DELab

DIGITAL RESEARCH STUDIES

WORKING PAPER # 4/2021

WYKORZYSTANIE TECHNOLOGII ROZPOZNAWANIA TWARZY W STANACH ZJEDNOCZONYCH AMERYKI

Autorka: Zuzanna Choińska

Opieka naukowa: dr hab. Magdalena Słok-Wódkowska

CYTOWANIE

Z. Choińska, WYKORZYSTANIE TECHNOLOGII ROZPOZNAWANIA TWARZY W STANACH ZJEDNOCZONYCH AMERYKI, DELab Digital Working Studies nr 4/2021, Warszawa 2021.

SPIS TREŚCI

Spis treści

STRESZCZENIE

Stany Zjednoczone charakteryzują się zupełnie innym podejściem do rozwoju technologii i jej regulacji, a także do ochrony danych osobowych, niż jest to przyjęte w Unii Europejskiej. Celem niniejszego artykułu jest przedstawienie, jaki wpływ ma rozwój i wykorzystanie technologii rozpoznawania twarzy w USA na przestrzeganie prawa podstawowego, jakim jest prawo do prywatności oraz na życie obywateli tego kraju. Analiza została przeprowadzona w oparciu o przyjęte oraz postulowane przepisy, aktualne zmiany w postrzeganiu możliwości zastosowania tej technologii oraz priorytety regulacyjne przyjęte na najbliższe lata przez władze amerykańskie.

WSTĘP

Stany Zjednoczone są obecnie prekursorem w zakresie rozwoju nowych technologii. Doprowadziło do tego wiele czynników, ale przede wszystkim określenie rozwoju technologii jako priorytetu ponad np. ochronę praw swoich obywateli. Oprócz tego aktualnie dużą rolę w amerykańskiej gospodarce odgrywają spółki big-tech. W związku z tym Stany Zjednoczone mają bardziej liberalny stosunek do regulacji nowych technologii, w tym do kwestii związanych z ochroną danych osobowych, niż ten przyjęty w UE. Niniejszy artykuł ma na celu przedstawienie, jaki wpływ ma rozwój i wykorzystanie technologii rozpoznawania twarzy (dalej jako „FRT") w USA na przestrzeganie praw podstawowych oraz życie obywateli tego państwa. Analiza została przeprowadzona w oparciu o przyjęte oraz postulowane przepisy, aktualne zmiany w postrzeganiu możliwości zastosowania tej technologii oraz priorytety regulacyjne przyjęte na najbliższe lata przez władze amerykańskie.

Na początku przedstawiam system ochrony prywatności oraz danych osobowych w Stanach Zjednoczonych. Następnie omawiam przepisy oraz propozycję przepisów relewantnych w zakresie uregulowania technologii. Szczególną uwagę poświęcam regulacjom z zakresu danych biometrycznych, które stanowią często jedyny środek ochrony przed nadużyciami wynikającymi ze stosowania technologii rozpoznawania twarzy. Kolejnym omawianym aspektem jest zobrazowanie, na jakim poziomie rozwoju znajduje się omawiana technologia poprzez przedstawienie przykładowych sposobów jej wykorzystania. W zakończeniu przedstawiam wnioski z prowadzonych rozważań.

I. System ochrony prywatności oraz danych osobowych

Na poziomie międzynarodowym Stany Zjednoczone są stroną najważniejszych umów międzynarodowych w zakresie praw człowieka, w tym prawa do prywatności, a mianowicie Powszechnej Deklaracji Praw Człowieka1 oraz Międzynarodowego Paktu Praw Obywatelskich i Politycznych[2].

Na poziomie regionalnym została uchwalona Amerykańska Konwencja Praw Człowieka[3] z 1969 r. Konwencja w dużym stopniu wzorowana była na swoim europejskim odpowiedniku, czyli Europejskiej Konwencji Praw Człowieka[4] (dalej jako „EKPCz")[5]. W zakresie prawa do prywatności wydaje się, że został zapewniony podobny zakres ochrony w tych dwóch aktach prawnych. Jednakże niezaprzeczalną wadą amerykańskiej regulacji jest brak możliwości sądowego dochodzenia wynikających z niej praw[6]. W tym zakresie, stopień ochrony jest na pewno niższy niż ten zapewniony w EKPCz. Co więcej, amerykański sposób uregulowania prywatności wskazuje, że w tamtym regionie rozumie się je, w szczególności, jako ochronę miru domowego, który wywodzi się z kulturowego poszanowania prywatności „domowej" każdego człowieka. Przejawem tego jest np. obowiązujące do dzisiaj uprawnienie do użycia broni w sytuacji wtargnięcia nieznanej osoby na czyjąś posesję. W Europie taka sytuacja byłaby niedopuszczalna.

Koncept prawa do prywatności ma swoje korzenie właśnie w Stanach Zjednoczonych. To tam, w XIX wieku, w amerykańskiej judykaturze pojawiały się pierwsze orzeczenia sądów dotyczące tego zagadnienia. W doktrynie, natomiast, za początek prawa do prywatności jako samodzielnej gałęzi prawa uznaje się wydany w 1890 r. słynny artykuł autorstwa prawników Samuela D. Warrena oraz Louisa D. Brandeisa[7], w którym autorzy zdefiniowali prawo do prywatności jako prawo do bycia pozostawionym w spokoju (a right to be let alone). Pomimo że nie zostało ono nigdy wpisa-

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

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

[3] Amerykańska Konwencja Praw Człowieka (Pakt z San José).

[4] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, Dz.U. 1993 Nr 61, poz. 284.

[5] M. Gołaś-Podolec, *Porównanie europejskiego i interamerykańskiego systemu ochrony praw człowieka*, Krakowskie Studia Międzynarodowe, nr 2, 2008, ss. 159-160.

[6] *Ibidem.*

[7] Powszechna Deklaracja Praw Człowieka (rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklam

ne bezpośrednio do Konstytucji USA, to uważane jest do dziś za jedno z najstarszych praw konstytucyjnych z długą tradycją orzeczniczą[8].

Amerykańskie sądy wywodzą prawo do prywatności z czwartej oraz dziewiątej poprawki do Konstytucji. Czwarta poprawka do konstytucji zapewnia ochronę obywatelom przed nieuzasadnioną rewizją osobistą oraz przeszukaniem ich domów i korespondencji, czyli zapewnia ochronę głównie tzw. miru domowego. Jednakże w amerykańskiej doktrynie oraz judykaturze uznano, że prawo do prywatności wywodzi się właśnie z tego przepisu. Specyfika ustroju prawnego opierającego się na prawie precedensowym pozwala na wywodzenie z orzeczeń sądów prawnie obowiązujących zasad prawnych. Zatem chociaż czwarta poprawka dotyczy jedynie ochrony domu obywatela przed nieuzasadnionym przeszukaniem przez władze publiczne, jej zakres przedmiotowy został rozszerzony przez orzecznictwo, które doprecyzowało, co stanowi przeszukanie w kontekście postępującego rozwoju technologicznego[9]. Przykładowo w 2014 r. Sąd Najwyższy USA orzekł, że prawo do prywatności, o którym mowa w czwartej poprawce, odnosi się do telefonów komórkowych i innych urządzeń cyfrowych używanych do komunikacji, oraz że władze rządowe potrzebują nakazu przeszukania takich urządzeń[10]. Natomiast zgodnie z dziewiątą poprawką, wyliczenie pewnych praw w Konstytucji USA nie może prowadzić do wniosków, że inne prawa przysługujące obywatelom zostały ograniczone lub zniesione[11].

Specyfika amerykańskiego systemu prawnego zapewniająca pewną „elastyczność" pozwala więc na dostosowywanie konkretnych przepisów do zmieniającej się rzeczywistości, następującej np. poprzez rozwój technologiczny. Nie jest to możliwe w systemie kontynentalnym, w którym orzeczenia sądów mają mniejszą moc prawną i w takiej sytuacji konieczne jest uchwalanie kolejnych przepisów prawnych.

owana w dniu 10 grudnia 1948 r.).

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

721174 (dostęp: 23.09.2021 r.).

[9] F.-S. Gady, *EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis*, Georgetown Journal of International Affairs , International Engagement on Cyber IV, 2014, s.13.

[10] J. Swaine, *Supreme court endorses cellphone privacy rights in sweeping ruling,* 2014, https://www.theguardian.com/law/2014/jun/25/supreme-court-police-cellphones-search (dostęp: 23.09.2021 r.).

[11] Z. Mielnik, *Prawo do prywatności (zagadnienia wybrane),* Ruch Prawniczy, Ekonomiczny i Socjologiczny, zeszyt 2, 1996, s. 29.

System ochrony danych osobowych w USA jest zupełnie odmienny od tego przyjętego w Unii Europejskiej. W obu regionach zaczęto tworzyć ramy prawne w tym zakresie mniej więcej w podobnym czasie, czyli w latach 70. XX wieku. Jednakże różnice kulturowe, polityczne oraz prawne, a także filozofia leżącą u podstaw danego podejścia odniosły skutek w postaci znacznych różnic zarówno w instrumentach prawnych, jak i w przyjętym poziomie ochrony. Podczas gdy UE tworzy regulacje prawne stanowiące o szerokiej ochronie danych osobowych jednostek, w USA ustawodawca przedstawia minimalistyczne podejście w tym zakresie i dużo większą uwagę przywiązuje, przynajmniej na poziomie federalnym, do regulacji dotyczących obrotu handlowego oraz państwowych agencji bezpieczeństwa[12]. Ma to swoje uzasadnienie w różnicach zarówno kulturowych, prawnych, jak i politycznych. Amerykańska kultura prawna nastawiona jest na reagowanie na problemy prawne, które się pojawiają, nie ma natomiast ogólnego prewencyjnego charakteru regulacji potencjalnych problemów. Zgodnie z tradycją common law, prawo amerykańskie rozwija się w odpowiedzi na konkretne, faktyczne przypadki. W związku z tym amerykańskie prawo ochrony danych jest również bardziej pragmatyczne i mniej szerokie koncepcyjnie. Jest ono zorientowane na reagowanie na konkretne nadużycia danych osobowych, ale nie zapewnia ogólnej ochrony prawnej przed samymi potencjalnymi zagrożeniami[13].

Duże znaczenie odgrywają tutaj również różnice w zbiorowych doświadczeniach politycznych krajów europejskich i Stanów Zjednoczonych, które przemawiają za bardziej ostrożnym podejściem europejskim. Doświadczenie reżimów totalitarnych, które podporządkowały sobie ludność m. in za pomocą gromadzenia danych osobowych tłumaczy wrażliwość na dane osobowe w wielu krajach europejskich. W USA nacisk kładzie się na inne wartości. Badania wskazują, że amerykański system konstytucyjny oparty jest w większym stopniu na równości, aniżeli reputacji i godności osobistej, która dominuje w krajach europejskich[14]. Jako że ogólne prawa do wolności i prywatności, które stanowią subsydiarną podstawę prawa do ochrony danych, są interpretowane w dużym stopniu w świetle godności osobistej, nie jest zaskakujące, że modyfikacja strukturalna, jak również interes wolności materialnej, od którego zależy ochrona danych, są słabiej rozwinięte w amerykańskiej kulturze prawnej. Przedstawione powyżej podstawowe założenia dominujące w obu

[12] E. Pernot-Leplay, *China's approach on data privacy law: a third way between the U.S. and the EU?,* Penn State Journal of Law & International Affairs, vol. 8, no. 1, 2020, ss. 56-58.

[13] R. Poscher, *The Right to Data Protection. A No-Right Thesis* [w:] R. A. Miller, *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair*, Cambridge University Press, 2017, s. 139.

[14] J. Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, Yale Law Journal, vol. 113, 2004, ss. 1211-1213.

systemach, kontynentalnym oraz common law, pomagają rzucić światło na strukturalne i materialne przyczyny transatlantyckich różnic w kwestii ochrony danych[15].

System prawa amerykańskiego ma też swoje inne specyficzne cechy, które wpływają na kształt aktualnego systemu ochrony danych osobowych w tym państwie. Należy mieć na względzie jego system polityczny, jakim jest system federacyjny. W związku z tym oddzielnie należy omawiać regulacje uchwalane na poziomie federalnym, a oddzielnie te uchwalane na poziomie stanowym. Oprócz tego w USA prywatność uważa się wyłącznie za prawo konsumenta, w przeciwieństwie do UE, gdzie prywatność w Internecie jest zarówno prawem człowieka, jak i konsumenta[16]. Pomimo zapewnienia prawa do prywatności w ustawie zasadniczej, jest to szczególnie widoczne w innych proponowanych regulacjach, gdzie zwraca się uwagę na zapewnienie ochrony konsumentowi przy jednoczesnym dbaniu o interesy przedsiębiorców, nie zważając na prywatność jako prawo wyższego rzędu, czyli prawo człowieka. Ponadto w USA stosuje się głównie podejście sektorowe i takie regulacje zdecydowanie częściej się proponuje w zakresie prywatności, aniżeli regulacje ogólne. Takie podejście opiera się również na tworzeniu regulacji na różnym poziomie, a więc połączeniu powszechnie obowiązującego ustawodawstwa, rozporządzeń wykonawczych, precedensów ustanawianych przez sądownictwo i samoregulacji przedsiębiorstw (czyli tzw. soft law), które stanowią zbiory wytycznych postępowania dla przedstawicieli biznesu, jednakże nie mają powszechnie obowiązującego charakteru[17]. Co więcej, w amerykańskim systemie prawnym nie ma konkretnego rozróżnienia na regulacje dotyczące jedynie prywatności albo jedynie danych osobowych, zazwyczaj zagadnienia te regulowane są wspólnie.

Na poziomie federalnym jednym z pierwszych i nielicznych aktów chroniących całokształt danych osobowych osób fizycznych w USA był uchwalony w 1974 r. Privacy Act[18]. Pomimo swojej innowacyjności oraz wprowadzenia takich idei jak minimalizacja danych czy prawo dostępu do swoich danych – jest ona ograniczona do danych zbieranych przez rząd USA od swoich obywateli. Nie miała ona wpływu na sektor prywatny, a w szczególności na dane gromadzone przez przedsiębiorstwa od konsumentów w Internecie[19]. W kolejnych latach opracowywane były już głównie

[15] R. Poscher, *op. cit.*, s. 140.

[16] A. Aaronson, P. Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, Journal of International Economic Law, 2018, s. 256.

[17] *Ibidem.*

[18] Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2018)).

[19] A. Green, *Complete Guide to Privacy Laws in the US*, 2021, https://www.varonis.com/blog/us-privacy-laws/ (dostęp: 23.09.2021 r.).

sektorowe przepisy o ochronie prywatności na szczeblu federalnym, takie jak ogólny statut o ochronie konsumentów, który powstał na mocy Ustawy o Federalnej Komisji Handlu (Federal Trade Commission Act)[20].

Pomimo że minęło ponad 50 lat od uchwalenia Privacy Act, w amerykańskim systemie ochrony danych na szczeblu federalnym nie zaszło zbyt wiele zmian w kierunku jej wzmocnienia. Propozycji kolejnych regulacji pojawiało się wiele, jednakże żadna z nich nie stała się powszechnie obowiązującym prawem. W lutym 2012 r. administracja prezydenta Baracka Obamy przedstawiła projekt ustawy o ochronie prywatności konsumentów (Consumer Privacy Bill of Rights) – był to zbiór wytycznych dotyczących ochrony danych użytkowników Internetu. Departament Handlu wezwał przedsiębiorców, obrońców prywatności i innych interesariuszy do opracowania i wdrożenia egzekwowalnych polityk prywatności opartych na tych wytycznych[21]. Jednakże do dzisiaj Kongres nie zatwierdził przepisów wzmacniających ochronę danych w USA ani nie był w stanie znaleźć wspólnej płaszczyzny dla nowych przepisów. Przedstawiony projekt był częścią planu wzmacniania regulacji dotyczących prywatności, tak aby uczynić je spójne z ramami prywatności przyjętymi przez międzynarodowych partnerów. Jednakże prace zostały wstrzymane za czasów prezydentury Donalda Trumpa, kiedy wzmocnienie regulacji danoosobowych zeszło na dalszy plan[22].

Niewątpliwie jednak celem na najbliższe lata w USA jest wprowadzenie nowych regulacji oraz zwiększenie ochrony obywateli w zakresie ich danych osobowych. Na przełomie 2018 i 2019 r. amerykańscy senatorowie przedstawili kilkanaście projektów ustaw dotyczących regulacji poszczególnych aspektów prywatności oraz ochrony danych osobowych. Wśród nich znalazły się np. Ustawa o prywatności i prawach konsumenta w mediach społecznościowych z 2018 r. (Social Media Privacy and Consumer Rights Act of 2018), Ustawa o innowacyjnym i etycznym wykorzystaniu danych z 2018 r. (Innovative and Ethical Data Use Act of 2018) czy Ustawa o odpowiedzialności algorytmicznej z 2019 r. (Algorithmic Accountability Act of 2019). Wszystkie z przedstawionych projektów związane były w jakiś sposób z regulacją ochrony danych użytkowników w sferze

[20] F.-S. Gady, *op. cit.*, s. 13.

[21] *We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online*, 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights (dostęp: 23.09.2021 r.).

[22] A. Aaronson, P. Leblond, *op. cit.,* s. 256.

cyfrowej i technologicznej[23]. Pomimo że żaden z nich nie został uchwalony, to mogą posłużyć jako użyteczne wskaźniki tego, w jakim kierunku zmierza obecnie federalne ustawodawstwo dotyczące prywatności w USA. Większość z tych projektów zawierała te same kluczowe prawa i mechanizmy ochrony danych. Najczęściej występującymi przepisami były prawo dostępu, prawo do poprawiania i usuwania danych osobowych, zgoda typu opt-in oraz powiadomienia o naruszeniu ochrony danych. Kolejną, pod względem częstości występowania, grupą były regulacje wymagające przeprowadzenia oceny ryzyka w zakresie ochrony danych lub prywatności. Najrzadziej występującymi przepisami były prawo do przenoszenia danych i prywatne prawo do wniesienia powództwa[24].

Co ciekawe, każdy z projektów przewidywał rozszerzenie kompetencji wspomnianej już powyżej Federalnej Komisji Handlu (dalej jako „FTC")[25]. Ta państwowa agencja odgrywa dużą rolę w kwestii ochrony danych amerykańskich konsumentów. Nie jest to, w rozumieniu europejskim, krajowy organ nadzoru do spraw ochrony danych, jednakże ze względu na przyznane kompetencje, zaczyna pełnić taką funkcję[26]. Prywatne przedsiębiorstwa oraz organizacje pozarządowe też stoją na stanowisku rozszerzenia kompetencji FTC tak, aby odgrywała wiodącą rolę w egzekwowaniu wszelkich nowych regulacji dotyczących prywatności i ochrony danych. Proponuje się przyznanie ustawowych uprawnień np. do nakładania kar cywilnych w działaniach na rzecz ochrony konsumentów czy do podejmowania działań przeciwko naruszeniom bezpieczeństwa i prywatności[27].

Podmioty z sektora prywatnego, a więc również największe amerykańskie korporacje, aktualnie opowiadają się także za uchwaleniem krajowej ustawy o ochronie prywatności, a przy tym za zwiększeniem kompetencji FTC z zakresu prywatności oraz ochrony danych osobowych ze względu na to, że dla nich byłoby to korzystne[28]. Obecnie powodu dużego rozproszenia regulacji z tego zakresu, przepisy, a co za tym idzie, obowiązki przedsiębiorców nie są w pełni jasne i precyzyjne. Uznając nadrzędną rolę FTC jako amerykańskiego organu egzekwującego prawo do prywatności, wykorzystano więc również okazję do wezwania do większej jasności co do tego, które praktyki ochrony prywatności i ochrony danych są rozsądne, a które irracjonalne. Przykładowo koalicja

[23] M. Fazlioglu, *White Paper – Consensus and Controversy in the Debate Over Federal Data Privacy Legislation in the United States*, International Association of Privacy Professionals, 2019, s. 7.

[24] *Ibidem.*

[25] *Ibidem,* s. 9.

[26] F.-S. Gady, *op. cit.*, s. 13.

[27] P. M. Schwartz, *Preemption and Privacy*, The Yale Law Journal, vol. 118, 2009, s. 904.

[28] M. Fazlioglu, *op. cit.,* s. 9.

stowarzyszeń reklamowych, kierowana przez Stowarzyszenie Reklamodawców Narodowych (Association of National Advertisers), zaproponowała, by federalna amerykańska ustawa o ochronie prywatności definiowała „nierozsądne praktyki" związane z danymi lub, bardziej szczegółowo, działania, które naruszyłyby ustawę, a także „rozsądne praktyki" lub takie, które „stwarzają niewielkie lub żadne ryzyko szkody dla konsumenta", a zatem byłyby dopuszczalne[29].

Pomimo braku federalnych regulacji danoosobowych FTC, na podstawie uprawnień przyznanych sobie na mocy Ustawy o FTC z 1914 r., znalazła sposób by przeciwdziałać niezgodnym z ochroną danych działaniom spółek z sektora prywatnego. Zgodnie z ustawą zabrania się im angażowania w „nieuczciwe lub wprowadzające w błąd działania lub praktyki". W związku z tym w połowie XX wieku FTC zaczęła zajmować się wprowadzającymi w błąd reklamami niektórych wiodących amerykańskich marek konsumenckich, a następnie postanowiła przyjrzeć się wprowadzającym w błąd „oświadczeniom" składanym przez wiodące spółki technologiczne i media społecznościowe na temat ochrony gromadzonych przez nie danych. Przykładem jest Facebook, który informował użytkowników w swoich aplikacjach i polityce prywatności, że nie sprzeda ich danych lub że użytkownicy mogą ograniczyć dostęp do danych, jeżeli klikną na pewne pola. W rzeczywistości było odwrotnie i FTC złożyła w 2012 r. skargę przeciwko Facebookowi, który zgodził się na ugodę. Następnie złożono kolejne skargi, które później zyskały duży rozgłos w mediach. W rezultacie doszło do ugody, zgodnie z którą Facebook zapłacił 5 miliardów dolarów kary[30].

Jeżeli jednak przedsiębiorstwo nie wspomina nic o prywatności danych na swojej stronie internetowej, w swoich produktach lub w reklamie, to FTC nie może podjąć żadnych działań, przynajmniej w ramach swoich uprawnień „wprowadzających w błąd działań lub praktyk". Ogólne federalne prawo o ochronie danych zmusiłoby przedsiębiorstwa do posiadania wymaganych prawem polityk prywatności i przestrzegania ich, zamiast przechodzenia przez pośredni (i niedoskonały) mechanizm egzekwowania prawa do prywatności przez FTC[31].

W związku z brakiem odpowiednich regulacji na poziomie federalnym i w odpowiedzi na rosnące obawy związane z ochroną danych swoich obywateli poszczególne stany zaczęły przygotowywać swoje propozycje[32]. Takie przepisy są ograniczone oczywiście do terytorium danego stanu, widać

[29] *Ibidem.*

[30] A. Green, *op. cit.*

[31] *Ibidem.*

[32] E. Pernot-Leplay, *op. cit.*, s. 60.

jednak, że te tworzone w jednym z nich inspirują do tworzenia kolejnych. W rezultacie możliwe że dzięki temu szybciej powstaną również regulacje na poziomie federalnym.

Najbardziej znanym przykładem stanowej regulacji danoosobowej, często porównywanym do europejskiego RODO[33], jest uchwalona w 2018 r. kalifornijska ustawa California Consumer Privacy Act (dalej jako „CCPA")[34]. Ustawa ta uznawana jest za najbardziej kompleksową, skoncentrowaną na środowisku cyfrowym regulację dotyczącą ochrony danych w USA[35]. Jednakże tak samo jak na poziomie federalnych, regulacje stanowe, w tym CCPA, chronią najczęściej jedynie prywatność konsumentów w relacjach z biznesem, a nie wszystkich osób fizycznych, których dane mogą być przetwarzane. Chociaż dyskutowano nad rozszerzeniem obowiązywania ustawy także na pracowników, to jednak nie zdecydowano się na wprowadzenie takiego rozwiązania. Pomimo że CCPA znacznie wzmacnia ochronę, pozostaje ustawą o węższym zakresie i słabszych zabezpieczeniach niż unijny standard, np. nie ustanawia wymogu określenia podstawy prawnej do gromadzenia i przetwarzania danych, a prawo do wniesienia skargi dla osób fizycznych jest ograniczone do kwestii bezpieczeństwa w kontekście naruszenia danych[36].

CCPA nie jest natomiast jedynym aktem z zakresu prywatności i ochrony danych przyjętych w Kalifornii. Kalifornijski ustawodawca zatwierdził California Privacy Rights Act (dalej jako „CPRA"), zwany również CCPA 2.0. Od 1 stycznia 2023 r. stanie się on obowiązującą regulacją i zastąpi CCPA. Ustawa opiera się na istniejących ramach CCPA, rozszerza prawa konsumentów do prywatności, aby lepiej dostosować się do unijnego RODO, nakłada dodatkowe obowiązki na przedsiębiorstwa i ustanawia pierwszą w kraju agencję zajmującą się regulowaniem i egzekwowaniem prywatności, Kalifornijską Agencję Ochrony Prywatności (California Privacy Protection Agency, CCPA)[37]. CPRA rozszerza swój zakres podmiotowy CCPA właśnie o dane pracownicze oraz dane przekazywane pomiędzy przedsiębiorcami[38].

---

[33] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz.UE.L 2016 Nr 119, s. 1.

[34] California Consumer Privacy Act of 2018 [California Civil Code 1798.100–1798.198].

[35] A. Green, *op. cit.*

[36] E. Pernot-Leplay, *op. cit.*, s. 60.

[37] M. Bahar, M. J. Wilson-Bilik, A. F. L. Sand, *California's new privacy law, the CPRA, was approved: Now what?*, 2020, https://www.lexology.com/library/detail.aspx?g=5a7edce9-26af-487c-8877-7a815945954d (dostęp: 23.09.2021 r.).

[38] *Ibidem.*

Za przykładem Kalifornii poszły również inne stany. Jak na razie, poza tym stanem, obowiązujące regulacje z zakresu ochrony prywatności ma jedynie Wirginia oraz Kolorado. Natomiast wiele stanów takich jak Ohio, Massachusetts czy Nowy Jork ma swoje przepisy w przygotowaniu[39]. Analizy wskazują, że większość ustaw bądź projektów ustaw zawiera te same kluczowe postanowienia w zakresie ochrony danych, jak np. prawo dostępu do swoich danych czy prawo do ich usunięcia[40]. Budzi to nadzieję na wypracowanie wspólnego standardu, a w rezultacie ogólne polepszenie standardu ochrony danych osobowych dla obywateli Stanów Zjednoczonych.

Analiza amerykańskiego systemu ochrony danych osobowych prowadzi do wniosków, że konieczne jest uchwalenie generalnej regulacji na poziomie federalnym, aby właściwie chronić prawa amerykańskich konsumentów, a także w celu dostosowania poziomu ochrony do międzynarodowych partnerów, przykładowo przedsiębiorców z Unii Europejskiej. Widać jednak, że taką potrzebę zauważyli także członkowie Kongresu, brakuje jedynie konsensusu co do odpowiedniego kształtu ustawy. O krok dalej znajdują się aktualnie ustawodawcy w poszczególnych stanach USA. Część z nich ma już w mocy swoje ustawy, a część jest na etapie procesu legislacyjnego. Podejmowane działania dają nadzieję na wypracowanie wspólnego standardu w najbliższej przyszłości.

II. Ramy regulacyjne dla sztucznej inteligencji oraz technologii rozpoznawania twarzy

Stany Zjednoczone są światowym liderem, jeżeli chodzi o rozwój systemów sztucznej inteligencji, a więc również technologii rozpoznawania twarzy. Szybki rozwój w tym zakresie kreuje potrzebę wprowadzenia odpowiednich regulacji prawnych, tak aby zapewnić odpowiednią ochronę obywatelom przed rodzącymi się zagrożeniami, do których należą np. naruszenia ich prywatności. Regulacje prawne stanowią swego rodzaju przeszkody dla rozwoju technologii, a na pewno ten rozwój spowalniają. Przykład Unii Europejskiej dobrze to pokazuje – unijni ustawodawcy skupili się na stworzeniu przepisów prawnych w pierwszej kolejności, tak aby chronić obywateli przed naduży-

[39] S. Rippy, *US State Privacy Legislation Tracker*, 2021, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (dostęp: 23.09.2021 r.).

[40] A. Green, *op. cit.*

ciami. W rezultacie w UE zaawansowane systemy SI powstają dużo wolniej. Wręcz przeciwnie sytuacja wygląda w USA. Zarówno tam, jak i w Chinach regulacje prawne pełnią drugorzędną rolę, a więc bez tych ograniczeń, technologia jest w stanie rozwijać się w dużo szybszym tempie.

Akty prawne regulujące stosowanie sztucznej inteligencji czy technologii rozpoznawania twarzy w USA w zasadzie nie istnieją, w środowisku zainteresowanych podmiotów pojawiają się jedynie pewne pomysły i rekomendacje. W 2018 r. utworzona została Narodowa Komisja Bezpieczeństwa do spraw sztucznej inteligencji (*The National Security Commission on Artificial Intelligence,* dalej jako „NSCAI"). Do jej zadań należy rozważenie metod i środków niezbędnych do przyspieszenia rozwoju sztucznej inteligencji i powiązanych technologii w celu kompleksowego zaspokojenia potrzeb bezpieczeństwa narodowego i obronności Stanów Zjednoczonych, a także przedstawianie Prezydentowi i Kongresowi raportów dotyczących ustaleń Komisji oraz zaleceń[41]. W marcu 2021 r. NSCAI wydała kompleksowy raport, w którym przedstawia „zintegrowaną strategię narodową mającą na celu reorganizację rządu, reorientację narodu oraz zmobilizowanie najbliższych sojuszników i partnerów do obrony i rywalizacji w nadchodzącej erze konkurencji i konfliktów napędzanych przez sztuczną inteligencję"[42].

Autorzy raportu podkreślają, że priorytetem powinna być poprawa bezpieczeństwa narodu amerykańskiego z jednej strony, a z drugiej ochrona wolności i prywatności poszczególnych obywateli[43]. Od czasu zamachu terrorystycznego z 11 września 2001 r. toczy się debata, jak osiągnąć oba te cele, a przynajmniej jak znaleźć pomiędzy nimi balans, gdy pojawiają się napięcia. Ostatnie dwie dekady to intensywne wysiłki zmierzające do pogodzenia uprawnień rządu do powstrzymania kolejnego ataku terrorystycznego z jego obowiązkami w zakresie poszanowania praw i wolności jednostki. Dostęp do sztucznej inteligencji prowadzi do podjęcia kolejnej debaty, ponieważ nowe technologie oferują agencjom rządowym potężniejsze sposoby gromadzenia i przetwarzania informacji, śledzenia zachowań i ruchów jednostek oraz podejmowania działań na podstawie analiz generowanych komputerowo[44].

W raporcie podkreśla się istnienie rosnących zagrożeń dla prywatności i wolności osobistych jednostek ze względu na błyskawiczny postęp w rozwoju SI i wykorzystaniu jej systemów przez ame-

[41] Zob. więcej https://www.nscai.gov/ (dostęp: 23.09.2021 r.).
[42] Final Report – National Security Commission on Artificial Intelligence, 2021, s. 8.
[43] *Ibidem*, s. 143.
[44] *Ibidem,* s. 143.

rykańskie agencje bezpieczeństwa, takie jak CIA czy FBI. W związku z tym NSCAI wskazuje na potrzebę opracowania aktów prawnych, zasad oraz procedur minimalizujących gromadzenie, przechowywanie i rozpowszechnianie danych amerykańskich obywateli, a także nadzór ze strony rządu. Rekomenduje również inwestowanie i przyjęcie narzędzi opartych na sztucznej inteligencji w celu wzmocnienia nadzoru i audytu na rzecz wspierania prywatności i swobód obywatelskich po to, aby wypracować zaufanie społeczne dla używania systemów SI przez organy władzy publicznej oraz zapewnić, że ich wykorzystanie jest skuteczne oraz zgodne z prawem. Wymaga to także przyznania osobom, na które wpływają działania rządu związane z SI, możliwości ubiegania się o zadośćuczynienie oraz zagwarantowania im sprawiedliwego procesu. Według NSCAI rząd powinien również powołać grupę zadaniową w celu oceny zmieniających się obaw dotyczących SI i prywatności, swobód obywatelskich i praw obywatelskich[45].

W kwestii technologii rozpoznawania twarzy raport nie rozstrzyga zbyt wiele. Zwraca jedynie uwagę na to, szybki postęp w dziedzinie technologii do celów egzekwowania prawa, w tym technik nadzoru biometrycznego, takich jak rozpoznawanie twarzy, może wyprzedzać zasady ich właściwego stosowania. Rząd musi zachować szczególną ostrożność w zarządzaniu ryzykiem dla podstawowych zasad konstytucyjnych, w tym np. wolności od nieuzasadnionych przeszukań i konfiskat. NSCAI podkreśla również, że badania wskazują, że korzystanie z algorytmów uczenia maszynowego, na którym oparte jest FRT, może prowadzić do niezamierzonych uprzedzeń, co może spowodować dyskryminacyjne traktowanie poszczególnych obywateli USA[46].

W kontekście braku kompleksowej regulacji na poziomie ogólnokrajowym dotyczącej technologii rozpoznawania twarzy czy nawet sztucznej inteligencji zarówno w sektorze prywatnym, jak i publicznym, raport wydany przez NSCAI wydaje się dobrym punktem wyjścia do dalszych dyskusji w tym zakresie. NSCAI wskazała w raporcie zagrożenia związane z szybkim rozwojem algorytmów SI oraz pewne rekomendacje, a także propozycje dalszych działań, aby zapobiegać tym zagrożeniom. Pozostaje jedynie obserwować, jakie kroki podejmie władza ustawodawcza w USA, gdyż niewątpliwie takie regulacje w najbliższym czasie są konieczne. Badania wskazują, że już w 2014 r. algorytmy wyprzedziły możliwości człowieka w dokładności rozpoznawania ludzkich twarzy[47], nato-

[45] *Ibidem,* ss. 144-147.
[46] *Ibidem*, ss. 144-145.
[47] *The Face Recognition Algorithm That Finally Outperforms Humans*, 2014, https://medium.com/the-physics-arxiv-blog/the-face-recognition-algorithm-that-finally-outperforms-humans-2c567adbf7fc (dostęp: 23.09.2021 r.).

miast w 2021 r. ich poziom rozwoju jest dużo wyższy, co może powodować więcej zagrożeń dla prywatności obywateli.

Obecnie nie istnieją żadne przepisy federalne regulujące wykorzystanie technologii rozpoznawania twarzy ani takie, które chroniłyby dane biometryczne konsumentów. Jedynie pojedyncze sektorowe amerykańskie przepisy dotyczące prywatności mogą ograniczać niektóre zastosowania systemów FRT w określonych sytuacjach[48]. Natomiast przywoływany już wcześniej *Privacy Act* zapewnia co prawda ochronę danych przed organami władzy publicznej, ale nie przed podmiotami w sektorze prywatnym. Co więcej, sam brak federalnych regulacji dotyczących danych biometrycznych pozwala rządowi nie stosować się do niektórych wymagań ustawy z pomocą nieuregulowanego sektora prywatnego[49].

Jednakże pewne próby wprowadzenia takich przepisów prawnych były podejmowane. Pierwsze próby uregulowania kwestii komercyjnego wykorzystania technologii rozpoznawania twarzy w celu identyfikacji lub uwierzytelnienia osoby fizycznej miały formę niewiążących wytycznych oraz zbiorów dobrych praktyk wydanych przez Federalną Komisję Handlu (FTC) w 2012 r. oraz Departament Handlu *National Telecommunications and Information Administration* w 2016 r. Jednakże żaden z tych instrumentów nie zawierał odpowiedniej definicji ani danych biometrycznych, ani technologii rozpoznawania twarzy. Określały one głównie kwestie powiadamiania o zbieraniu i analizie danych oraz zbierania zgody przed dokonaniem identyfikacji[50].

Kongres przedstawił w 2017 r. projekt Ustawy o ochronie prywatności konsumentów[51] (*Consumer Protection Privacy Act of 2017*), która wymagałaby od przedsiębiorstw, aby informowały swoich użytkowników o naruszeniach i niewłaściwym wykorzystaniu danych osobowych „tak szybko, jak to możliwe". Chociaż przepisy te miałyby na celu chronić dane biometryczne, projekt nie przewidywał wymogu zebrania zgody lub powiadomienia przed tym, jak administrator zacznie zbierać lub wykorzystywać dane. Co więcej, ustawodawstwo to obejmowałoby swoim zakresem tylko te podmioty, które zbierają dane biometryczne co najmniej 10 000 Amerykanów rocznie, co znacznie

[48] S. duPont, *On Facial Recognition, the U.S. Isn't China—Yet*, 2020, https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet (dostęp: 23.09.2021 r.).
[49] F. Q. Nguyen, *The Standard for Biometric Data Protection*, 2018, Journal of Law & Cyber Warfare, Vol. 7, No. 1, s. 66.
[50] *Facial recognition regulation in the USA: an efficient legal patchwork?,* 2020, https://www.avocats-mathias.com/donnees-personnelles/facial-recognition-usa (dostęp: 23.09.2021 r.).
[51] H.R.4081 - Consumer Privacy Protection Act of 2017.

zawęziłoby możliwości stosowania ustawy, a przy tym obniżyłoby poziom przyznanej konsumentom ochrony[52].

W lutym 2020 r. dwóch senatorów zgłosiło projekt ustawy, która miała chronić prywatność konsumentów przed „szybko rozwijającą się technologią rozpoznawania twarzy i praktykami gromadzenia danych, które zwiększają ryzyko nadmiernego nadzoru i nadmiernej inwigilacji". Ustawa o etycznym korzystaniu z technologii rozpoznawania twarzy (*Ethical Use of Facial Recognition Act*) miałaby na celu ochronę prawa Amerykanów do prywatności poprzez wprowadzenie moratorium na korzystanie z tej technologii przez władze publiczne do czasu, aż Kongres przyjmie przepisy określające konkretne zasady stosowania tej technologii. Ustawa ta przewidywała powołanie komisji, której zadaniem byłoby opracowanie zaleceń w celu zapewnienia, że jakiekolwiek przyszłe federalne wykorzystanie technologii rozpoznawania twarzy będzie ograniczone do odpowiedzialnych zastosowań, które promują bezpieczeństwo publiczne i chronią prywatność obywateli[53]. W Senacie odbyło się dwukrotne czytanie projektu ustawy, a następnie została ona skierowana do Komisji Bezpieczeństwa Wewnętrznego i Spraw Rządowych (*Committee on Homeland Security and Governmental Affairs*)[54].

Natomiast na przełomie 2019 i 2020 Kongres wyraził zamiar przyjęcia ustawy regulującej wymóg uzyskania nakazu sądowego na stosowanie technologii rozpoznawania twarzy (*Facial Recognition Technology Warrant Act*). Ustawa ta zmusiłaby organy ścigania do uzyskania, przed jakimkolwiek wykorzystaniem rozpoznawania twarzy, nakazu opartego na prawdopodobnej przyczynie działalności przestępczej. Takie nakazy mogłyby być wydawane na maksymalny okres 30 dni i nakładałyby na organy ścigania obowiązek ograniczenia do minimum pozyskiwania, zatrzymywania i rozpowszechniania informacji dotyczących osób, które nie są objęte zakresem nakazu. Ustawa ta zapewniłaby również pewien nadzór nad decyzjami sędziów, nakładając na nich obowiązek zgłaszania wyników każdego wniosku do Biura Administracyjnego Sądów Stanów Zjednoczonych. Ten organ musiałby prowadzić rejestr i sporządzać sprawozdania dla Senatu i Izby Reprezentantów USA[55].

[52] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, Journal of Law and Policy, vol. 26, no. 2, 2018, s. 800.
[53] *Facial recognition regulation in the USA: an efficient legal patchwork?, op. cit.*
[54] https://www.congress.gov/bill/116th-congress/senate-bill/3284/actions (dostęp: 23.09.2021 r.).
[55] *Ibidem.*

Dotychczas nie pojawiła się jednak propozycja przepisów na poziomie federalnym dotyczących przetwarzania danych biometrycznych ani stosowania FRT przez sektor prywatny. Jednym z powodów takiego stanu rzeczy może być fakt, że spółki technologiczne są coraz bardziej świadome ryzyka pozwów sądowych na podstawie ustaw o ochronie danych. W związku z tym zaczęły agresywnie lobbować przeciwko wszelkim ustawom, które mogłyby regulować wykorzystanie danych biometrycznych[56]. Przykładowo Facebook sprzeciwia się wszelkim formom regulacji dotyczących tej technologii. Odegrał on znaczącą rolę w blokowaniu wielu stanowych ustaw, które regulowałyby wykorzystanie danych biometrycznych. Trafne może być założenie, że jeśli federalne ustawodawstwo biometryczne zostałoby zaproponowane, spółka byłaby jedną z pierwszych, która zdecydowanie podjęłaby pewne kroki, aby do tego nie dopuścić[57].

Przedstawione powyżej propozycje federalnych przepisów regulujących wykorzystanie technologii rozpoznawania twarzy bądź przetwarzania danych biometrycznych to tylko pojedyncze przykłady z wielu przedstawionych projektów w ostatnim czasie. Powstaje więc pytanie, dlaczego – pomimo wielu prób i projektów ustaw – nie udało się do tej pory uchwalić w tym zakresie federalnych regulacji. Oprócz działań korporacji technologicznych, takich jak Facebook, wskazuje się, że jednym z największych wyzwań przy tworzeniu federalnych regulacji chroniących dane biometryczne może być brak wypracowanej spójnej definicji terminu „biometria", przez co proponowane projekty grzęzną już na początku swojej legislacyjnej drogi. Z jednej strony jest to problem dla ustawodawców w konkretnych stanach, które proponują swoje ustawodawstwo w tym zakresie, natomiast z drugiej, dla spółek technologicznych stanowi to dużą szansę na stworzenie definicji najbardziej korzystnej dla ich modeli biznesowych[58]. Kolejną obawą wyrażaną przez niektórych ekspertów jest to, że federalne ustawodawstwo regulujące dane biometryczne może naruszać pierwszą poprawkę do Konstytucji USA, a także tzw. *Commerce Clause*, ze względu na możliwe wystąpienie dyskryminacji co do treści[59]. Jednakże ten argument przeciwko ustawodawstwu biometrycznemu wydaje się mniej istotny niż interes w postaci zapewnienia odpowiedniego poziomu ochrony danych kon-

[56] C. Pope, *op. cit.,* s. 798.
[57] C. Burt, Facebook lobbying against facial recognition laws, 2017, https://www.biometricupdate.com/201708/facebook-lobbying-against-facial-recognition-laws (dostęp: 23.09.2021 r.).
[58] B. J. Buyer, *Washington's New Biometric Privacy Law: What Businesses Need to Know*, 2017, https://www.dwt.com/insights/2017/07/washingtons-new-biometric-privacy-law-what-busines (dostęp: 23.09.2021 r.).
[59] Zob więcej J. Bambauer, J. E. Rogers, *Biometric privacy laws: How a Little-Known Illinois Law Made Facebook Illegal*, Program on Economics & Privacy, 2017, https://pep.gmu.edu/wp-content/uploads/sites/28/2017/06/Biometric-Privacy-Laws-FINAL_really_6.20-.pdf (dostęp: 23.09.2021 r.).

sumentów. Jest to jak na razie problem teoretyczny, gdyż żaden sąd nie wydał do tej pory orzeczenia w sprawie kwestii konstytucyjnych związanych z gromadzeniem danych biometrycznych[60].

Zupełnie inaczej sytuacja wygląda na poziomie stanowym, gdzie przepisów dotyczących przetwarzania danych biometrycznych jest znacznie więcej. Już w 2008 r. pojawiła się kompleksowa ustawa w stanie Illinois zwana *Illinois Biometric Information Privacy Act* (dalej jako „BIPA")[61], której uchwalenie sprawiło, że także inne stany zaczęły rozważać wprowadzenie swoich własnych przepisów. Niedługo potem do Illinois dołączyły stany, takie jak Texas, Waszyngton czy Kalifornia. Jednakże wiele stanów nadal pozostaje bez swoich regulacji.

Zgodnie z BIPA, przedsiębiorstwom i innym organizacjom zabrania się nabywania, przechwytywania lub uzyskiwania osobistych „informacji biometrycznych", chyba że przedsiębiorstwo najpierw poinformuje lub otrzyma pisemną zgodę podmiotu, którego dane są zbierane. Wśród opinii publicznej podnosi się, że ponieważ ustawa BIPA została przyjęta prawie dziesięć lat temu, stała się ona przestarzała w stosunku do obecnej technologii. BIPA była do tej pory podstawą większości sporów dotyczących prywatności danych biometrycznych. Jednakże BIPA dała mieszkańcom Illinois środki, za pomocą których mogą oni ścigać gigantów technologicznych, takich jak Facebook, za bezprawne zbieranie ich danych biometrycznych. Facebook z kolei wynajął przedsiębiorstwo lobbingowe z siedzibą w Illinois, aby pracować nad zmianą prawa stanowego, tak aby było ono bardziej przychylne spółkom technologicznym gromadzącym dane biometryczne[62]. Chociaż BIPA nie jest idealna ani w pełni aktualna, jest prawdopodobnie najlepszym istniejącym aktem prawnym dla konsumentów, w którego założeniach jest zakwestionowanie niezgodnego z prawem gromadzenia danych biometrycznych.

Waszyngton może pochwalić się dwoma ustawami, które swoim zakresem obejmują zarówno sektor publiczny, jak i prywatny. Jest to jedyny stan, który ma uchwalone regulacje w kontekście przetwarzania danych biometrycznych przez władze publiczne[63]. W 2020 r. przyjęto w Waszyngtonie najbardziej kompleksowe prawo dyscyplinujące rządowe wykorzystanie technologii rozpoznawania twarzy. Choć krytykowana za to, że nie jest wystarczająca i sprzyja interesom spółek technologicznych, ustawa wprowadza znaczne ograniczenia w wykorzystaniu FRT przez organy

[60] C. Pope, *op. cit.,* s. 799.
[61] Illinois Biometric Information Privacy Act, 740 ILCS 14/1-99 (2008).
[62] J. Bennett, *Saving Face: Facebook Wants Access Without Limits,* 2017, Https://Publicintegrity.Org/%202017/07/31/21027/Saving-Face-Facebook-Wants-Access-Without-Limits. (dostęp: 23.09.2021 r.).
[63] S. duPont, *op. cit.*

ścigania, które mają określać cel użycia tej technologii oraz publikować tzw. „raport odpowiedzialności"[64]. Przepisy wymagają weryfikacji przez człowieka każdej decyzji podjętej przy użyciu technologii rozpoznawania twarzy, która miałaby skutki prawne lub „podobnie znaczące skutki" dla danej osoby, także w takich obszarach jak mieszkanie, edukacja, zatrudnienie, ubezpieczenie lub prawa obywatelskie[65]. Ustawa zakłada również, aby agencje rządowe testowały technologię w „warunkach operacyjnych" i udostępniły interfejs programowania aplikacji (API), aby ułatwić testowanie technologii przez osoby trzecie. Być może najważniejsze jest to, że prawo ogranicza możliwość wykorzystywania technologii rozpoznawania twarzy do nadzoru w czasie rzeczywistym. Władze mogą przeprowadzać takie skanowanie na żywo tylko po uzyskaniu nakazu, podczas próby odnalezienia zaginionej osoby lub w „wyjątkowych okolicznościach". Taka regulacja przywodzi na myśl przepisy proponowane w unijnym projekcie rozporządzenia w sprawie SI, gdyż są one w zasadzie tożsame. Ponadto władze nie mogą używać technologii rozpoznawania twarzy do rejestrowania korzystania z praw wynikających z pierwszej poprawki do Konstytucji – np. podczas protestu lub w trakcie obrzędów religijnych[66].

W 2017 r. w Waszyngtonie uchwalono natomiast ustawę o ochronie danych biometrycznych skierowaną do sektora prywatnego, a w szczególności do przedsiębiorstw, które gromadzą i sprzedają dane biometryczne bez wiedzy użytkowników. Waszyngtońska ustawa była jednak przedmiotem poważnych nacisków ze strony korporacji technologicznych, takich jak Google i Facebook[67]. Facebook ponownie wynajął lobbystów, aby agresywnie pracowali nad zatrzymaniem ustawy w miejscu, a w rezultacie powstała znacznie złagodzona wersja ustawy z Illinois[68]. Co warte podkreślenia, ustawa ta nie obejmuje fotografii cyfrowych ani nagrań głosowych w definicji „identyfikatora biometrycznego", co oznacza, że programy takie jak funkcja oznaczania twarzy Facebooka nie wchodzą w zakres ustawy. Prokurator generalny stanu Waszyngton jest jedyną osobą w stanie, która ma prawo egzekwować przepisy ustawy. Statut zabrania także wnoszenia prywatnych pozwów przeciwko spółkom naruszającym prawo. Popularny jest pogląd, że ten wyjątek dla danych dotyczących twarzy, w połączeniu z zakazem wnoszenia pozwów, sprawia, że prawo waszyngtońskie jest bardziej przyjazne dla biznesu niż ustawa uchwalona np. w Illinois[69]. Ustawa o ochro-

[64] *Ibidem.*
[65] S. Chun, Facial Recognition Technology: A Call For The Creation Of A Framework Combining Government Regulation And A Commitment To Corporate Responsibility, North Carolina Journal of Law & Technology Vol. 21, Issue 4, 2020, ss. 118-119.
[66] S. duPont, *op. cit.*
[67] K. Mehrotra, *Tech Companies are Pushing Back Against Biometric Privacy Laws*, 2017, https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws (dostęp: 23.09.2021 r.).
[68] J. Bennett, *op. cit.*
[69] C. Pope, *op. cit.,* s. 792-793.

nie danych biometrycznych w Waszyngtonie dobrze ilustruje, jakie mogą być następstwa tego, gdy korporacje technologiczne są skłonne zainwestować duże ilości czasu i pieniędzy, aby zapobiec niekorzystnej dla siebie ustawie.

Najnowszą ustawą, który swoim zakresem obejmuje również dane biometryczne jest wspominana już wcześniej CCPA. Ta kompleksowa ustawa uchwalona w Kalifornii w 2018 r. nie tylko chroni ogólnie prywatność i dane osobowe obywateli, ale zawiera także oddzielne regulacje dotyczące danych biometrycznych. CCPA włącza dane z rozpoznawania twarzy do definicji danych biometrycznych i danych osobowych[70]. Jest ona zbieżna z wieloma wymogami określonymi w RODO. Wymaga przykładowo od podmiotów, które mają roczny dochód brutto przekraczający 25 milionów dolarów lub otrzymują dane osobowe ponad 50 000 konsumentów w ciągu roku, aby, między innymi, informowały konsumentów o tym, że przedsiębiorstwo gromadzi dane osobowe, zapewniały konsumentom dostęp do ich danych na żądanie klienta i umożliwiały im usunięcie takich danych, jeśli sobie tego życzą. Spółki, które nie przestrzegają wymogów określonych w ustawie CCPA, są narażone na pozwy sądowe oraz wysokie kary pieniężne nakładane przez kalifornijskiego Prokuratora Generalnego[71].

Co więcej, poszczególne miasta całkowicie zakazują stosowania technologii rozpoznawania twarzy. Na przykład kilkanaście miast w Kalifornii i Massachusetts całkowicie zakazało stosowania FRT przez władze publiczne, podczas gdy Portland w Oregonie rozważa pójście dalej i zakazanie stosowania tej technologii zarówno w sektorze publicznym, jak i prywatnym. Natomiast trzy stany zakazały stosowania technologii rozpoznawania twarzy w policyjnych aparatach fotograficznych (mimo że co najmniej jedna spółka reklamuje swoje policyjne aparaty fotograficzne pod kątem ich zdolności do rozpoznawania twarzy w czasie rzeczywistym)[72].

Pojawia się również pytanie, czy w Stanach Zjednoczonych konieczne jest uchwalenie prawa na poziomie federalnym, skoro istnieje wiele regulacji na poziomie stanowym. Niestety praktyka pokazuje, że regulacje stanowe nie są wystarczające. Największe technologiczne korporacje działają jednak na obszarze całego kraju, więc lokalne ograniczanie ich działań nie jest wystarczające. W postępowaniu sądowym przeciwko Facebookowi[73] powodowie wnieśli pozew na podstawie BIPA,

[70] S. Chun, op. cit., s. 118.
[71] Robert B., *Biometrics and the CCPA*, https://www.termsfeed.com/blog/ccpa-biometrics/ (dostęp: 23.09.2021r.).
[72] S. duPont, *op. cit.*
[73] *In re Facebook Biometric Info. Privacy Litig.,* 185 F.Supp.3d 1155 (2016).

zarzucając, że Facebook bezprawnie gromadził i przechowywał dane biometryczne wizerunków twarzy powodów w celu identyfikacji ich na zdjęciach w ramach swojego programu *Tag Suggestions*. W odpowiedzi Facebook złożył wniosek o oddalenie powództwa i argumentował, że prawo stanu Illinois nie ma zastosowania ze względu na przepis wyboru prawa w umowie użytkowników, zgodnie z którym prawem właściwym jest prawo kalifornijskie. Drugim argumentem Facebooka było to, że nawet jeśli BIPA zapewnia powodom podstawę do wniesienia powództwa za zbieranie i wykorzystywanie ich danych biometrycznych, sugestie znaczników Facebooka nie są chronionymi danymi biometrycznymi w rozumieniu BIPA[74].

Sąd obszernie omówił każdy z tych argumentów obrony, stwierdzając, że umowne postanowienie wyboru prawa kalifornijskiego nie będzie egzekwowane, ponieważ stan Illinois ma istotnie większy interes w rozstrzygnięciu sprawy[75]. Sąd zauważył również, że do celów wniosku o odrzucenie pozwu powodowie przedstawili wystarczające fakty, aby wykazać, że sugestie zawarte w *tagach* mogą być chronione na mocy ustawy BIPA, gdyż definiuje ona dane biometryczne jako „skan geometrii dłoni lub twarzy". W przedmiotowej sprawie powodowie twierdzili, że Facebook skanuje zdjęcia załadowane przez użytkowników w celu stworzenia „unikalnej cyfrowej reprezentacji twarzy w oparciu o geometryczne relacje ich rysów twarzy". Zarzut ten mieścił się w zakresie skanowania geometrii twarzy, o którym mowa w ustawie. Sąd przyjął za prawdziwe twierdzenia powodów, że technologia rozpoznawania twarzy stosowana przez Facebooka obejmowała skanowanie geometrii twarzy, które zostało wykonane bez zgody powodów[76]. Wniosek Facebooka o odrzucenie pozwu został przez sąd odrzucony.

W innej sprawie, w postępowaniu przeciwko Google[77], powodowie zarzucali naruszenie ustawy BIPA w związku z bezprawnym wykorzystaniem przez nią podobnej do Facebooka technologii skanowania twarzy. Google przedstawił trzy argumenty. Pierwszy z nich stanowił, że skargi powodów dotyczyły „wykorzystania przez Google ich fotografii, a BIPA nie obejmuje fotografii ani informacji pochodzących z fotografii". Drugi dotyczył tego, że Google nie prowadzi swojej działalności w stanie Illinois, więc prawo tego stanu nie może mieć zastosowania. W trzecim natomiast Google podniósł, że „jeśli BIPA rzekomo obejmuje działanie Google poza Illinois, to ustawa stano-

[74] F. Q. Nguyen, *op. cit*., ss. 68-69.
[75] In re Facebook Biometric Info. Privacy Litig. - 185 F. Supp. 3d 1155 (N.D. Cal. 2016), https://www.lexisnexis.com/community/casebrief/p/casebrief-in-re-facebook-biometric-info-privacy-litig (dostęp: 23.09.2021 r.).
[76] *Ibidem.*
[77] *Rivera v. Google*, Inc. 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

wa w rzeczywistości koliduje z federalną konstytucyjną klauzulą *Dormant Commerce Clause*"[78]. Chociaż sąd odrzucił wniosek Google'a o oddalenie sprawy, to uznał również, że BIPA „nie miała i nie ma zastosowania eksterytorialnego" i że potrzeba więcej faktów, aby sąd mógł przeanalizować, jak „konkretne działania Google pasują do obecnego stanu prawnego dotyczącego internetowych naruszeń *Commerce Clause*"[79].

Powyższe przykłady wskazują, że istnienie jedynie stanowych regulacji w zakresie ochrony danych biometrycznych w związku z technologią rozpoznawania twarzy zdecydowanie nie jest wystarczające. W przywołanym sprawach pozwani wnieśli o oddalenie powództwa na podstawie przepisu o wyborze prawa. Prawdopodobnie będzie się tak działo nadal, jeśli odpowiednie przepisy będą istniały tylko w niektórych stanach albo gdy wprowadzane standardy ochrony będą zróżnicowane[80].

Oprócz tego rozwój ustawodawstwa poszczególnych stanów następuje często zbyt wolno, aby sprostać szybkości gromadzenia i przetwarzania danych biometrycznych. Ponadto zróżnicowane definicje mogą chronić konsumentów w niektórych stanach, ale szkodzić im w innych, w których prawa ochronne są słabsze lub nie ma ich wcale. Przedsiębiorstwa mogą po prostu zbierać informacje od mieszkańców stanów o łagodniejszym prawie ochrony. W rezultacie stany, które wolniej wprowadzają przepisy, będą narażone na przetwarzanie danych biometrycznych bez ochrony. Co więcej, dla podmiotów, które mają klientów w wielu stanach, przestrzeganie przepisów może stać się mylące i uciążliwe. W rezultacie, przestrzeganie przepisów przez amerykańskich przedsiębiorców byłoby bardziej prawdopodobne, gdyby istniał jeden jasny krajowy standard minimalny, do którego musiałyby się stosować i który byłby egzekwowany przez sądy[81]. Z drugiej strony jednolity krajowy standard zapewniłby konsumentom odpowiedni poziom ochrony ich danych biometrycznych.

W obliczu braku regulacji na poziomie federalnym, Federalna Komisja Handlu edukuje prywatne spółki w zakresie najlepszych praktyk i zobowiązuje je do konkretnego działania za pomocą dekretów. Przedstawiane wytyczne są jednak jedynie sugestiami, a nie obowiązującym prawem[82]. W rezultacie wyznaczają one jednak pewien standard postępowania dla całego sektora, co może być korzystne dla obu stron – zarówno przedsiębiorców, jak i konsumentów.

[78] F. Q. Nguyen, *op. cit*., s. 69.
[79] *Ibidem.*
[80] *Ibidem,* ss. 71-72.
[81] *Ibidem,* ss. 71-72.
[82] *Ibidem*, s. 66.

Co więcej, w 2020 r. ze względu na nadużycia ze strony organów władzy państwowej, korporacje takie jak IBM, Amazon czy Microsoft zaczęły odmawiać sprzedaży oraz dostarczania swoich systemów FRT sektorowi publicznemu, dopóki ustawodawca nie ureguluje stosowania tej technologii[83]. Doprowadziły do tego naciski aktywistów broniących praw człowieka, a także sami pracownicy tych korporacji. Powodem było wykrycie, że systemy te mogą nieprawidłowo identyfikować osoby o ciemniejszej karnacji skóry, czyli przejawiać tzw. uprzedzenia i doprowadzać do dyskryminacji na tle rasowym[84]. Nadużycia ze strony władzy mogące godzić w wolności obywateli nie są żadną tajemnicą, a wręcz z rozwojem systemów rozpoznawania twarzy używane są coraz częściej do kolejnych celów, które mają na celu inwigilacje obywateli. W maju 2021 r. Amazon potwierdził, że podtrzymuje swoją decyzję i nadal nie będzie dostarczał swojego oprogramowania władzom publicznym. Nie wiadomo jak długo jeszcze potrwa taki stan rzeczy[85].

Powyższe przykłady pokazują, że potrzeba ustanowienia kompleksowych regulacji obejmujących cały kraj oraz zarówno sektor prywatny i publiczny, niewątpliwie istnieje, skoro kroki w tym kierunku podjęły nawet największe amerykańskie korporacje. Przedsiębiorcy, a także stanowi legislatorzy, zdają sobie również sprawę, do jakich celów służy dostarczana przez nich sektorowi publicznemu technologia. Bez odpowiednich przepisów prawnych istnieje wysokie ryzyko inwigilacji obywateli ze strony państwa, a więc łamania podstawowego prawa do prywatności. W taki sposób okazują oni swój sprzeciw wobec takich działań. Ten oddolny ruch największych korporacji oraz władz stanowych ma na celu wywieranie presji na rządzących, aby jak najszybciej uchwalili nowe regulacje[86].

III. Rozwój technologii rozpoznawania twarzy i przykłady jej zastosowania

[83] R. Heilweil, *Big tech companies back away from selling facial recognition to police. That's progress*, 2020, https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police (dostęp: 23.09.2021 r.).
[84] *Amazon to continue pause on police use of facial recognition technology*, 2021, https://www.business-standard.com/article/technology/amazon-to-continue-pause-on-police-use-of-facial-recognition-technology-121051900053_1.html (dostęp: 23.09.2021 r.).
[85] *Ibidem.*
[86] R. Heilweil, *op. cit.*

To Stany Zjednoczone są krajem, w którym technologia rozpoznawania twarzy miała swój początek. Są również miejscem, gdzie odbywano pierwsze testy i pierwsze implementacje – najpierw w sektorze publicznym, a następnie prywatnym. Połączenie tego czynnika z dostępem do światowej klasy naukowców, a także niskim poziomem regulacji prawnych w tych zakresie sprawiły, że rozwój tej technologii w USA jest niezwykle wysoki. W rezultacie spadły również koszty jej używania i aktualnie jest ona stosowana w wielu celach, zarówno w sposób komercyjny, jak i publiczny. Nie sposób jest wymienić wszystkich możliwości zastosowania technologii rozpoznawania twarzy w USA, dlatego skupię się jedynie na kilku najbardziej znanych przykładach, zarówno z sektora prywatnego, jak i publicznego.

Ze względu na to, że swoje początki technologia rozpoznawania twarzy miała w USA, tamtejsze agencje rządowe jako pierwsze na świecie testowały systemy na niej oparte dla celów skuteczniejszego wykrywania przestępców czy zabezpieczania imprez masowych. Jednakże z czasem rosła tendencja do wykorzystywania tej technologii, a także rosły zagrożenia z tego wynikające. Natomiast regulacje prawne, w związku z nową sytuacją nie nadążały za rozwojem technologii i niewystarczająco chroniły prawa i wolności obywateli. Po 2001 r. i zamachu na WTC postanowiono jeszcze bardziej wzmocnić bezpieczeństwo kraju, a w rezultacie ucierpiała ochrona prywatności poszczególnych jednostek.

Technologia rozpoznawania twarzy została po raz pierwszy powszechnie użyta podczas finałów *Super Bowl* w 2002 r. Był to jeden z większych testów i pomimo wykrycia kilku drobnych przestępców, uznany został za porażkę ze względu na wiele fałszywych wyników[87]. W 2009 r. powstała pierwsza kryminalistyczna baza danych stworzona przez Biuro Szeryfa Hrabstwa Pinellas znajdującego się na Florydzie, która pozwoliła funkcjonariuszom na dostęp do archiwów fotograficznych stanowego Departamentu Bezpieczeństwa Autostrad i Pojazdów Samochodowych (*Department of Highway Safety and Motor Vehicles*). Do 2011 r. ok. 170 funkcjonariuszy zostało wyposażonych w kamery, które pozwalały im robić zdjęcia podejrzanych, które mogły być porównywane z bazą danych. Dzięki temu dokonano więcej aresztowań i wszczęto więcej dochodzeń niż byłoby to możliwe w innym przypadku[88].

[87] J. D. West, *The history of face recognition*, 2017, https://www.facefirst.com/blog/brief-history-of-face-recognition-software/ (dostęp: 23.09.2021 r.).
[88] *Ibidem.*

Nie trzeba było długo czekać, aż pomysł stworzenia bazy danych zostanie przeniesiony na poziom ogólnokrajowy. Już w 2014 r. FBI ogłosiło stworzenie do 2015 r. bazy danych, w której miało się znaleźć 51 milionów zdjęć wizerunków twarzy obywateli. Dostęp do bazy mieli uzyskać również policjanci w całym kraju, nie tylko funkcjonariusze FBI[89]. W 2019 r. baza rozrosła się do 640 milionów fotografii, a celem agencji stało się uzyskanie dostępu do zdjęć prawie każdego Amerykanina po to, aby zamieścić je w swoim systemie. Takie działanie FBI wzbudziło protesty obrońców praw człowieka, ponieważ „budowa infrastruktury masowej inwigilacji" prowadzona była bez wyraźnego upoważnienia Kongresu czy środków zabezpieczających, nie była też poprzedzona konsultacjami społecznymi[90]. Niewątpliwie, dostęp służb do takiej bazy, gdzie bez zgody zarówno osoby, której dane dotyczą, jak i amerykańskiej władzy ustawodawczej stanowi pogwałcenie praw podstawowych Amerykanów, którzy zostali pozbawieni wpływu na przetwarzanie jednej ze swoich najwrażliwszych danych.

Duże kontrowersje wzbudziło również stosowanie systemu *Clearview AI* przez organy ścigania w całych Stanach Zjednoczonych – od lokalnych policjantów po FBI oraz Departament Bezpieczeństwa Wewnętrznego. Ten przełomowy system FRT, opracowany przez australijskiego programistę, dysponuje bazą danych zawierającą ponad 3 miliardy zdjęć, które zostały pobrane z Facebooka, YouTube, a także milionów innych stron internetowych. Następnie system może porównać twarz zarejestrowaną przez kamerę bezpieczeństwa z ich bazą danych, aby pokazać możliwe dopasowania. Sam twórca twierdzi, że możliwości tego systemu wykraczają daleko poza wszystko, co kiedykolwiek zostało stworzone przez rząd USA lub korporacje technologiczne z Doliny Krzemowej[91]. Obrońcy praw człowieka ostrzegają, że narzędzie to odbierze jednostkom zdolność do anonimowego poruszania się po ulicach miast, a także spowoduje koniec prywatności, jaką znamy i pozbawi w zasadzie podstawowego „prawa do bycia pozostawionym w spokoju"[92], które powinno obejmować prawo do tego, by wizerunki twarzy nie były bez naszej zgody pobierane z Internetu, abyśmy mogli być identyfikowani podczas poruszania się po świecie. Bez odpowiednich regulacji prawnych nie będzie możliwe zapewnienie ochrony prawa podstawowego, jakim jest prawo do prywatności przynależne każdemu człowiekowi.

---

[89] J. Pagliery, *FBI launches a face recognition system*, 2014, https://money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition (dostęp: 23.09.2021 r.).
[90] N. S. Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, 2019, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through (dostęp: 23.09.2021 r.).
[91] K. Hill, *Meet Clearview AI, the secretive company that might end privacy as we know it*, 2020, https://www.chicagotribune.com/nation-world/ct-nw-nyt-clearview-facial-recognition-20200119-dkdqz7ypaveb3id42tpz7ymase-story.html (dostęp: 23.09.2021 r.).
[92] S. duPont, *op. cit.*

Jednym z niewielu systemów rozpoznawania twarzy używanym przez organy ścigania w USA, który podlega pewnym ustalonym wytycznym i regulacyjnym ograniczeniom jest *Next Generation Identification-Interstate Photo System* (dalej jako „NGI-IPS"). W dużej mierze wspiera on stanowe i lokalne organy ścigania. NGI-IPS zawiera zdjęcia kryminalne zarówno twarzy, jak i blizn czy tatuaży wraz z powiązanymi z nimi 10-odciskami palców oraz rejestrami historii kryminalnej, a dzięki temu umożliwia uprawnionym funkcjonariuszom poszukiwanie potencjalnych tropów śledczych[93]. Aby skorzystać z NGI-IPS, funkcjonariusz przesyła zdjęcie „próbne", które zostało uzyskane w wyniku autoryzowanego dochodzenia, w celu przeszukania repozytorium zdjęć. NGI-IPS zwraca galerię zdjęć „kandydatów" obejmującą od 2 do 50 osób. W drugim etapie procesu organy ścigania dokonują ręcznego przeglądu zdjęć kandydatów i przeprowadzają dalsze dochodzenie w celu ustalenia, czy któryś z nich odpowiada osobie ze zdjęcia[94]. FBI zwraca uwagę, że wyszukiwanie w systemie NGI-IPS na podstawie rozpoznawania twarzy nie może samo w sobie zapewnić pozytywnej identyfikacji. Wyniki muszą zostać ręcznie zweryfikowane przez przeszkolonego funkcjonariusza. Ponadto organom ścigania zabrania się opierać wyłącznie na wynikach wyszukiwania z NGI-IPS w celu podjęcia formalnych działań związanych z egzekwowaniem prawa (np. dokonania aresztowania lub zatrzymania w związku z przestępstwem)[95].

Zasady stosowania systemu NGI-IPS określone są w wytycznych zawartych w dokumencie *NGI Policy and Implementation Guide*. Upoważnieni użytkownicy systemu NGI-IPS są zobowiązani do przestrzegania tych zasad, jak również standardów wydawanych przez Naukową Grupę Roboczą ds. Identyfikacji Twarzy (*Facial Identification Scientific Working Group*, dalej jako „FISWG")[96] dotyczących porównywania twarzy[97]. Zasady przedstawione w przewodniku zawierają między innymi informacje o tym, jak przesłać zdjęcia do rejestracji w NGI-IPS, przeprowadzić śledcze wyszukiwanie zdjęć, pobrać dodatkowe dane biometryczne związane z prawdopodobnym podejrzanym, powiadomić FBI o potencjalnym dopasowaniu w wyniku śledczego wyszukiwania zdjęć czy zażądać usunięcia zestawu biometrycznego, który został wprowadzony do NGI-IPS[98]. Ponadto FBI prosi, aby użytkownicy korzystali z *Mugshot Implementation Guide*, który stanowi punkt odniesienia przy przekazywaniu FBI odpowiednich zdjęć twarzy. W dokumencie zaznaczono, że na jakość obrazu

[93] K. Finklea, L. A. Harris, A. F. Kolker, J. F. Sargent, *Federal Law Enforcement Use of Facial Recognition Technology*, Congressional Research Service, R46586, 2020, s. 5.
[94] *Ibidem.*
[95] Zob. więcej na https://www.fbibiospecs.cjis.gov/Face (dostęp: 23.09.2021 r.).
[96] Zob. więcej na https://fiswg.org/ (dostęp: 23.09.2021 r.).
[97] K. Finklea, L. A. Harris, A. F. Kolker, J. F. Sargent, *op. cit.,* s. 7.
[98] FBI, *Next Generation Identification (NGI) Interstate Photo System (IPS) Policy and lmplementation Guide: Version 1.3*, 2015.

mają wpływ kamera, tło, oświetlenie oraz sposób ustawienia osoby[99]. FBI wymaga również, aby użytkownicy NGI-IPS ukończyli szkolenie z rozpoznawania twarzy, które jest zgodne z wytycznymi FISWG[100].

Dla zachowania bezpieczeństwa zewnętrznego, Stany Zjednoczone wykorzystują również systemy rozpoznawania twarzy do weryfikacji tożsamości podróżnych na swoich granicach. Departament Bezpieczeństwa Wewnętrznego (dalej jako „DHS") opracowuje zautomatyzowany biometryczny system wjazdów i wyjazdów dla cudzoziemców podróżujących przez amerykańską granicę[101].

DHS oraz Urząd Celny i Ochrona Granic (dalej jako „CBP") przeprowadziły kilka pilotażowych programów, w których wykorzystali szereg technologii biometrycznych, jak np. odciski palców, skanowanie tęczówki czy rozpoznawanie twarzy. Po ich przeprowadzeniu zdecydowano, że rozpoznawanie twarzy jest optymalnym podejściem ze względu na szybkość zastosowania oraz względną dokładność wyników. Ta usługa weryfikacji podróżnych (dalej jako „TVS")[102] jest wynikiem publiczno-prywatnego partnerstwa pomiędzy rządem federalnym a prywatnymi liniami lotniczymi oraz portami lotniczymi. Jest on wdrażany przez CBP i Administrację Bezpieczeństwa Transportu. Działa obecnie w 27 portach lotniczych, 7 portach morskich i 5 punktach granicznych w Stanach Zjednoczonych, jak również w 4 międzynarodowych punktach odprawy wstępnej. TVS obecnie przechwytuje ok. 60% podróżnych objętych kontrolą opuszczających Stany Zjednoczone[103].

TVS porównuje zdjęcia podróżnych, zrobione w czasie rzeczywistym przez system FRT, ze zdjęciami w bazie danych. W przypadku osób podróżujących drogą lotniczą i morską, CBP wykorzystuje dane biograficzne uzyskane z manifestów lotniczych i statkowych za pośrednictwem Systemu Zaawansowanego Informowania Pasażerów (*Advance Passenger Information System*), aby zebrać wszystkie powiązane zdjęcia twarzy z zasobów DHS (np. zdjęcia z paszportów amerykańskich, wiz amerykańskich, inspekcji wjazdowych CBP oraz wszelkich innych spotkań z DHS). Następnie w

[99] FBI, *Mugshot lmplementation Guide: Photographic Considerations Related to Facial Recognition Software and Booking Station Mug Shots*, 2013
[100] K. Finklea, L. A. Harris, A. F. Kolker, J. F. Sargent, *op. cit*., s. 7.
[101] Zob. więcej Congressional Research Service, *Biometric Entry-Exit System: Legislative History and Status,* IF11634, 2020.
[102] Zob. więcej na https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service (dostęp: 23.09.2021 r.).
[103] K. Finklea, L. A. Harris, A. F. Kolker, J. F. Sargent, *op. cit.,* s. 7.

ciągu dwóch sekund TVS podaje wynik dopasowania lub braku dopasowania. W przypadku tego drugiego wyniku, tożsamość podróżnego jest sprawdzana ręcznie przez pracownika CBP[104].

Ze względu na aktualnie szeroką dostępność technologii rozpoznawania twarzy, w sektorze prywatnym ma ona bardzo szerokie zastosowanie. Już w latach 90. XX wieku *Defense Advanced Research Projects Agency* (dalej jako „DARPA") oraz National Institute of Standards and Technology (dalej jako „NIST") rozpoczęły program *Face Recognition Technology* (dalej jako „FERET") którego celem było pobudzenie innowacji w tym zakresie na komercyjnym rynku rozpoznawania twarzy, co miało zaowocować bardziej wydajnymi systemami FRT. Projekt obejmował stworzenie bazy danych obrazów twarzy. Baza danych została zaktualizowana w 2003 r. – w zestawie testowym znalazło się 2 413 nieruchomych obrazów twarzy 856 osób[105].

Kolejne innowacje postępowały już dużo szybciej. W 2010 r. Facebook jako pierwszy zaczął wdrażać funkcję rozpoznawania twarzy, która pomaga identyfikować ludzi, których twarze pojawiają się na zdjęciach[106]. Program *Suggestion Tag* stał się natychmiast kontrowersyjny ze względu na łamanie prawa do prywatności użytkowników serwisu. Jak wskazywałam powyżej, Facebook na podstawie stanowej ustawy BIPA został kilka razy pozwany, jednakże ze względu na swoją siedzibę w Kalifornii argumentował, że nie podlega przepisom tej ustawy. W takiej sytuacji wiele zależy od interpretacji dokonanej przez sąd. Brak natomiast odpowiednich i efektywnych narzędzi dla użytkowników mediów społecznościowych, żeby bronić się przed takimi nadużyciami z ich strony. Z tego punktu widzenia uchwalenie federalnej ustawy chroniącej prywatność oraz dane osobowe obywateli jest konieczne dla zapewnienia odpowiednich środków ochrony.

Co więcej, na początku 2021 r. Facebook ogłosił, że zamierza zaimplementować do opracowywanych aktualnie okularów AR (z rozszerzoną rzeczywistością) technologię rozpoznawania twarzy. Użytkownicy takich okularów byliby w stanie identyfikować w czasie rzeczywistym mijane na ulicy osoby. Pomysł ten został skrytykowany od razu po ogłoszeniu ze względu na niemożliwość pogodzenia tego rozwiązania z ochroną prywatności jednostek[107].

---

[104] *Ibidem.*
[105] J. D. West, *op. cit.*
[106] *Ibidem.*
[107] R. Bellan, *Facebook AR Glasses To Release This Year, Might Include Facial Recognition*, 2021, https://www.forbes.com/sites/rebeccabellan/2021/02/28/facebook-ar-glasses-to-release-this-year-might-include-facial-recognition/ (dostęp: 23.09.2021 r.).

Ciekawym przykładem wydaje się działająca od 2016 r. baza wizerunków twarzy stworzona przez Microsoft. Jej celem było dostarczenie łatwo dostępnych danych do trenowania algorytmów sztucznej inteligencji przez środowiska akademickie. Jednakże informacje pobierane były ze stron internetowych bez zgody osób, których te dane dotyczyły, a jednocześnie ze względu na swoją ogólnodostępność baza zaczęła być wykorzystywana także przez chińskie przedsiębiorstwa takie jak Megvii czy SenseTime, jak i amerykański IBM. Była to największa taka baza, gdyż zawierała 10 milionów zdjęć ok. 100 tysięcy jednostek. W 2019 r. Microsoft postanowił po cichu usunąć bazę ze względu na pojawiające się wokół obiekcje co do zgodności z unijnym RODO. Pomimo usunięcia bazy, większość rekordów nadal jest dostępna w Internecie, ponieważ udostępniają je inni użytkownicy[108].

W ostatnich latach bardzo popularne stało się odblokowywanie telefonów komórkowych za pomocą skanowania wizerunku twarzy. Amerykańska korporacja Apple jako pierwsza zaimplementowała w 2017 r. do swoich urządzeń system FRT. Ze względu na unikalność wizerunku twarzy każdego człowieka technologia rozpoznawania twarzy uznawana jest za jedno z najlepszych zabezpieczeń dla urządzeń mobilnych[109]. Niedługo potem także inni producenci zaczęli wdrażać te systemy do swoich urządzeń.

Nie sposób nie wspomnieć jeszcze, że to największe amerykańskie korporacje technologiczne dostarczają swoje systemy FRT do organów ścigania takich jak FBI czy CIA. System *Rekognition* Amazona był testowany przez policję w Orlando na Florydzie łączył dane z przekazów wideo na żywo z technologią rozpoznawania twarzy, aby obserwować i śledzić ludzi w czasie rzeczywistym[110]. Naukowcy z MIT odkryli, że system dawał gorsze wyniki w przypadku kobiet i osób o ciemniejszej karnacji, co mogło przełożyć się na błędy w rozpoznawaniu poszczególnych osób[111]. Pod naciskami obrońców praw człowieka, a także swoich pracowników, Amazon, a następnie również IBM oraz Microsoft ogłosiły, że nie będą sprzedawać swoich programów organom ścigania do czasu uchwalenia przepisów regulujących ich wykorzystywanie w przestrzeni publicznej. To jednak nie powstrzymuje federalnych ani lokalnych organów ścigania od wykorzystywania systemów FRT z innych źródeł. *Center on Privacy & Technology w Georgetown Law Center* odkryło, że *US Immigration*

[108] Madhumita Murgia, *Microsoft quietly deletes largest public face recognition data set*, 2019, https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 (dostęp: 23.09.2021 r.).
[109] J. D. West, *op. cit.*
[110] S. Ghaffary , *How facial recognition became the most feared technology in the US,* 2019, https://www.vox.com/recode/2019/8/9/20799022/facial-recognition-law (dostęp: 23.09.2021 r.).
[111] *Ibidem.*

and Customs Enforcement miało dostęp do baz danych zdjęć z prawa jazdy z 21 stanów, które następnie mogło zostać użyte bez wiedzy w cyfrowej wersji kryminalnej kartoteki[112]. Wydaje się jednak, że wycofanie się największych amerykańskich korporacji technologicznych ze sprzedaży swoich systemów FRT organom ścigania to pierwszy krok do wywołania nacisku na ustawodawcę w kwestii uchwalenia nowych przepisów.

Niestety pomimo ciągłego rozwijania algorytmów sztucznej inteligencji, cały czas wykazuje się, że wyniki zwracane z systemów technologii rozpoznawania twarzy obarczone są dużym ryzykiem błędu. W eksperymencie przeprowadzonym w 2018 r. przez Amerykańską Unię Wolności Osobistych (*American Civil Liberties Union*) na członkach amerykańskiego Kongresu wykazało, że system *Rekognition* Amazona błędnie zidentyfikował 28 członków Kongresu jako wcześniej aresztowanych przestępców. Ponownie większe problemy z odpowiednią identyfikacją, system miał z osobami o innym kolorze skóry niż biały[113]. Przedstawiony przykład daje kolejny argument za ostrożniejszym wprowadzaniem systemów FRT do przestrzeni publicznej, a także za uprzednim uregulowaniem tej technologii po to, aby zapewnić odpowiedni poziom ochrony praw i wolności obywatelskich.

IV. Przetwarzanie danych biometrycznych przez podmioty prywatne oraz publiczne

Problemem amerykańskiego system prawnego jest brak odpowiednich przepisów regulujących przetwarzanie danych biometrycznych zarówno przez sektor publiczny, jak i prywatny. Niestety taka sytuacja prowadzi do wielu nadużyć opisanych pokrótce powyżej. Istniejące regulacje są szczątkowe, a często są to jedynie wytyczne, które nie stanowią powszechnie obowiązującego prawa. Co więcej regulacje istnieją jedynie w poszczególnych stanach i tylko tam sięga ich zasięg, natomiast brak jest jakichkolwiek federalnych regulacji, pomimo przedstawianych wielu projektów

[112] *Ibidem.*
[113] J. Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 (dostęp: 23.09.2021 r.).

ustaw. Wprowadzenie takich regulacji pozwoliłoby na ujednolicenie standardu stosowania technologii rozpoznawania twarzy.

Na poziomie federalnym amerykańskiego prawa nie zostało uchwalone żadne powszechnie obowiązujące prawo, funkcjonują jednakże pewne wytyczne, które określają zasady stosowania FRT przez władze publiczne, a przy tym zasady przetwarzania danych biometrycznych wizerunków twarzy. Jedne z takich wytycznych zostały opracowane przez FISWG. Jest to jedna z naukowych grup roboczych, które wspierają Organizację Komitetów Obszaru Naukowego dla Nauk Sądowych (zarządzaną przez Narodowy Instytut Norm i Technologii, który wspiera rozwój różnego rodzaju standardów). FISWG opublikowała szereg dokumentów związanych z FRT, przeznaczonych dla praktyków kryminalistyki. Na przykład wydała ona wytyczne i zalecenia dotyczące ustanowienia i prowadzenia szkoleń w zakresie porównywania twarzy, przewodniki dotyczące pozyskiwania obrazów twarzy, które mogą być wykorzystywane w systemach rozpoznawania twarzy, oraz zalecane metody i techniki wykorzystywania systemów rozpoznawania twarzy[114].

Warto też zwrócić uwagę, że FBI przeprowadziło również audyty w celu oceny, czy użytkownicy opisywanego powyżej systemu NGI-IPS przestrzegają zasad dotyczących ich stosowania. W zeznaniach składanych przed Kongresem FBI wskazało, że do maja 2019 r. przeprowadzono dziewięć audytów i żaden z nich nie wykazał żadnych uchybień dotyczących braku zgodności i nie zaobserwowano nieuprawnionych wniosków lub niewłaściwego wykorzystania systemu. Ponadto audyt FBI z 2018 r. dotyczący innego systemu FRT – FACE[115] wykazał, że system ten również działa zgodnie z polityką FBI i odpowiednimi przepisami dotyczącymi prywatności[116]. Ustalanie wytycznych też przyczynia się w jakimś stopniu do ochrony danych jednostek, natomiast jest to działanie doraźne, które powinno być jedynie elementem uzupełniającym dla kompleksowych przepisów krajowych.

Na poziomie stanowym obowiązuje jedynie opisywana powyżej ustawa uchwalona w Waszyngtonie. Wprowadza ona dosyć wysokie wymagania, takie jak weryfikacja każdej decyzji przez człowieka, udostępnianie interfejsu oprogramowania (API) czy ogólny zakaz stosowania systemów w czasie rzeczywistym (z pewnymi wyjątkami)[117]. Cieszy sam fakt, że taką ustawę udało się uchwa-

[114] K. Finklea, L. A. Harris, A. F. Kolker, J. F. Sargent, *op. cit*.
[115] Zob. więcej na https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit (dostęp: 23.09.2021 r.).
[116] K. Finklea, L. A. Harris, A. F. Kolker, J. F. Sargent, *op. cit*., s. 8.
[117] S. duPont, *op. cit*.

lić, natomiast może mieć ona wpływ jedynie na lokalnie działające organy, takie jak np. policja. Jedna stanowa ustawa nie sprawi, że organy władzy publicznej w całym kraju zaczną stosować technologię rozpoznawania twarzy z poszanowaniem prawa do prywatności oraz ochrony danych biometrycznych obywateli. Jednocześnie brak uchwalonej ogólnokrajowej legislacji sprawia, że trudno stwierdzić w jaki sposób organy władzy publicznej mają postępować, skoro brak jest standardu, którym miałyby się kierować. Pojedyncze wytyczne czy ustawy lokalne nie są wystarczające, aby ten standard ustanowić. Nie można więc jednoznacznie obwiniać podmiotów publicznych, takich jak FBI czy CIA, gdyż postępują w duchu ochrony wartości, która stała się dominująca po 2001 r., czyli zapewnienia bezpieczeństwa narodowego. Wartość ta bezsprzecznie przeważa w amerykańskim systemie prawnym ponad ochronę danych pojedynczych jednostek. Pomimo że trend ten zmienia się i coraz więcej mówi się o wzmocnieniu ochrony prywatności i danych, to najprawdopodobniej potrzeba jeszcze wielu lat, aby ten ogólnonarodowy amerykański standard uległ zmianie.

Wydaje się, że zmiana nastawienia w sektorze prywatnym postępuje szybciej niż w publicznym. Może mieć to związek z szybkim rozwojem Internetu oraz usług internetowych, a także z tym, że konsumenci stają się coraz bardziej świadomi swoich praw. Pomimo że w tym zakresie standard ogólnokrajowy nie został także ustanowiony, to większa liczba ustaw stanowych kreuje pewne standardy. Pierwsza ustawa dotycząca przetwarzania danych biometrycznych uchwalona w 2008 r. w stanie Illinois – BIPA – wyznaczyła kierunek także innym stanom[118]. Aktualnie, najbardziej kompleksowe przepisy dotyczące ochrony danych konsumentów, w tym danych biometrycznych posiada Kalifornia. Już ustawa CCPA zapewnia dosyć wysoki poziom ochrony[119], natomiast kolejna ustawa, która ma wejść w życie 1 stycznia 2023 r. – CPRA ma ten standard ochrony jeszcze podnieść. Ustawa zakłada powołanie Kalifornijskiej Agencji Ochrony Prywatności (*California Privacy Protection Agency),* a także wprowadzenie nowej podkategorii danych – danych wrażliwych, do których będą zaliczać się dane biometryczne[120]. Konsumenci będą mieli zwiększone prawa w przypadku wrażliwych danych osobowych, w tym nowe prawo do ograniczenia wykorzystania i ujawnienia takich danych[121]. Kalifornia jest stanem, gdzie siedzibę mają największe korporacje technologiczne, takie jak Facebook czy Apple, więc dobrze, że to w tym stanie powstaje bardziej rygorystyczne prawo chroniące konsumentów.

[118] *Ibidem.*
[119] Robert B., *op. cit.*
[120] M. Bahar, M. J. Wilson-Bilik, A. F. L. *Sand, California's new privacy law, the CPRA, was approved: Now what?*, 2020, https://www.lexology.com/library/detail.aspx?g=5a7edce9-26af-487c-8877-7a815945954d (dostęp: 23.09.2021 r.).
[121] *Ibidem.*

Jednakże w skali całego kraju, podwyższanie poziomu ochrony danych biometrycznych na poziomie stanowym nie jest jednak wystarczające. Pokazują to choćby opisywane powyżej postępowania sądowe przeciwko Facebookowi czy Google. Jeżeli powodowie wszczynają postępowanie na podstawie innego prawa niż kalifornijskie (w opisanych przypadkach była to ustawa BIPA ze stanu Illinois), prawnicy pozwanych podnoszą argument, że takie postępowanie może się toczyć jedynie na podstawie prawa stanu Kalifornia[122]. Co prawda kilka razy sądy odrzucały taką argumentacje i przyznawały rację powodom, jednakże niewątpliwie system ten nie jest w pełni efektywny. I pewnie nie stanie się do czasu uchwalenia ustawy ogólnokrajowej, na którą będą mogli powoływać się obywatele wszystkich stanów.

Pewien oddolny standard ochrony stara się kreować również Federalna Komisja Handlu, która prowadzi dla prywatnych przedsiębiorstw programy edukacyjne w zakresie dobrych praktyk i zobowiązuje je do konkretnego postępowania za pomocą wydawanych przez siebie dekretów[123]. Jednakże takie działania na dłuższą metę również są nieefektywne w sytuacji braku kompleksowej ustawy na poziomie federalnym.

[122] Zob. Więcej F. Q. Nguyen, *op. cit.*, ss. 68-71.
[123] *Ibidem,* s. 69.

ZAKOŃCZENIE

Pomimo podobnych początków w latach 70. XX wieku, amerykański system prawny z zakresu danych osobowych poszedł w zupełnie odmiennym kierunku niż unijny. Do dzisiaj oprócz uchwalonej w 1974 r. *Privacy Act*, nie powstała żadna ustawa danoosobowa na poziomie federalnym. Ma to swoje przełożenie na obecny brak odpowiedniej ochrony praw i wolności obywateli. Jednakże Amerykanie dążą do zmiany w tym zakresie, od paru latach przedstawiane są w Kongresie USA kolejne projekty ustaw, które mogłyby zmienić aktualny stan rzeczy. Do tej pory nie udało się jednak dojść do porozumienia na tej płaszczyźnie.

Dużą rolę w najbliższym czasie może odegrać Federalna Komisja Handlu, która w naturalny sposób zaczęła przejmować kompetencje z zakresu ochrony danych osobowych, pomimo że do jej przyznanych uprawnień należy głównie ochrona konsumentów przez przeciwdziałanie nieuczciwym praktykom rynkowym. Postuluje się jednak rozszerzenie kompetencji FTC tak, aby odgrywała wiodącą rolę w egzekwowaniu wszelkich nowych regulacji dotyczących prywatności i ochrony danych. Proponuje się przyznanie ustawowych uprawnień np. do nakładania kar cywilnych. FTC może więc stać się w niedalekiej przyszłości organem nadzoru do spraw ochrony danych.

Sytuacja wygląda nieco odmiennie na poziomie stanowym, gdzie regulacji jest więcej. Najbardziej znanym przykładem stanowej regulacji danoosobowej, często porównywanym do europejskiego RODO, jest uchwalona w 2018 r. kalifornijska CCPA. Ustawa ta uznawana jest za najbardziej kompleksową, skoncentrowaną na środowisku cyfrowym regulację dotyczącą ochrony danych w USA. Za przykładem Kalifornii poszły również inne stany. Jak na razie, poza tym stanem, obowiązujące regulacje z zakresu ochrony prywatności ma jedynie Wirginia oraz Kolorado. Natomiast wiele stanów takich jak Ohio, Massachusetts czy Nowy Jork ma swoje przepisy w przygotowaniu. Jednakże analizy wskazują, że większość ustaw bądź projektów ustaw zawiera te same kluczowe postanowienia w zakresie ochrony danych, a to budzi nadzieje na wypracowanie wspólnego standardu.

W obliczu postępującego rozwoju technologii rozpoznawania twarzy, problem na pewno stanowi brak przepisów regulujących jej wykorzystywanie. Raport wydany przez NSCAI stanowi co prawda dobry prognostyk do stworzenia takich regulacji, jednakże droga do ich faktycznego wejścia w życie będzie na pewno długa. Jedynym narzędziem do ochrony obywateli przed zagrożeniami wynikającymi z rozwoju technologii rozpoznawania twarzy pozostają aktualnie przepisy regulujące ochronę danych biometrycznych. Tutaj jednak również brakuje regulacji na poziomie federalnym, a

na poziomie stanowym jest ich jedynie kilka. Nie jest to wystarczające narzędzie, gdyż regulacje stanowe działają jedynie lokalnie, a to utrudnia ochronę przed amerykańskimi korporacjami technologicznymi. To pokazuje potrzebę uchwalenia kompleksowych regulacji w najbliższym czasie, w szczególności na poziomie krajowym.

Wniosek na temat potrzeby uchwalenia kolejnych regulacji można wysnuć również na podstawie analizy sposobów wykorzystania systemów FRT na terytorium USA. Są one szeroko stosowane zarówno przez sektor publiczny, w szczególności organy ścigania, jak i sektor prywatny, czyli korporacje technologiczne. Z jednej strony wielokrotnie wykazywano nadużycia oraz postępowanie łamiące prawo do prywatności, a także niezgodne z ochroną danych, natomiast z drugiej, przeprowadzane eksperymenty często pokazują, że systemy FRT nie są idealne i zwracane przez nie wyniki nadal są obarczone dużym ryzykiem błędu, w szczególności wobec osób o innym kolorze skóry niż biały. Jedynym rozwiązaniem dla zapobiegania takim sytuacjom jest ustanowienie odpowiednich regulacji, które mogłyby ograniczyć swobodę korzystania z technologii rozpoznawania twarzy oraz ustanowić zasady jej wykorzystywania.

BIBLIOGRAFIA

1. Aaronson S. A., Leblond P., Another Digital Divide: The Rise of Data Realms and its Implications for the WTO, Journal of International Economic Law, 2018.
2. Amerykańska Konwencja Praw Człowieka zawarta w San José dnia 22 listopada 1969, No. 17955, Vol. 1144. I-I7955.
3. Bambauer J., Rogers J. E., Biometric privacy laws: How a Little-Known Illinois Law Made Facebook Illegal, Program on Economics & Privacy, 2017.
4. California Consumer Privacy Act of 2018 [California Civil Code 1798.110–1798.199].
5. Chun S., Facial Recognition Technology: A Call For The Creation Of A Framework Combining Government Regulation And A Commitment To Corporate Responsibility, North Carolina Journal of Law & Technology Vol. 21, Issue 4, 2020.
6. Fazlioglu M., White Paper – Consensus and Controversy in the Debate Over Federal Data Privacy Legislation in the United States, International Association of Privacy Professionals, 2019.
7. FBI, Mugshot Implementation Guide: Photographic Considerations Related to Facial Recognition Software and Booking Station Mug Shots, 2013.
8. FBI, Next Generation Identification (NGI) Interstate Photo System (IPS) Policy and Implementation Guide: Version 1.3, 2015.
9. Final Report – National Security Commission on Artificial Intelligence, 2021.
10. Finklea K., Harris L. A., Kolker A. F., Sargent J. F., Federal Law Enforcement Use of Facial Recognition Technology, Congressional Research Service, R46586, 2020.
11. Gady F. S., EU/U. S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis, Georgetown Journal of International Affairs, International Engagement on Cyber IV, 2014.
12. Gołaś-Podolec M., Porównanie europejskiego i interamerykańskiego systemu ochrony praw człowieka, Krakowskie Studia Międzynarodowe, nr 2, 2008.
13. H.R.4081 - Consumer Privacy Protection Act of 2017.
14. Illinois Biometric Information Privacy Act, 740 ILCS 14/1-99 (2008).
15. In re Facebook Biometric Info. Privacy Litig. - 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

16. Katz v. United States, 389 U.S. 347 (1967).
17. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, Dz.U. 1993 Nr 61, poz. 284.
18. Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167).
19. Nguyen F. Q., The Standard for Biometric Data Protection, Journal of Law & Cyber Warfare, Vol. 7, No. 1, 2018.
20. Pope C., Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data, Journal of Law and Policy, vol. 26, no. 2, 2018.
21. Poscher R., The Right to Data Protection. A No-Right Thesis [w:] Miller R. A., Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA-Affair, Cambridge University Press, 2017.
22. Powszechna Deklaracja Praw Człowieka (rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana w dniu 10 grudnia 1948 r.).
23. Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2018)).
24. Rivera v. Google, Inc. 238 F. Supp. 3d 1088 (N.D. Ill. 2017).
25. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz.UE.L 2016 Nr 119, s. 1.
26. Schwartz P. M., Preemption and Privacy, The Yale Law Journal, vol. 118, 2009.
27. Warren S. D., Brandeis L. D., The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, 1890.
28. Whitman J. Q., The Two Western Cultures of Privacy: Dignity Versus Liberty, Yale Law Journal, vol. 113, 2004.

ŹRÓDŁA INTERNETOWE:

1. Amazon to continue pause on police use of facial recognition technology, 2021, https://www.business-standard.com/article/technology/amazon-to-continue-pause-on-police-use-of-facial-recognition-technology-121051900053_1.html.
2. B. R., Biometrics and the CCPA, https://www.termsfeed.com/blog/ccpa-biometrics/
3. Bahar M., Wilson-Bilik M. J., Sand A. F. L., California's new privacy law, the CPRA, was approved: Now what?, 2020, https://www.lexology.com/library/detail.aspx?g=5a7edce9-26af-487c-8877-7a815945954d.
4. Bellan R., Facebook AR Glasses To Release This Year, Might Include Facial Recognition, 2021, https://www.forbes.com/sites/rebeccabellan/2021/02/28/facebook-ar-glasses-to-release-this-year-might-include-facial-recognition/.
5. Bennett J., Saving Face: Facebook Wants Access Without Limits, 2017, Https://Publicintegrity.Org/%202017/07/31/21027/Saving-Face-Facebook-Wants-Access-Without-Limits.
6. Burt C., Facebook lobbying against facial recognition laws, 2017, https://www.biometricupdate.com/201708/facebook-lobbying-against-facial-recognition-laws.
7. Buyer B. J., Washington's New Biometric Privacy Law: What Businesses Need to Know, 2017, https://www.dwt.com/insights/2017/07/washingtons-new-biometric-privacy-law-what-busines.
8. duPont S., On Facial Recognition, the U.S. Isn't China—Yet, https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet.
9. Facial recognition regulation in the USA: an efficient legal patchwork?, 2020, https://www.avocats-mathias.com/donnees-personnelles/facial-recognition-usa.
10. Ghaffary S., How facial recognition became the most feared technology in the US, 2019, https://www.vox.com/recode/2019/8/9/20799022/facial-recognition-law.
11. Green A., Complete Guide to Privacy Laws in the US, 2021, https://www.varonis.com/blog/us-privacy-laws/.
12. Guliani N. S., The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database, 2019, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through.

13. Head T., Where Did the Right to Privacy Come From? Constitutional Merits and Congressional Acts, 2019, https://www.thoughtco.com/right-to-privacy-history-721174.
14. Heilweil R., Big tech companies back away from selling facial recognition to police. That's progress, 2020, https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police.
15. Hill K., Meet Clearview AI, the secretive company that might end privacy as we know it, 2020, https://www.chicagotribune.com/nation-world/ct-nw-nyt-clearview-facial-recognition-20200119-dkdqz7ypaveb3id42tpz7ymase-story.html.
16. https://fiswg.org/.
17. https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.
18. https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.
19. https://www.fbibiospecs.cjis.gov/Face.
20. https://www.nscai.gov/.
21. In re Facebook Biometric Info. Privacy Litig. - 185 F. Supp. 3d 1155 (N.D. Cal. 2016), https://www.lexisnexis.com/community/casebrief/p/casebrief-in-re-facebook-biometric-info-privacy-litig.
22. Mac R., Facebook Is Considering Facial Recognition For Its Upcoming Smart Glasses, 2021, https://www.buzzfeednews.com/article/ryanmac/facebook-considers-facial-recognition-smart-glasses.
23. Mehrotra K., Tech Companies are Pushing Back Against Biometric Privacy Laws, 2017, https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws.
24. Murgia M., Microsoft quietly deletes largest public face recognition data set, 2019, https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2.
25. Pagliery J., FBI launches a face recognition system, 2014, https://money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition.
26. Rippy S., US State Privacy Legislation Tracker, 2021, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
27. Snow J., Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
28. Swaine J., Supreme court endorses cellphone privacy rights in sweeping ruling, 2014, https://www.theguardian.com/law/2014/jun/25/supreme-court-police-cellphones-search.

29. The Face Recognition Algorithm That Finally Outperforms Humans, 2014, https://medium.com/the-physics-arxiv-blog/the-face-recognition-algorithm-that-finally-outperforms-humans-2c567adbf7fc.
30. We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online, 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.
31. West J. D., The history of face recognition, 2017, https://www.facefirst.com/blog/brief-history-of-face-recognition-software/.

ZESTAWIENIE SPISÓW

Wykaz skrótów

BIPA	Illinois Biometric Information Privacy Act
CBP	(amerykański) Urząd Celny i Ochrona Granic
CCPA	California Consumer Privacy Act
CPRA	The California Privacy Rights Act
DARPA	(amerykański) Defense Advanced Research Projects Agency
DHS	(amerykański) Departament Bezpieczeństwa Wewnętrznego
Dz. U.	Dziennik Ustaw Rzeczypospolitej Polskiej
Dz. Urz. UE	Dziennik Urzędowy Unii Europejskiej
EKPCz	Europejska Konwencja Praw Człowieka
FERET	(system) Face Recognition Technology
FISWG	Naukowa Grupa Robocza ds. Identyfikacji Twarzy (Facial Identification Scientific Working Group)
FRT	technologia rozpoznawania twarzy (Facial Recognition Technology)
FTC	(amerykańska) Federalna Komisja Handlu (Federal Trade Commission)
NGI-IPS	Next Generation Identification-Interstate Photo System
NIST	(amerykański) National Institute of Standards and Technology
NSCAI	(amerykańska) Narodowa Komisja Bezpieczeństwa do spraw sztucznej inteligencji (The National Security Commission on Artificial Intelligence)
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) (Tekst mający znaczenie dla EOG)
SI	sztuczna inteligencja
UE	Unia Europejska
USA	Stany Zjednoczone Ameryki Północnej