Tomasz Klepacz, Władysław Przyjemski

Współczesne zagrożenia dla przetwarzania danych osobowych w kontekście RODO i sprawy Facebook – Cambridge Analytica

JEL: K24. **DOI:** 10.24136/atest.2019.205.
Data zgłoszenia: 18.06.2019. **Data akceptacji:** 27.09.2019.

W artykule przedstawiono współczesne zagrożenia wynikające z przetwarzania danych osobowych w systemach komputerowych z wykorzystaniem technik Big Data na przykładzie wydarzenia o największej w ostatnich latach wadze – Facebook – sprawa Cambridge Analytica. Dzięki ujawnieniu sprawy opinia publiczna otrzymała informacje o metodach wykorzystywanych w przetwarzaniu danych osobowych, ich potencjalnej skuteczności w marketingu biznesowym i politycznym, a także skali i łatwości dostępu do nich. To, co przez wiele lat było oczywiste dla każdego użytkownika Internetu, że wiele drobnych informacji o jego działalności jest gromadzonych przez dostawców różnego rodzaju usług, stało się oczywistością. Użytkownicy otrzymują obecnie szeroki zakres informacji, dostępny dzięki konsolidacji danych przez kilku głównych potentatów oraz ogromnej, powszechnie dostępnej, mocy obliczeniowej. Pozwala to oddziaływać na zachowanie i postawy osób, których dane dotyczą. Przestraszyło to zarówno zwykłych obywateli, jak i rządy. Artykuł stanowi próbę odpowiedzi na pytanie, czy ogólne, unijne rozporządzenie o ochronie danych może przeciwdziałać istniejącym zagrożeniom.

Słowa kluczowe: dane osobowe, Unia Europejska, ochrona danych, Facebook, Cambridge Analytica.

Wstęp

Głównym celem niniejszego artykułu jest próba odpowiedzi na pytanie, na ile RODO – 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), które zaczęło obowiązywać w państwach członkowskich UE dnia 25 maja 2018 r. – jest skuteczną odpowiedzią na współczesne zagrożenia związane z gromadzeniem i przetwarzaniem danych osobowych przez podmioty prywatne. Założenia zawarte w RODO zostaną zestawione z wydarzeniami, o których głośno stało się dzięki rewelacjom prasowym opublikowanym 17 marca 2018 r. [12], jakoby Cambridge Analytica (w dalszej części tekstu używany będzie skrót CA na określenie Cambridge Analytica) miała w sposób nielegalny pozyskać dane osobowe z blisko 50 milionów kont z portalu społecznościowego Facebook, a następnie przetwarzać je i wykorzystać m.in. do wsparcia prezydenckiej kampanii wyborczej Donalda Trumpa w 2016 r.

Artykuł ma podział problematyczny. W pierwszej kolejności przedstawione zostaną wydarzenia, które miały się rozegrać w latach 2014–2016. Omówione zostaną również zagadnienia prawne – wewnętrzne regulacje Facebooka – w celu identyfikacji, na ujawnianie jakich prywatnych informacji zgadzają się użytkownicy portalu, w jaki sposób ich dane osobowe są chronione przez Facebooka, gdzie popełniono błędy, a w końcu – jakich czynności należy/należało dokonać, aby problem nie zaistniał i nie powrócił. Na koniec wykonana zostanie krytyczna analiza zapisów RODO w kontekście wcześniej poczynionych uwag. Tym samym nastąpi próba odpowiedzi na pytanie, na ile nowa regulacja odpowiada współczesnym zagrożeniom dla ochrony danych osobowych i czy posiada potencjalnie skuteczne narzędzia do walki z tymi zagrożeniami.

Najwięcej informacji na temat tego, co rzeczywiście miało się wydarzyć w interesującym nas okresie, uzyskujemy za pośrednictwem słów byłego Dyrektora ds. Badań Naukowych Cambridge Analytica (od 2013 r. do lipca 2014 r.) Christophera Wylie, z którym amerykańskie i brytyjskie media przeprowadziły szereg wywiadów [22], a którym to w końcu zainteresowała się także brytyjska komisja parlamentarna, badająca, czy kampania referendalna w sprawie Brexitu była przeprowadzona w sposób w pełni legalny [10]. Za podstawę źródłową niniejszego artykułu posłużą także wywiady z Alexandrem Nixem (CEO CA) [19], Markiem Zuckerbergiem (założyciel i szef FB) [23], Dr. Aleksandrem Koganem (twórca aplikacji MyDigitalLife) [18], Brittany Kaiser (była dyrektor CA) [20], Stevem Bannonem (szef kampanii wyborczej D. Trumpa) [3] oraz fragment z przesłuchania A. Nixa przed brytyjską komisją parlamentarną [2]. Pomocne okazały się także tajne nagrania ze spotkań z członkami kierownictwa CA (A. Nix, Mark Turnbull, Dr Adam Tayler), które zostały sporządzone przez dziennikarzy z Channel 4 News [15, 16]. Głównymi źródłami prawnymi będą wzmiankowane już RODO [13] oraz wewnętrzne regulacje Facebooka.

Cambridge Analytica, Global Science Research i Facebook – geneza problemu

Ch. Wylie miał od 2013 r. pracować dla Alexandra Nixa (późniejszy CEO CA) w SCL Group (w komórce SCL Elections), która zajmowała się przygotowywaniem analiz i strategii działań (w tym kampanii wyborczych) dla organizacji rządowych i militarnych na całym świecie [14], a która to firma w chwili obecnej jest firmą-matką dla Cambridge Analytica. Wszystko zmieniło się wraz z pojawieniem się Steve'a Bannona, ówczesnego redaktora naczelnego prawicowego „Breitbart News", a potem wiceprezydenta CA (w latach 2013–2016) i szefa kampanii wyborczej D. Trumpa. S. Bannon pragnął broni, która umożliwi mu zmianę ludzkich zachowań na zgodne z politycznymi potrzebami jego obozu, tj. takie, które zapewnią uzyskanie poparcia w czasie wyborów (wywiad Ch. Wylie dla „The Guardian"). Wraz z pojawieniem się na horyzoncie tak ambitnego klienta pracownicy SCL Group powołali do życia Cambridge Analytica, która miała początkowo służyć za przykrywkę, a w końcu stała się pełnoprawnym tworem.

Mając już zadanie przed sobą, należało się zastanowić, skąd uzyskać pieniądze na tak ambitne przedsięwzięcie. Pomocną

rękę w tym momencie wyciągnął miliarder Robert Mercer, w późniejszych latach znany ze swojego wsparcia finansowego dla D. Trumpa. W 2016 r. Mercer miał wspomóc republikanów kwotą 22,5 mln dolarów [6]. Podczas ich wspólnego spotkania w Nowym Jorku, w którym udział wzięli A. Nix, Ch. Wylie, S. Bannon i R. Mercer, przedstawiono cel, jaki zainteresowani pragnęli zrealizować, mianowicie utworzenie narzędzia zdolnego do wykorzystania metody *microtargeting* w oparciu o parametry psychofizyczne danej osoby. *Microtargeting* to narzędzie marketingowe, które – za pomocą informacji na temat danej osoby – potrafi przewidzieć jej zachowanie, a następnie wpłynąć na jej poczynania zgodnie ze swoim celem. Plan przypadł do gustu Mercerowi, a ten zainwestował w ten projekt 15 mln dolarów. Warto przypomnieć, że Mercer, wspierając kampanię wyborczą republikanów w 2016 r., wsparł ich kwotą 22,5 mln dolarów. Wobec tego suma 15 mln wskazywała na znaczące zaangażowanie miliardera w to przedsięwzięcie.

Problemem, przed jakim teraz stanęła CA, były dane. Należało uzyskać albo dostęp do narzędzi, które zapewnią ich pozyskanie, albo same dane uprzednio wydobyte przez stronę trzecią. Wybrano opcję drugą. Ch. Wylie miał odbyć spotkanie z wykładowcą z Departamentu Psychologii z Cambridge Dr. Aleksandrem Koganem (założycielem Global Science Research), który dla celów naukowych stworzył działającą w środowisku Facebooka aplikację MyDigitalLife. Wywiad Dr. A. Kogana z BBC Radio 4: „I got really interested in trying to understand how we could model human behavior through social media". Współpracę z Dr. Koganem potwierdza także CEO CA A. Nix w przesłuchaniu przed PMs: „We had a relationship with GSR (firma Dr. Kogana – T.K.), they did some research for us back in 2014, that research proved to be fruitless". Ta opinia jest jednak sprzeczna z mailem A. Nixa, którego treść udostępnia Channel 4 News w tym nagraniu: „I think we can all be proud of the work completed thus far". Celem spotkania było pozyskanie danych zebranych przez jego aplikację. Miała ona działać w sposób następujący: warunkami użytkowania aplikacji było wniesienie opłaty (koszt – 3–4 $) oraz wyrażenie zgody na dostęp do danych z FB. Rekrutacją chętnych miała zajmować się firma Qualtrics, ogółem cały proces pozyskiwania danych miał kosztować 700–800 tys. USD. Użytkownicy wypełniali formularz, który był narzędziem badawczym, pozwalającym na ocenę ich osobowości. Co najistotniejsze, bez informowania użytkowników aplikacja pobierała dane także jej przyjaciół, którzy nie mieli odpowiednio dostosowanych ustawień prywatności. Informację tę uzyskujemy z wywiadu Ch. Wylie dla Channel 4 News: „...thousands of Facebook users were paid to download an app... the app didn't just mine the respondents data. Crucially it swept up that of their friends to those who hadn't adjusted their privacy settings". Dzięki temu, pomimo tego, że aplikację pobrało jedynie 270 tys. osób, uzyskano dane dotyczące około 50 mln kont FB. Potwierdza to Ch. Wylie w wywiadzie dla „The Guardian": „Upwards of 50, 60 million profiles were collected in a two or three month period". Sama transakcja dokonana między GSR a CA okazała się być niezarobkowa, co potwierdzają zarazem Wylie, jak i Dr Kogan. CA miała jedynie zwrócić koszt zdobycia tych danych, czyli około 800 tys. $, które jednak i tak zostały przekazane do Qualtrics, czyli firmy, która zatrudniła osoby skore do wzięcia udziału w badaniach Dr. Kogana.

Jakie dane uzyskano dzięki temu? Aplikacja miała pobierać informacje z profilu danej osoby, a ponadto aktualizacje statusu, polubienia, a czasami nawet prywatne wiadomości. Na podstawie tych informacji CA była w stanie określić takie cechy człowieka, jak płeć, wiek czy nawet poziom IQ, światopogląd czy cechy charakteru itp. Dowodem na to jest e-mail wysłany przez Dr. Kogana do Ch. Wyliego, w którym to Dr Kogan przedstawia cechy, które są możliwe do zbadania za pomocą posiadanych danych. E-mail został umieszczony w artykule *How Trump Consultants Exploited the Facebook Data of Millions* [12]. Wszystko to zaś miało służyć ustaleniu tego, na jaki przekaz dany typ osoby jest podatny. Dr Alex Taylor (chief data officer CA) powiedział w tajnym nagraniu: „If you're collecting data on people and you're profiling them thath gives you more insight... to give them messaging about issues that they care about and language, and imagery that they're likely engage with". Sztab ludzi złożony ze specjalistów od marketingu tworzyłby z kolei odpowiednie przekazy medialne, które następnie umieszczano by w Internecie lub telewizji. Przekaz medialny to np. spoty wyborcze/reklamowe czy świeżo utworzone strony internetowe i blogi, które za pomocą swojej treści odpowiednio wpływałyby na odbiorcę. Potwierdza to Ch. Wylie w wywiadzie dla „The Guardian": „We would know what kinds of messaging you'd be susceptible to... and then how many times did we need to touch you with that in order to change how you think about something".

Facebook, który zapewnił GSR i CA warunki do przeprowadzenia swoich badań, dowiedział się o transakcji między obiema firmami dopiero w 2015 r. Reakcją była blokada aplikacji Dr. Kogana i żądanie wysunięte do obu firm, aby te usunęły uzyskane w ten sposób dane oraz zapewniły pisemnie FB o wykonaniu polecenia. Informację tę potwierdził Mark Zuckerberg w poście z dn. 21 marca 2018 r. [9]. Nie przeprowadzono żadnych audytów ani nie zażądano audytu wewnętrznego ani od GSR, ani od CA, co może pobudzać do myślenia na temat roli FB w tym przedsięwzięciu. Niezależnie od certyfikatów otrzymanych od GSR i CA, dane uzyskane za pośrednictwem aplikacji MyDigitalLife miały zostać wykorzystane w prezydenckiej kampanii wyborczej w 2016 r. w USA, wspierając tym samym kandydatów partii republikańskiej – Teda Cruza i Donalda Trumpa. Rewelacje te ujawniły media 17 marca 2018 r.: „The New York Times", Channel 4 News i „The Guardian", opierając się w swych artykułach na słowach byłych pracowników CA oraz dokumentach i mailach dostarczonych za ich pośrednictwem. Reakcją portalu społecznościowego była blokada usług dla CA oraz wymóg przeprowadzenia audytu zewnętrznego przez firmę wybraną przez FB. Otwartym pytaniem pozostaje kwestia tego, dokąd dalej mogły powędrować dane osobowe uzyskane przez CA. Pojawiają się tropy wskazujące na kontakty w tej sprawie z prywatną firmą Palantir Technologies, ściśle współpracującą z władzami USA – chociażby w sprawach dotyczących bezpieczeństwa (terroryzm, przestępstwa finansowe) [8]. Tego typu pytania są tym bardziej zasadne, że CA była głównym bohaterem także innych afer, w tym o wymiarze międzynarodowym. Świadczą o tym cytowane już tajne nagrania udostępnione przez Channel 4 News, na których to kierownictwo CA (A. Nix, M. Turnbull i Dr. A. Taylor) przechwala się swoimi dokonaniami w dziedzinie prowadzenia kampanii wyborczych na innych kontynentach (Afryka, Azja, Europa), jak i narzędzi, które im w tym służą, a które z praworządnością i moralnością nie mają nic wspólnego (dyskredytacja za pomocą ustawianego wręczania łapówek czy korzystania z podstawionych prostytutek). CA (a dokładnie kanadyjska firma będąca prawdopodobnie przykrywką dla CA) podejrzewana jest również o nielegalny (brytyjskie prawo wyklucza udział zagranicznych firm w kampaniach politycznych) udział w kampanii dotyczącej referendum w sprawie Brexitu. Informację tę przedstawił w wywiadzie dla Channel 4 News Shamir

Sanni [24]. W tej sprawie przed brytyjską komisją parlamentarną byli przesłuchiwani kolejno A. Nix i Ch. Wylie, na których słowa powoływano się we wcześniejszej części artykułu.

Facebook wobec współczesnych zagrożeń dla danych osobowych

Przedstawiwszy wydarzenia, które stały się dla niniejszego artykułu koronnym przykładem współczesnych zagrożeń dla ochrony danych osobowych, przejdziemy teraz do zagadnień prawnych, zaczynając od regulacji wewnętrznych FB. Wydarzenia wyżej opisane są doskonałym papierkiem lakmusowym dla tych regulacji. Sprawdzimy, na udostępnianie jakich informacji zgadzają się użytkownicy, w jaki sposób FB chroni swych użytkowników przed powtórką wydarzeń sprzed lat, a w końcu odpowiemy na pytanie, gdzie popełniono błędy ze strony portalu społecznościowego i co można było zrobić, aby temu zapobiec.

Już w Zasadach Facebooka [26], będących swoistą konstytucją tego portalu, możemy przeczytać, jakoby jego użytkownicy mieli prawo do własności i kontroli nad informacjami. Oznacza to, że udostępniają oni swoje treści tym podmiotom, którym chcą. Kolejne informacje na temat praw do ochrony danych osobowych użytkowników FB uzyskujemy za pośrednictwem regulaminu portalu [11]. Znajdziemy w nim potwierdzenie wyżej zacytowanego prawa do kontroli nad informacjami, które głosi, jakoby administrator gromadzący dane od użytkowników musiał uzyskać ich zgodę, poinformować, że to on, a nie FB, tego dokonuje oraz powiadomić zainteresowanych o danych, jakie pobiera, oraz sposobie, w jaki zostaną one wykorzystane [11, art. 7, ust. 5]. Dodatkowo dodaje się do tego zakaz gromadzenia danych o użytkownikach za pomocą narzędzi automatycznych bez zezwolenia FB [11, art. 3, ust. 2] oraz zakaz działalności niezgodnej z prawem lub wprowadzającej w błąd [11, art. 3, ust. 9]. O ochronie danych osobowych mówią także regulacje dotyczące aplikacji [1]. Zakazują one przesyłania informacji uzyskanych za pomocą aplikacji do stron trzecich, jak i nakazują, aby w przypadku, gdy pobiera się dane od przyjaciół osoby, która zainstalowała aplikację, uzyskać od nich zgodę [1, art. 3, ust. 10 i 14].

W tym momencie wypada zapytać, jak to się ma do wydarzeń związanych z CA i GSR. Można zaryzykować stwierdzenie, że wiele z ww. regulacji zostało naruszonych przez obie firmy.

Aplikacja MyDigitalLife została utworzona w celach naukowych, a informacje uzyskane za jej pośrednictwem miały wspomóc badania Dr. A. Kogana nad zachowaniami ludzi w mediach społecznościowych. Dr Kogan uzyskał na to pozwolenie FB, a osoby, które zainstalowały aplikację, musiały wyrazić zgodę na wgląd w ich dane (polubienia, zmiany statusu, informacje z profilu, posty na ścianie, a nawet prywatne wiadomości) przez feralną aplikację. Problem zaczyna się w tym miejscu, bowiem – jak się okazało – aplikacja pobierała dane nie tylko od osoby, która ją zainstalowała, ale i od jej przyjaciół. W ten sposób pozyskiwano informacje od osób, które były kompletnie tego nieświadome i tym samym nie wyraziły na to zgody. W momencie, o którym mówimy (rok 2013), było to wciąż jeszcze możliwe; dopiero rok później FB wprowadził nowe zabezpieczenia, które uniemożliwiały podobny proceder (przyjaciele od teraz musieli zezwolić tego typu aplikacjom na pobranie ich danych). Wskazuje na to post M. Zuckerberga z 21 marca [9]. Z jednej strony wypada niewątpliwie pogratulować kierownictwu FB za taką reformę, która sprawiła, że GSR i CA uzyskały dane 50 mln osób, a nie 500 mln (bo nie zdążyły), a z drugiej strony zapytać – z punktu widzenia osoby, która zna skutek tego przeoczenia – jak mogło dojść do takiego zaniedbania. Czy osobom odpowiadającym w FB za legislacje nie były znane zasady prawne typowe dla cywilizowanego świata, w którym to powszechnie zakłada się, że przetwarzanie danych osobowych jest możliwe jedynie za zgodą osoby, której one dotyczą? Taki zapis prawny obecny jest chociażby w polskiej ustawie o ochronie danych osobowych z dn. 29 sierpnia 1997 r.: art. 23, ust. 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. A może osoby te nie wiedziały, w jaki sposób działa ta aplikacja? Wobec tego na podstawie jakiej wiedzy zezwolono na jej wprowadzenie do platformy FB? Kolejne pytanie brzmi: czy nikt wcześniej nie był w stanie zauważyć, że aplikacja Dr. Kogana uzyskała dostęp do niebotycznej ilości danych, skoro, wedle Facebook Platform Policy, portal ma prawo do przeprowadzenia audytu w podejrzanej firmie, która udostępniła aplikację, jak i do tego, aby zbadać, co robi dana aplikacja, do jakich danych ma dostęp, a w końcu i wymusić na niej odpowiednie działania [1, art. 6, ust. 2, 8, 15 i 16]? Samo posiadanie danych o znaczącej wartości liczebnej nie jest nielegalne, lecz winno z pewnością obudzić czujność FB i spowodować przynajmniej prewencyjną reakcję.

Mimo posiadania odpowiednich narzędzi i praw do ich użycia do niczego takiego nie doszło. A FB rzekomo miał się dowiadywać o poczynaniach GSR i CA z gazet, odpowiednio wtedy na nie reagując (blokada aplikacji, nakaz usunięcia uzyskanych danych). Po raz kolejny reakcja FB wskazuje bądź na nieudolność, bądź na złą wolę, skoro po uzyskaniu wiedzy w 2015 r. o nielegalnej wymianie danych między GSR a CA pojawił się nakaz usunięcia danych przez obie firmy, wraz z pisemnym potwierdzeniem wykonania polecenia. Jak widać, wystarczającym dowodem na usunięcie danych pobranych z 50 mln kont FB może być kartka papieru to potwierdzająca. Spójrzmy na wypowiedź Ch. Wylie dla Channel 4 News: „– Did they check that you deleted the data? – No they were just satisfied with the form". Pierwsze poważne kroki (nakaz przeprowadzenia audytu zewnętrznego) podjęto wraz z ukazaniem się artykułów prasowych z dnia 17 marca 2018 r., które twierdziły, jakoby CA wciąż korzystało z tych danych, a wcześniej używało ich do przeprowadzenia kampanii D. Trumpa. W ten sposób widzimy, że FB działał jedynie wtedy, kiedy znajdował się w medialnych reflektorach i podejmował wymuszone kroki, które zmyłyby z niego przynajmniej część winy. Tak ogromna nieporadność FB może rodzić pytania, czy aby przypadkiem portal nie wiedział już wcześniej o działaniach podejmowanych przez CA. W takim przypadku działania FB zmierzające do ukrócenia tej nielegalnej działalności byłyby jedynie wymuszane przez prasę i przybierały formę możliwie najłagodniejszą, dopóki sytuacja na to pozwalała. Jednakże pojawia się w tym pewien zgrzyt na polu ideologicznym, gdyż trudno wyobrazić sobie, aby kierownictwo FB, które jest bardziej tożsame z liberalnymi poglądami, wspierało jawnie prawicową organizację analityczną, za którą stali tacy ludzie, jak S. Bannon i R. Mercer, czyli osoby bliskie D. Trumpowi. Z drugiej strony można założyć, że wśród szanujących się biznesmenów pieniądz jest pieniądzem, niezależnie od jego proweniencji politycznej. Facebook jako portal w pełni darmowy musi się z czegoś utrzymywać. Oficjalnie służą temu reklamy, nieoficjalnie – dostęp do ogromnej bazy danych i użytek z niej. B. Kaiser w wypowiedzi dla „The Guardian" stwierdził: „Corporation like Google, Facebook, Amazon, all of these large companies are making tens or hundreds of billions of dollars of monetizing people's data".

Kwestia wyżej poruszona jest o tyle istotna, że Facebook gromadzi bardzo dużo informacji na temat swoich użytkowników

(na co oczywiście zgadza się każdy zakładający swoje konto). Mówimy tu chociażby o aktywności członków społeczności na FB: profili i stron, jakie odwiedzają, czasie spędzanym na przeglądaniu portalu, komentarzach czy polubieniach, a nawet zakupach dokonywanych za pośrednictwem portalu. FB otrzymuje również dostęp do zdjęć, wiadomości i siatek kontaktów swoich użytkowników. Z łatwością da się również sprawdzić lokalizację danej osoby, chociażby za pośrednictwem języka, jakiego używa w swoim systemie komputerowym, jego strefy czasowej, metadanych załączanych zdjęć zawierających lokalizację (plik exif) czy po prostu za pomocą adresu IP, sygnału GPS lub lokalizacji Wi-Fi [25]. Co ważne, wyżej wymienione dane nie dotyczą tylko samego FB, ale i firm z nim powiązanych, takich jak: Instagram, WhatsApp, Moves [17].

Nie dziwią wobec powyższego starania niektórych firm analitycznych/marketingowych czy politycznych o uzyskanie dostępu do niemalże niewyczerpywalnej skarbnicy wiedzy, jaką jest Facebook. Wedle danych ze stycznia 2018 r. liczba użytkowników FB przekroczyła już 2,10 mld osób [7]! Dane te stanowić mogą doskonały sposób na zbadanie czyichś poglądów, preferencji, a nawet, jak pokazuje to e-mail z CA, zagłębienie się w psychikę osób i odkrycie ich charakteru, żądz i strachu, a następnie odpowiednie wykorzystanie tej wiedzy w przeprowadzeniu takiej kampanii medialnej, która sprawi, że określona grupa osób kupi produkt lub zagłosuje na odpowiedniego kandydata. Co ponadto zwiększa wartość tego typu zbioru danych to fakt, że – po uzyskaniu do nich dostępu – trudno wyśledzić, kto jeszcze miał do nich dostęp. Przykład CA i GSR pokazuje nam, że trwać to może nawet dwa lata, a i tak wciąż pozostają wątpliwości, komu jeszcze CA użyczyła pozyskanego zbioru danych. Afera z Cambridge Analytica raz jeszcze daje przykład tego, że walne bitwy w świecie współczesnej polityki są rozgrywane już od kilku lat na arenie mediów społecznościowych i przy użyciu technik Big Data, a nie – jak było to do tej pory – na wiecach, przemarszach czy w telewizji. Te ostatnie stają się jedynie potwierdzeniem dominacji uzyskanej na innym polu.

Facebook niemniej zastrzega, że – zapewniając dostęp do swoich danych firmom reklamowym czy instytucjom naukowym – anonimizuje je. Jednakże nawet wówczas, gdy nie mamy możliwości odkrycia, kim jest dokładnie dana osoba (z imienia i nazwiska), to wciąż mamy (my jako firma posiadająca te dane) wgląd w jej prywatność (odwiedziny stron, polubienia). Załóżmy, że posiadamy taką wiedzę o milionie obywateli Polski; ich sposób myślenia za pośrednictwem algorytmów jest nam znany, a dzięki temu możemy używać w stosunku do nich skutecznych technik perswazyjnych – czy to do celów marketingowych (zgodnie z prawem FB), czy politycznych (niezgodnie z prawem FB). W przeszłości działań tego typu było znacznie więcej; przykładem może być Internet Research Agency, firma z siedzibą w Petersburgu, ewidentnie związana z FSB i GRU – jej pracownicy, udając blogerów – tworzyli fałszywe konta w portalach społecznościowych i rozpisywali się między innymi o heroizmie rosyjskich żołnierzy w Syrii. Jednak poziom automatyzacji procesów wynikających z metod wykorzystanych przez CA, pozwalających na oddziaływanie na znacznie większe populacje, wnosi przedmiotowe działania na zupełnie inny, nieznany do tej pory, poziom.

RODO wobec współczesnych zagrożeń dla danych osobowych

Tak jak wyżej wzmiankowane uregulowania prawne Facebooka zauważają aktualne zagrożenia związane z przetwarzaniem danych osobowych i dają narzędzia do ich ochrony, tak i RODO, jak niżej zostanie to przedstawione, wychodzi im naprzeciw.

Dostrzega się, że w dobie wszechobecnego Internetu, którego nie można wpisać w granice wyłącznie jednego państwa, podmioty zarządzające danymi osobowymi obywateli UE mogą znajdować się poza europejskim kontynentem. W ten sposób, jak głosi art. 3, ust. 2: rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii, przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii. Co prawda w przypadku FB problem ten nie występuje, gdyż otworzono swoje filie również w Europie (w tym w Polsce), jednakże przepis ten dowodzi, że prawodawca zdaje sobie sprawę, że obecnie chodzi nie tyle o miejsce, w którym znajduje się firma gromadząca i przetwarzająca dane, co o osoby, których te dane dotyczą, a które mogą być oddalone setki, jeżeli nie tysiące, kilometrów od miejsca, w których te informacje się gromadzi. Jest to modernizacja istotna, zważywszy na fakt, że polska ustawa o ochronie danych osobowych nie dotyczy podmiotów, które nie mają filii na polskim terytorium, co się zmieniło wraz z wejściem w życie RODO. Należy zaznaczyć, że Cambridge Analytica ma swoją europejską placówkę w Wielkiej Brytanii, która jest w fazie opuszczania wspólnoty europejskiej.

Osobną kwestią jest możliwość egzekwowania przepisów w stosunku do podmiotów spoza UE. W wyżej omawianej sytuacji dotyczącej GSR i CA ważnym zagadnieniem była także zgoda osoby na pobieranie z jej profilu danych osobowych. W jaki sposób reguluje tę kwestię RODO? Definiując zgodę, twierdzi się, że winna ona oznaczać dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Ponadto art. 6, ust. 1 rozwija ten problem, uznając, że przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów. Ponadto podmiot pragnący uzyskać czyjeś dane osobowe musi zapewnić odpowiednie warunki do zapoznania się z warunkami, na jakich dane te będą gromadzone i przetwarzane oraz utworzyć taki mechanizm uzyskiwania zgody, aby następnie zgoda ta mogła stanowić dowód na wykonanie tej czynności. Zagadnienie to reguluje art. 7, ust. 1, mówiąc: „Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych".

Użytkownicy aplikacji MyDigitalLife zostali opłaceni i wyrazili zgodę na przetwarzanie ich danych osobowych. Jednakże wydaje się, że zasada świadomości przy wyrażaniu zgody nie została w pełni zachowana. Wedle słów Ch. Wylie żaden z użytkowników tej aplikacji miał nie zdawać sobie sprawy z tego, że dane będą pobierane nie tylko od niego (na co wyrażał zgodę), ale i od jego przyjaciół. Na gromadzenie danych od przyjaciół nie wyraziły zgodę ani osoby, które instalowały tę aplikację (po prostu nie były tego świadome), ani owi przyjaciele, którzy nawet nie zdawali sobie sprawy, że GSR gromadzi o nich informacje, a więc tym bardziej nie mogły wyrazić na to zgody. Wobec tego cała ta sprawa wykazuje się cechami złamania prawa (obecnego, lecz nie ówczesnego, gdyż FB w tamtych latach nie regulował tej kwestii) już u swego podłoża, a nie doszliśmy jeszcze do udziału w tym wszystkim CA.

Kolejną istotną kwestią, którą warto poruszyć w niniejszym artykule, są dane osobowe, które posiadały GSR i CA, oraz cele, w jakich miały im służyć. Art. 9, ust. 1 zaznacza, że zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych. Z kolei art. 9, ust. 2 odnosi się do ust. 1, uznając, że nie ma on zastosowania, jeżeli spełniony jest jeden z poniższych warunków: a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach.

Ta regulacja jest ciekawa, bowiem GSR i CA uzyskały dostęp do między innymi takich danych, jak: polubienia czy informacje profilowe. Jak pokazała to korespondencja między Dr. Koganem a Ch. Wylie, opublikowana przez „The New York Times", dane, jakie posiadały obie firmy, umożliwiały im poznanie zarazem przekonań religijnych, poglądów politycznych i światopoglądowych, jak i orientacji seksualnej czy pochodzenia rasowego i etnicznego. [12]. Oczywiście były to przewidywania, mniej lub bardziej trafne, a nie jasne informacje na ten temat uzyskane za pośrednictwem tych osób. Niemniej w części przypadków efekt analizy musiał zgadzać się z rzeczywistością, niezależnie od tego, jak podchodzimy do skuteczności Big Data. Czy zatem osoby, od których uzyskano dane, wyraziły zgodę na przetwarzanie informacji o swoich poglądach politycznych, światopoglądowych itd.? Użytkownicy MyDigitalLife niewątpliwie wyrazili zgodę na dostęp do swoich informacji profilowych i polubień, ale czy zdawali sobie sprawę z tego, że tego typu informacje posłużą za przesłanki umożliwiające wyciągnięcie tego typu wniosków? Czy w ogóle spodziewali się, że aplikacja utworzona przez wykładowcę Cambridge będzie dążyć do pozyskania takich informacji, niezależnie od tego, czy byłoby to możliwe za pośrednictwem tych czy innych przesłanek? Odpowiedzi nasuwają się same. Ponadto widać tu rozbieżności między regulacjami FB a RODO. FB nie wspomina ani słowem o zakazie przetwarzania tego typu wrażliwych danych osobowych. Spodziewać się można, że w przyszłości zostaną na nich wymuszone zmiany w tym zakresie, zważywszy na przewidywaną przez RODO karę pieniężną w wysokości 20 mln euro lub 4% rocznego dochodu przedsiębiorstwa, co – *notabene* – jest kolejną ważną zmianą, gdyż do tej pory taka możliwość sankcji nie istniała, a miejmy nadzieję, że spełni ona swoją funkcję odstraszającą.

Kolejny z warunków, o którym mowa w art. 9, ust. 2, głosi, że art. 9, ust. 1 traci moc prawną również, gdy: przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą. Jest to kolejna zagadka prawna do rozwiązania przez praktykę sądową oraz komentarze prawne, niemniej warto tutaj podkreślić wątpliwość tego, co jest w sposób oczywisty upubliczniony, a co nie jest. O ile informacje profilowe można uznać za upublicznione w sposób oczywisty, chociażby z tego powodu, że przeglądać je może (przeważnie) osoba niemająca konta na Facebooku, o tyle już wcześniej wspomniane polubienia, które okazały się tak istotne przy profilowaniu, są już większym problemem do zrozumienia.

Co ważne, w RODO pojawia się termin profilowania, do tej pory nieobecny w polskim prawie. Można uznać to za kolejny przejaw pójścia z duchem czasu przez europejskich prawodawców. Wydaje się, że nie należy uznawać je za upublicznione w sposób oczywisty z jednego ważnego powodu. Mianowicie, polubienia są co prawda widoczne dla wszystkich użytkowników FB (dla tych niemających kont, wtedy gdy zostały użyte na profilach o charakterze publicznym), ale brak fizycznej możliwości (która obyłaby się bez użycia zautomatyzowanych procesów), aby osoba zainteresowana ich pozyskaniem potrafiła dotrzeć do wszystkich. Mówimy więc tu o ogromnej czasochłonności takiego procesu, który sprawiłby, że stałby się on nieopłacalny.

Kolejne uchylenia zauważymy, zestawiając wydarzenia powiązane z GSR i CA z art. 13, ust. 1, który głosi: jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:... e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją. Regulacja ta tyczy się wymiany danych osobowych między GSR a CA. GSR o przekazaniu danych do CA oczywiście nie poinformowało użytkowników swojej aplikacji, gdyż w innym przypadku Facebook dowiedziałby się o tym wcześniej, a nie dopiero w 2015 r. za pośrednictwem mediów. Ponadto samo przekazanie danych stronie trzeciej było sprzeczne z ówczesnymi wewnętrznymi regulacjami FB, co może stanowić formę wytłumaczenia, dlaczego tego nie uczyniono. Jest to kwestia ważna, ponieważ nie wiedząc, gdzie przetwarzane są dane osobowe danej osoby, nie może ona powołać się na swoje prawa wynikające z art. 15–22. Tym samym jej prawa stają się martwe, a jedyną nadzieją staje się reakcja administratora (w tym wypadku FB, o którego możliwościach w tej materii pisano na wcześniejszych stronach) lub organu nadzorczego. Stąd ich reakcja w 2015 r. Podobnie podchodzi do tego RODO, stwierdzając w art. 27, ust. 2, że podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora.

Uprawnienia organu nadzorczego, mającego stać na straży przestrzegania RODO, zostały w rozporządzeniu opisane dość szczegółowo w art. 58 i można je podzielić na działania prewencyjne oraz działania następcze (podjęte po stwierdzeniu naruszeń). Interesować nas będą wyłącznie czynności prewencyjne, które mogły potencjalnie zapobiec nieszczęściu związanemu z GSR i CA.

Art. 58, ust. 1 (dotyczący działań prewencyjnych) stanowi, jakoby każdy organ nadzorczy mógł żądać potrzebnych mu informacji od administratora i podmiotu przetwarzającego lub ich przedstawiciela. Ponadto może przeprowadzać audyty (tego zabrakło w reakcji FB w 2015 r.), zawiadamiać administratora lub podmiot przetwarzający o naruszeniu RODO, uzyskiwać dostęp od administratora lub podmiotu przetwarzającego do danych osobowych przez nich posiadanych oraz do wszelkiego sprzętu używanego przez oba podmioty do przetwarzania danych osobowych.

Biorąc pod uwagę wydarzenia, które służą za przykład współczesnych zagrożeń, można powiedzieć, że najważniejszym prawem organu nadzorczego jest prawo do audytu i powiązanego z nim prawa do korzystania z urządzeń służących przetwarzaniu danych osobowych przez kontrolowane podmioty. A więc mówimy o działaniach kontrolnych, mających na celu sprawdzenie, czy czynności podejmowane przez kontrolowanych są zgodne z prawem, któremu podlegają. Wydaje się, że organ nadzorczy może podjąć taką czynność ze swojej własnej inicjatywy, nawet gdy brak informacji, jakoby administrator lub podmiot przetwarzający mogli złamać prawo. Ale przy założeniu, że organ nadzorczy nie dowiedziałby się wpierw o nieprawidłowościach względem przetwarzania danych osobowych w GSR lub CA, szansa na to, że podjąłby działania ze swojej własnej woli, przez

nikogo niepowiadomiony o ryzyku złamania prawa, jest bardzo niska. Ukazuje to nam rolę administratora (a więc FB) w ochronie danych osobowych. To on ma bezpośredni wgląd w to, komu zezwala na pozyskiwanie i przetwarzanie danych osobowych od swoich użytkowników, i tym samym powinien, jak już była o tym mowa, podjąć bardziej zdecydowane działania, nie wzbraniając się chociażby przed prewencyjnymi periodycznymi audytami zewnętrznymi skierowanymi przeciwko GSR. Skoro firma ta uzyskała tak olbrzymią bazę danych, tak wiele oczu winno być skierowanych na nią, aby zapobiec nieodpowiedniemu ich wykorzystaniu. Trudno wymagać takich działań od nowo powstałej małej firmy, lecz co innego, gdy mamy do czynienia z *de facto* monopolistą na rynku mediów społecznościowych, na którego platformie zarejestrowało się ponad 2 mld ludzi.

Zakończenie

Przyrównując współczesne metody marketingowe i propagandowe, polegające na profilowaniu i wykorzystywaniu tych danych do tworzenia odpowiednich przekazów, do tradycyjnej propagandy, łatwo zauważyć, że trudniej jest spostrzec próbę manipulacji, surfując w Internecie i przeglądając dziesiątki, jeżeli nie setki, filmów, zdjęć i stron zawierających w sobie mniej lub bardziej ukryty przekaz. Należy się jednak zastanowić, czy aby przypadkiem problem, z którym mamy tutaj do czynienia, nie jest czymś, z czym mamy styczność od momentu upowszechnienia się mediów. Kwestia bańki informacyjnej to nie tylko problem Internetu, którego algorytmy podsuwają treści, które się nam spodobają, ale i samej ludzkiej psychiki. Dysonans poznawczy to stan psychiczny, którego nasz umysł unika za wszelką cenę i to przez to osoba o poglądach konserwatywnych lub liberalnych zazwyczaj nie sięgnie po media (prasa, TV) wykazujące się sprzecznymi poglądami na dany temat. Jednakże porównując media tradycyjne (prasa, TV) z nowoczesnymi (Internet), łatwo dostrzec, że o ile prasa i telewizja mają obecnie dość ograniczony zasięg odbiorców i krótki czas oddziaływania, o tyle Internet jest w tym względzie ograniczony jedynie wolą człowieka, który decyduje, ile czasu pragnie poświęcić na użytkowanie Internetu. Dla przykładu dziennik „Gazeta Wyborcza" posiada nakład w wysokości 190 tys. [5]. Z kolei stacja TVN, ciesząca się największą oglądalnością swoich programów informacyjnych, może liczyć na 3,16 mln widzów [4]. Tym bardziej więc powinniśmy dołożyć wszelkich starań, zarówno ze strony prawnej, jak i szarego użytkownika Internetu, aby uchronić nasze dane osobowe przed nielegalnym pozyskiwaniem i przetwarzaniem w celach, na które wielu nie mogłoby się zgodzić, gdyby tylko zostali o tym skutecznie poinformowani. O ile regulacje prawne, zarazem ze strony FB, jak i państw (RODO), są obecnie przystosowane lub szybko przystosowują się do nowych zagrożeń dla danych osobowych, jak można było zauważyć na poprzednich stronach, o tyle sami ludzie wciąż nie zdają sobie sprawy z zagrożenia, jakie wynika z korzystania ze zbiorów danych osobowych pozyskanych w Internecie. Wnioski, jakie można wyciągnąć na podstawie kilkudziesięciu polubień czy informacji profilowych z FB, sprawiają, że osoby, których się to tyczy, stają się na poły zwierzętami hodowlanymi w rękach firm posiadających wiadomości na ich temat. Mniejszy problem z tego wynika, gdy w efekcie tego kupią produkt, na który w świecie poza Internetem nawet nie zwróciliby uwagi. Problem staje się istotny, gdy manipulacja umysłami i sercami ludzkimi staje się narzędziem w walce politycznej. Jak wiemy, to nic nowego. Jednakże skala i potencjalna skuteczność tego procederu przeraża.

Bibliografia:

1. *Facebook Platform Policy*: https://developers.facebook.com/policy (dostęp: 02.04.18).
2. Fragment przesłuchania A. Nixa przed brytyjską komisją parlamentarną: *Cambridge Analytica boss under fire from MPs*: https://www.youtube.com/watch?v=u5aQgS2Uh1M (dostęp: 01.04.18).
3. Fragment wywiadu S. Bannona dla CBS News: Bannon S., *Let's talk about Cambridge Analytica*: https://www.youtube.com/watch?v=fiJPUFF7ZWw (dostęp: 01.04.18).
4. http://www.wirtualnemedia.pl/artykul/ogladalnosc-programow-informacyjnych-luty-2018-wydarzenia-wyprzedzily-wiadomosci (dostęp: 01.04.18).
5. https://www.prasaplus.pl/ titlesReports/titleReport/6431/11/8 (dostęp: 01.04.18).
6. Mayer J., *The reclusive hedge-fund tycoon behind the Trump presidency*: https://www.newyorker.com/magazine/2017/03/27/the-reclusive-hedge-fund-tycoon-behind-the-trump-presidency (dostęp: 01.04.18).
7. *Most famous social network sites worldwide as of January 2018, ranked by number of active users (in millions)*: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (dostęp: 02.04.18).
8. O'Sullivan D., *Facebook whistleblower says more companies had access to user data*: http://money.cnn.com/2018/03/27/technology/palantir-cambridge-analytica-facebook-peter-thiel/index.html (dostęp: 01.04.18).
9. Post Marka Zuckerberga z dn. 21 marca 2018 r.: https://www.facebook. com/zuck/posts/10104712037900071 (dostęp: 01.04.18).
10. Przesłuchanie Ch. Wylie przed brytyjską komisją parlamentarną: *Cambridge Analytica whistleblower Christopher Wylie appears before Mps*: https://www.youtube.com/ watch?v=X5g6IJm7YJQ (dostęp: 01.04.18).
11. *Regulamin Facebooka*: https://www.facebook.com/legal/terms (dostęp: 02.04.18).
12. Rosenberg M., Confessore N., Cadwalladr C., *How Trump Consultants Exploited the Facebook Data of Millions*: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (dostęp: 01.04.18).
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)*: https://giodo.gov.pl/pl/ 569/9276 (dostęp: 03.04.18).
14. Strona główna SCL Group: https://sclgroup.cc/home (dostęp: 01.04.18).
15. Tajne nagrania Channel 4 News: *Cambridge Analytica Uncovered: Secret filming reveals election tricks*: https://www.youtube.com/watch?v=mpbeOCKZFfQ (dostęp: 01.04.18).
16. Tajne nagrania Channel 4 News: *Cambridge Analytica: Undercover secrets of Trump's Data Firm*: https://www.youtube.com/watch?v=cy-9iciNF1A (dostęp: 01.04.18).
17. *Wykaz firm należących do Facebooka*: https://www.facebook.com/help/ 111814505650678 (dostęp: 03.04.18).
18. Wywiad A. Kogana dla BBC Radio 4: *Aleksander Kogan – interview BBC Radio 4*: https://www.youtube.com/watch?v=vvtCNPnQtnY (dostęp: 01. 04. 18).

19. Wywiad A. Nix dla BBC Newsnight: *Exclusive: Alexander Nix – BBC Newsnight*: https://www.youtube.com/watch?v=bTE-JuLY1pW0 (dostęp: 01.04.18).
20. Wywiad B. Kaiser dla „The Guardian": *Britanny Kaiser, former Cambridge Analytica director: „I voted for Bernie"*: https://www.youtube.com/watch?v=krY8DW3V2NU (dostęp: 01.04.18).
21. Wywiad Ch. Wylie dla Channel 4 News: *Cambridge Analytica: Whistleblower reveals data grab of 50 million Facebook profiles*: https://www.youtube.com/watch?v=zb6-xz-geH4 (dostęp: 01. 04. 18).
22. Wywiad Ch. Wylie dla „The Guardian": *Cambridge Analytica whistleblower: We spent $1 harvesting millions of Facebook profiles*: https://www.youtube.com/watch?v=FXdYSQ6 nu-M (dostęp: 01.04.18).
23. Wywiad M. Zuckerberga dla CNN: *Mark Zuckerberg Full Interview with CNN*: https://www.youtube.com/watch?v=v18dGTpzUCM (dostęp: 01.04.18).
24. Wywiad z Shamir Sanni dla Channel 4 News: *Brexit campaign was „totally illegal", claims whistleblower*: https://www.youtube.com/watch?v=nQ0bFAgTGwk (dostęp: 03.04.18).
25. *Zasady dotyczące danych*: https://www.facebook.com/about/privacy (dostęp: 02.04.18).
26. *Zasady Facebooka*: https://www.facebook.com/principles.php (dostęp: 02.04.18).

Modern threats to the processing of personal data in the context of EU General Data Protection Regulation and the case Facebook – Cambridge Analytica

The article presents contemporary threats resulting from the processing of personal data in computer systems using Big Data techniques on the example of an event with the largest in recent years weight – Facebook – Cambridge Analytica case. Thanks to the disclosure of the case, the public opinion received information about the methods used in the processing of personal data, their potential effectiveness in business and political marketing as well as the scale and ease of access to them. What for many years was obvious to every Internet user, that a lot of small pieces of information about his activity is collected by suppliers of various types of services has become a matter of course. However, users now get information what, by consolidating data from several major tycoons, thanks to the huge computing power commonly available, Big Data techniques, machine processing and artificial intelligence can be done with them. How seriously the behavior and attitudes of the data subjects can be influenced. It frightened both ordinary citizens and governments. The article is an attempt to answer whether the EU General Data Protection Regulation is able to respond to new threats.

Kewords: personal data, European Union, data protection, Facebook, Cambridge Analytica.

Autorzy:
Tomasz Klepacz – Społeczna Akademia Nauk w Warszawie, Wydział Nauk o Zarządzaniu i Bezpieczeństwie
dr **Władysław Przyjemski** – Społeczna Akademia Nauk w Warszawie, Wydział Nauk o Zarządzaniu i Bezpieczeństwie