prawa Handlowego 2008, nr 11.
85. Szymielewicz K., Adamska W., *Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?* 2017.
86. Szymielewicz K., Iwańska K., *Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem*, 2019.
87. Utz C., Degeling M., Fahl S., Schaub F., Holz T., *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security 2019.
88. Viķe-Freiberga V., Däubler-Gmelin H., Hammersley B., Póiares Pessoa Maduro L.M., *A free and pluralistic media to sustain European democracy*, High Level Group on Media Freedom and Pluralism 2013.
89. Villarronga E.F., Kieseberg P., Li.T., *Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten*, Computer Law & Security Review: The International Journal of Technology Law and Practice 2017.
90. Wang W., Yang L., Chen Y., Zhang Q., *A privacy-aware framework for targeted advertising*, Computer Networks 2015, nr 79.
91. Wiewiórowska-Domagalska A., Kunkiel-Kryńska A. (w:) Osajda K. (red.) *Prawo konsumenckie. Komentarz, Tom VII*, Warszawa 2019.

92. Witkowska-Nowakowska K., *Komentarz do art. 35 (w:) Bielak-Jomaa E., Lubasz D. (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.
93. Wojtaszek-Mik E., *Informacja konsumencka w świetle orzecznictwa Europejskiego Trybunału Sprawiedliwości (w:) Ślęzak K. (red.), Studia i analizy Sądu Najwyższego. Tom VII*, Warszawa 2014.
94. Wójcik P., *Psychometria konsumentów*, Lublin 2017.
95. Xu Z., Dukes A., *Personalization, Customer Data Aggregation, and The Role of List Price*, 2020.
96. Zhe Jin G., *Artificial intelligence and consumer privacy*, National Bureau of Economic Research Working Paper Series 2018.
97. Zieliński M.A., Czerniak A., Dąbek S., Żylińska J. (red.), *Iloraz sztucznej inteligencji. Potencjał AI w polskiej gospodarce*, Warszawa 2018.
98. Zuiderveen Borgesius F.J., *Discrimination, artificial intelligence, and algorithmic decision-making*, The Directorate General of Democracy, Rada Europy, Strasburg 2018.
99. Zuiderveen Borgesius F.J., Trilling D., Möller J., Bodó B., De Vreese C., Helberger N., *Should we worry about filter bubbles?* Internet Policy Review 2016, nr 5(1).

1. Consultative Committee of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Rada Europy, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 2017.
2. Dokument Roboczy Służb Komisji, *Wytyczne dotyczące wykonania/stosowania dyrektywy 2005/29 w sprawie nieuczciwych praktyk handlowych*. SWD/2016/0163 final, 2016.
3. Europejska Rada Ochrony Danych, *Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą*, 2019.
4. Europejska Rada Ochrony Danych, *Oświadczenie 03/2021 w sprawie rozporządzenia o prywatności i łączności elektronicznej*, 2021.
5. Europejska Rada Ochrony Danych, *Guidelines on Consent under Regulation 2016/679*, 2017.
6. Europejska Rada Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679*, 2020.
7. Europejska Rada Ochrony Danych, *Guidelines 8/2020 on the targeting of social media users*, Version, 2.0, 2021.
8. Europejski Inspektor Ochrony Danych, *Opinia 3/2018, EDPS Opinion on online manipulation and personal data*, 2018.
9. Europejski Inspektor Ochrony Danych, *Opinion 5/2016 Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)*, 2016.
10. Experian, *Addressable TV. Harness the power of audience data for one-to-one targeting*, 2016.
11. FIGI Security, Infrastructure and Trust Working Group, *Big data, machine learning, consumer protection and privacy*, 2020.
12. Forbrukerrådet, *Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*, 2018.
13. Fundacja Panoptikon, raport *Kto (naprawdę) Cię namierzył? Facebook w polskiej kampanii wyborczej*.
14. Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, *Społeczeństwo informacyjne w Polsce w 2020 r.*, 2021.
15. Grupa ekspertów wysokiego szczebla ds. SI, *Definicja SI: główne funkcje i dyscypliny naukowe*, 2019.
16. Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2010 w sprawie internetowych reklam behawioralnych*, 2010.

17. Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 4/2007 w sprawie pojęcia danych osobowych*, 2007.
18. Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinion 03/2013 on purpose limitation*, 2013.
19. Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679*, 2017.
20. Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679*, 2018.
21. Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Dokument roboczy 2/2013 przedstawiający wytyczne w sprawie pozyskiwania zgody na zapisywanie plików cookie*, 2013.
22. Ipsos, London Economics, Deloitte consortium, *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*. Request for Specific Services 2016 85 02 for the implementation of Framework Contract EAH/2013/CP/04, 2018.
23. Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*, COM(2020) 65 final.
24. Komisja Europejska, *Consumer Condition Scoreboard. Consumers at Home in the Single Market*, 2019.
25. Komisja Europejska, Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Zwalczanie dezinformacji w internecie: podejście europejskie*, COM/2018/236 final.
26. Komisja Europejska, Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Platformy internetowe i jednolity rynek cyfrowy. Szanse i wyzwania dla Europy*, COM/2016/0288 final, 2016.
27. Komisja Europejska, Komunikat do Parlamentu Europejskiego i Rady, *Nowy program na rzecz konsumentów. Poprawa odporności konsumentów na potrzeby trwałej odbudowy*, COM(2020) 696 final, 2020.
28. Komisja Europejska, Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka*, COM/2019/168 final.
29. Komisja Europejska, Komunikat do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie stosowania dyrektywy o nieuczciwych praktykach handlowych. *Osiąganie wysokiego poziomu ochrony konsumentów. Budowanie zaufania do rynku wewnętrznego*, COM(2013) 138 final.
30. Komitet Ministrów Rady Europy, Zalecenie CM/Rec (2020) 1 dla państw członkowskich z dnia 8.04.2020 r. w sprawie wpływu systemów algorytmicznych na prawa człowieka.

31. Komitet Ministrów Rady Europy, Deklaracja z dnia 13.02.2019 r. w sprawie możliwości manipulacyjnych procesów algorytmicznych, 2019.
32. KPMG.pl, *[Cyfrowy] klient nasz pan. Jak marki na polskim rynku zarządzają doświadczeniami klientów*, 2019.
33. PwC, *Insurance 2020: The digital prize - Taking customer connection to a new level*, 2020.
34. Rekomendacja CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, 2010.
35. The Council of Economic Advisers, *Big data and differential pricing*, 2015.
36. The Data Protection Commission, *Report by the Data Protection Commission on the use of cookies and other tracking technologies*, 2020.

Źródła internetowe

1. <https://www.europarl.europa.eu/news/pl/headlines/society/20200918STO87404/sztuczna-inteligencja-szanse-i-zagrozenia>
2. <https://www.3ds.com/newsroom/press-releases/ces-2020-survey-cite-research-dassault-systemes-consumers-want-personalized-products-wont-wait-them-and-expect-cost-benefit-their-data>
3. <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx>
4. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777081
5. https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf
6. <https://payhowyudrive.pl/>
7. <https://themarkup.org/ask-the-markup/2020/04/28/why-am-i-paying-60-for-that-bag-of-rice-on-amazon-com>
8. <https://www.elementsofai.com/>
9. <https://patents.google.com/patent/US10380501B2/en>
10. <https://panoptikon.org/ktocienamierzyl-raport>
11. <https://www.ft.com/cms/s/0/5fd7d8a8-28e5-11e2-b92c-00144feabdc0.html>
12. <http://jakrobicmarketing.pl/jak-znalezc-zadluzonego-wlasciciela-mieszkania-ktory-chce-je-sprzedac-mozliwosci-ultraprecyzyjnego-targetowania-reklamy-na-facebook/>
13. https://ec.europa.eu/info/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#sweep2020
14. <https://www.facebook.com/business/help/711488016082996?id=986554971804174&helpref=search&sr=20&query=personalizacja%20reklam>

15. <https://support.google.com/adspolicy/answer/143465#547>
16. <https://support.google.com/google-ads/answer/6383030?hl=pl>
17. <https://www.cyberdefence24.pl/tiktok-przechowuja-dane-ze-schowka-bez-wiedzy-uzytownikow>
18. <https://www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-d-egli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Facebook>
19. <https://edition.cnn.com/2012/06/26/tech/web/orbitz-mac-users/index.html>
20. <https://www.nytimes.com/2021/02/11/style/disabled-fashion-facebook-discrimination.html?fbclid=IwAR2WoFFm0tTVG2jlv9uRcnJTD6fHCss5UFRuK500fXclaXSI462lqOcGjC4>
21. <https://www.bbc.com/news/business-50432634>
22. <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>
23. <https://caselaw.findlaw.com/us-5th-circuit/1292810.html>
24. E. Pariser, Beware online “filter bubbles”, 2011 https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles#t-241191
25. <https://www.facebook.com/help/1974897772766979>
26. <https://adtechexplained.com/cookie-syncing-explained>
27. http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf
28. <https://www.gov.pl/web/rodzina/koniec-z-profilowaniem-pomocy-dla-bez-robotnych>
29. <https://ico.org.uk/media/action-weve-taken/mpns/2259583/lifecycle-marketing-mother-and-baby-ltd-mpn-8-august-2018.pdf>,
30. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne>
31. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pl
32. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3696483
33. <https://support.google.com/adspolicy/answer/143465?hl=pl>
34. <https://www.likeabadmovie.eu/>
35. <https://www.pcworld.pl/news/Google-rezygnuje-z-plikow-cookies-Firma-nie-bedzie-sledzic-uzytownikow,425920.html>
36. <https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland>
37. <https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core>

38. <https://prawo.gazetaprawna.pl/artykuly/1498889,kary-za-ciasteczka-google-amazon.html>
39. <https://panoptykon.org/sledzic-czy-nie-sledzic>
40. <https://openjur.de/u/30714.html>
41. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

Wykaz aktów prawnych

1. *Traktat o funkcjonowaniu Unii Europejskiej*, Dz.Urz.UE C 202 z dnia 7.06.2016 r., s. 1.
2. *Karta praw podstawowych Unii Europejskiej*, Dz.Urz.UE. C 202 z dnia 7.06.2016 r., s. 389.
3. *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*, Dz.Urz.UE L 281 z dnia 23.11.1995 r., s. 31.
4. *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej („Dyrektywa o prywatności i łączności elektronicznej”)*, Dz. Urz.UE. C 201 z dnia 31.07.2002 r., s. 37.
5. *Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11.05.2005 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 („Dyrektywa o nieuczciwych praktykach handlowych”)*, Dz.Urz.UE L 149 z dnia 11.06.2005 r., s. 22.
6. *Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym*, Dz.Urz. UE L 376 z 27.12.2006 r., s. 36.
7. *Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25.10.2011 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 304 z dnia 22.11.2011 r., s. 64.
8. *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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 z dnia 4.05.2016 r., s. 1.
9. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych*, Dz.Urz.UE L 136 z dnia 22.05.2019 r., s. 1.

10. Dyrektywa 2019/2161 z dnia 27.11.2019 r. zmieniająca 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 328 z dnia 18.12.2019 r., s. 7.
11. Rezolucja Parlamentu Europejskiego z dnia 3.05.2018 r. w sprawie pluralizmu mediów i wolności mediów w Unii Europejskiej (2017/2209(INI)), Dz.Urz.C 41 z 6.02.2020 r., s. 64-75.
12. Rezolucja Parlamentu Europejskiego z dnia 16.02.2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, Dz.Urz.UE C 252 z dnia 18.07.2018 r.
13. Rezolucja z dnia 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL).
14. Rezolucja Parlamentu Europejskiego z dnia 20.10.2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych, 2020/2022(INI).
15. Rezolucja Parlamentu Europejskiego z dnia 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie Kodeksu usług cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego do podmiotów komercyjnych działających online. 2020/2019 (INL).
16. 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.
17. Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.
18. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM(2021) 206 final.
19. Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. High-risk AI systems referred to in article 6(2), COM(2021) 206 final.
20. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP 2017/0003(COD).
21. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final).

22. Ustawa z dnia 11.09.2015 r. o działalności ubezpieczeniowej i reasekuracyjnej. Dz.U. z 2015 r., poz. 1844.
23. Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów. Dz.U. z 2007 r., Nr 50, poz. 331.

Wyroki

1. Wyrok TS z 16.07.1998 r. w sprawie C-210/96 *Gut Springenheide i Tusky v. Oberkreisdirektor des Kreises Steinfurt - Amt für Lebensmittelüberwachung*, ECLI:EU:C:1998:369.
2. Wyrok TS z 23.04.2009 r. w sprawach połączonych C-261/07 i C-299/07 *VTB-VAB NV v. Total Belgium NV oraz Galatea BVBA v. Sanoma Magazines Belgium NV*, ECLI:EU:C:2009:244.
3. Wyrok TS z dnia 9.11.2010 r. w sprawach połączonych C-92/09 i 93/09 *Volker und Markus Schecke GbR i Hartmut Eifert v. Land Hessen*, ECLI:EU:C:2010:66.
4. Wyrok TS z 24.11.2011 r. w sprawie C-70/10 *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, ECLI:EU:C:2011:771.
5. Wyrok TS z 19.09.2013 r. w sprawie C-435/11, *CHS Tour Services GmbH v. Team4 Travel GmbH*, ECLI:EU:C:2013:574.
6. Wyrok TS z 16.04.2015 r. w sprawie C-388/13 *Nemzeti Fogyasztóvédelmi Hatóság v. UPC Magyarország Kft*, ECLI:EU:C:2015:225.
7. Wyrok TS z 7.09.2016 r. w sprawie C-310/15 *Vincent Deroo-Blanquart v. Sony Europe Limited*, ECLI:EU:C:2016:633.
8. Wyrok TS z 19.10.2016 r. w sprawie C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.
9. Wyrok TS z 29.07.2019 r. w sprawie C-40/17 *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629.
10. Wyrok TS z 1.10.2019 r. w sprawie C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*, ECLI:EU:C:2019:801.
11. Wyrok Regionalnego Sądu Administracyjnego Lazio (Rzym) z 10 stycznia 2020 r. w sprawie Facebook, sygn. 261/20.
12. Wyrok Wyższego Sądu Okręgowego we Frankfurcie nad Menem z dnia 29.01.2009 r., sprawa nr 6 U 90/08.



Anna Nowak – absolwentka Wydziału Prawa i Administracji Uniwersytetu Łódzkiego, czterokrotna stypendystka stypendium rektora Uniwersytetu Łódzkiego dla najlepszych studentów. Uczestniczka międzynarodowego projektu Klinika Prawa Technologii Przyszłości. Aplikantka I roku aplikacji radcowskiej w Okręgowej Izbie Radców Prawnych w Łodzi. Autorka artykułów z zakresu sztucznej inteligencji i prawa nowych technologii.

Urząd Ochrony Konkurencji i Konsumentów
pl. Powstańców Warszawy 1, 00-950 Warszawa
www.uokik.gov.pl

ISBN 978-83-64681-37-0



9 788364 681370