Erwin Ryter[1]

PROFILOWANIE JAKO ZDARZENIE SPRZYJAJĄCE NARUSZENIU PRAWA DO PRYWATNOŚCI W KONTEKŚCIE PRAWA UNIJNEGO

DOI: 10.5604/01.3001.0013.3351

Wprowadzenie

Niniejszy artykuł ma na celu ramowe wskazanie najważniejszych problemów nierozerwalnie związanych ze zjawiskiem profilowania, jak również ma przedstawić wyzwania z jakimi może się spotkać ustawodawca wskutek naruszenia prawa do prywatności w konsekwencji stosowania rozmaitych technik profilowania. Zagadnienie profilowania, ze względu na to, że obejmować może całe spektrum obszarów, których pośrednio lub bezpośrednio dotyczy – na potrzeby niniejszego artykułu – zostanie zawężone do najbardziej ogólnych, a zarazem wielopłaszczyznowych, sfer jako wstęp do rozwinięcia poszczególnych i znacznie bardziej ścisłych sytuacji prawnych, w których proces ten może mieć miejsce oraz mających istotne znaczenie dla prowadzenia rozważań zarówno teoretycznych, jak i praktycznych.

Autor pragnie zwrócić uwagę na to, że profilowanie i w ramach tego procesu, zautomatyzowane podejmowanie decyzji, stanowi jedno z najbardziej dyskusyjnych zagadnień w ochronie danych osobowych, a także w poszanowaniu prawa do prywatności osoby fizycznej.

Proces profilowania, nieodłącznie kojarzony z danymi osobowymi znany był już Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883), gdzie w art. 26a akcentowano niedopuszczalność podejmowania ostatecznych rozstrzygnięć w indywidualnej sprawie na podstawie danych osobowych, jeśli treść tego rozstrzygnięcia

[1] Mgr Erwin Ryter, Katedra Prawa Karnego Wykonawczego, Uniwersytet Łódzki, adres e-mail: doradztwoprawne.ryter@op.pl

jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym[2]. Z kolei na gruncie aktualnie obowiązujących przepisów, problem profilowania, który stał się niezwykle aktualny, został zdefiniowany w szczególności w art. 4 pkt 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)[3].

Istnieje kilka potocznych, jak również bardziej precyzyjnych, wykładni pojęcia profilowanie i to nie tylko na gruncie prawa ochrony danych osobowych. W językoznawstwie termin profilowanie[4] oznacza nadawanie czemuś określonego charakteru, zakresu lub kierunku. Jest to zatem określony proces, dzięki któremu uwypukla się na pierwszy plan pewną cechę lub zespół cech, zaś następnie na tej podstawie, tworzy się profil.

Z kolei, jak podał Jerzy Niklas, profilowanie zazwyczaj jest metodą opartą na pewnych wzorach matematycznych, które nie uwzględniają wszystkich skomplikowanych sytuacji życiowych[5].

Natomiast na gruncie nauk penalnych profilowanie kryminalne[6] oznacza szereg czynności wykonywanych najczęściej w przypadku seryjnych zabójstw, napaści seksualnych i podpaleń, w celu typowania cech nieznanego przestępcy, w oparciu o analizę danych pochodzących z miejsca zbrodni, cech ofiary oraz wiedzę na temat podobnych, wcześniej popełnionych przestępstw. Wyróżnia się profilowanie geograficzne, mające na celu ograniczenie obszaru poszukiwań poprzez wskazanie najbardziej prawdopodobnego miejsca zamieszkania nieznanego sprawcy serii przestępstw. W Polsce

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133, poz. 883).

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016).

[4] Definicja przytoczona na podstawie informacji dostępnych na stronie internetowej https://sjp.pwn.pl/szukaj/profilowanie.html, dostęp 14.05.2019.

[5] J. Niklas, *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji,* opinia dla Polskiego Towarzystwa Prawa Antydyskryminacyjnego, http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf, dostęp: 15.05.2019.

[6] J. Gołębiowski, K. Grochowska, *Profilowanie kryminalne na potrzeby sądu. Kontrowersje wokół przydatności*, w: *Innowacyjne metody wykrywania sprawców przestępstw. Materiały z konferencji*, M. Szostak, I. Dembowska, Wrocław 2014, s. 119.

profilowaniem kryminalnym zajmuje się między innymi Bogdan Lach, który stoi na stanowisku, że integralną część profilowania kryminalistycznego stanowią przypuszczenia dotyczące stałych mechanizmów osobowościowych poszukiwanego sprawcy, jego stanu psychicznego *tempore criminis* oraz hipotetycznego przebiegu jego procesów motywacyjnych leżących u podstaw analizowanych czynów skorelowanych z ujawnionymi śladami kryminalistycznymi[7].

Profilowanie kryminalne jest niezwykle popularne i cieszy się ogromnym uznaniem w amerykańskiej nauce o sprawcy przestępstwa. To właśnie stamtąd czerpie się inspirację dla unowocześniania i podnoszenia jakości profilowania w innych krajach, dzięki czemu techniki jakimi posługują się profilerzy są coraz bardziej doskonałe i jednocześnie pozwalają na coraz szybsze i znacznie bardziej precyzyjne odtworzenie portretu sprawcy przestępcy.

W Polsce zainteresowanie profilowaniem kryminalnym datuje się od chwili stworzenia pierwszego profilu zabójstwa kobiety w Dąbrowie Tarnowskiej, który wykonał zespół naukowców z Instytutu Ekspertyz Sądowych w Krakowie[8]. Jednakże na potrzeby niniejszego opracowania analizowana będzie wyłącznie problematyka profilowania na gruncie prawa ochrony danych osobowych z uwzględnieniem możliwych konsekwencji jakie w toku tego procesu mogą się ujawnić.

Niezwykle interesującym przykładem profilowania jest ponadto tzw. profilowanie rasowe. Termin ten pojawił się w związku próbami zaszeregowania osób fizycznych ze względu na ich pochodzenie rasowe lub etniczne, w tym na podstawie koloru skóry.

Zakaz bezpośredniej dyskryminacji ma tak zasadnicze znaczenie, że zgodnie z prawem międzynarodowym nie można jej stosować nawet w sytuacjach nadzwyczajnych[9].

Genezy tzw. profilowania rasowego można upatrywać się w sprawie Rosalind Williams Lecraft przeciwko Hiszpanii, która miała miejsce w 2009 r., w której Komitet Praw Człowieka Organizacji Narodów Zjednoczonych uznał za niezgodną z prawem dyskryminację w formie profilowania rasowego. Stan faktyczny odnosił się do sytuacji, w której funkcjonariusze Policji zatrzymali na peronie kolejowym skarżącą i zażądali od niej oka-

[7] B. Lach, *Profilowanie kryminalistyczne*, Warszawa 2014, s. 220.

[8] S.J. Hicks, B.D. Sales, *Profilowanie kryminalne*, Warszawa 2015, s. 163.

[9] Art. 4 ust. 1 Międzynarodowego paktu praw obywatelskich i politycznych (ICCPR). Zob. United Nations Human Rights Committee (2001), ust. 8; Scheinin (2007), ust. 41.

zania dokumentu tożsamości podając za powód kontroli jej czarny kolor skóry. Mimo iż w wyroku uznano, że funkcjonariusze Policji dysponują możliwością legitymowania osób ze względu na bezpieczeństwo i porządek publiczny, to jednak jednym z ważniejszych wyznaczników zainicjowania tego typu kontroli w stosunku do konkretnych osób nie może być wyłącznie kolor skóry bądź inne cechy wskazujące na odmienne pochodzenie rasowe lub etniczne. W sprawie tej uznano, że doszło do naruszenia godności osoby legitymowanej oraz zaakcentowania postawy ksenofobicznej przez funkcjonariuszy publicznych[10].

Wyrok ma szczególne znaczenie, ponieważ po raz pierwszy organ na poziomie ONZ wydał wyrok potępiający prowadzone przez Policję kontrole tożsamości oparte na pochodzeniu rasowym i etnicznym[11].

Ogólne rozporządzenie jest pierwszym aktem prawa unijnego, które zawiera definicję legalną profilowania[12]. Zwrócić trzeba uwagę, że ostateczny kształt definicji profilowania został wprowadzony dopiero w wyniku negocjacji jakie odbyły się pomiędzy Komisją Europejską, Radą Unii Europejskiej a Parlamentem Europejskim. Profilowanie, które wielokrotnie prowadzić może do naruszenia prawa do prywatności, będzie przedmiotem zainteresowania oraz analizy na gruncie niniejszego artykułu. Autor przede wszystkim pragnie zwrócić uwagę na to, że skutki profilowania – nie zawsze pożądane oraz pozytywne – mogą znaleźć swoje odzwierciedlenie w sferach najbardziej intymnych i najbardziej chronionych przez osoby fizyczne, jako atrybuty ich prawa do zachowania autonomii oraz odrębności od czynników mogących mieć dalekosiężny wpływ na zaburzenie prywatności jednostki.

---

[10] Sprawa Rosalind Williams Lecraft v. Spain (Rosalind Williams Lecraft przeciwko Hiszpanii) Comm nr 1493/2006 z dnia 30 lipca 2009 r. pkt 7.2. Inne wyroki wyrażające zasadę, że nie należy wyłącznie z powodu pochodzenia rasowego lub etnicznego legitymować osób, została wyrażona i potwierdzona w międzynarodowym orzecznictwie: Europejski Trybunał Praw Człowieka w sprawie Timishev v. Russia (Timiszew przeciwko Rosji), pkt 58; Europejski Trybunał Praw Człowieka w sprawie Abdulaziz, Cabales and Balkandali v. UK (Abdulaziz, Cabales i Balkandali przeciwko Zjednoczonemu Królestwu) nr 9214/80 z dnia 28 maja 1985 r., pkt 78.

[11] Informacja pobrana z przewodnika: *Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu*, s. 17. Przewodnik jest dostępny na stronie https://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_PL.pdf, dostęp: 29.08.2019.

[12] M. Czerniawski, w: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Komentarz do artykułu 4 pkt 4, red. E. Bielak-Jomaa, D. Lubasz, s. 200.

1. Dziedziny mające istotne znaczenie dla procesu profilowania

Jednym z bardziej popularnych rodzajów profilowania jest profilowanie zawodowe, za pomocą którego dąży się do wyodrębnienia najistotniejszych z punktu widzenia pracodawcy cech i umiejętności potencjalnego pracownika, w celu jak najbardziej wydajnego wykonywania przez niego określonych prac i zadań, które będą najbardziej zbliżone do indywidualnych predyspozycji zawodowych oraz kwalifikacji określonej osoby. Ten rodzaj profilowania stał się tematem dla polemiki w związku z możliwymi do realizacji uprawnieniami pracodawcy w stosunku do pracowników w kontekście nadmiernego analizowania sylwetki kompetencyjnej pracownika i wkraczania w sfery, które nie podlegają uprawnieniom kontrolnym bądź analitycznym pracodawcy względem pracownika. Mogłoby to nawet prowadzić do naruszenia sfery prywatności podlegającej ścisłej ochronie prawnej. Jednym z rodzajów tego rodzaju profilowania, z jakim autor miał możliwość spotkać się w jednej z korporacji zajmującej się świadczeniem usług na dużą skalę, była tzw. matryca kompetencji, której celem było delegowanie – na podstawie zebranych na bieżąco danych – pracowników poszczególnych zmian do wykonywania zadań jak najbardziej odpowiadających ich aktualnym kompetencjom i umiejętnościom lub nawet pomysłom w związku z realizacją danego projektu technologicznego. Na matrycy kompetencji gromadziło się, a następnie analizowało, bieżące cechy zespołu pracowników z rozgraniczeniem poszczególnych kompetencji do każdego pracownika z osobna (np. szybkość działania, kreatywność, analityczne myślenie, nowe pomysły, wizje etc.). Opieranie się na aktualnych wynikach matrycy, miało zminimalizować zarówno straty czasowe, jak i ekonomiczne w firmie w odniesieniu do tych pracowników, którzy nie do końca byliby w stanie wykorzystać swój aktualny potencjał i wypełnić określone zadania na dany dzień, a mogliby znacznie lepiej zająć się innymi obowiązkami, do realizacji których byli odsyłani przez swojego kierownika, który uprzednio dokonał analizy matrycy. Tak więc na podstawie rzeczonej tablicy kierownicy poszczególnych zmian – w oparciu o wyniki analizowane na bieżąco, tj. przed każdą nową zmianą – podejmowali decyzje o przydziale nowych obowiązków dla poszczególnych pracowników danej zmiany. Oceny podlegały przetwarzaniu na zasadzie z góry założonych algorytmów, aby finalnie wy-

odrębnić pewną wypadkową uzyskanych wyników charakteryzujących pracowników tej firmy. Choć system ten zapewniał pracodawcy doskonałe narzędzie do jak najbardziej efektywnego delegowania obowiązków dla poszczególnych pracowników i ostatecznie pozytywnego wzmożenia efektów produkcji, to trudno się oprzeć wrażeniu, iż istotnie, system ten opierał się na zautomatyzowanym przetwarzaniu danych osobowych o jakim jest mowa w art. 4 pkt 4 RODO[13]. Co istotne, analizie w tym konkretnym przypadku nie podlegały dane anonimowe, lecz dotyczące każdego wyodrębnionego pracownika, dla którego utworzono odrębne konto kompetencji zawodowych.

W kontekście profilowania niezwykle istotne jest rozróżnienie procesu profilowania i procesu podejmowania decyzji na podstawie stworzonego profilu osoby fizycznej. Podejmowanie decyzji na podstawie profilu może z kolei mieć zarówno charakter zautomatyzowany, jak i niezautomatyzowany. Doskonałym przykładem zautomatyzowanego podejmowania decyzji będzie wyświetlanie reklam obuwia sportowego dla osoby, która uprawia sport oraz dokonuje zakupów obuwia w internetowych sklepach sportowych. Natomiast niezautomatyzowane decyzje mogą zapadać na podstawie profilu osoby fizycznej starającej się o uzyskanie kredytu, która uprzednio złożyła wniosek kredytowy poddany następnie analizie przez pracownika banku, który na tej podstawie podejmuje indywidualną decyzję o przyznaniu bądź odmowie przyznania kredytu.

Proces tworzenia profili osób fizycznych na podstawie informacji o tych osobach może prowadzić do utworzenia zarówno profili grupowych, jak i indywidualnych, z czym nieodłącznie wiąże się pojęcie *data mining*, oznaczające również eksplorację wiedzy[14]. Rozwój *data mining* jest z kolei wynikiem rosnącej w świecie ilości informacji. *Data mining*, zwane również „odkrywaniem wiedzy w bazach danych", definiuje się ponadto jako wydobywanie danych z ukrytej, wcześniej nieznanej i potencjalnie użytecznej informacji[15].

---

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016).

[14] Eksploracja wiedzy jest najszerzej wykorzystywana w dziedzinach takich jak medycyna, ekonomia, astronomia czy technika.

[15] M. Gulczyński, *Techniki „odkrywania wiedzy" (data mining) oraz ich zastosowania*, „Polskie Towarzystwo Zarządzania Wiedzą", Seria Studia i Materiały, 2004, nr 2, s. 102.

Sam mechanizm profilowania, ze względu na to, iż jest oparty na pewnym przyjętym algorytmie, przy uwzględnieniu niepełnych bądź nawet błędnych danych, stwarza niestety potencjalne ryzyko dla wyodrębnienia niezgodnych z rzeczywistością wniosków. Wtedy też może dochodzić do różnego rodzaju naruszeń, bądź nawet nadużyć, przed którymi osoby fizyczne chronić mają sprzyjające im regulacje RODO. Jednym z najbardziej realnych zagrożeń może być naruszenie prawa do prywatności podczas dokonywania profilowania dalece ingerującego w informacje na temat konkretnej osoby. Interesującym przypadkiem, w którym doszło do naruszenia prawa do prywatności w związku z praktycznie automatycznym przypisaniem kobiecie trudnienia się prostytucją, była sytuacja w której podczas kontroli Policji znaleziono wśród puli wizytówek wizytówkę tej kobiety, co w opinii śledczych mogło wskazywać na to, że potajemnie zajmowała się nierządem. W aktach sprawy, przy jej nazwisku, bezrefleksyjnie odnotowano „prostytutka", co stało się wynikiem nieudolnego stworzenia profilu tej osoby. Pomimo tego, że wzmianka na temat tej kobiety została później zastąpiona słowem „krawcowa", to jednak wcześniejsze określenie jej mianem „prostytutki" zdążyło już trafić do akt innych spraw karnych i wskutek dalszego zaniedbania nie zostało już stamtąd usunięte. Sprawa stała się ostatecznie przedmiotem analizy przez Europejski Trybunał Praw Człowieka, który jednoznacznie zaakcentował naruszenie art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[16]. Przedstawiony stan faktyczny jest doskonałym przykładem nadania osobie fizycznej pewnego statusu jedynie na podstawie zebranych, lecz niezweryfikowanych danych, na zasadzie dopasowania cech tych danych do kryteriów określonej działalności.

Dziedziny, dla których rezultaty profilowania mają szczególnie doniosłe znaczenie, to przede wszystkim marketing, scoring kredytowy, służba zdrowia czy media społecznościowe. Oczywiście wyliczenie to nie stanowi katalogu zamkniętego, a jedynie przykładowo obrazuje sytuacje, w których proces ten jest wykorzystywany często i na szeroką skalę. Stąd też – we wskazanych przypadkach – istnieje zwiększone ryzyko naruszenia prawa do prywatności w chwilach tworzenia profili osób fizycznych w oparciu o informacje nie do końca zweryfikowane bądź zaktualizowane.

[16] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 18.10.2011 r., 16188/07, Lex nr 1001176. Zob. Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. 1993 Nr 61, poz. 284).

Warto przy tym wskazać, że nieprawidłowo lub nadmiarowo stosowane profilowanie może niestety powodować bądź nasilać problem dyskryminacji, jak również może poważnie zagrażać autonomii informacyjnej[17] osoby fizycznej, która – co do zasady – nie będzie dysponowała możliwością uzyskania wiedzy w zakresie profilowanych na temat jej osoby danych oraz zostanie w ten sposób pozbawiona możliwości obrony przed różnego rodzaju nadużyciami i niezgodnym z rzeczywistością wykorzystaniem informacji będących efektem tego rodzaju analizy.

2. Zagadnienie profilowania z perspektywy RODO

Jak wskazał Jędrzej Niklas, profilowanie na bardzo ogólnym poziomie, można porównać do kategoryzowania osób na podstawie różnych cech. Zarówno tych „niezmiennych" (np. płeć, pochodzenie etniczne, rok urodzenia, kolor oczu), jak i „zmiennych" (zachowanie, zwyczaje, preferencje)[18].

Z kolei zgodnie z wydaną przez Generalnego Inspektora Ochrony Danych Osobowych – jeszcze przed wejściem w życie RODO od 25.05.2018 r. – broszurą informacyjną[19], profilowanie to dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny osoby fizycznej, w szczególności do analizy lub prognozy efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania.

Natomiast zgodnie z pkt 4 ust. 4 RODO, 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.

---

[17] Zagadnienie to oznacza, że każda osoba fizyczna ma prawo do zachowania wyłącznie dla siebie określonych informacji na swój temat co pozostaje w jej całkowitej woli oraz gestii bądź może powierzyć te informacje wybranym przez siebie osobom trzecim.

[18] Informacja zaczerpnięta z opracowania Jędrzeja Niklasa na stronie: http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf, dostęp: 15.05.2019.

[19] Opracowanie GIODO, *Gotowi na RODO*, dostępne na stronie https://archiwum.giodo.gov.pl/550, dostęp 14.05.2019.

W aktualnym świecie, w którym coraz częściej zatraca się granica pomiędzy światem materialnym a wirtualnym, dochodzi do ogromnego przepływu i wymiany danych, co określić można wspólnym mianem przetwarzania. Jednym z następstw profilowania jest ponadto rozwój różnego rodzaju technologii z nim związanych, jak choćby „Internet rzeczy"[20] czy „big data"[21], dzięki którym dochodzi do przetwarzania informacji i danych, czasem bardzo skrajnie precyzyjnych.

Pojęcie przetwarzania składa się z dwóch elementów, tj. ogólnej definicji oraz otwartego katalogu wskazującego przykłady przetwarzania. Czynność będzie przetwarzaniem, jeżeli kumulatywnie wystąpi: operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany[22]. Proces ten tylko pozornie może wydawać się skomplikowany, choć w rzeczywistości przetwarzanie danych może odbywać się błyskawicznie z powodu łatwości w dostępie do ogromnej ilości danych[23].

RODO w swoich motywach[24], a szczególnie w motywie 30, odnosząc się do profilowania, wskazuje, że tworzenie profili osób fizycznych w powiązaniu z ich identyfikacją może mieć miejsce w sytuacji, w której dochodzi do przypisania określonym osobom określonych identyfikatorów. I tak na przykład adres IP komputera to identyfikator komputerowy, zaś różnego rodzaju urządzenia, aplikacje czy inne narzędzia to identyfikatory generowane przez działanie plików cookies. Poprzez ich oddziaływanie,

---

[20] Internet rzeczy jest to koncepcja, zgodnie z którą jednoznacznie identyfikowalne podmioty mogą pośrednio lub bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem instalacji elektrycznej inteligentnej KNX lub sieci komputerowej. Najważniejszym celem Internetu rzeczy jest stworzenie inteligentnych przestrzeni, takich jak miasta, budynki, systemy zdrowia czy systemy związane z codziennym życiem.

[21] Big data jest pojęciem charakteryzującym różnorodne zbiory danych, które mogą podlegać różnym zmiennym. Przetwarzanie tych danych jest z jednej strony skomplikowanym procesem, zaś z drugiej dzięki niemu uzyskuje się cenne informacje, które mogą nawet prowadzić do uzyskania nowej wiedzy.

[22] P. Naklicka, A. Gawron, *Rodosłowniczek, czyli omówienie podstawowych pojęć RODO wraz z przykładami*, w: *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami,* red. M. Gawroński, Warszawa 2018, s. 83.

[23] Zgodzić się należy z M. Molendą, który wskazał, że na przykład plastikowe karty zapewniające szybkość transakcji bezgotówkowych sprawiły, że zbieranie informacji jest łatwe jak nigdy dotąd (zob. M. Molenda, *Płynna inwigilacja rozmowy, Zygmunt Bauman, David Lyon [recenzja]*, „Uniwersyteckie Czasopismo Socjologiczne" 2014, nr 9, s. 120)

[24] Ogólne rozporządzenie o ochronie danych osobowych (RODO) zawiera 173 motywy.

dochodzi do wyodrębniania pewnych śladów działalności użytkownika, które w powiązaniu z identyfikatorami lub innymi informacjami mogą stać się źródłem cennych danych budujących profile osób fizycznych, z czego osoby te mogą nie zdawać sobie sprawy. Może w ten sposób dochodzić do naruszenia prywatności użytkowników, wskutek ich działalności w sieci i generowania w stosunku do nich określonego profilu.

Z kolei w motywie 24 wskazuje się na „monitorowanie zachowania", w odniesieniu do którego wszelkie analizy tego zachowania należy rozpatrywać z punktu widzenia ewentualnego przypisywania tych analiz do prognozowania osobistych preferencji, zachowań czy postaw osób fizycznych. Najczęściej dochodzi do tego w czasie aktywności zakupowej, która dostarcza na temat użytkownika konkretnych informacji odnoszących się do płci, stanu cywilnego, wieku, preferowanych produktów czy na przykład ulubionych kolorów. Następnie utworzone na tej podstawie profile wykorzystuje się do budowania strategii marketingowych bądź tworzenia spersonalizowanych reklam.

Nie mniej istotna jest ponadto kwestia poinformowania osoby fizycznej na temat profilowania, co jest przedmiotem motywu 60, zgodnie z którym zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Co więcej, motyw ten rekomenduje informowanie profilowanej osoby o możliwych skutkach profilowania. Wynikiem tej wiedzy może być z kolei chęć skorzystania przez osobę fizyczną z prawa do dostępu do danych jej dotyczących, o czym mowa w motywie 63, co będzie niekoniecznie przychylnie postrzegane przez podmioty dokonujące analiz danych i tworzenia w oparciu o nie profili.

Niebezpieczeństwo profilowania może mieć negatywny wydźwięk dla osoby fizycznej, gdy dochodzi do zbierania, przetwarzania, a następnie profilowania na podstawie tych danych jej określonych zdolności bądź predyspozycji, a nawet cech niepożądanych, w oparciu o które dochodzić może do podejmowania określonych decyzji. Sytuacja taka może mieć na przykład miejsce w momencie wypełniania elektronicznego wniosku o dobór odpowiedniej polisy ubezpieczeniowej. Ponadto ryzyko stworzenia profilu osoby, obarczonego błędami, wzrasta w momencie, gdy dochodzi do automatycznego podejmowania określonych decyzji, a zatem bez udziału człowieka.

Jak wskazał Maciej Gawroński, jeśli decyzje zapadają w wyniku zautomatyzowanego procesu decyzyjnego, a ponadto na ich podstawie następuje

odmowa wykonania usługi, to należy o tym fakcie poinformować osobę, która została objęta profilowaniem[25].

Zgodnie z motywem 71 w szczególności analizie podlegać mogą czynniki określające cechy danej osoby fizycznej, takie jak: sytuacja materialna, stan zdrowia, stan rodzinny, zainteresowania, wiarygodność, wykonywany zawód i kwalifikacje zawodowe, stabilność życiowa bądź jej brak. W omawianym motywie wyrażono pogląd, że podejmowanie wobec osoby fizycznej decyzji w związku z przetwarzaniem danych, o jakich może być mowa powyżej, powinno być dozwolone jedynie w sytuacji, gdy możliwość taką dopuszcza prawo Unii Europejskiej lub prawa państwa członkowskiego.

W dalszej kolejności należy wskazać, że zgodnie z motywem 72 profilowanie podlega przepisom rozporządzenia ogólnego, takim jak przepisy określające podstawy prawne przetwarzania lub zasady ochrony danych.

3. Wpływ profilowania na naruszenie prawa do prywatności

Prawo do prywatności – jedno z najbardziej fundamentalnych praw człowieka – przeniknęło do krajowych oraz europejskich standardów ochrony danych osobowych. Można rzec, że nie ma ochrony danych osobowych bez jednoczesnego poszanowania prawa do prywatności.

Przyjmuje się, że pojęcie prawa do prywatności wprowadzili w 1890 r. w Ameryce Samuel Warren i Louis Brandeis w artykule pt. *The Right to Privacy*. Choć podwalin wyróżniania prywatności niektórzy autorzy doszukują się już w Biblii, a później w myśli Benjamina Constanta czy Johna Stuarta Milla, to dla doktryny prawa szczególne znaczenie miał wspomniany artykuł[26].

Nie należy zapominać, iż prawo do prywatności kwalifikuje się także jako jedno z dóbr osobistych[27]. Pojęcie to nie zostało prawnie zdefiniowane,

---

[25] M. Gawroński, *Prawa jednostki*, w: *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami,* red. M. Gawroński, Warszawa 2018, s. 221.

[26] A. Gonschior, *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej*, w: *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego – aspekty teoretyczne i praktyczne*, red. D. Kornobis-Romanowska, Warszawa 2017, s. 242.

[27] W kwestii pojęcia i ochrony dóbr osobistych, jak również zakwalifikowania prawa do prywatności jako dobra, które można ująć w ramach katalogu otwartego, o którym mowa w art. 23 k.c., szeroko i wielokrotnie wypowiadały się sądy powszechne. Na przykład Sąd Najwyższy w wyroku z dnia 18 stycznia 1984 r., I CR 400/83, wskazał otwarty katalog dóbr osobistych (art. 23 i art. 24 k.c.), który obejmuje także dobra osobiste związane ze sferą życia

natomiast w doktrynie podnosi się, iż są to „wartości niemajątkowe, wiążące się z osobowością człowieka, uznane powszechnie w społeczeństwie”[28]. Przykładowy katalog dóbr osobistych został zawarty w art. 23 k.c., przy czym prywatność nie została w nim wprost ujęta. Pomimo tego prawo do prywatności zasługuje na szczególną ochronę prawną, biorąc pod uwagę m.in. rozwój „społeczeństwa informacyjnego”, którego członkowie zyskują coraz większe techniczne możliwości ingerowania w to dobro, w tym także wskutek procesu profilowania. W związku z tym ochrona prawa do prywatności znalazła swoje uzasadnienie zarówno w umowach międzynarodowych, jak na przykład w Europejskiej Konwencji Praw Człowieka, oraz w prawie krajowym, a zwłaszcza w Konstytucji RP, jak również w prawie ochrony danych osobowych czy w prawie prasowym. Odrębne miejsce ochronie prawa do prywatności poświęciły ponadto regulacje RODO[29], które w jeszcze większym stopniu akcentują potrzebę ochrony tej szczególnej sfery życia każdej osoby fizycznej. Z kolei na gruncie cywilnoprawnej ochrony prawa do prywatności, w art. 24 k.c., wskazano możliwe roszczenia i żądania z jakimi może wystąpić osoba poszkodowana w stosunku do osoby, która dopuściła się naruszenia określonego dobra.

W celu dokonania rzeczowej analizy korelacji pomiędzy prawem do prywatności a zjawiskiem profilowania, wyjaśnić należy ich wzajemne powiązania bądź wykluczenia, a w szczególności granice profilowania, po przekroczeniu których może dojść do naruszenia sfery prywatnej osoby fizycznej. Z pewnością analiza danych prowadząca do ich zautomatyzowanego przetwarzania i następnie na tej podstawie tworzenia określonego profilu osoby pociąga za sobą prawdopodobieństwo naruszenia niektórych praw i wolności, w tym prawa do prywatności. Trzeba bowiem wskazać, że w praktyce osoba podlegająca procesowi profilowania może zupełnie nie zdawać sobie sprawy w tego, że do tego zjawiska dochodzi

prywatnego, rodzinnego, ze sferą intymności. Ochrona w tym zakresie może odnosić się do wypadków ujawnienia faktów z życia osobistego i rodzinnego, nadużywania uzyskanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać (OSNCP 1984, nr 11, poz. 195). Zob. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2019, poz. 1145 t.j.).

[28] A. Szpunar, *Ochrona dóbr osobistych*, PWN, Warszawa 1979, s. 106.

[29] W motywie 4 RODO wskazano, że rozporządzenie ogólne poprzez swoje regulacje nie narusza prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej.

oraz, że dane jej dotyczące zostaną wykorzystane w określony sposób. Natomiast możliwość stanowienia o własnym życiu oraz wyborze procesów, w których chce się uczestniczyć, wydaje się być nieodłącznym przymiotem prawa do prywatności każdej osoby fizycznej.

Lawinowe narastanie problemu naruszenia prawa do prywatności, wskutek procesów przetwarzania danych w celu ich profilowania, nastąpił wraz z dynamicznym rozwojem infrastruktury internetowej, w tym w związku z pojawieniem się serwisów społecznościowych, których znamienną cechą jest powszechne i jednocześnie bezrefleksyjne udostępnianie oraz upublicznianie własnych danych przez użytkowników tych serwisów. Dzięki temu prężnie zaczęła się rozwijać branża nastawiona na zarabianie pieniędzy poprzez wykorzystywanie tych danych i tworzenie na ich podstawie określonych profili, szczególnie w celu jak najbardziej trafnego doboru konkretnej reklamy do typowo indywidualnych preferencji danego użytkownika sieci, od którego – w wyniku jego aktywności – zbiera się określone informacje, bardzo często charakteryzujące jego prywatne poglądy, predyspozycje czy ulubione marki bądź zainteresowania.

Prawo do prywatności, które może być nagminnie naruszane w efekcie profilowania, zostało wyartykułowane zarówno przez polskie, jak i pozakrajowe ustawy, deklaracje oraz inne akty prawne, w tym w RODO[30]. Zwłaszcza w motywie 4 podkreślono znaczenie ochrony danych dla prawa do prywatności poprzez wskazanie jego rangi jako prawa uznanego w Karcie Praw Podstawowych Unii Europejskiej[31]. W szczególności istotne znaczenie ma poszanowanie życia prywatnego i rodzinnego jako najbardziej intymny i osobisty, jak również niczym niezastąpiony, element bytu każdego człowieka.

W polskiej Konstytucji ochrona danych osobowych została nijako wyjęta przed nawias prawa do prywatności i uregulowana szczegółowo w osobnych przepisach[32].

---

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 04.05.2016).

[31] Karta praw podstawowych UE jest aktem prawnym koncentrującym najistotniejsze prawa człowieka oraz obowiązki obywatelskie. Akt ten został uchwalony i podpisany w dniu 07.12.2000 r. na szczycie Rady Europejskiej w Nicei. Karta praw podstawowych w swoich 54 artykułach traktuje na temat: godności człowieka, wolności, równości, solidarności, praw obywatelskich, wymiaru sprawiedliwości, postanowień ogólnych.

[32] W. Brzozowski, A. Krzywoń, M. Wiącek, *Prawa człowieka*, Warszawa 2018, s. 179.

Oznacza to, że w Konstytucji Rzeczypospolitej Polskiej[33] poświęcono miejsce na regulacje odnoszące się do ochrony życia prywatnego, a zatem zagadnienie to wykazuje się dużą doniosłością i znaczeniem dla zagwarantowania ochrony prawnej sfery najbardziej intymnej człowiekowi. W art. 47 wskazano, że każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym, zaś w art. 51 statuuje się potrzebę ochrony danych osobowych w celu ochrony życia prywatnego obywatela.

Konstytucjonalizacja ochrony danych osobowych posiada niewątpliwie największe znaczenie ze względu na wpływ, jaki wywiera na sytuację prawną jednostki[34].

Natomiast biorąc pod uwagę akty prawa międzynarodowego, zgodnie z art. 12 Powszechnej Deklaracji Praw Człowieka[35], nikt nie może być poddany arbitralnemu ingerowaniu w jego życie prywatne, rodzinne, domowe lub korespondencję, ani też atakom na jego honor lub dobre imię. Każdy człowiek ma prawo do ochrony prawnej przeciwko takim atakom lub ingerencjom. Podobnie traktuje art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych, zgodnie z którym nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię[36]. Wreszcie art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności stanowi o tym, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji, a także art. 7 Karty Praw Podstawowych EU, zgodnie z którym każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, domu i komunikowania[37]. Co więcej, w art. 8 Karty Praw Podstawowych EU wskazano, że każdy ma prawo do ochrony danych osobowych, które go dotyczą.

---

[33] Zob. Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483, z późn. zm.).

[34] P. Sobczyk, *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze UKSW" 9.1, s. 301, 307.

[35] Zob. Powszechna Deklaracja Praw Człowieka (rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana w dniu 10 grudnia 1948 r.).

[36] Zob. Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.

[37] Zob. Karta Praw Podstawowych Unii Europejskiej (2007/C 303/01) (Dz.U.UE C z dnia 14 grudnia 2007 r.).

Analizując wskazane regulacje, uzasadniona wydaje się być teza, że prawo do prywatności stanowi pochodną prawa do ochrony danych osobowych i jest z nim bardzo ściśle powiązane. A w takim kontekście naruszenie prawa do prywatności wskutek profilowania można będzie analizować także i pod względem naruszenia danych osobowych osoby profilowanej.

Związek jaki istnieje między prawem do prywatności a ochroną danych osobowych można określić jako związek materialny. Ochrona prywatności w dużym stopniu jest bowiem zależna od ochrony danych osobowych, które dotyczą jednostki[38].

Istotność ochrony prawa do prywatności podkreśla ponadto Marek Safjan, twierdząc, że: „prywatność ma podlegać ochronie właśnie dlatego i tylko dlatego, że przyznaje się każdej osobie prawo do wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a w której wolność od ciekawości innych jest swoistą *conditio sine qua non* swobodnego rozwoju jednostki"[39].

A zatem mając świadomość, jak procesy przetwarzania danych mogą być blisko powiązane z prawem do prywatności, istnieje znaczne prawdopodobieństwo naruszenia tego prawa w wyniku profilowania. Na przykład niektóre badania pokazują, że analiza danych zgromadzonych w serwisie Facebook pozwala na dość łatwe przypisanie określonej osobie fizycznej jej preferencji seksualnych, choć osoba ta nigdy takowych danych nie ujawniała[40].

Okoliczności w jakich może dojść do naruszenia prawa do prywatności w wyniku profilowania wynikać mogą w szczególności z coraz bardziej ekspansywnych technik śledzenia użytkowników zwłaszcza w sieci. Najczęściej profilowaniu ulegają dane odnoszące się do sytuacji materialnej, rodzinnej, stanu zdrowia, nałogów, a także określonych preferencji lub cech fizycznych. Na tej podstawie użytkownicy Internetu są kategoryzowani, aby wykorzystać wiedzę na ich temat w bardzo konkretnych celach. Ponadto, z jednej strony znaczny postęp techniczny, zaś z drugiej dostęp użytkowników do różnego rodzaju urządzeń mobilnych powoduje, że profilowanie stało się jeszcze łatwiejsze i przynosi coraz więcej oczekiwanych efektów. Można się spotkać z urządzeniami monitorującymi lokalizację, które po zainstalowaniu na przykład w pojeździe, będą moni-

---

38 *Ibidem*.

39 M. Safjan, *Prawo do ochrony życia prywatnego*, w: *Szkoła Praw Człowieka, Helsińska Fundacja Praw Człowieka*, Warszawa 2006, s. 211 i n.

40 M. Kosinski, D. Stillwell, T. Graepel, *Private traits and attributes are predictable from digital records of human behawior*, PNAS Early Edition, 2013, https://www.pnas.org/content/pnas/early/2013/03/06/1218772110.full.pdf, dostęp: 06.06.2019.

torowały przemieszanie się danej osoby i na tej podstawie możliwe będzie generowanie raportów z najczęściej odwiedzanych miejsc przez daną osobę. Pozwala to na statystyczne określenie kiedy i w jakich lokalizacjach najczęściej i najrzadziej przebywała profilowana osoba, zaś informacje te mogą zostać wykorzystane w różnych, nie zawsze w pełni zgodnych z prawem, celach.

Standardowo korzystanie z aplikacji mobilnych generuje tzw. metadane, które w połączeniu z informacjami na temat tego, w jaki sposób dana osoba korzystała z określonej aplikacji lub usługi, generuje bardzo precyzyjny profil użytkownika obejmujący także jego cechy osobowości i opis przyzwyczajeń i indywidualnego trybu życia, a tego typu dane mają bardzo często zarówno wrażliwy charakter, jak i głęboko ingerują w prywatność[41].

Powszechne oraz codzienne okoliczności, w związku z którymi użytkownik sieci mimowolnie staje się obiektem profilowania wiążą się z pozornie nieznaczącymi sytuacjami, dzięki którym obecność użytkownika zostaje utrwalona w „pamięci" Internetu. Mogą to być między innymi czynności wykonywane w związku z uruchomieniem dostępu do swoich kontaktów, do kalendarza, do historii przeglądanych witryn czy załączników do e-maili. Innym przykładem stwarzającym idealne warunki do uzyskiwania szczegółowych danych np. na temat użytkownika karty kredytowej, jest jej darmowa obsługa w sytuacji, gdy dany użytkownik wykona za jej pomocą określoną przez bank ilość transakcji bezgotówkowych w ciągu miesiąca. Możliwość uzyskania danych na temat aktywności zakupowej właściciela karty jest dla banku znacznie bardziej atrakcyjnym źródłem korzyści, niż uzyskanie wpływu należności z tytułu znikomego wykorzystywania karty do transakcji bezgotówkowych. Praktyczna nieuchronność, jak również masowość śledzenia lokalizacji i aktywności użytkowania poprzez różnego rodzaju aplikacje tworzy – z jednej strony potężne narzędzie dla celów związanych z profilowaniem, zaś z drugiej, generuje poważne problemy w sferze nienaruszania prawa do prywatności użytkownika takich aplikacji.

Profilowanie, które stało się obiektem wzmożonego zainteresowania w związku z wejściem w życie RODO, istnieje w polskiej oraz zagranicznej

[41] Informacja pobrana z opracowania K. Szymielewicz zatytułowanego *Śledzenie i profilowanie w sieci* dostępnego na stronie https://panoptykon.org/sites/default/files/publikacje/sledzenie_i_profilowanie_w_sieci_scenariusze_po_reformie_ue_wrzesien_2017.pdf, dostęp: 20.06.2019.

rzeczywistości tak naprawdę od dawna. W stosunku do profilowania odbywającego się w celu realizacji uzasadnionego interesu administratora, a zatem na podstawie art. 6 ust. 1 lit. e lub f RODO, istnieje możliwość złożenia sprzeciwu zgodnie z art. 21 ust. 1 RODO. Przy czym prawo to może być w pełni skuteczne wyłącznie wtedy, gdy przetwarzanie danych osobowych odbywa się w celach realizacji marketingu bezpośredniego. Wystarczy zatem złożenie przez użytkownika oświadczenia o określonej treści. Z kolei zgodnie z motywem 59 RODO administrator powinien zapewnić możliwość wniesienia sprzeciwu także drogą elektroniczną. Co istotne, o fakcie profilowania administrator danych powinien poinformować osobę fizyczną już na etapie zbierania od niej danych, jak również na wniosek danej osoby. Taki obowiązek został sformułowany w art. 21 ust. 4 RODO.

Wiedza na temat działań oraz zainteresowań osoby fizycznej uzyskiwana w wyniku profilowana, może być wykorzystywana dla różnych celów. Z jednej strony analizowanie aktywności zakupowej i zainteresowań użytkownika sieci może znacząco ułatwiać dopasowywanie oraz kierowanie celowanych reklam i ofert pod przewidywane zapotrzebowanie na te produkty przez daną osobę. Z kolei banki czy towarzystwa ubezpieczeń mogą weryfikować konta użytkowników sieci w ich profilach w celu badania wiarygodności czy też ich stabilności finansowej. Co ciekawe, aktywność w sieci tego samego użytkownika, lecz realizowana na różnych urządzeniach, może prowadzić do odmiennych wniosków w wyniku profilowania tej osoby i w tym znaczeniu autor upatruje się możliwości zaingerowania, a tym samym naruszenia prawa do prywatności. Tytułem przykładu może bowiem dojść do przypisania osobie, która chwilowo lub nawet okresowo użyczyła swojego urządzenia – komputera przenośnego innej osobie, która poprzez konkretny numer IP komputera „jest widziana" jako pierwotny użytkownik tego urządzenia, zaś aktywność przypadkowego użytkownika może zostać w tym wypadku przypisana do profilu właściwej osoby. Gdyby w tej sytuacji użytkownik tymczasowy wypełniał na przykład ankietę uwzględniającą jego sytuację rodzinną, majątkową czy poglądy polityczne, które znacząco odbiegałyby od wyznawanych przez właściwego użytkownika, to wynik profilowania oparty na tych danych i później mający wpływ na wydanie decyzji niekorzystnej dla użytkownika pierwotnego istotnie mógłby przesądzać o naruszeniu prawa do prywatności. Wynikałoby to niewątpliwie z błędnego przypisania osobie cech, które w rzeczywistości jej nie dotyczą, a znalazły się przypadkowo w jej profilu, który może zostać następnie poddany analizie przez kluczowe podmioty. I choć przytoczona sytuacja wydaje

się być historią jedynie hipotetyczną, to jednak nie sposób jej całkowicie wykluczyć jak również przyjąć, że się nie przyczyni do utworzenia zakłamanego profilu mogącego stać się podstawą do wydania określonej decyzji, na przykład odmawiającej udzielenia kredytu z powodu stwierdzenia, że osoba profilowana prowadzi rozwiązły tryb życia, a ponadto znajduje się w niekorzystnej sytuacji majątkowej. Tak wygenerowany profil – w opinii autora – istotnie narusza prawo do prywatności osoby fizycznej.

Autor w pełni zgadza się z poglądem wyrażonym przez M. Safijana, zgodnie z którym problem ochrony prawa do prywatności, zwłaszcza ochrony danych osobowych i autonomii informacyjnej, pojawia się na etapie, w którym zagrożenie prywatności osiąga apogeum. Prywatność w tym oto znaczeniu, w jakim mówi się o autonomii informacyjnej jednostki, zaczyna podlegać ochronie na takiej zasadzie, na jakiej chroni się ginący gatunek flory lub fauny[42].

Podsumowanie

Biorąc pod uwagę rosnący postęp technologiczny, wielokierunkowość przetwarzania danych osobowych czy praktyczny brak możliwości trwałego usunięcia danych z sieci, które choćby raz do niej trafiły, problem profilowania w odniesieniu do naruszenia prawa do prywatności, jak również danych uznawanych przez użytkowników za wrażliwe, wydaje się być realnym i trudnym do opanowania zagadnieniem. Może to w szczególności wynikać z braku możliwości nadzorowania lub innej formy kontrolowania w wystarczającym stopniu danych ze strony osób, których one dotyczą. Innym realnym zagrożeniem wydaje się być także kwestia braku dostępu do wiedzy na temat funkcjonujących w sieci profili osób fizycznych, które mogą podlegać analizom przez różnego rodzaju instytucje oraz podmioty, jak również zautomatyzowane urządzenia. Istotnie problem ten uwidacznia się na przykład podczas procesów profilowania objętych tajemnicą handlową, co może mieć miejsce podczas scoringu kredytowego. Może się bowiem zdarzyć, że osoby fizyczne nie uzyskają dostępu do danych, jakie są przetwarzane w wyniku utworzonego w ten sposób profilu. Dlatego przepisy prawne powinny w jasny i przejrzysty

[42] M. Safijan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6, s. 7.

sposób konkretyzować zarówno sytuacje naruszeń, jak i uprawnienia osoby fizycznej, za pomocą których będzie ona miała możliwość zapoznania się z wytycznymi, w oparciu o które został utworzony dany profil, w celu ochrony jej praw. Niewątpliwie namacalnym uprawnieniem byłaby ponadto gwarancja dopuszczenia zainteresowanej osoby fizycznej do katalogu zebranych na jej temat danych, na podstawie których profil jest tworzony i następnie analizowany.

Wspomniane w niniejszym artykule zagrożenia płynące z nieprawidłowych bądź nadmiarowych technik profilowania niewątpliwie generują niebezpieczeństwo naruszenia prawa do prywatności i w konsekwencji prawa ochrony danych, co z kolei powinno podlegać szczególnej ochronie prawnej.

W opinii autora, niezwykle istotną kwestią, wymagającą szczególnego zwrócenia uwagi zarówno ze strony praktyków, jak i teoretyków prawa, jest skutek w postaci naruszenia prawa do prywatności będący rezultatem zastosowanego profilowania, szczególnie w jego nieudolnej formie. Wiązać się z tym może prawo osoby poszkodowanej do uzyskania adekwatnego do rozmiaru naruszenia odszkodowania bądź zadośćuczynienia. Pojawić się tutaj może problem określenia granic odpowiedzialności za naruszenie, biorąc pod uwagę między innymi kwestię aktualizacji danych czy zakres bądź rodzaj informacji, jakimi posłużył się podmiot stosujący profilowanie. Odrębnym zagadnieniem jest ponadto kwestia dowodowa oraz zakres poniesionej przez osobę fizyczną szkody w kontekście ewentualnego miarkowania wysokości odszkodowania bądź innej formy rekompensaty.

Zgodnie z art. 92 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[43], w zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny[44].

A zatem w sytuacji naruszenia dobra osobistego, jakim jest niewątpliwie prawo do prywatności, na gruncie Kodeksu cywilnego, a ściślej art. 24 § 1, osoba której dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba, że nie jest ono bezprawne. W sytuacji, gdy już dojdzie do naruszenia dóbr, można żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków. Ponadto można domagać się zadośćuczynienia pieniężnego

[43] Zob. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).

[44] Zob. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2019, poz. 1145 t.j.).

lub przekazania odpowiedniej sumy pieniężnej na wskazany cel społeczny. Natomiast jeśli wskutek naruszenia dobra osobistego powstanie szkoda majątkowa, można domagać się jej naprawienia według zasad ogólnych.

Odnosząc się z kolei do odpowiedzialności z tytułu naruszenia danych osobowych, jaka została określona w ogólnym rozporządzeniu, wskazać należy na art. 79 oraz 82. Biorąc pod uwagę treść pierwszego z nich, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jej danych z naruszeniem niniejszego rozporządzenia. Natomiast drugi w wymienionych artykułów statuuje prawo do odszkodowania w tym znaczeniu, iż każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

Wspomnieć jeszcze należy o dwóch przepisach karnych mających zastosowanie w przypadku naruszenia Ustawy o ochronie danych osobowych[45]. Zgodnie z art. 107.1, kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Zaostrzenie kary może mieć miejsce w przypadku, gdy dojdzie do niezgodnego z prawem przetwarzania danych szczególnego rodzaju. Natomiast zgodnie z art. 108.1, odpowiedzialność karną może ponieść osoba udaremniająca bądź w inny sposób utrudniająca prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych. Tej samej karze podlega ponadto ten, kto w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej nie dostarcza danych niezbędnych do określenia podstawy wymiaru lub dostarcza dane, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej.

Podsumowując założenia oraz treść niniejszych rozważań warto wskazać, że niektórzy przedstawiciele doktryny prawniczej nie uznają, że ochrona danych osobowych typowo łączy się z prawem do prywatności. I tak, w opinii J. Barty i R. Markiewicza, pomiędzy ochroną prawa do prywatności a ochroną danych osobowych zachodzi stosunek krzyżowania się w tym tylko sensie, że istnieją zachowania, które mogą równolegle naruszać ochronę przewidzianą w obu rozważanych płaszczyznach. Są to przy tym reżimy

[45] Zob. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).

wzajemnie niezależne[46]. Idąc tym tokiem rozumowania stwierdzić zatem można, że w pewnych sytuacjach naruszenie danych osobowych łączyć się może jednocześnie z naruszeniem prawa do prywatności. W takim wypadku środki ochrony prawnej jakie przysługują jednostce, której prawa zostały naruszone, zawarte są nie tylko w art. 23 k.c., ale także w przepisach ochrony danych osobowych wspomnianych powyżej.

Kwestia naruszenia prawa do prywatności wskutek procesu profilowania stwarza znaczne wyzwanie do jeszcze większego doprecyzowania oraz udoskonalenia przepisów sankcjonujących naruszenie prawa ochrony danych osobowych, szczególnie wskutek rozmaitych technik profilowania. Aktualnie, a zwłaszcza w związku z rewolucją jaką nastąpiła w dziedzinie ochrony danych osobowych po wejściu w życie RODO, obserwuje się wśród administratorów danych znacznie większą dbałość o poprawne stosowanie systemów ochrony danych, tj. na adekwatnym do możliwego stopnia ich naruszenia poziomie, a przez to zapewnienie poszanowania prywatności osoby fizycznej. Jednakże zarówno stopień zaawansowania różnorodnych technik przetwarzania danych, który ma miejsce przede wszystkim w Internecie, jak i masowość stosowania rozmaitych form profilowania, zwłaszcza w oparciu o zautomatyzowane systemy, powoduje, że jakakolwiek próba uregulowania tego zjawiska, szczególnie w związku z dość surowymi regulacjami RODO, może okazać się w pewnych sytuacjach wyzwaniem niezwykle trudnym do opanowania. W ocenie autora, zjawisko profilowania, które niewątpliwie w wielu sytuacjach narusza w mniejszym bądź większym stopniu prywatność osób fizycznych, jako powszechny trend, może generować coraz więcej skarg i roszczeń, nie tylko ze względu na rosnącą świadomość prawną społeczeństwa, ale także ze względu na niezwykle szybko postępujący rozwój narzędzi i technik informatyzacji.

[46] J. Barta, R. Markiewicz, *Prawo do prywatności w społeczeństwie informatycznym*, „Ethos" 1999, rok 12, nr 1–2 (45–46), s. 380.

Bibliografia

Literatura

Brzozowski W., Krzywoń A., Wiącek M., *Prawa człowieka*, Warszawa 2018.

Czerniawski M., w: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Komentarz do artykułu 4 pkt 4, red. E. Bielak-Jomaa, D. Lubasz.

Gawroński M., *Prawa jednostki*, w: *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, red. M. Gawroński, Warszawa 2018.

Gołębiowski J., Grochowska K., *Profilowanie kryminalne na potrzeby sądu. Kontrowersje wokół przydatności*, w: *Innowacyjne metody wykrywania sprawców przestępstw. Materiały z konferencji*, M. Szostak, I. Dembowska, Wrocław 2014.

Gonschior A., *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej*, w: *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego – aspekty teoretyczne i praktyczne*, red. D. Kornobis-Romanowska, Warszawa 2017.

Gulczyński M., *Techniki „odkrywania wiedzy" (data mining) oraz ich zastosowania*, „Polskie Towarzystwo Zarządzania Wiedzą", Seria Studia i Materiały, 2004, nr 2.

Hicks S.J., Sales B.D., *Profilowanie kryminalne*, Warszawa 2015.

Lach B., *Profilowanie kryminalistyczne*, Warszawa 2014.

Molenda M., *Płynna inwigilacja rozmowy, Zygmunt Bauman, David Lyon [recenzja],* „Uniwersyteckie Czasopismo Socjologiczne" 2014, nr 9.

Naklicka P., Gawron A., *Rodosłowniczek, czyli omówienie podstawowych pojęć RODO wraz z przykładami*, w: *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, red. M. Gawroński, Warszawa 2018.

Safijan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6, s. 7.

Safjan M., *Prawo do ochrony życia prywatnego*, w: *Szkoła Praw Człowieka, Helsińska Fundacja Praw Człowieka*, Warszawa 2006.

Sobczyk P., *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze UKSW" 9.1.

Szpunar A., *Ochrona dóbr osobistych*, PWN, Warszawa 1979, s. 106.

Akty prawne

Karta Praw Podstawowych Unii Europejskiej (2007/C 303/01) (Dz.U.UE C z dnia 14 grudnia 2007 r.).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483, z późn. zm).

Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. 1993 Nr 61, poz. 284).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. 1977 Nr 38, poz. 167).

Powszechna Deklaracja Praw Człowieka (rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana w dniu 10 grudnia 1948 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2019, poz. 1145 t.j.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133, poz. 883).

Orzecznictwo

Komitet Praw Człowieka ONZ – Rosalind Williams Lecraft v. Spain (Rosalind Williams Lecraft przeciwko Hiszpanii) Comm No. 1493/2006, 30 July 2009.

Wyrok Europejskiego Trybunału Praw Człowieka – Timishev v. Russia (Timiszew przeciwko Rosji) ECtHR App. No. 55762/00, 13 December 2005.

Wyrok Europejskiego Trybunału Praw Człowieka – Abdulaziz, Cabales and Balkandali v. UK (Abdulaziz, Cabales i Balkandali przeciwko Zjednoczonemu Królestwu) ECtHR App. No. 9214/80, 28 May 1985.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 18.10.2011 r., 16188/07, Lex nr 1001176.

Źródła internetowe

Generalny Inspektor Ochrony Danych Osobowych, Narodowy Instytut Wolności, *Gotowi na RODO*, pobrane z: https://archiwum.giodo.gov.pl/550, dostęp 14.05.2019.

https://sjp.pwn.pl/szukaj/profilowanie.html, dostęp 14.05.2019.

Kosinski M., Stillwell D., Graepel T., *Private traits and attributes are predictable from digital records of human behawior*, PNAS Early Edition, 2013. Pobranez:https://www.pnas.org/content/pnas/early/2013/03/06/1218772110.full.pdf, dostęp 06.06.2019.

Niklas J., *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji.* Pobrane z: http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf, dostęp 15.05.2019.

Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu. Pobrane z: https://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_PL.pdf, dostęp 29.08.2019.

Szymielewicz K., *Śledzenie i profilowanie w sieci*, Fundacja Panoptykon, 2017. Pobrane z: https://panoptykon.org/sites/default/files/publikacje/sledzenie_i_profilowanie_w_sieci_scenariusze_po_reformie_ue_wrzesien_2017.pdf, dostęp 20.06.2019.

Słowa kluczowe: profilowanie, prawo do prywatności, RODO

Streszczenie

Autor publikacji podjął się analizy problemu związanego z procesem profilowania i podejmowania na jego podstawie zautomatyzowanych bądź niezautomatyzowanych decyzji wobec osób fizycznych, mogących oddziaływać na sferę prywatności osoby poddanej temu procederowi, a w szczególności w kontekście naruszenia granic prywatności i braku poszanowania sfery osobistej osoby fizycznej. W szczególności autor bada, czy określone w art. 4 pkt 4 RODO zjawisko profilowania należy odbierać jako pozytywny przejaw reformy ochrony danych osobowych i jej kluczowych regulacji oraz czy nowe technologie i rozwiązania nadążają i radzą sobie z koniecznością zapewnienia osobom fizycznym należytych zabezpieczeń i gwarancji przed ingerencją w ich

prawo do prywatności podczas procesu profilowania. Dostrzega się bowiem wiele zagrożeń dla prywatności w związku ze zbieraniem i analizowaniem informacji na temat osób fizycznych. Autor zwraca ponadto uwagę na to, że skala przetwarzania danych jest zjawiskiem dotąd niespotykanym i obejmującym znaczną rzeszę osób fizycznych. Bardzo trudną i wymagającą wielu wyzwań kwestią jest ponadto globalizacja sieci internetowej oraz podniesienie rangi handlu międzynarodowego, w związku z którym dochodzi do przetwarzania danych na masową skalę, jak również transgranicznego przepływu danych osobowych, a przy okazji tych procesów, także i do profilowania.

Key words: profiling, right to privacy, GDPR

PROFILING AS AN EVENT CONDUCIVE TO INFRINGEMENTS OF THE RIGHT TO PRIVACY IN THE CONTEXT OF EU LAW

Abstract

This paper contains an analysis of the issue related to profiling and making automated or nonautomated decisions related to natural persons on its basis, which may affect the privacy of persons subjected to profiling, especially in the context of breaching their privacy and showing a lack of respect for their personal life. In particular, the article examines whether profiling as defined in Article 4(4) GDPR should be regarded as a positive manifestation of the reform that personal data protection and key regulations pertaining thereto have undergone as well as whether the new technologies and solutions catch up and deal with the necessity to ensure due safeguards and guarantees for natural persons against interference into their right to privacy during profiling. In the context of this phenomenon, there are many threats to privacy resulting from the collection and analysis of the data of natural persons that can be observed. Moreover, the article points to the fact that the scale of personal data processing is unprecedented, covering a substantial lot of natural persons. Furthermore, the globalization of the Internet and the growth of importance of international trade, which entails large-scale data processing and cross-border transfers of personal data, with profiling occurring during these processes too, is also a very difficult and challenging issue.