RZECZNIK PRAW OBYWATELSKICH

Adam Bodnar

Warszawa, 30.03.2018r.

VII.520.14.2018.AG

Pani
Edyta Bielak-Jomaa
Generalny Inspektor Ochrony
Danych Osobowych

Szanowna Pani Minister

W ostatnich dniach światowe i polskie media doniosły o sprawie Cambridge Analytica[1], **wiążącej się z wykorzystaniem danych około 50 milionów użytkowników popularnego portalu społecznościowego Facebook**. Dane miały być wykorzystane m.in. po to, by wpłynąć na wyniki wyborów w Stanach Zjednoczonych Ameryki. Wiele dostępnych informacji wskazuje, że firma Cambridge Analytica tworzyła psychologiczne profile użytkowników, aby następnie kierować do tych osób przekazy o określonej, dopasowanej treści, które mogły oddziaływać na ich wybory, w tym wybory polityczne. Firma Cambridge Analytica sięgała przy tym do danych nie tylko tych osób, które instalowały określoną aplikację, ale również do danych powiązanych z nią użytkowników, a na takie działania zgadzać się miał Facebook[2]. Media donoszą również, że firma

[1] Przykładowo: http://wyborcza.pl/7,156282,23182834,afera-cambridge-analytica-facebook-wybral-amerykanom.html (dostęp 24.03.2018); https://bezprawnik.pl/cambridge-analytica/ (dostęp 26.03.2018); https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach (dostęp 24.03.2018); https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (dostęp 24.03.2018).

[2] Założyciel Facebooka w dniu 21 marca 2018 r. przedstawił oświadczenie, w którym odniósł się do całego problemu. Zob. https://www.facebook.com/zuck/posts/10104712037900071.

Cambridge Analytica mogła prowadzić działania, które w efekcie wpłynęły na wyniki referendum w sprawie Brexit w Wielkiej Brytanii[3], czy też na wybory w Kenii[4].

Problem ten, chociaż wiąże się aktualnie z działalnością konkretnej firmy i konkretnego portalu społecznościowego, w istocie uwypukla o wiele poważniejsze zagadnienie, związane z udostępnianiem danych osobowych oraz wykorzystywaniem ich – bez świadomości albo za zgodą wyrażoną przez użytkownika poprzez zaakceptowanie skomplikowanego regulaminu usług – do wpływania na wybory i decyzje użytkownika. **To rodzi zagrożenie nie tylko dla prawa do prywatności użytkownika sieci internetowej, ale również dla szeroko pojętych procesów demokratycznych i ochrony praw obywatelskich w kraju.**

Chyba nikt obecnie nie ma żadnych wątpliwości co do tego, że dostęp do wewnętrznych danych Facebooka oznacza pozyskanie ogromnej ilości wiedzy o tych, którzy dane udostępnili, a wykorzystanie posiadanych przez ten i inne podobne portale informacji w nim zawartych może być skutecznym narzędziem kształtowania rzeczywistości, za mocą wiedzy uzyskanej z obróbki tych danych. W sprawie Cambridge Analytica szczególne działania podjął brytyjski Komisarz ds. Informacji - *Information Commissioner*[5], wszczynając postępowanie w sprawie wykorzystania danych osobowych i ich analizy przez Cambridge Analytica do celów kampanii politycznych, dla celów partii i podmiotów komercyjnych. Brytyjski organ nadzorczy sprawdza również okoliczności, w jakich dane pozyskane z Facebooka mogły zostać wykorzystane, w szczególności do tzw. mikrotargetowania wyborców. Wskazuje przy tym i podkreśla, jak istotne jest, by społeczeństwo było w pełni świadome metod, w jakie informacje są wykorzystywane i w nowoczesnych kampaniach politycznych oraz ich potencjalnego wpływu na prawo do prywatności.

Mikrotargetowanie (ang. *microtargeting*) jest techniką znaną w kampaniach wyborczych na świecie i wykorzystywaną przez partie polityczne. Polega na przeszukiwaniu predyktywnym rynku po to, by wyłowić potencjalnych wyborców i do nich

[3] https://openintelligence.uk/news/politics/micro-targeting-privacy-agenda-anyone-paying-attention/ (dostęp 27.03.2018)
[4] http://www.bbc.com/news/world-africa-43471707 (dostęp 27.03.2018).
[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/ico-statement-investigation-into-data-analytics-for-political-purposes/ (dostęp 28.03.2018).

konkretnie skierować swój przekaz. Z prowadzonych badań naukowych jasno wynika, że kampanie polityczne w chwili obecnej łączą badania na temat potencjalnych wyborców w oparciu o posiadane dane ze spersonalizowaną reklamą polityczną, co nazywane jest w literaturze angielskim terminem: „online political micromarketing”[6]. W ten sposób partia polityczna jest w stanie zidentyfikować osoby, które jest w stanie z ogromnym prawdopodobieństwem przekonać do swoich poglądów. W takim przypadku możliwe jest bowiem powiązanie treści przekazywanego komunikatu ze szczególnymi zainteresowaniami potencjalnego wyborcy. Jak wynika z literatury, co potwierdza również sprawa Cambridge Analytica, techniki te są wykorzystywane głównie w Stanach Zjednoczonych Ameryki. W ostatnim okresie zyskały jednak na popularności również w Europie[7].

Wykorzystywanie techniki mikrotargetowania może stanowić z jednej strony korzyść dla osoby, polegającą na pozyskaniu pewnych informacji, ale z drugiej strony stanowić zagrożenie dla jej prywatności oraz ogólnie zagrożenie dla mechanizmów demokratycznych w państwie prawa. Taka kampania może bowiem z jednej strony zapewnić jednostce dostęp do informacji (chociaż niemal wyłącznie o określonej treści) i pośrednio w ten sposób zachęcić do udziału w wyborach, co w efekcie zwiększy ogólnie frekwencję wyborczą. Jednocześnie jednak jest to zagrożenie, bowiem wiąże się z bardzo głębokim wnikaniem w podejmowane decyzje. Zagrożenie dla prywatności, w powiązaniu z możliwością manipulacji i ignorowania indywidualnego zdania wyborcy jest najpoważniejszym zagrożeniem dla obywateli.

Stosowanie tych technik wiąże się z przetwarzaniem danych osobowych i zbieraniem informacji na masową skalę, w szczególności zbieraniem danych wrażliwych, dotyczących preferencji politycznych. W ocenie badaczy tematu, uświadomienie istnienia takich techniki i ich stosowania, co ma miejsce w ostatnich dniach, może wręcz prowadzić do efektu mrożącego, czyli do sytuacji, w której ludzie, którzy przypuszczają, że ich zachowanie jest monitorowane, mogę dostosowywać swoje zachowanie w taki sposób, by uniknąć

[6] Zob. Np. Zuiderveen Borgesius, F.J. et al., (2018), *Online Political Microtargeting: Promises and Threats for Democracy*, Utrecht Law Review. 14(1), pp. 82–96.

[7] Tamże, s. 84. Zob. Też np. T. Ross, *Secrets of the Tories' election "war room*, www.telegraph.co.uk/news/politics/11609570/Secrets-of-the-Tories-election-warroom.html (dostęp 28.03.2018); albo D. Wring & S. Ward, *Exit velocity: The media election*, (2015) 68 Parliamentary Affairs, issue suppl_1, https://doi.org/10.1093/pa/gsv037 (dostęp 28.03.2018) s. 224-240.

zainteresowania swoją osobą. Wiąże się to również z naturalnym brakiem komfortu po stronie użytkowników sieci podczas korzystania z niektórych stron internetowych i ograniczeniem aktywności po to, by uniknąć możliwości zebrania informacji na swój temat[8].

Wysoce prawdopodobne jest również zaistnienie sytuacji, w której dochodzi do naruszenia zasad ochrony danych osobowych. Nie zawsze bowiem wszystkie informacje przekazywane przez portale muszą być oparte na zgodzie użytkownika, a także – nawet jeśli zgoda została wyrażona – dane mogą być wykorzystywane w celu innym niż ten, do którego zostały zebrane. Jednym z przykładów jest sytuacja z 2017 r., kiedy to firma marketingowa zatrudniona przez amerykańską Partię Republikańską doświadczyła naruszenia zasad ochrony danych, ujawniając dane prawie 200 milionów obywateli amerykańskich. Wśród ujawnionych danych poza „klasycznymi" danymi osobowymi, typu imię i nazwisko znajdowały się również informacje dotyczące wyznania religijnego, czy pochodzenia etnicznego[9].

Możliwość wywierania wpływu na wyborców jest zagrożeniem jeszcze dalej idącym. Dzięki adresowaniu konkretnego przekazu do konkretnego odbiorcy można maksymalnie zwiększyć lub też maksymalnie zmniejszyć zaangażowanie wyborcze. Partie polityczne mogą wykorzystywać te techniki do wpływania na poparcie, ale także na powstrzymanie się wyborców od głosowania na przeciwników politycznych. Wykorzystywanie techniki polegającej na tym, że informacje określonej treści pojawiają się wyłącznie u docelowej grupy odbiorców, a nie u wszystkich korzystających z danej platformy, może spowodować przekształcenie potencjalnych wyborców w obiekty manipulacji. Może też doprowadzić do zmniejszenia sfery debaty politycznej, przy jednoczesnym zwiększeniu polaryzacji politycznej. Jest to również powiązane z łatwym dość rozpowszechnianiem się tzw. *fake news*[10]. Sytuacje w których techniki te są wykorzystywane w taki sposób, że odbiorca

[88] Zob. F. Zuiderveen, op. cit., s. 87. Zob . również J. Carrie Wong & O. Solon, *US government demands details on all visitors to anti-Trump protest website*, The Guardian 15 August 2017, <https://www.theguardian. com/world/2017/aug/14/donald-trump-inauguration-protest-website-search-warrant-dreamhost> (dostęp 28 marca 2018 r.

[9] 'Personal details of nearly 200 million US citizens exposed', *BBC News*, 19 June 2017, <www.bbc.com/news/technology-40331215 (dostęp 28.03.2018).

[10] W. Gorton, *Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy*, (2016) 38 *New Political*.
Science, no. 1, https://doi.org/10.1080/07393148.2015.1125119, s. 62.

przekazu słyszy wyłącznie o jednym problemie, jakim dana partia się zajmuje, prowadzi w prosty sposób do braku przejrzystości w działaniu partii politycznych. Wyborcy w ten sposób mogą w ogóle nie poznać poglądów danej partii na zupełnie inne tematy[11]. Wreszcie, w ten sposób część potencjalnych wyborców może w ogóle zostać wykluczona z procesu wyborczego. Kampania polityczna może nie być dostępna dla określonej grupy użytkowników sieci, np. dlatego, że partia nie spodziewa się ich udziału w wyborach, a zatem nie przekazuje im określonych informacji[12]. Te wszystkie zagrożenia wiążą się z potencjalnym wykorzystaniem danych osobowych, do których dostęp mogą mieć firmy typu Cambridge Analytica[13].

Bez wątpienia, w kontekście europejskim sytuacja nie jest tak poważna jak w Stanach Zjednoczonych, głównie ze względu na wyższy standard ochrony danych osobowych niż w USA, a także niższe budżety przewidziane na kampanie wyborcze. Wpływ na zapewnienie lepszej ochrony może mieć też treść przepisów prawa UE, w tym w szczególności mające wkrótce być stosowane rozporządzenie ogólne o ochronie danych osobowych, ale także mające być wkrótce przyjęte rozporządzenie w sprawie e-prywatności. **Przepisy te mogą wpłynąć na prawidłową realizację praw osób, w szczególności w odniesieniu do zakresu informacji gromadzonych na nasz temat przez firmy typu Facebook, ale także poprzez możliwość wglądu w swój pełny profil w celu skorygowania lub usunięcia danych.** Zresztą, jak wynika z oświadczenia Marka Zuckerberga, Facebook zmienił już swoją politykę i obecnie transfer danych, bez zgody użytkowników, naruszałby regulamin Facebooka. Nie zmienia to jednak faktu, że – jak słusznie podkreśla Fundacja Panoptykon – „Facebook istnieje właśnie po to, żeby eksploatować nasze dane – odczytywać je z okruchów pozornie nieistotnych informacji i zlepiać w wartościowe profile. Czy zrobi to swoimi rękami (na swoich serwerach, w oparciu o własne algorytmy), czy za pomocą innej firmy, to sprawa drugorzędna”[14]. Panoptykon podkreśla też, że „sposób działania mediów społecznościowych i możliwości niejawnego, precyzyjnego targetowania przekazu politycznego w sieci powinny się

[11] Zob. F. J. Zuiderveen, op. cit., s. 87.
[12] Tamże, s. 88.
[13] Zob. również wyniki badań Iry Rubinsteina, które opublikował w artykule *Voter privacy in the age of big data*, Wisconsin Law Review 2014 861, http://wisconsinlawreview.org/wp-content/uploads/2015/02/1-Rubinstein-Final-Online.pdf (dostęp 27.03.2018).
[14] https://panoptykon.org/wiadomosc/nie-blad-tylko-logiczna-konsekwencja-modelu-biznesowego-facebooka

przełożyć na zmiany w prawie wyborczym. Każdy sponsorowany komunikat, który serwują nam sztaby wyborcze lub wynajęte przez nie firmy, powinien być oznaczany, tak by nie było wątpliwości, że to nie jest neutralny news, ale próba wpłynięcia na nasze poglądy".

Od maja 2018 r. sytuacja powinna ulec zmianie o tyle, że jasno określone zostaną te reguły, które dotyczą prawa właściwego do oceny działań rozmaitych aplikacji. Przekazywanie naszych danych osobowych innym firmom w celach marketingowych, w tym brokerom danych, którzy agregują dane z różnych źródeł i tworzą własne profile, będzie wymagało świadomej, poinformowanej zgody. Jednak można spodziewać się, że wiele firm nadal będzie dokonywało takiej interpretacji przepisów, która będzie sprzyjała kontynuowaniu prowadzenia przez nie działalności w dotychczasowym kształcie. Być może przygotowywanie analiz dotyczących sposobu spędzania wolnego czasu faktycznie obydwa się – jak twierdzi np. firma Selectivv[15], która przedstawia takie analizy – w oparciu o dane zanonimizowane. Jednak możliwe jest również, że świadczenie innych usług typu przekazywanie sprofilowanej reklamy na telefon, odbywa się w oparciu o unikatowy numer użytkownika. To jasno wskazuje, że tego typu firmy mogą jednak przetwarzać dane osobowe, posługując się np. identyfikatorami przypisanymi do osób lub telefonów. Tym samym dochodzić może do realnej ingerencji w naszą prywatność.

Przykładów sytuacji, w których wykorzystywane są dane użytkowników aplikacji, czy portali internetowych, jest w ostatnim czasie więcej. Nie zawsze wiązały się z użyciem techniki mikrotargetowania, jednak w każdym przypadku ilość gromadzonych danych, sposób ich pozyskiwania – nie zawsze jasny dla użytkowników, a także możliwość ich analizy rodzi wątpliwości z punktu widzenia praw obywatelskich[16]. Omówione wyżej przypadki to zatem wyłącznie przykłady problemów, jakie wiążą się z funkcjonowaniem firm typu Cambridge Analytica oraz ich powiązaniem z portalami gromadzącymi informacje na temat obywateli, takimi jak Facebook czy Google.

W chwili obecnej nie są jeszcze znane wszystkie okoliczności sprawy Cambridge Analytica. Jak widać jednak, technika ta może być wykorzystywana również przez inne

[15] Zob. np. informacje zamieszczone w tekście dotyczącym działalności firmy Selectivv http://www.newsweek.pl/biznes/gospodarka/jak-inwigiluja-nas-specjalisci-od-reklamy-sprawdz-jak-cie-sledza,artykuly,424806,1.html (dostęp 28.03.2018).

[16] Zob. też ostatnie informacje dotyczące wykorzystywania danych pochodzących z smsów, wysyłanych za pośrednictwem aplikacji: http://next.gazeta.pl/nextnext/56,162552,23191620,facebook-zmaga-sie-z-kolejnymi-oskarzeniami-o-naruszenie-prywatnosci.html#A_BoxOpImg1 (dostęp 28.03.2018).

firmy i na inne sposoby. Jeżeli potwierdziłyby się obawy wskazujące na istotne zagrożenia dla prawa do prywatności i podstawowych reguł demokracji, konieczne byłoby podjęcie szerszej dyskusji w kierunku wypracowania stosownego rozwiązania. Takie rozwiązanie musiałoby oczywiście spełniać wymogi wynikające z ogólnych standardów ochrony praw człowieka, np. art. 10 Konwencji o ochronie praw człowieka i podstawowych wolności[17]. Do tego jednak potrzebne są dokładniejsze badania i analiza sytuacji. Nie jest to łatwe w sytuacji, w której partie polityczne nie są skłonne do ujawniania informacji, np. o wydatkach na marketing polityczny i kreowanie wizerunku[18]. To tylko potwierdza, że konieczne jest znalezienie rozwiązań, które doprowadziłyby do znalezienia sposobu na kontrolę politycznego mikrotargetowania.

W związku z powyższym, mając na względzie zagrożenia dla ochrony danych osobowych wynikające z działań firm typu Cambridge Analytica, działając na podstawie art. 13 ust. 1 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2017 r. poz. 958) **uprzejmie proszę Panią Minister o informację, czy GIODO prowadzi analizy tego typu przypadków i czy w ocenie Pani Minister ustawodawstwo polskie odpowiada na sygnalizowane zagrożenia dla ochrony danych osobowych. Proszę także uprzejmie o wskazanie, czy w tej konkretnej sprawie – tak, jak ma to miejsce w Wielkiej Brytanii – podjęte zostanie postępowanie przez GIODO. Wreszcie, zwracam się do Pani Minister także o ocenę, czy przepisy unijnego rozporządzenia ogólnego o ochronie danych oraz przyszłego rozporządzenia o e-prywatności będą w stanie zapobiec zagrożeniom tego typu w przyszłości.**

Adam Bodnar

Do wiadomości:

Pan Marek Zagórski

Sekretarz Stanu w Ministerstwie Cyfryzacji

[17] *TV Vest AS v Norway*, application No. 21132/05, Merits and Just Satisfaction, 11 December 2008, para. 78, para. 66.
[18] www.tokfm.pl/Tokfm/7,103454,22360094,dbanie-o-pr-i-social-media-partie-nie-chca-ujawnic-komu-i.html