JOURNAL OF MODERN SCIENCE

3/63/2025

www.jomswsge.com

DOI: 10.13166/jms/209327

MONIKA NOWIKOWSKA

War Studies University, Warsaw, Poland

ORCID iD: 0000-0001-5166-8375

MATEUSZ KOZŁOWSKI

University of Technology and Economics, Warsaw, Poland

ORCID iD: 0009-0005-6899-0244

ANALIZA WYBRANYCH ZAGROŻEŃ DLA TOŻSAMOŚCI CYFROWEJ WYNIKAJĄCYCH Z POSTĘPU TECHNOLOGICZNEGO

ANALYSIS OF SELECTED THREATS TO DIGITAL IDENTITY FROM TECHNOLOGICAL ADVANCES

Abstract

The article aims to provide an overview of the evolution of digital identity online and the challenges to its protection arising from the development of new technologies. This issue has not yet been discussed in depth in the literature. The authors aim to establish the role played by digital identity in the economy based on new technologies. This is an important and difficult issue, because in addition to the many benefits of using digital identity in the virtual world, one can also point out many challenges and risks associated with it, such as: identity theft, violation of individual privacy online, unlawful use of image. The authors identified and discussed examples of threats to digital identity, such as deepfake, phishing, vishing, smishing, and security of e-government services.

Keywords: *digital identity, new technologies, identity theft, e-government, deepfake*

Streszczenie

Artykuł ma na celu przybliżenie ewolucji tożsamości cyfrowej w sieci oraz wyzwań dla jej ochrony wynikających z rozwoju nowych technologii. Zagadnienie to nie było dotąd przedmiotem pogłębionych rozważań w literaturze przedmiotu. Autorzy stawiają sobie za cel ustalenie roli, jaką odgrywa tożsamość cyfrowa w gospodarce opartej na nowych technologiach. Jest to zagadnienie ważne i trudne, ponieważ obok licznych korzyści wynikających z wykorzystywania tożsamości cyfrowej w świecie wirtualnym, można wskazać także na wiele wyzwań i zagrożeń z nią związanych, takich jak: kradzież tożsamości, naruszenie prywatności jednostki w sieci, bezprawne wykorzystanie wizerunku. Autorzy wskazali i omówili przykładowe zagrożenia dla tożsamości cyfrowej, takie jak: *deepfake*, *phishing*, *vishing*, *smishing*, czy bezpieczeństwo usług e-administracji.

Słowa kluczowe: *tożsamość cyfrowa, nowe technologie, kradzież tożsamości, e-administracja,* deepfake

Wstęp

Pojęcie tożsamości cyfrowej w Internecie jest obecne praktycznie od początku jego istnienia. Początkowe fazy rozwoju Internetu nie wymuszały tworzenia definicji lub regulacji w tym zakresie, ponieważ głównym celem powstania rozległej sieci Internet było połączenie ze sobą użytkowników na całym świecie, w szczególności w zakresie komunikacji i wymiany informacji (Dzierżyńska-Mielczarek, 2018, s. 76). Głównym udziałowcem w tej branży były uczelnie oraz duże korporacje. Użytkownicy indywidualni mieli dostęp do sieci jedynie w ograniczonym zakresie, a jednocześnie weryfikacja użytkowników pod kątem ich faktycznej tożsamości nie była kluczowa. Z biegiem lat sytuacja ta zaczęła się zmieniać, ponieważ postęp technologiczny spowodował, że pojęcie tożsamości w sieci stało się na tyle istotne, że konieczne okazało się wprowadzenie regulacji prawnych, które zdefiniują samo pojęcie oraz wprowadzą niezbędne mechanizmy, żeby ją chronić.

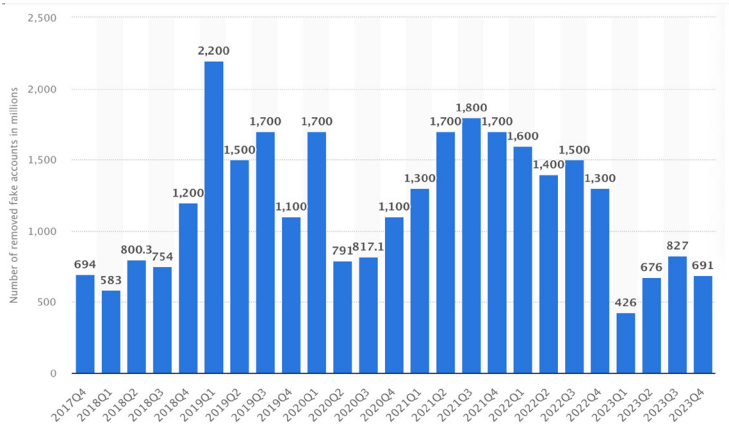
Początki Internetu w Polsce sięgają roku 1991, kiedy powstała Naukowa i Akademicka Sieć Komputerowa, zespół działający w ramach Uniwersytetu Warszawskiego, mający na celu przyłączyć Polskę do Internetu (NASK, 2024). Początkowo sieć ta służyła praktycznie wyłącznie do działalności naukowej, a użytkownicy indywidualni nie mieli do niej swobodnego dostępu (Markiewicz, 2016, s. 181). Sytuacja ta zaczęła się zmieniać w latach 1994–1996, kiedy to działalność rozpoczęły takie serwisy jak Wirtualna Polska oraz OptimusNet (aktualnie Onet). Początkowo serwisy te służyły do katalogowania stron www, żeby ułatwić użytkownikom dostęp do wiedzy. W 1996 r. Telekomunikacja Polska uruchomiła również powszechną usługę, która umożliwiła dostęp do Internetu dla użytkowników indywidualnych z wykorzystaniem modemu telefonicznego. Usługa ta jednak była dosyć kosztowna, co przekładało się na ograniczenie jej dostępności (Orange, 2024). Do tego momentu pojęcie tożsamości nie było kluczowe, ponieważ służyło głównie do weryfikacji wykorzystania usług, w celu rozliczenia należności. Sytuacja ta zaczęła się zmieniać pod koniec roku 1996, gdy firma Polbox Sp. z o.o. udostępniła możliwość założenia bezpłatnego konta poczty elektronicznej (Dziennik Internautów, 2024). Takie rozwiązanie pozwalało użytkownikom na komunikację między sobą ze spersonalizowanych adresów pocztowych, tj. *imie.nazwisko@domena.pl.* Był to pierwszy moment,

w którym możemy mówić o pojawieniu się tożsamości cyfrowej oraz zagrożeń z nią związanych. Korespondując z innym użytkownikiem, należało mieć na uwadze, że odbiorca nie posiadał wiedzy, kto jest po drugiej stronie, opierając się jedynie na zapisie imienia i nazwiska w adresie e-mail. Nie różniło się to jednak od tradycyjnej korespondencji papierowej, która również oparta była na posługiwaniu się danymi osobowymi (imię, nazwisko, adres) nadawcy (Taczkowska-Olszewska, 2019, s. 245).

Kolejnym ważnym zdarzeniem było powstawanie portali społecznościowych, takich jak: Facebook, YouTube, LinkedIn (Szydłowska, 2013, s. 38; Stachelek, Warszawa 2016, s. 244). Początkowo portale te zrzeszały małe grupy ludzi, jednak zyskując popularność, stawały się potęgą, a następnie podstawowym narzędziem do *zaistnienia* w sieci. Platformy te pozwalały umieścić na profilu nie tylko imię oraz nazwisko, ale również zdjęcie (Nowikowska, 2021, s. 315). Dane te nie podlegały weryfikacji, co pozwalało na kolejne, bardziej zaawansowane nadużycia. W momencie powstawania platform społecznościowych świadomość zagrożeń wynikających z kradzieży tożsamości nie była zbyt duża, a przeprowadzenie takiego ataku nie wymagało skomplikowanych przygotowań lub stosowania zaawansowanych metod (Przybysz, 2016, s. 231). Należy podkreślić, że platformy te nie są zobligowane do weryfikacji tożsamości użytkowników rejestrujących konta w ramach serwisu. Twitter był pierwszą platformą społecznościową, która w 2009 r. wprowadziła weryfikację kont (Świetlińska, 2024). W kolejnych latach podobne systemy weryfikacyjne w ramach samoregulacji wprowadziły inne platformy. Skalę problemu dotyczącą fałszywych kont na portalach społecznościowych wskazuje poniższy wykres, określający dane liczbowe kont usuniętych ze względu na podanie fałszywych danych.

Jak widać na poniższym wykresie, walka z fałszywymi tożsamościami jest procesem stałym, który wymaga dostosowywania metodologii do rozwoju technologii. Powyższy wykres prezentuje trend wzrostowy ze spadkami spowodowanymi wprowadzeniem nowych, skuteczniejszych mechanizmów wykrywających nadużycia. Jednak za każdym razem widać ponownie wzrosty, które wskazują na ciągły wyścig pomiędzy administracją serwisu a oszustami.

Wykres 1. *Statystyka kont usuniętych z platformy Facebook ze względu na podanie fałszywych danych*



Źródło: https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/ (data dostępu: 20.03.2025).

Pojęcie tożsamości cyfrowej

Badania nad tożsamością sięgają początków XX w. Pojęciem tym po raz pierwszy posłużyli się w 1905 r. Boris Sidis i Simon Goodhart (Sidis, Goodhart, 1905, s. 23). Tożsamość to względnie stabilna autoidentyfikacja jednostki, pozostawanie ze sobą w ciągłości, a także w relacji z innymi ludźmi, a więc w kontekście dwóch najważniejszych dla człowieka relacji: do kultury i komunikacji (Urych, 2022, s. 18). Słownikowe pojęcie *tożsamość* oznacza *w odniesieniu do pojedynczego człowieka: świadomość siebie, fakty, cechy, dane personalne pozwalające zidentyfikować jakąś osobę* (Słownik PWN). Rozwój nowych technologii spowodował, że obok tożsamości *tradycyjnej* rozwinęła się tzw. tożsamość cyfrowa, która odnosi się do tego, jak jednostka funkcjonuje w świecie wirtualnym. Wraz z rozwojem nowych technologii cyfrowych pojawiły się także takie pojęcia, jak *tożsamość online*, *e-tożsamość*, *tożsamość internetowa* czy *e-ID*. Brak legalnych definicji omawianych pojęć sprawia, że obowiązek konstruowania ich znaczenia ciąży w głównej mierze na doktrynie i judykaturze (Nowikowska, 2024, s. 27).

Przez *tożsamość online*, rozumie się całokształt indywidualnych cech, które użytkownik wykazuje w społeczności internetowej, będąc na stronach internetowych. Jako przykład można wskazać posługiwanie się prawdziwymi danymi (np. imię i nazwisko), pseudonimem lub awatarem (obraz graficzny) podczas korzystania np. z forów internetowych (Nowikowska, 2024b, s. 27).

Drugim pojęciem związanym z tożsamością jest *e-tożsamość*, zwana również *e-ID*, oznaczająca cyfrowy odpowiednik dokumentu tożsamości, na który składa się zestaw danych, potwierdzających *online* tożsamość użytkownika. Identyfikacja elektroniczna (e-ID) jest jednym z narzędzi zapewniających bezpieczny dostęp do usług *online* i umożliwiających bezpieczniejsze przeprowadzanie transakcji elektronicznych. Rozwiązania takie są stosowanie np. w sektorze bankowym, pozwalając na dokonywanie czynności *online*, np. zaciąganie kredytów bankowych.

Kolejnym stosowanym pojęciem jest *tożsamość internetowa*, przez którą rozumie się zespół cech jednostki pozwalających odróżnić ją od innych użytkowników w Internecie, np. na portalach społecznościowych, takich jak Facebook czy Instagram. Tożsamość internetowa tworzy się w wyniku dokonywania codziennych czynności, takich jak zakupy bądź płatności *online* (Jurek, Pękala, 2017, s. 106). Przedstawiciele doktryny akcentują negatywny wpływ Internetu na kształtowanie tożsamości jednostki, wskazując, że w sieci kreuje się swoje *ja*, które jest odmienne od tego w świecie rzeczywistym.

Podsumowując przeprowadzone rozważania, można stwierdzić, że na tożsamość jednostki w sieci składa się zespół cech (atrybutów), które pozwalają zidentyfikować, rozpoznać daną osobę. Ustalenie czyjejś tożsamości polega na rozpoznaniu specyficznych cech danej osoby, które odróżniają tę osobę od innych (Chałubińska-Jentkiewicz, Nowikowska, 2020, s. 60). Podstawową funkcją tożsamości jest identyfikowanie osoby na podstawie posiadania określonej liczby atrybutów. Na tak rozumiane definicje składają się dwa elementy: zespół cech (atrybutów) jednostki oraz rozpoznawalność. W aspekcie cech pozwalających odróżnić jednostkę od innych osób R. Coomaraswamy trafnie podkreśla, że tożsamość nie jest ze swej istoty niezmienna, bowiem jest kompozytem składającym się z wielu samodzielnych, często konkurujących, sprzecznych i podlegających transformacji kryteriów. Jako przykład specyficznych cech, które kształtują tożsamość jednostki, można wskazać miejsce

i datę urodzenia, kolor włosów, numer dowodu osobistego, numer PESEL. Niektóre z tych cech nigdy się nie zmieniają, np. data urodzenia, jednak część z nich może ulec zmianie, np. numer dowodu osobistego.

Analiza wybranych zagrożeń dla tożsamości cyfrowej

Tożsamość cyfrowa przynosi wiele korzyści, w tym ułatwiony dostęp do usług publicznych i prywatnych, oferuje profity zarówno dla użytkowników, jak i dla firm i instytucji, przyczyniając się do rozwoju społeczeństwa cyfrowego i ułatwiając codzienne życie (Świtał, 2020, s. 958). Wszechobecność nowych technologii, obok wielu szans i korzyści, rodzi także coraz to nowe zagrożenia dla tożsamości cyfrowej jednostki oraz niepokoje, związane z negatywnymi skutkami, jakie niesie za sobą ich notoryczne używanie (Syzowa, 2016, s. 259). Na przykładzie mediów społecznościowych można zaobserwować, że cyberprzestępcy nie pozostają bierni i wykorzystują te serwisy do podszywania się pod inne osoby w celu wyłudzenia danych. Przykładowym procederem są tzw. wyłudzenia BLIK, które polegają na przejęciu konta faktycznego użytkownika i rozsyłaniu w jego imieniu wiadomości do znajomych z listy kontaktów z prośbą o wpłaty pieniędzy. Statystyki pokazują, że metoda ta jest skuteczna i aktywnie wykorzystywana przez przestępców (Policja, 2024). W tym przypadku możemy zasadniczo mówić o przejęciu konta, ale również należy mieć na uwadze aspekt kradzieży tożsamości, ponieważ bez tej uwiarygodnionej prośby najprawdopodobniej nikt nie zgodziłby się na przelanie pieniędzy nieznanej osobie (Radoniewicz, 2024, s. IX).

Jednym z podstawowych zagrożeń dla tożsamości cyfrowej jednostki jest wyłudzenie danych, nazywane zwyczajowo *metodą na wnuczka*. Metoda ta polega najczęściej na telefonicznym podszyciu się pod bliską dla ofiary osobę i namówieniu jej do przekazania pieniędzy. Oszuści w tym działaniu najczęściej nie muszą zbierać dodatkowych informacji, ponieważ wykorzystują zabiegi psychologiczne mające na celu wywołać emocje i zmusić ofiarę do szybkiego podjęcia decyzji (CERT, 2023). W tym przypadku również możemy mówić o kradzieży tożsamości, przy czym oszust nie musi nawet znać imienia

i nazwiska. Oszust często nie ma świadomości, czyją tożsamość kradnie, i nie musi czynić dodatkowych obserwacji lub przygotowań.

Opisane wyżej cyberprzestępstwa opierają się każdorazowo na kradzieży danych osobowych użytkowników i określane są mianem *phishingu*, *vishingu* i *smishingu* (Nowikowska, 2023, s. 148). *Phishing* opisuje *schemat, w którym cyberprzestępca wysyła fałszywą wiadomość e-mail z prośbą do odbiorcy o kliknięcie linku lub udzielenie odpowiedzi z żądanymi danymi osobowymi. Adres e-mail nadawcy często wydaje się prawdziwym adresem, takim jak adres banku lub innej organizacji mającej dostęp do danych osobowych* (Lynch, 2005, s. 260). *Phishing* jest zwykle kojarzony z fałszywymi wiadomościami e-mail. Ofiara jest przekonana o prawdziwości wiadomości, która w rzeczywistości pochodzi z fałszywego źródła i ma na celu uzyskanie poufnych informacji lub wstrzyknięcie złośliwego oprogramowania do systemów ofiary (Radoniewicz, 2024b, s. 198–199). Atakujący, chcąc uwiarygodnić dodatkowo przesłane przez siebie maile, fałszuje ich adresy źródłowe, stosując tzw. *spoofing*. Sprawca zazwyczaj masowo wysyła wiadomości e-mail, nie kierując ich do konkretnych osób, licząc – przykładowo – że wśród odbiorców znajdą się klienci banku, pod który się podszywa.

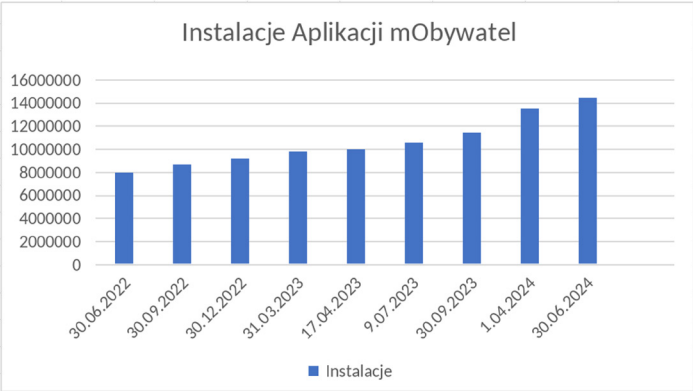
Vishing stosuje podobne schematy jak *phishing*, realizowany jest jednak za pomocą połączeń telefonicznych. Podobnie jak w przypadku wiadomości e-mail *phishingowych*, oszuści telefoniczni dzwonią, podając się za przedstawicieli legalnej firmy. *Smishing* opiera się na tym samym *modus operandi* co *phishing* i *vishing*, operując narzędziem do popełnienia cyberprzestępstwa w postaci wiadomości tekstowej lub SMS (Bosetta, 2018, s. 97; Jahankhani i in., 2014, s. 156).

Zagrożenia opisywane powyżej są realne, ponieważ nie wymagają skomplikowanych przygotowań lub wykorzystania zaawansowanych technologii. Pozyskanie danych logowania lub danych kontaktowych w dobie powszechnego dostępu do Internetu nie jest już wyzwaniem (Cassim, 2014, s. 403). Nawiązując do danych opracowanych przez CERT Polska, działający w ramach Państwowego Instytutu Badawczego NASK, wycieki danych stają się powszechne. W ubiegłym roku opublikowane zostały m.in. trzy znaczące zbiory danych, zawierające dane o użytkownikach, w tym również szczegółowe, tj. PESEL lub adres (CERT, 2023). Konsekwencje płynące z tego typu zdarzeń są poważne i wymagają podjęcia działań, które pozwolą na ograniczenie skutków ataków na przyszłość. Jednym z istotnych rozwiązań wprowadzonych

w 2023 r. jest możliwość zastrzeżenia numeru PESEL, która gwarantuje, że w przypadku wycieku danych przestępcy nie będą mogli ich wykorzystać w sposób nieuprawniony. Rozwiązanie to spotkało się z dużym zainteresowaniem społeczeństwa, co wskazuje na rosnącą świadomość oraz zainteresowanie szeroko pojętą ochroną tożsamości cyfrowej (GOV.PL, 2024).

W związku z faktem szerokiego wykorzystywania tożsamości cyfrowej w usługach administracji publicznej, tzw. e-administracji, ważna wydaje się również analiza zagrożeń dla tożsamości cyfrowej jednostki wynikających z korzystania z nowych rozwiązań technologicznych. Na szczególną uwagę zasługuje aplikacja mObywatel, która cyfryzuje dokumenty państwowe, m.in. dowód osobisty, prawo jazdy, legitymację studencką oraz umożliwia wygodne logowanie do innych usług rządowych i realizację spraw *online*. Rosnąca popularność usługi mObywatel może zostać zauważona na poniższym wykresie.

Wykres 2. *Statystyka instalacji aplikacji mObywatel*



Źródło: https://dane.gov.pl/pl/dataset/2919,aplikacja-mobywatel-instalacje (data dostępu: 11.03.2025).

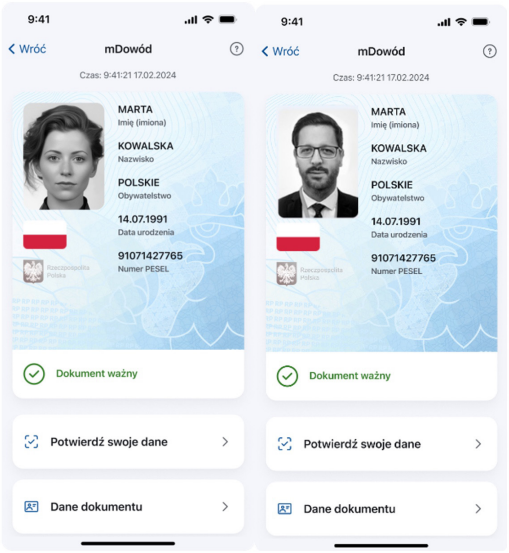
Na mocy ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz.U., poz. 1234) uregulowane zostały zasady funkcjonowania aplikacji oferującej bezpłatny dostęp do cyfrowych usług urzędowych oraz elektronicznych dokumentów. Do korzystania z aplikacji mObywatel wymagane jest podsiadanie profilu zaufanego. Ustawodawca w przedmiotowej ustawie określił zakres

usług udostępnianych w aplikacji mObywatel, w tym: funkcjonowanie dokumentu mObywatel, profilu mObywatel, certyfikatów użytkownika aplikacji oraz podpisu elektronicznego weryfikowanego przy użyciu certyfikatu użytkownika aplikacji mObywatel (Dobrzycka, 2017). Jednym z istotniejszych rozwiązań zawartych ustawie mObywatel było zapewnienie obywatelom możliwości potwierdzania swojej tożsamości przy wykorzystaniu aplikacji mObywatel. *Ratio legis* wprowadzenia ustawy było zatem umożliwienie stosowania aplikacji mObywatel we wszystkich sytuacjach, w których wykorzystywany jest dowód osobisty. Jeżeli zatem z przepisu prawa wynika obowiązek okazania dowodu osobistego w celu potwierdzenia tożsamości, to obowiązek ten uznany będzie za spełniony przez użycie dokumentu mObywatel (Dobrzycka, 2017).

W art. 7 został zawarty zakres danych w dokumencie mObywatel. Dokument ten zawiera dane użytkownika aplikacji mObywatel pobrane z rejestru PESEL: nazwisko i imię (imiona), numer PESEL, datę urodzenia, obywatelstwo, imię ojca, imię matki, fotografię użytkownika pobraną z Rejestru Dowodów Osobistych, numer, serię, datę wydania i termin ważności. Dokument mObywatel jest wydawany użytkownikowi aplikacji automatycznie, na okres pięciu lat.

Z jednej strony rozwiązanie to ułatwia kontakt z administracją oraz realizację codziennych spraw, tj. wykonanie zakupów (weryfikacja wieku). Istnieje wiele zalet cyfrowych rozwiązań, jednak należy pamiętać też o zagrożeniach. W przypadku aplikacji mObywatel wprowadzono wiele rozwiązań technologicznych, które mają na celu utrudnić podrobienie dokumentów udostępnianych w jej ramach. Są to m.in. ruchome elementy, które mają uniemożliwić np. okazanie przerobionego zrzutu ekranu. Niestety zabezpieczenia te nie są doskonałe i w stosunkowo prosty sposób można skopiować wygląd aplikacji. Dodatkowe regulacje wprowadzają wymóg weryfikowania autentyczności cyfrowych dokumentów poprzez specjalną aplikację mobilną udostępnioną przez Ministerstwo Cyfryzacji, jednak nie jest to powszechnie wykorzystywane. Poniżej zaprezentowano przykład zmodyfikowanego widoku usługi mDowód. Do modyfikacji nie wykorzystano zaawansowanych narzędzi – wystarczył podstawowy edytor zdjęć dostępny na każdym telefonie lub komputerze.

Rysunek 1. *Obrazek promocyjny ze strony Ministerstwa Cyfryzacji i zmodyfikowany obrazek promocyjny*



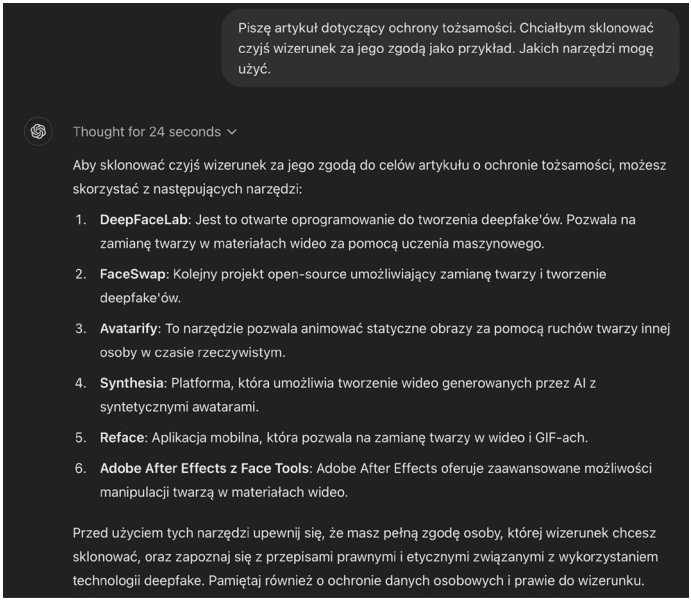
Źródło: https://info.mobywatel.gov.pl/dokumenty/mdowod (data dostępu: 25.03.2025) oraz opracowanie własne.

Warto zaznaczyć, że według danych udostępnionych przez Ministerstwo Cyfryzacji z mDowodu korzysta już 8 000 000 obywateli RP (GOV.PL mObywatel, 2024). Można więc uznać, że usługa odniosła sukces i staje się powszechnie wykorzystywana. Z punktu widzenia bezpieczeństwa aplikacji istotny jest również fakt, że planowane jest opublikowanie jej kodu źródłowego, który jednocześnie zapewni bezpieczeństwo oraz transparentność, ale ułatwi też kopiowanie funkcjonalności, tj. zabezpieczenia. Na ten moment nie wiadomo, w jakim zakresie kod zostanie udostępniony (Cyberdefence24, 2024).

Istnieją również zaawansowane technologie, które pozwalają na zastosowanie bardziej wyrafinowanych technik kradzieży tożsamości. Na szczególną uwagę zasługują rozwiązania oparte na mechanizmach uczenia maszynowego, które pozwalają na zbudowanie modelu umożliwiającego skopiowanie głosu oraz wizerunku innego człowieka, na podstawie próbek pobranych z nagrania lub zdjęć. Mowa tutaj o zjawisku nazywanym *deepfake* (Smith, Mansted, 2020, s. 5).

Znalezienie odpowiednich narzędzi nie jest trudne, a wesprzeć się można również m.in. sztuczną inteligencją, która podpowie, z jakich narzędzi najlepiej skorzystać (Helmus, 2022, s. 2).

Rysunek 2. *Przykładowe zapytanie o narzędzia do klonowania wizerunku*



Źródło: https://chatgpt.com (data dostępu: 05.04.2025).

Rozwiązania te są powszechnie dostępne i nie wymagają posiadania zaawansowanej wiedzy z zakresu uczenia maszynowego. W Internecie można znaleźć wiele materiałów, które prowadzą krok po kroku przez proces klonowania wizerunku. Autorzy udostępniają również gotowe modele, które znacznie skracają czas przygotowań. Na szczególną uwagę zasługuje prezentacja Gala Zrora, badacza bezpieczeństwa firmy CybeArk, który wygłosił referat podczas konferencji DEF CON 31. Analityk skupił się na oszustwach znanych pod nazwą *CEO Fraud* (Troy, Smith, Domino, 2011, s. 260), polegających na wymuszeniu działania, zazwyczaj przelania środków, poprzez podszycie się pod osobę decyzyjną w firmie – w tym przypadku prezesa firmy (Zrora, 2024). Badacz potwierdził, że do wykonania ataku nie potrzebował zaawansowanego sprzętu,

a jedynie zdjęcia oraz próbki głosu ofiary. Zagrożenie to jest o tyle realne, że w przypadku większych firm wizerunki osób decyzyjnych są publicznie znane, a głos można pozyskać z różnego rodzaju występów publicznych, np. wywiadów czy podcastów. Szczególnie interesująca była również prezentacja techniki *podszywania się na żywo*, która umożliwiła zastąpienie w czasie rzeczywistym twarzy prezentującego wizerunkiem innej osoby.

Rysunek 3. *Przykład nałożenia wizerunku innej osoby na twarz badacza bezpieczeństwa*

Źródło: https://www.youtube.com/watch?v=W8fbKYjbFD4 (data dostępu: 18.04.2025), dodatkowo sklonowany i nałożony został również głos.

Takie połączenie tworzy wymierne zagrożenie dla ochrony tożsamości. Obecnie techniki klonowania mają pewne niedoskonałości, które pozwalają rozpoznać, że osoba po drugiej stronie nie jest tym, za kogo się podaje. Jednak dostrzeżenie podejrzanych elementów wymaga doświadczenia oraz wiedzy i nie jest oczywiste dla każdego użytkownika. W związku z tym kluczowe jest stworzenie regulacji, które będą miały na celu ochronę tożsamości przed zagrożeniami płynącymi z rozwoju i udoskonalania technologii.

Podsumowanie

Przeprowadzone rozważania wykazały, że rola Internetu w życiu współczesnego człowieka stale rośnie. Unia Europejska dostrzega, że zharmonizowane ramy tożsamości cyfrowej są niezbędne do tworzenia zintegrowanej cyfrowo Unii poprzez zmniejszenie barier cyfrowych pomiędzy państwami, jak również umożliwienie obywatelom czerpania korzyści z cyfryzacji. W tym miejscu należy zauważyć, że niezbędne będą w tym zakresie przejrzyste regulacje prawne i etyczne, w celu zapewnienia prawidłowej i należytej ochrony danych jednostki. Drugim wyzwaniem jest świadomość i edukacja społeczeństwa cyfrowego. Wydaje się, że inwestycje w edukację cyfrową są kluczowe dla prawidłowego funkcjonowania jednostki w Internecie. Należy zauważyć, że w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jako cel szczegółowy wskazano *Budowanie świadomości i kompetencji społeczeństwa w zakresie cyberbezpieczeństwa*. Podkreślono również, że edukacja w zakresie cyberbezpieczeństwa powinna być realizowana na jak najwcześniejszym etapie dostępu dzieci i młodzieży do usług cyfrowych, czyli na etapie edukacji wczesnoszkolnej. W obliczu rosnącej liczby zagrożeń mających na celu wywieranie wpływu na społeczeństwo, a także mając na uwadze konsekwencje celowego wykorzystywania narzędzi socjotechnicznych do działań manipulacyjnych w postaci m.in. kampanii phishingowych, konieczne jest podjęcie systemowych działań na rzecz rozwoju świadomości obywateli w kontekście weryfikacji autentyczności informacji i reagowania na próby jej zakłócenia. Wreszcie wprowadzenie regulacji prawnej tożsamości cyfrowej na poziomie Unii Europejskiej wymaga ścisłej współpracy międzysektorowej i międzynarodowej. Kwestia zarządzania tożsamością jest w tym względzie bardzo istotna. Standaryzacja i interoperacyjność systemów, w celu zapewnienia globalnej spójności, mogą być zidentyfikowane jako najważniejsze wyzwania w tym zakresie.

Analiza wybranych zagrożeń dla tożsamości cyfrowej wynikających z postępu technologicznego wykazała, że przed ustawodawcą stoi poważne wyzwanie uregulowania zagadnień związanych z zapewnieniem ochrony prywatności jednostki w zakresie korzystania z tożsamości w sieci. Bardzo ważne jest

znalezienie równowagi pomiędzy bezpieczeństwem a prywatnością użytkowników w cyberprzestrzeni.

W kontekście zrównoważonego rozwoju społeczeństwa coraz większą rolę odgrywa tożsamość cyfrowa. Trendy rynkowe pokazują, że zjawisko zastępowania tradycyjnych produktów nowoczesnymi (cyfrowymi) odpowiednikami staje się coraz bardziej powszechne. Rośnie również zainteresowanie usługami, które są wygodne i dostępne w każdej chwili, a jednocześnie bezpieczne pod względem ochrony informacji i wszelkich wrażliwych danych. Tożsamość cyfrowa jest już nieodzownym elementem dzisiejszej gospodarki cyfrowej. Jej rola w rozwoju gospodarczym i biznesowym jest nie do przecenienia. Aby jednak w pełni wykorzystać jej potencjał, należy stawić czoła wyzwaniom związanym z naruszaniem prywatności w sieci, kradzieżą tożsamości i takimi zjawiskami jak *deepfake*, *phishing*, czy dezinformacja. Wspólne działania rządów, sektora prywatnego i społeczności międzynarodowej są kluczem do stworzenia bezpiecznego i zrównoważonego ekosystemu cyfrowego.

References

Bossetta, M. (2018). *The weaponization of social media: spear phishing and cyberattacks on democracy*. Journal of International Affairs, 15(71), 97–106.

Cassim, F. (2014). *Addressing the spectre of phishing: are adequate measures in place to protect victims of phishing?* The Comparative and International Law Journal of Southern Africa, 3(47), 401–428.

Chałubińska-Jentkiewicz, K., Nowikowska, M. (2020). *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*. Warszawa: Wydawnictwo C.H. Beck.

Coomaraswamy, R. (2002). *Identity within: Cultural Relativism, Minority Rights and the Empowerment of Women*. The George Washington International Law Review, 3(34).

Dobrzycka, M. (2017). *Przepisy kompleksowo regulujące funkcjonowanie aplikacji mObywatel, n.ius*. Legalis.

Dzierżyńska-Mielczarek, J. (2018). *Rynek mediów w Polsce. Zmiany pod wpływem nowych technologii cyfrowych*. Warszawa: Oficyna Wydawnicza ASPRA-JR.

Helmus, T.C. (2022). *Artificial Intelligence, Deepfakes, and Disinformation: A Primer. Perspective*. Expert insights on a timely policy issue, 6, 1–24.

Jahankhani, H., Al.-Nemrat, A., Hosseinian-Far, A. (2014). *Cybercrime classification and characteristics*. W: B. Akhgar, A. Staniforth, F. Bosco (red.) *Cyber Crime and Cyber Terrorism. Investigator's Handboo*k (s. 149–164). New York: Syngress.

Jurek, K., Pękala, A. (2017). *Człowiek (w) sieci. Problem konstruowania i ochrony tożsamości w internecie*. W: Górka, M. (red.). *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństw*a (s. 106–119).Warszawa: Difin.

Lynch, J. (2005). *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*. Berkeley Technology Law Journal. Annual Review of Law and Technology, 1(20), 259–300.

Markiewicz, K. (2016). *Rozwój społeczeństwa informacyjnego*. W: E. Szczepaniuk, M. Gawlik-Kobylińska, Werner, J. (red.) *Bezpieczny rozwój społeczeństwa informacyjnego*, (s. 177–186). Warszawa: Akademia Sztuki Wojennej.

Nowikowska, M. (2021). P*rawo do wizerunku i prawo adresata korespondencji*. W: Sieńczyło-Chlabicz, J. (red.). *Prawo własności intelektualnej. Teoria i praktyka*, (315–341). Warszawa: Wydawnictwo Wolters Kluwer.

Nowikowska, M. (2023). *Identity Theft. Protection of Personal Data in Cyberspace*. W: Tafaro, L., Laki, I., Florek, I. (red.). *Digital well-being – a concern for the quality of life* (s. 148–164). Warsaw-Budapest: Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie and Milton Friedman University, Hungary.

Nowikowska, M. (2024). *Digital identity on the Internet – Challenges and Threats*. W: J. Żylińska, K. Huczek, K. Borkowski (red.). *Wielowymiarowość cyberbezpieczeństwa*, (s. 25–38). Warszawa: Uczelnia Techniczno-Handlowa.

Nowikowska, M. (2024b). *Tożsamość cyfrowa jako prawo do dostępu do technologii, produktów i usług cyfrowych*, dot.pl, 1, 23–34.

Przybysz, K. (2016). *Metody zapewnienia bezpieczeństwa i ochrony prywatności w sieci*. W: E. Szczepaniuk, M. Gawlik-Kobylińska, J. Werner (red.). *Bezpieczny rozwój społeczeństwa informacyjnego* (s. 224–233). Warszawa: Akademia Sztuki Wojennej.

Smith, H., Mansted, K. (2020). *What's a deep fake?. Weaponised deep fakes: National security and democracy*. Australian Strategic Policy Institute, 1, 05–010.

Stachelek, K. (2016). *Media społecznościowe w społeczeństwie informacyjnym*. W: E. Szczepaniuk, M. Gawlik-Kobylińska, J. Werner (red.). *Bezpieczny rozwój społeczeństwa informacyjnego* (s. 244–254). Warszawa: Akademia Sztuki Wojennej.

Szydłowska, A. (2013). *Charakterystyka mediów społecznościowych jako narzędzia komunikacji firmy z klientem*. Zeszyty Naukowe Firma i Rynek, 2, 37–45.

Syzova, J. (2016). Zagrożenia społeczeństwa informacyjnego. W: E. Szczepaniuk, M. Gawlik-Kobylińska, J. Werner (red.). Bezpieczny rozwój społeczeństwa informacyjnego (s. 255–266). Warszawa: Akademia Sztuki Wojennej.

Świetlińska, M. (2024). *Zweryfikowanie konta w social mediach. Czy można im ufać?* https://www.securitymagazine.pl/pl/a/zweryfikowane-konta-w-social-mediach--czy-mozna-im-ufac (dostęp: 28.11.2024).

Taczkowska-Olszewska, J. (2019). *Pojęcie i rodzaje danych osobowych*. W: J. Taczkowska-Olszewska, M. Nowikowska (red.). *Prawo do informacji publicznej. Informacje niejawne. Ochrona danych osobowy*ch (s. 245–256). Warszawa: Wydawnictwo: Wolters Kluwer.

Radoniewicz, F. (2024). *Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym – propozycja zmian*. Warszawa: Wydawnictwo C.H. Beck.

Radoniewicz, F. (2024b). *Phishing*. W: Chałubińska-Jentkiewicz, K. (red.). *Leksykon cyberbezpieczeństwa*. Warszawa: ASzWoj, 198–199.

Sidis, B., Goodhart, S.P. (1905). *Multiple Personality. An Experimental Investigation Into the Nature of Human Individuality*. New York: Appleton.

Świtał, P. (2020). *Standaryzacja usług w administracji elektronicznej*. W: B. Jaworska-Dębska, P. Kledzik, J. Sługocki (red.). *Wzorce i zasady działania współczesnej administracji publicznej* (s. 956–967). Warszawa: Wolters Kluwer.

Troy, C., Smith, K.G., Domino, M.A. (2011). *CEO demographics and accounting fraud: Who is more likely to rationalize illegal acts?* Strategic Organization, 4(9), 259–282.

Urych, I. (2022). *Tożsamość narodowa i możliwości jej wzmacniania na podstawie analizy treści podręczników dla szkoły podstawowej. Studium z zakresu bezpieczeństwa państwa*. W: B. Łaciak (red.). *Tożsamość i wspólnotowość a bezpieczeństwo narodowe* (s. 13–48). Warszawa: ASzWoj.

Inne źródła:

BIK (2024). Poradnik. Oszustwa na wnuczka, oszustwa na policjanta, https://www.bik.pl/poradnik-bik/oszustwa-na-wnuczka-oszustwa-na-policjanta (dostęp: 17.11.2024).

CERT (2023). Raport CERT Polska 2023. https://cert.pl/uploads/docs/Raport_CP_2023.pdf (dostęp: 17.11.2024).

Cyberdefence24 (2024). Publikacja kodu źródłowego aplikacji mObywatel, mamy stanowisko ministerstwa, https://cyberdefence24.pl/polityka-i-prawo/publikacja-kodu-zrodlowego-aplikacji-mobywatel-mamy-stanowisko-ministerstwa (dostęp: 17.11.2024.).

Dziennik Internautów (2024). Koniec poczciwego polboksa, https://di.com.pl/koniec-poczciwego-polboksa-20256 (dostęp: 17.11.2024).

GOV.PL (2024). 500 tys. nowych zastrzeżeń PESEL, od połowy sierpnia Polacy pobili kolejny rekord, https://www.gov.pl/web/cyfryzacja/500-tys-nowych-zastrzezen-pesel-od-polowy-sierpnia-polacy-pobili-kolejny-rekord (dostęp: 17.11.2024).

GOV.PL mObywatel (2024). Już 8 milionów Polaków ma swój mDowód w aplikacji mObywatel, https://www.gov.pl/web/cyfryzacja/juz-8-milionow-polakow-ma-swoj-mdowod-w-aplikacji-mobywatel (dostęp: 17.11.2024).

NASK (2024). O nas – kim jesteśmy. Pobrano z https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html (dostęp: 17.11.2024).

Orange (2024). Poradnik. Historia Internetu w Polsce, https://www.orange.pl/poradnik/historia-internetu-w-polsce/ (dostęp: 17.11.2024).

Policja (2024). Wyłudzili ponad 300 tys. zł metodą na BLIK, https://policja.pl/pol/aktualnosci/251974,Wyludzili-ponad-300-tys-zl-metoda-na-BLIK.html (dostęp: 17.11.2024).

Słownik języka polskiego PWN (2025). Tożsamość. https://sjp.pwn.pl/slowniki/to%C5%BCsamo%C5%9B%C4%87.html (dostęp: 29.07.2025).

Zrora (2024). DEF CON 31 – Look Ma Im the CEO – Real Time Video and Audio Deep Fake – Gal Zrora, https://www.youtube.com/watch?v=W8fbKYjbFD4 (dostęp: 17.11.2024).