Biometryczne rozpoznawanie twarzy – podejście na świecie i testy systemu Face Pay w moskiewskim metrze

Informację opracował Janusz POLIŃSKI[1]

Streszczenie

W przestrzeni publicznej coraz częściej wykorzystuje się biometryczne rozpoznawanie twarzy. Ta technologia wykorzystywana na całym świecie do zapewnienia bezpieczeństwa, coraz częściej wychodzi poza ten obszar. Wzbudza to jednak uzasadnione obawy naruszania prywatności, czego efektem stają się prawne ograniczenia rozpowszechniania tej metody. W zależności od politycznego systemu i poziomu demokracji, metoda jest rozwijana bez ograniczeń, z ograniczeniami lub wręcz zakazywana. Podstawowa wiedza na ten temat jest potrzebna do określenia miejsc stosowania metody Face Pay do wnoszenia opłat za towar lub usługę, czego przykładem jest wprowadzane rozwiązanie w moskiewskim metrze.

Słowa kluczowe: inteligentne analizy wideo, rozpoznawanie i przetwarzanie obrazu twarzy, system Face Pay, moskiewskie metro

Biometria, to prawdopodobnie najwygodniejszy i najbezpieczniejszy sposób potwierdzania tożsamości. Biometryczne rozpoznawanie twarzy jest elementem szybko rozwijanych technologii cyfrowych, a w nich inteligentnych analiz obrazów wideo. Technologia rozpoznawania twarzy wydaje się być ekscytująca i bardzo perspektywiczna, jednak w każdym postępie niesionym przez rozwój poszczególnych dziedzin nauki, praktyczne rozwiązania bardzo często niosą wiele korzyści, ale także zagrożeń.

Rozwiązania dotyczące sztucznej inteligencji umożliwiającej identyfikować twarze, znajdują zastosowanie w policji i służbach bezpieczeństwa, które dopiero testują lub już wprowadziły tę technologię do kontrolowania miejsc, w których mogą znajdować się duże grupy ludzi. Dotyczy to w szczególności stadionów, dworców kolejowych i lotniczych lub centrów handlowych. Kamery wideo, w połączeniu z odpowiednim oprogramowaniem i bazami danych, mogą identyfikować ludzi na podstawie wyglądu twarzy. W wielu państwach takie systemy są wykorzystywane na przejściach granicznych, dworcach, a nawet uczelniach, umożliwiając identyfikację studentów. Wielu producentów popularnych urządzeń elektronicznych zastosowało oprogramowania rozpoznawania twarzy, dzięki którym można odblokować telefon lub automatycznie odszukać znajomych w galeriach zdjęć.

Na świecie są obserwowane różne podejścia do obszarów wykorzystywania identyfikacji twarzy. Można je podzielić na trzy grupy:

- zastosowanie bez ograniczeń,
- ograniczenie możliwości stosowania,
- zakaz stosowania.

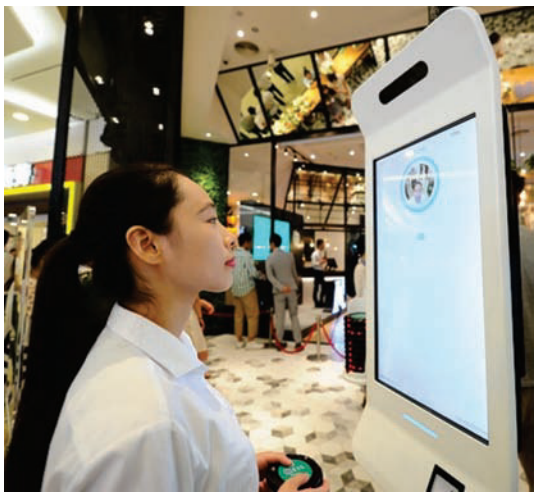
Przykładem szerokiego zastosowania biometrycznego rozpoznawania twarzy są Chiny. W Państwie Środka systemy rozpoznające twarz są praktycznie wszędzie obecne – od dworców kolejowych, autobusowych i lotniczych, centrów miast, po wejścia do parków, a nawet w publicznych toaletach (co obywatelom przestaje się podobać) [3]. Rozpoznawanie twarzy dość powszechnie stosuje się do uwierzytelniania płatności mobilnych lub wejścia/wyjścia z niektórych miejsc pracy.

Rozwój systemu został przyspieszony przez pandemię. Zdjęcie maski zwiększało zagrożenie zarażeniem wirusem, dlatego tak ważne było, aby systemy rozpoznawania twarzy potrafiły poprawnie rozpoznać osoby noszące maseczki. Opracowano metodę, która umożliwia zidentyfikowanie osób bez maseczki, gdyż informacja czy osoba ma zakrytą twarz zgodnie z zaleceniami stała się bardzo ważna. Jednocześnie, system musi zasygnalizować, gdy ktoś ma zakrytą twarz, co ma znaczenie w przypadku włamań lub ataków terrorystycznych. Metoda umożliwia także rozpoznanie tożsamości zamaskowanej osoby. System jest praktycznie nieomylny (rozpoznawanie w 99,95%) i radzi sobie z odmienną mimiką twarzy i ze szczegółami jak kapelusz na głowie, okulary lub zapuszczona broda [4].

Twarz stała się naszą unikalną daną. Dokonywanie płatności przez system rozpoznawania twarzy to podobno przyszłość. Świat nieskomplikowanych płatności

[1] Dr inż., emerytowany pracownik Instytutu Kolejnictwa, e-mail: jpolin53@vp.pl.

bezgotówkowych kusi, jednak jego ceną jest udzielenie wizerunku, aby stał się naszym, indywidualnym cyfrowym obrazem. W Chinach, firma Yitu Technology wprowadziła system rozpoznawania twarzy w ponad 20 tysiącach bankomatów; system w swojej bazie danych gromadzi dane przynajmniej 2 mld potencjalnych użytkowników. We wrześniu 2017 roku, uruchomiono taką usługę w KFC we wschodnim mieście Hangzhou w Chinach, który jako pierwszy fizyczny sklep na świecie zaczął używać technologii do rozpoznawania twarzy do regulowania płatności. Klienci KFC składają zamówienie w terminalu, który skanuje ich twarz. Jeśli skan zgadza się z obrazem zapisanym w systemie, płatność jest realizowana [4]. Widok terminala pokazano na rysunku 1.



Rys. 1. Terminal zamówień i płatności w KFC [5]

Ograniczenie możliwości skanowania twarzy rozważa Unia Europejska. Komisja Europejska prowadzi prace związane z zakazem stosowania systemów automatycznego rozpoznawania twarzy w miejscach publicznych na okres do pięciu lat. Organy regulacyjne potrzebują czasu, aby wypracować sposoby zapobiegania nadużywania tej technologii. Od zakazu miałyby obowiązywać wyjątki zastosowania systemu we wszystkich rozwiązaniach dotyczących bezpieczeństwa. Komisja Europejska opracowała 18-stronicowy dokument, w którym proponuje wprowadzenie nowych zasad, które miałyby lepiej chronić prywatność obywateli UE oraz ich dane. W dokumencie znalazły się też propozycje nowych obowiązków, które miałyby dotyczyć zarówno twórców, jak i użytkowników sztucznej inteligencji. Pojawiła się także propozycja powołania do życia instytucji, która miałaby monitorować wypełnianie tych obowiązków [6].

Proponowane regulacje zakładają wprowadzenie czterech kategorii oceny poziomu ryzyka związanego z wykorzystaniem sztucznej inteligencji. Wszystko będzie zależało od poziomu „niebezpieczeństwa", jakie wniesie technologia:

- niedopuszczalne ryzyko,
- wysokie ryzyko,
- ograniczone ryzyko,
- niskie ryzyko.

Pierwsze dwa poziomy ryzyka będą zabronione w Unii Europejskiej. Do tej grupy zaliczono np. technologie tak zwanej „zdalnej identyfikacji biometrycznej". Jest ona wykorzystywana choćby do identyfikowania w czasie rzeczywistym ludzi z tłumu dzięki zastosowaniu aplikacji do rozpoznawania twarzy na żywo [7].

Sposób wykorzystania danych biometrycznych uregulowano w przepisach Rozporządzenia Parlamentu Europejskiego i Rady [2]. Według brzmienia art. 4 ust 14 dane biometryczne (…) *oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne* (…). Należą one do specjalnej kategorii danych, których przetwarzanie wedle ogólnej zasady jest zabronione. Ustawodawca unijny uznał, że przetwarzanie niektórych rodzajów danych osobowych może stanowić poważną ingerencję w sferę prywatności osób, których dane dotyczą lub może pociągać za sobą znacznie większe zagrożenia niż przetwarzanie tzw. danych zwykłych [8].

W związku z rosnącymi obawami obywateli dotyczącymi wykorzystywania nowoczesnych technologii, Komisja Europejska podjęła prace nad dokumentem wskazującym zalecenia i zagrożenia w sprawie sztucznej inteligencji. Dokument zatytułowany Białą Księgą [14], traktuje także o technologiach dotyczących rozpoznawania twarzy.

Pomimo tego, w wielu państwach europejskich wdraża się technologie umożliwiające rozpoznawanie twarzy. W Niemczech już wprowadzono automatyczne rozpoznawanie twarzy na 134 dworcach kolejowych i 14 lotniskach. Podobne inwestycje poczyniła Francja. Francuski rząd wprowadza dowody tożsamości z funkcją rozpoznawania twarzy mimo protestów grup działających na rzecz praw cyfrowych. Na Węgrzech ministerstwo spraw wewnętrznych zainstalowało w Budapeszcie i w pozostałej części kraju 35 tysięcy kamer mających rejestrować zarówno twarze, jak i tablice rejestracyjne pojazdów drogowych [7].

Organy regulacyjne Unii Europejskiej dotyczące ochrony danych wezwały w 2021 r. do wprowadzenia ogólnego zakazu wykorzystywania sztucznej inteligencji do rozpoznawania twarzy, a także innych „sygnałów biometrycznych i behawioralnych" w przestrzeni publicznej. We wspólnej opinii, Europejska Rada Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) również stwierdzili, że powszechne wykorzystywanie sztucznej inteligencji, np. do ocen społecznych, powinno być zakazane. EROD, a także EIOD wezwały do zakazania (…) *rozpoznawania twarzy, chodu, odcisków palców, DNA, głosu, naciśnięć klawiszy oraz innych sygnałów biometrycznych lub behawioralnych w dowolnym kontekście* (…) w miejscach publicznych. Zdaniem tych organizacji, wykorzystywanie danych biometrycznych w systemach sztucznej inteligencji do kategoryzowania ludzi „w klastry na podstawie pochodzenia etnicznego, płci, orientacji politycznej lub seksualnej", a także innego rodzaju klasyfikacji, przez które mogą być dyskryminowani [10],

powinno być nielegalne. EROD jest zdania, że (…) *Ogólny zakaz korzystania z rozpoznawania twarzy w miejscach publicznie dostępnych jest niezbędnym punktem wyjścia, jeśli chcemy zachować nasze wolności i stworzyć ramy prawne sztucznej inteligencji zorientowane na prawa człowieka* (…) [12].

Według Europejskiego Inspektora Ochrony Danych, technologia rozpoznawania twarzy powinna być zabroniona w Europie ze względu na „głęboką i niedemokratyczną ingerencję" w życie prywatne. Z tego względu wszystkie rodzaje identyfikacji biometrycznej uznano za technologie wysokiego ryzyka. Stosowanie ich w miejscach publicznych takich jak parki, centra miast, urzędy będzie w UE zakazane. Wyjątkiem mają być takie okoliczności, jak walka z przestępczością lub poszukiwanie osób zaginionych, w przypadku których pozwolenie będzie musiał wydać sąd [15]. W Stanach Zjednoczonych coraz więcej państwowych instytucji wykorzystuje systemy do rozpoznawania twarzy, co wynika z raportu organizacji *Government Accountability Office*. Według analityków, dziesięć federalnych agencji planuje w swoich działaniach rozszerzyć zakres stosowania tej technologii [9]. Z tego tytułu coraz aktywniejsi są przeciwnicy tej technologii. Mają oni duży wpływ na władze poszczególnych miast.

Zakaz stosowania biometrycznych technologii rozpoznawania twarzy wprowadzono już w niektórych miastach USA, gdzie ze względu na brak jednoznacznych przepisów metoda rozpowszechniła się tak szybko jak w Chinach.

San Francisco, jako pierwsze miasto w USA zakazało monitoringu z funkcją rozpoznawania twarzy w miejscach publicznych. Władze miejskie uznały to za zbyt dużą ingerencję w prywatność. Według władz miasta San Francisco, tego typu monitoring przynosi więcej strat niż korzyści. Monitoring zagraża prawom cywilnym i swobodom obywatelskim i służy do profilowania obywateli ze względu na rasę, płeć lub orientację seksualną. Według inicjatorów zakazu, miejscy urzędnicy mają zbyt łatwy dostęp do ogromnej liczby danych, a w połączeniu z systemem kamer rozpoznających twarz, mogliby stworzyć system totalnej inwigilacji mieszkańców [10]. W ślad za San Francisco poszły władze Bostonu i Oakland. Rada miasta Portland uchwaliła najsurowszy zakaz rozpoznawania twarzy w USA, blokując zarówno publiczne, jak i prywatne korzystanie z tej technologii [11].

Z petycjami dotyczącymi zakazu stosowania w przestrzeni publicznej biometrycznego skanowania twarzy można zapoznać się na stronach Internetowych UE oraz USA:

- Unia Europejska: https://reclaimyourface.eu/,
- USA: https://www.banfacialrecognition.com/.

Pomimo wielu problemów związanych z zasadami korzystania z elektronicznej identyfikacji twarzy w przestrzeni publicznej, istnieje cienka linia pomiędzy problematyką zapewniania bezpieczeństwa i wykorzystaniem tych możliwości do innych celów. Można podzielić je na sprzeczne z ochroną prywatności osób w przestrzeni publicznej i wspomagające lub ułatwiające codzienne funkcjonowanie. W odniesieniu do tego przypadku interesujące rozwiązanie jest stosowane w moskiewskim metrze. Stolicę Rosji obsługuje jeden z największych systemów monitoringu na świecie, obejmujących moskiewskie metro, które jest obsługiwane przez 241 stacji na odcinku o długości 415 km.

W 2019 roku Departament Transportu wraz z policją i Departamentem Spraw Wewnętrznych uruchomił system rozpoznawania twarzy w moskiewskim metrze, aby m.in. odnaleźć „zagubionych ludzi i ukrywających się przestępców" oraz wyegzekwować opłatę za przejazd. We wdrożenie nowego systemu zaangażowało się kilka rosyjskich firm: *VisionLabs*, *Ntechlab* i *Tevian*. Obecnie trwa kluczowa faza pilotażu uwzględniająca podróżnych. Już wcześniej z *Face Pay*[2] korzystali pracownicy metra, którzy dzięki technologii rozpoznawania twarzy przeszli przez bramki ponad 1 mln razy. System płatności za przejazdy *Face Pay* przechodzi testy i jest przygotowywany do wdrożenia w kasach i wybranych bramkach moskiewskiego metra. System oznaczono specjalnym piktogramem na posadzce (rys. 2) i wyposażono w kamery wideo, które umożliwią rozpoznanie twarzy nawet z maską medyczną, co wiąże się z opłaceniem podróży. W Rosji nie ma barier w korzystaniu z tej technologii w przeciwieństwie do wielu krajów europejskich, w których narusza ona przepisy dotyczące danych osobowych.

Rys. 2. Bramka dostosowana do opłaty za pomocą skanowania twarzy [13]

Istotnym elementem projektu jest część serwerowa, w tym odpowiednie oprogramowanie oraz część peryferyjna, która objęła zakup specjalnych bramek wraz z wyposażeniem oraz system ich połączenia na stacji, a także połączeniem stacji między sobą. Koszt części serwerowej oszacowano na 300 milionów rubli. Do prób wybrano czwartą linię, na której zamontowano 2000 przejść testowych.

[2] *Face Pay* – technologia rozpoznawania twarzy.

Inwestycje w części peryferyjnej zaplanowano zrefundować z istniejącego budżetu metra. Metro zapewnia jedynie infrastrukturę związaną z biometrią, a osobiste dane płatnicze są przechowywane i obsługiwane w bankach.

W celu skorzystania z tej formy płatności, należy zalogować się na internetowej stronie metra, a następnie trzeba zainstalować aplikację mobilną przewoźnika, przesłać zdjęcie swojej twarzy oraz dodać dane karty debetowej lub kredytowej swojego banku. Na stacji metra należy podejść do specjalnie oznaczonej bramki i spojrzeć w kamerę. Jeżeli system rozpozna twarz i przetworzy dane, to po chwili bramka otworzy się, a należność będzie pobrana ze spersonalizowanej karty bankowej.

Wiele pytań przyszłych użytkowników systemu dotyczy bezpieczeństwa danych biometrycznych. Szef analityki i projektów specjalnych w *InfoWatch Group of Companies*, uważa że (…) *Ryzyko wycieków z baz danych biometrycznych istnieje, nawet pomimo najnowocześniejszych systemów bezpieczeństwa wykorzystujących szyfrowanie. Nie da się wykluczyć nieuczciwego wykorzystania danych biometrycznych, w tym wykorzystania technologii deepfake*[3]*, które szybko rozwijają się*. (…) Za bezpieczeństwo danych płatniczych systemu odpowiadają banki [14].

Czołowy ekspert z Kaspersky Lab uważa, że ważne jest, aby cyberbezpieczeństwo znalazło się w centrum tworzenia systemu, który będzie miał dostęp do bazy danych z danymi biometrycznymi. (…) *Jeśli jednak przestrzegane są wszelkie środki bezpieczeństwa dotyczące przechowywania i przetwarzania takich informacji, to wszelkie dane biometryczne są przechowywane nie jako obrazy, ale w postaci kodu numerycznego, który uzyskuje się w wyniku analizy tych danych według określonych algorytmów. Tak więc, nawet w przypadku wycieku, kod ten nie pozwoli cyberprzestępcom na przeprowadzenie jakichkolwiek operacji finansowych.* (…) [14].

Jak przekonują przedstawiciele transportu publicznego ze stolicy Rosji, moskiewskie metro jest obecnie liderem pod względem liczby metod płatności za przejazd i wszystkie one pozostaną również dostępne po wprowadzeniu systemu *Face Pay*. Płatność za pomocą biometrii twarzy ma być kolejną wygodną usługą dla podróżnych, ale nie obowiązkową.

Bibliografia

1. Biała Księga Komisji Europejskiej w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania. Bruksela, dnia 19.2.2020 r. COM(2020) 65 final.
2. 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.

Źródła internetowe

3. https://www.chip.pl/2020/01/komisja-europejska-zakaz-rozpoznawania-twarzy-przez-5-lat/ [dostęp 30.08.2021].
4. https://www.chinskiraport.pl/blog/rozpoznawanie-twarzy-a-platnosci/ [dostęp 30.08.2021].
5. http://finance.sina.com.cn/money/lczx/2017-09-07/doc-ifykuftz4995765.shtml [dostęp 30.08.2021].
6. https://www.chip.pl/2020/01/komisja-europejska-zakaz-rozpoznawania-twarzy-przez-5-lat/ [dostęp 30.08.2021].
7. https://www.speedtest.pl/wiadomosci/esej/skanowanie-twarzy-w-czasie-rzeczywistym-zabronione-przez-unie-europejska/ [dostęp 30.08.2021].
8. https://biznesprawnik.pl/2020/05/26/stanowisko-komisji-europejskiej-w-sprawie-systemow-do-zdalnego-rozpoznawania-twarzy/ [dostęp 30.08.2021].
9. https://www.cyberdefence24.pl/w-usa-rosnie-korzystanie-z-systemow-rozpoznawania-twarzy-uzywa-ich-19-agencji-rzadowych [dostęp 31.08.2021].
10. https://cyfrowa.rp.pl/technologie/34288-pierwsze-miasto-wolne-od-monitoringu-ze-skanowaniem-twarzy [dostęp 31.08.2021].
11. https://www.cyberfeed.pl/portland-uchwala-najsilniejszy-zakaz-rozpoznawania-twarzy-w-usa/ [dostęp 31.08.2021].
12. https://ithardware.pl/aktualnosci/unia_europejska_chce_bana_na_systemy_rozpoznawania_twarzy_w_miejscach_publicznych-16702.html [dostęp 31.08.2021].
13. https://www.interfax.ru/moscow/781825 [dostęp 31.08.2021].
14. https://www.comnews.ru/content/212591/2021-01-19/2021-w03/face-pay-propustit-metro [dostęp 31.08.2021].
15. https://cyfrowa.rp.pl/technologie/62518-strasza-ai-i-rozpoznawaniem-twarzy-to-niedemokratyczne [dostęp 31.08.2021].

[3] *Deepfake* – zbitka wyrazowa od ang. deep learning „głębokie uczenie" oraz fake „fałszywy". Technika obróbki obrazu, polegająca na łączeniu obrazów twarzy ludzkich za pomocą technologii sztucznej inteligencji.