

Zuzanna Choińska
Uniwersytet Warszawski
Wydział Prawa i Administracji
z.choinska@student.uw.edu.pl
ORCID: [0000-0003-0229-8739](https://orcid.org/0000-0003-0229-8739)

Wykorzystanie technologii rozpoznawania twarzy w Chińskiej Republice Ludowej

The use of facial recognition technology in the People's Republic of China

Streszczenie

Technologia odgrywa coraz większą rolę w życiu człowieka, co wiąże się z wieloma korzyściami, w tym ułatwieniem życia i funkcjonowania. Jej rozwój stwarza również wiele zagrożeń dla jednostek, co sprawia, że dyskusja nad jej prawną regulacją nabiera znaczenia. Chińska Republika Ludowa charakteryzuje się zupełnie innym podejściem do rozwoju technologii i jej regulacji, a także do ochrony danych osobowych, niż to znane w Unii Europejskiej. Celem niniejszego artykułu jest przedstawienie, jaki wpływ ma rozwój i wykorzystanie technologii rozpoznawania twarzy w Chinach na przestrzeganie praw podstawowych i życie obywateli tego kraju. Analiza zostanie przeprowadzona poprzez omówienie przyjętego ustawodawstwa, dzisiejszych zmian w postrzeganiu tej technologii oraz priorytetów przyjętych przez chińskie władze.

Słowa kluczowe

dane osobowe, technologia rozpoznawania twarzy, prywatność, prawa podstawowe, prawa człowieka, dane biometryczne, sztuczna inteligencja

Abstract

Technology is playing an increasingly important role in people's lives which is associated with many benefits, including making life and functioning easier. On the other hand, its development also creates many risks for individuals, which makes the discussion on its legal regulation gain importance. The People's Republic of China is characterized by a completely different approach to the development of technology and its regulation, as well as to the protection of personal data, than the approach known in the European Union. This article aims to present what impact the development and use of facial recognition technology in China has on compliance with fundamental law and the lives of its citizens. The analysis will be conducted by discussing the adopted legislation, today's changes in the perception of the technology and the priorities adopted by the Chinese authorities.

Keywords

personal data, facial recognition technology, privacy, fundamental rights, human rights, biometric data, artificial intelligence

1. Wstęp

W dzisiejszych czasach technologia odgrywa w życiu człowieka coraz większą rolę. W szczególności sztuczna inteligencja (dalej jako „SI”) zyskała na popularności i naukowcy na całym świecie dążą do jej szybkiego rozwoju. Z jednej strony wiąże się to z ułatwieniem życia oraz usprawnieniem wielu sfer funkcjonowania, ale z drugiej jej rozwój kreuje wiele zagrożeń dla jednostek. W związku z tym technologia staje się coraz częściej przedmiotem dyskusji w kontekście jej prawnego uregulowania w celu zniwelowania potencjalnych negatywnych skutków. Okazuje się to jednak dla legislatorów na całym świecie trudnym zadaniem ze względu na jej szybki rozwój oraz powolne wprowadzanie nowych regulacji prawnych.

Chińska Republika Ludowa charakteryzuje się zupełnie odmiennym od znanego w Unii Europejskiej podejściem do rozwoju technologii oraz regulacji prawnych dotyczących tego zagadnienia, a także ochrony danych osobowych. Niniejszy artykuł ma na celu przedstawienie, jaki wpływ ma rozwój i wykorzystanie technologii rozpoznawania twarzy (dalej jako „FRT”) w Chinach na przestrzeganie praw podstawowych oraz życie obywateli tego państwa. Analiza zostanie przeprowadzona poprzez omówienie przyjętych przepisów prawnych, dzisiejszych zmian w postrzeganiu technologii oraz przyjętych przez chińskie władze priorytetów.

Na początku przedstawiony zostanie system ochrony danych osobowych. Następnie przejdę do omówienia przepisów, ewentualnie propozycji przepisów relewantnych w zakresie uregulowania technologii. Szczególna uwaga zostanie poświęcona również przepisom z zakresu danych biometrycznych, które stanowią często jedyny środek ochrony przed nadużyciami wynikającymi ze stosowania technologii rozpoznawania twarzy. Kolejnym aspektem będzie zobrazowanie, na jakim poziomie rozwoju znajduje się omawiana technologia, poprzez przedstawienie przykładowych sposobów jej wykorzystania. W zakończeniu przedstawione zostaną wnioski z prowadzonych rozważań.

2. System ochrony danych osobowych

Pierwsze regulacje prawne dotyczące ochrony danych osobowych w Chinach zaczęły się kształtować dopiero ok. 2010 r. Stało się tak, ponieważ dopiero wtedy pojawiła się realna potrzeba ich uchwalenia, którą zauważyły również chińskie władze. Okres ten zbiegł się z dynamicznym rozwojem technologii w Chinach¹, czego skutkiem była produkcja ogromnej ilości danych, nad którą należało zapanować, aby technologia mogła się dalej rozwijać. Wynika to z tego, że odpowiednia ilość i jakość danych jest jednym

¹ K.F. Lee, *Inteligencja sztuczna, rewolucja prawdziwa, Chiny, USA i przyszłość świata*, Media Rodzina 2020, tłum. K. Hejwowski, s. 70-73.

z podstawowych czynników koniecznych do tego postępu. Zważywszy na ustrój polityczny Chin, można przypuszczać, że ochrona praw obywateli była w tej sytuacji drugorzędnym powodem do stworzenia odpowiednich regulacji.

Początkowo były to jedynie przepisy sektorowe regulujące przepływ i przetwarzanie danych tylko w poszczególnych gałęziach prawa i gospodarki kraju. Przykładowo chińskie prawo karne zaczęło penalizować nielegalny obrót dużymi ilościami danych, którymi dysponują przedsiębiorstwa i organizacje, zarówno prywatne, jak i publiczne. Celem regulacji było wdrożenie przez przedsiębiorstwa odpowiednich środków ochrony danych w swojej działalności oraz zbudowanie świadomości pracowników tych podmiotów w zakresie ochrony prywatności i danych².

Ważne dla ochrony danych jednostek w Chinach są również Ogólne Zasady Prawa Cywilnego (dalej jako „OZPC”)³, których nowelizacja z 2017 r. po raz pierwszy uznała ochronę danych za część prawa cywilnego⁴. Artykuł 111 zapewnia ochronę dobrego imienia obywateli (*right of reputation*)⁵. Kolejne przepisy zapewniają ochronę nazwiska, wizerunku oraz honoru danej osoby. Chińskie prawo cywilne, pomimo zapewnienia ochrony poszczególnych elementów prywatności, nie uznaje więc prawa do prywatności jako niezależnego prawa jednostki⁶. Zgodnie z wykładnią, jakiej dokonał Najwyższy Sąd Ludowy, różne formy ujawniania danych osobowych należy traktować jako naruszenie dobrego imienia jednostki⁷.

Poza opisanymi powyżej ustawami w zakresie ochrony danych osobowych w chińskim porządku prawnym istnieje również grupa bardziej wyspecjalizowanych przepisów dotyczących jedynie sektora prywatnego. Nie przyjmują one rangi ustaw, a jedynie decyzji czy wytycznych, jednakże w większości ich charakter jest prawnie wiążący dla podmiotów, których dotyczą⁸. Jedną z pierwszych takich regulacji był wydany w 2011 r. (a obowiązujący od 2012 r.) przez Ministerstwo Gospodarki i Technologii (dalej jako „MIIT”) zbiór standardów wiążący wszystkich dostawców internetowych usług infor-

² H. Xue, *Privacy and personal data protection in China: An update for the year end 2009*, “Computer Law & Security Review” 2010, no. 26, s. 285.

³ Ogólne Zasady Prawa Cywilnego do czasu wejścia w życie chińskiego Kodeksu cywilnego (*Civil Code of the People's Republic of China*) pełniły funkcję ustawy regulującej niektóre działy prawa cywilnego w Chinach, zob. więcej <http://www.npc.gov.cn/englishnpc/lawsofthepc/202001/c983fc8d3782438fa775-a9d67d6e82d8.shtml> [dostęp: 23.09.2021].

⁴ A. Geller, *How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective*, “GRUR International” 2020, Vol. 69, no. 12, s. 2.

⁵ Ogólne Zasady Prawa Cywilnego Chińskiej Republiki Ludowej (General Provisions of the Civil Law of the PRC), tłumaczenie na angielski: <http://www.npc.gov.cn/englishnpc/lawsofthepc/202001/c983fc8d3782438fa775a9d67d6e82d8.shtml> [dostęp: 23.09.2021].

⁶ G. Greenleaf, *Asian Data Privacy Law*, Oxford University Press 2014, s. 200-201.

⁷ *Ibidem*.

⁸ A. Geller, *op. cit.*

macyjnych⁹. Również w 2012 r. Stały Komitet Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych (dalej jako: „OZPL”) wydał Decyzję (dalej jako „Decyzja Stałego Komitetu OZPL”) dotyczącą bezpośrednio ochrony informacji w Internecie¹⁰, która stała się jednym z najważniejszych aktów prawnych w Chinach dotyczących danych osobowych. Decyzja ta stanowi podstawowe źródło oraz punkt odniesienia dla późniejszych przepisów dotyczących ochrony „informacji elektronicznych” w Chinach¹¹.

Należy zaznaczyć, że chińskie regulacje z zakresu danych osobowych są bardzo chaotyczne oraz fragmentaryczne. Na gruncie europejskim konkretne ustawy regulują to zagadnienie, natomiast w Chinach konieczne jest korzystanie z wielu różnych aktów prawnych. W związku z tym w niniejszym artykule, odnosząc się do legislacji danoosobowej, będę odwoływać się również do regulacji innego rodzaju, jeżeli będą przedstawiać znaczenie także dla ochrony danych. W związku z powyższym pewnym przełomem dla chińskiej legislacji danoosobowej stało się uchwalenie w Chinach obowiązującej od 2017 r. ustawy o cyberbezpieczeństwie. Choć jej celem jest głównie ochrona bezpieczeństwa cybernetycznego i bezpieczeństwa narodowego, to jest to również pierwszy akt prawny w Chinach, który tak szeroko reguluje kwestie ochrony danych, a przez to stanowi pozytywny krok w kierunku bardziej kompleksowego systemu ochrony danych¹². Uchwalenie ustawy było rezultatem narastającej liczby oszustw internetowych obejmujących nielegalną odsprzedaż danych osobowych jednostek, która wynikała z braku zapewnienia odpowiedniego poziomu ochrony. Oszustwa częstokroć doprowadzały do śmierci osób oszukanych. Szerokim echem w chińskich mediach odbił się przypadek studenta, który utracił wszystkie środki, które przez wiele lat jego rodzina zbierała na jego edukację. Ze względu na doświadczony stres mężczyzna zmarł na zawał dwa dni po oszustwie¹³. Nie był to jednak odosobniony przypadek. Realna potrzeba nakłoniła więc chiński rząd do rozpoczęcia prac nad wzmocnieniem ochrony danych osobowych¹⁴.

Celem nowej regulacji było przede wszystkim wzmocnienie ochrony w zakresie transgranicznego przetwarzania danych osobowych oraz danych wrażliwych. Większą ochroną zostały objęte wszystkie kategorie danych, które są przetwarzane przez podmioty prowadzące działalność gospodarczą w Chinach i chcące przysyłać dane do państw trzecich¹⁵. Do ustawy zaimplementowane zostały podstawowe zasady z unijnego ogólnego

⁹ G. Greenleaf, *op. cit.*, s. 204-207.

¹⁰ *Ibidem*.

¹¹ *Ibidem*.

¹² *Ibidem*.

¹³ J. Meng, W. Fan, *China strengthens its data protection legislation*, IAPP, 15.11.2016, <https://iapp.org/news/a/china-strengthens-its-data-protection-legislation/> [dostęp: 23.09.2021].

¹⁴ *Ibidem*.

¹⁵ M. Abu Gholeh, D. Kuźnicka, *Ochrona danych osobowych w wybranych państwach Azji*, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2019, s. 64.

rozporządzenia o ochronie danych (dalej jako „RODO”)¹⁶, ale nie tylko. Przykładowo podstawowe wymagania dotyczą zbierania zgody na przetwarzanie, przejrzystości i bezpieczeństwa czy lokalizacji danych i ograniczeń w ich eksporcie. To właśnie ścisły wymóg lokalizacji danych został przyjęty z zaniepokojeniem zarówno wśród krajowych przedsiębiorców, jak i przedsiębiorców z państw trzecich, którzy świadczyli swoje usługi na terenie Chin¹⁷. Podnoszone były głosy, że takie regulacje umożliwiać będą dyskryminację podmiotów spoza Chin¹⁸, ułatwią nadzór aparatu państwowego nad ich działalnością oraz utrudnią rozwój działalności gospodarczej¹⁹. Co prawda przyjęte przepisy zmusiły niektóre firmy zagraniczne, w szczególności dostawców usług chmurowych, do wycofania się z Chin²⁰, jednakże ustawa weszła w życie zgodnie z zapowiedziami – 1 czerwca 2017 r. Od tego czasu stanowiła solidną podstawę dla dalszego rozwoju regulacji danoosobowych w Chinach²¹.

W 2020 r. pojawiły się w Chińskiej Republice Ludowej dwa projekty ustaw mające na celu dalsze rozszerzanie ochrony danych osobowych oraz prywatności chińskich obywateli. Pierwszy z nich – ustawa o ochronie danych osobowych (*Personal Information Protection Law*, dalej jako „PIPL”), został uchwalony 20 sierpnia 2021 r. i po wejściu w życie, czyli od 1 listopada 2021 r., stanowi pierwszą kompleksową regulację w Chinach dotyczącą ochrony danych osobowych.

Analizując PIPL, łatwo zauważyć, że wiele przepisów zawartych w nim jest inspirowanych unijnym RODO²². W ustawie rozszerzono zakres danych osobowych oraz określono kluczowe pojęcia i zasady ich przetwarzania, w tym przykładowo ustanowiono zasady przejrzystości, sprawiedliwości, ograniczania celu, minimalizacji danych czy ich rozliczalności²³. W przeciwieństwie do ustawy o cyberbezpieczeństwie PIPL rozszerza katalog podstaw przetwarzania danych, który do tej pory oparty był tylko na zgodzie²⁴ i od teraz będzie zbliżony do tego zawartego w RODO. Co więcej, definicja zgody

¹⁶ 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 119 z 4.05.2016 r., s. 1.

¹⁷ Y. Feng, *The future of China's personal data protection law: challenges and prospects*, „Asia Pacific Law Review” 2019, vol. 27, iss. 1, s. 72.

¹⁸ M. Parasol, *The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams*, „Computer Law & Security Review” 2018, no. 34, s. 68.

¹⁹ Y. Feng, *op. cit.*, s. 72.

²⁰ *Ibidem*.

²¹ J. Meng, W. Fan, *op. cit.*

²² X. Ke, V. Liu, Y. Lao, Z. Yu, *Analyzing China's PIPL and how it compares to the EU's GDPR*, IAPP, 24.08.2021, <https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/> [dostęp: 23.09.2021].

²³ *Ibidem*.

²⁴ M. Chan, C. Yue, J. Gong, T. Ke, S. Zhang, *The Gloves Are Off! China's Personal Information Protection Law was Passed and will Come into Effect on 1 November 2021*, Lexology, 23.08.2021, <https://www.lexology.com/library/detail.aspx?l=6444444>.

na mocy PIPL w dużej mierze pokrywa się ze ścisłymi wymogami RODO w tym zakresie, a więc zgoda musi być wyraźna, świadoma, udzielona dobrowolnie i może być później wycofana. Ustawa wymaga jednak odrębnej zgody w przypadku niektórych czynności przetwarzania, a mianowicie np. gdy podmiot przetwarzający publicznie ujawnia dane osobowe, przetwarza szczególnie chronione dane osobowe lub przekazuje dane osobowe za granicę²⁵.

Analogicznie do przepisów przyjętych w unijnym rozporządzeniu PIPL zakłada również rozszerzenie zasięgu terytorialnego obowiązywania do wszystkich zagranicznych podmiotów i osób fizycznych, które przetwarzają dane osobowe osób znajdujących się na terytorium Chin, niezależnie od ich narodowości²⁶. Bez wątpienia będzie to miało znaczący wpływ na firmy prowadzące działalność w Chinach lub zorientowane na działalność na rynku chińskim. Przedsiębiorcy będą musieli dostosować się do nowych, bardziej wymagających przepisów bądź wycofać się z działalności na rynku chińskim, tak jak postąpili niektórzy przy implementacji ustawy o cyberbezpieczeństwie. Niewątpliwie jednak chiński rynek stwarza dla przedsiębiorców ogromne możliwości rozwoju, szczególnie w zakresie nowych technologii. Przyjęte regulacje nie powinny być na tyle wymagające, aby były niemożliwe do spełnienia dla zagranicznych podmiotów. W mojej ocenie byłoby to niekorzystne zarówno dla przedsiębiorców zagranicznych, jak i samej gospodarki Chin. Jednak analiza przepisów nowej ustawy nie daje podstaw do twierdzenia, że przyjęte wymagania są nadmierne – w końcu wiele z nich stanowi bezpośrednią implementację rozwiązań przyjętych w RODO.

PIPL wydaje się jednak korzystny dla podmiotów, których dane będą przetwarzane. Zakłada on znaczne wzmocnienie i poszerzenie przysługujących im praw, a także nałożenie większych obowiązków na administratorów oraz podmioty przetwarzające dane. Po raz pierwszy chińskim obywatelom przysługiwać będą takie prawa jak obywatelom UE, czyli chociażby prawo do informacji i wyjaśnień dotyczących przetwarzania danych, prawo dostępu do danych osobowych i żądania ich kopii, prawo do sprostowania danych, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do wycofania zgody oraz prawo do usunięcia danych²⁷. Z drugiej strony ustawa przewiduje różne środki zarządzania i bezpieczeństwa, takie jak regularne audyty zgodności, oceny ryzyka, okresowe szkolenia pracowników, rejestry czynności przetwarzania danych osobowych, protokoły reagowania na żądania osób, których dane dotyczą, zgłaszanie naruszeń ochrony danych, środki zaradcze w przypadku naruszenia ochrony danych oraz wyznaczenie inspektora ochrony danych. PIPL wymaga więc od podmiotów przetwarzających

lexology.com/library/detail.aspx?g=b11a28d4-a023-4af0-b7c3-d49ce8e80646 [dostęp: 23.09.2021].

²⁵ *Ibidem*.

²⁶ X. Ke, V. Liu, Y. Lao, Z. Yu, *op. cit.*

²⁷ *Ibidem*.

dane osobowe przyjęcia całościowego programu zgodności z przepisami w celu ochrony danych osobowych²⁸.

Dopełnienie dla kompleksowego systemu ochrony danych osobowych tworzonego przez PIPL oraz ustawę o cyberbezpieczeństwie ma stanowić ustawa o bezpieczeństwie danych (*Data Security Law*), która weszła w życie 1 września 2021 r. Dzieli ona dane na trzy kategorie, a mianowicie dane podstawowe dla państwa (*core state data*), dane ważne i dane ogólne. Ustawa ustanawia hierarchiczny system zarządzania klasyfikacją danych i ich ochrony, który uwzględnia znaczenie różnych rodzajów danych dla gospodarki narodowej, bezpieczeństwa narodowego i interesu publicznego²⁹. W zakresie przeciwdziałania niewłaściwemu przetwarzaniu danych podstawowych dla państwa ustawa o bezpieczeństwie danych przewiduje wyposażenie prezydenta Chin w szeroki wachlarz uprawnień. Przede wszystkim daje mu prawo do nakładania kar pieniężnych, a nawet decydowania o zamykaniu przedsiębiorstw, które niewłaściwie obchodzą się z danymi³⁰. Celem takiego rozwiązania jest przejęcie kontroli nad ogromnymi ilościami danych przetwarzanych głównie przez korporacje technologiczne działające na terenie Chin.

Ostatnim aktem prawnym wpisującym się w chiński system ochrony danych osobowych, a jednocześnie wartym omówienia, jest Kodeks cywilny³¹, który wszedł w życie 1 stycznia 2021 r. W Chinach do tej pory nie istniała kompleksowa regulacja dotycząca prawa cywilnego. Istniały Ogólne Zasady Prawa Cywilnego wspomniane przeze mnie powyżej oraz oddzielnie ustawa regulująca odpowiedzialność deliktową. Omawiany Kodeks cywilny zastąpił te akty prawne i wprowadził jedną kompleksową regulację³². W przeciwieństwie do OZPC Kodeks cywilny wprowadza oddzielny rozdział poświęcony bezpośrednio prawie do prywatności oraz ochronie danych. Jest to pierwszy raz, kiedy w chińskim prawie cywilnym zapisano prawo do prywatności i zasady ochrony danych osobowych. Definiuje on dane osobowe i określa podstawę prawną przetwarzania danych osobowych, obowiązki podmiotów przetwarzających dane osobowe, prawa osób fizycznych do ich danych osobowych oraz obowiązki organów administracyjnych. W najnowszej wykładni sądowej dotyczącej wprowadzanej regulacji, opublikowanej w grudniu 2020 r., Najwyższy Sąd Ludowy wyraźnie określił „spór o ochronę danych osobowych” jako przyczynę wniesienia powództwa cywilnego na podstawie Kodeksu

²⁸ *Ibidem*.

²⁹ J. Sheng, C. Xu, E. Tao, *China Adopts New Data Security Law*, Pillsbury, 07.09.2021, <https://www.pillsburylaw.com/en/news-and-insights/china-adopts-new-data-security-law.html> [dostęp: 23.09.2021].

³⁰ C. Murphy, J. Li, C. Liu, L. Liu, *China's New Data Law Gives Xi the Power to Shut Down Tech Firms*, Bloomberg, 11.06.2021, <https://www.bloomberg.com/news/articles/2021-06-10/china-passes-law-to-strengthen-control-over-tech-firms-data> [dostęp: 23.09.2021].

³¹ *Civil Code of the People's Republic of China*, tłumaczenie na angielski: <http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf> [dostęp: 23.09.2021].

³² A. Geller, *op. cit.*

cywilnego³³. Aktualna regulacja jest także dużo lepiej dostosowana do ochrony praw jednostek w świecie cyfrowym, w którym coraz łatwiej o naruszenia. Szybko rozwijające się platformy cyfrowe stwarzają pole do publikowania różnych treści, także tych o charakterze zniesławiającym czy obrażającym³⁴. Potrzebne są więc narzędzia prawne, dzięki którym możliwe będzie skuteczne dochodzenie swoich praw.

W latach 2010-2021 pojawiło się w Chińskiej Republice Ludowej bardzo wiele regulacji z zakresu danych osobowych. Jednakże czynniki takie jak duża różnorodność podmiotów uchwalających przepisy, odmienna moc ich obowiązywania oraz skierowanie ich do różnych sektorów powodują duże rozproszenie tych przepisów, a co za tym idzie, brak jednolitości ochrony dla podmiotów, których dane są przetwarzane. Prowadzi to do wniosku, że system ochrony danych w Chinach, na tym etapie, nie zapewnia odpowiedniej ochrony dla obywateli. Z uwagą należy obserwować implementację omawianej ustawy o ochronie danych osobowych. Ustawa ta jest pierwszym, kompleksowym aktem prawnym dotyczącym ochrony danych osobowych w Chinach. Czy okaże się także skuteczna dla ochrony praw jednostek, przekonamy się w najbliższej przyszłości.

3. Ramy regulacyjne dla technologii

Technologie takie jak sztuczna inteligencja nie zostały jeszcze włożone w odpowiednie ramy prawne w żadnym państwie na świecie, więc Chiny nie stanowią tutaj wyjątku. Jest to spowodowane dużo szybszym tempem rozwoju technologii w porównaniu do rozwoju regulacji prawnych oraz brakiem odpowiedniej wiedzy, w jaki sposób powinna ona być uregulowana. Bez wątpienia takie regulacje są konieczne, aby technologia mogła funkcjonować w sposób bezpieczny i przejrzysty dla społeczeństwa. Brak właściwych przepisów może prowadzić przykładowo do nadużyć w stosowaniu pewnych narzędzi przez władze, co niestety możemy zaobserwować w Chinach w związku z coraz szerszym wykorzystywaniem technologii rozpoznawania twarzy. Obecnie pojawiają się dopiero pierwsze propozycje prawne, ale najprawdopodobniej jeszcze długa droga do ich wejścia w życie. Pierwszą regulacją, która ma na celu kompleksowe uregulowanie stosowania systemów SI, jest projekt rozporządzenia o SI³⁵ przedstawiony przez Komisję Europejską.

³³ M. Robinson, N. Lau, J. Gong, *China cybersecurity and data protection: Review of 2020 and outlook for 2021*, 18.01.2021, Lexology, <https://www.lexology.com/library/detail.aspx?g=44eee916-38fc-4132-8924-44377262ab4d> [dostęp: 23.09.2021].

³⁴ Z. Yangfei, *Draft civil code emphasizes personality rights*, ChinaDaily Hong Kong, 21.05.2020, <https://www.chinadailyhk.com/article/131295> [dostęp: 23.09.2021].

³⁵ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane zasady dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM(2021) 206 final.

Na gruncie chińskim nie ma więc prawodawstwa bezpośrednio regulującego wykorzystywanie SI, a tym bardziej wykorzystywanie technologii rozpoznawania twarzy. Jest jednak grupa przepisów, która może stanowić dobry początek dla bardziej kompleksowych uregulowań w tej materii.

W 2017 r. Rada Państwa ogłosiła Plan rozwoju sztucznej inteligencji następnej generacji (*Next Generation Artificial Intelligence Development Plan*, dalej jako „Plan rozwoju SI”), czyli narodowy plan, który przedstawia chińskie ambicje zostania liderem światowego przemysłu SI do 2030 r. Plan ten zakłada, że Chiny mają stać się liderem nie tylko w zakresie technologii, ale także w zakresie etyki oraz regulacji prawnych dotyczących SI³⁶. Zgodnie z jego założeniami Chiny staną się światowym centrum innowacji, rozwoju i zarządzania SI, a na ten cel przeznaczone zostaną ogromne publiczne fundusze. We wstępnym planie nie ma zbyt wielu konkretnych i istotnych szczegółów dotyczących tego, w jaki sposób rozwój będzie zarządzany oraz jak miałyby zapewnić korzyści dla społeczeństwa i przywództwo Chin w tej dziedzinie. W związku z tym Plan rozwoju SI należy traktować bardziej jako sposób na ogłoszenie światu swojej dominacji w zakresie sztucznej inteligencji w niedalekiej przyszłości³⁷.

Pomimo dużej ogólności sformułowanego Planu rozwoju SI można zauważyć, że na tym nie skończyły się działania chińskiego rządu. Już niecały rok później, w 2018 r., został ogłoszony przez MIIT Plan Działania na lata 2018-2020, który w sposób bardziej szczegółowy określa kluczowe obszary działania na dany okres³⁸. W celu wykonania Planu rozwoju SI powołany został również Krajowy Komitet Zarządzający ds. sztucznej inteligencji nowej generacji (*National New Generation of Artificial Intelligence Governance Committee*), który w 2019 r. opublikował osiem zasad, których powinny przestrzegać osoby pracujące nad rozwojem sztucznej inteligencji. Są to: harmonia, uczciwość i sprawiedliwość, poszanowanie prywatności, bezpieczeństwo, przejrzystość, odpowiedzialność i współpraca³⁹.

Krajowy Komitet Techniczny ds. normalizacji bezpieczeństwa informacji (*National Information Security Standardisation Technical Committee*, dalej jako „TC260”) opublikował w 2021 r. zbiór niewiążących wytycznych dotyczących etyki sztucznej inteligencji, będących kontynuacją standardów opublikowanych w 2019 r. Wytyczne TC260 mają zastosowanie do wszystkich systemów SI, a na tym etapie nie stanowią próby ustanowie-

³⁶ K. Lucero, *Artificial Intelligence Regulation and China's Future*, “Columbia Journal of Asian Law” 2019, vol. 33, no. 1, s. 101.

³⁷ *Ibidem*, s. 102.

³⁸ A. Kaja, Y. Luo, *Covington Artificial Intelligence Update: China's Vision for The Next Generation of AI*, Inside Privacy, 24.03.2018, <https://www.insideprivacy.com/artificial-intelligence/chinas-vision-for-the-next-generation-of-ai/> [dostęp: 23.09.2021].

³⁹ S. O'Meara, *Will China lead the world in AI by 2030?*, Nature, 21.08.2019, <https://www.nature.com/articles/d41586-019-02360-7> [dostęp: 23.09.2021].

nia szczegółowych zasad dla poszczególnych sektorów. Pomimo że są niewiążące, to ich celem jest wypracowanie narodowego standardu, którym kierować się mogą przedsiębiorstwa w całym kraju⁴⁰. Wytyczne TC260 rozpoczynają się od określenia zestawu potencjalnych obaw związanych z zaawansowanymi zastosowaniami SI, które ściśle pokrywają się z wytycznymi UE w sprawie etyki dla godnej zaufania SI. Wytyczne zakładają chociażby zapewnienie właściwego nadzoru ze strony człowieka nad mechanizmami SI, dokumentowanie kluczowych decyzji w zakresie badań i rozwoju, takich jak wybór zbiorów danych i algorytmów, konieczność dokładnego, kompletnego i jednoznacznego wyjaśnienia użytkownikom funkcji, zagrożeń dla bezpieczeństwa i możliwego wpływu SI. Wprowadzają również zakaz polegania na SI jako jedynej podstawie automatycznego podejmowania decyzji w dziedzinie usług publicznych, finansowych, zdrowia, opieki społecznej i edukacji⁴¹.

Duże znaczenie dla regulacji sztucznej inteligencji, a w szczególności technologii rozpoznawania twarzy, mają przepisy dotyczące ochrony danych osobowych, a zwłaszcza danych biometrycznych. Wizerunek twarzy jest daną szczególnej kategorii, a więc powinien być zabezpieczony prawnie w wyższym stopniu niż inne dane, które do tej kategorii nie należą.

W chińskim systemie ochrony danych nie było do tej pory definicji danych biometrycznych, a tym bardziej samych danych dotyczących wizerunku twarzy. W Decyzji Stałego Komitetu OZPL z 2012 r. dane osobowe zostały po raz pierwszy zdefiniowane jako „informacje, które mogą zidentyfikować osoby fizyczne i które dotyczą prywatności osób fizycznych”⁴². Szersza definicja tego pojęcia została przedstawiona cztery lata później, w ustawie o cyberbezpieczeństwie z 2016 r. Jej art. 76 ust. 5. stanowi, że „dane osobowe odnoszą się do różnego rodzaju informacji zarejestrowanych za pomocą środków elektronicznych lub innych, które niezależnie od siebie lub w połączeniu z innymi informacjami mogą zostać użyte do zidentyfikowania osoby fizycznej, w tym osobistych informacji biometrycznych, które następnie w sposób dorozumiany obejmują dane dotyczące wizerunku twarzy”⁴³. Ustawa ta nakłada obowiązki prawne na operatorów sieci, określając wymogi dotyczące gromadzenia, wykorzystywania i ochrony informacji umożliwiających identyfikację osób, które obejmują dane biometryczne. Dane biometryczne nie są jednak głównym przedmiotem zainteresowania powyższych regulacji

⁴⁰ R. Bird, *China “standardises” AI ethics*, Freshfields, 26.01.2021, <https://digital.freshfields.com/post/102gpfp/china-standardises-ai-ethics> [dostęp: 23.09.2021].

⁴¹ *Ibidem*.

⁴² M. Tan, *China: Facial recognition and its legal challenges*, OneTrust DataGuidance, 2020, <https://www.dataguidance.com/opinion/china-facial-recognition-and-its-legal-challenges> [dostęp: 23.09.2021].

⁴³ *Ibidem*.

i nie są omawiane poza sekcją dotyczącą definicji w ustawie o cyberbezpieczeństwie⁴⁴. Przywołane dokumenty nie zawierały więc jeszcze oddzielnej regulacji danych biometrycznych, chociaż ta druga definicja już bardziej odnosiła się do rozwijającego się cyfrowego świata i zwracała uwagę na fakt wytwarzania danych.

Kolejne uchwalane normy krajowe dotyczące ochrony danych osobowych już wyraźnie odnoszą się do tematu danych osobowych dotyczących wizerunku twarzy. Zaktualizowana Specyfikacja Bezpieczeństwa Danych Osobowych (*Personal Information Security Specification*, dalej jako „Specyfikacja”), która weszła w życie w październiku 2020 r., wprowadza pojęcie „wrażliwych danych osobowych”. Oznacza to, że takie informacje, w przypadku ich wycieku, nielegalnego udostępnienia lub niewłaściwego wykorzystania, mogą zagrażać bezpieczeństwu osobistemu i majątkowemu oraz prawdopodobnie spowodują m.in. naruszenie reputacji osobistej, uszczerbek na zdrowiu fizycznym i psychicznym oraz dyskryminacyjne traktowanie. Określa ona również wytyczne dotyczące przetwarzania i ochrony danych, aby zapobiec nielegalnemu gromadzeniu, nadużywaniu i dostępowi do danych osobowych – w tym danych biometrycznych⁴⁵. Przykłady wrażliwych danych osobowych przedstawione w Specyfikacji dotyczą osobistych biochemicznych informacji identyfikacyjnych, które obejmują również cechy rozpoznawania twarzy⁴⁶. Pomimo braku kar Specyfikacja jest uważana za dokument ustanawiający najlepsze praktyki i służy jako ważny punkt odniesienia dla agencji rządowych w kwestii budowania zrównoważonego środowiska dla technologii rozpoznawania twarzy⁴⁷.

Pierwszą ustawą krajową o charakterze wiążącym, która ustanawia wyższy standard ochrony dla szczególnych kategorii danych osobowych, jest opisywana powyżej ustawa o ochronie danych osobowych. Przykłady wrażliwych danych osobowych w ustawie obejmują informacje identyfikujące rasę, narodowość, przekonania religijne, dane biometryczne, historię medyczną, stan zdrowia, sytuację finansową i lokalizację danej osoby. Zgodnie z PIPL na przetwarzanie wrażliwych danych osobowych wymagana będzie odrębna zgoda. Osoby fizyczne muszą być dodatkowo informowane o tym, dlaczego konieczne jest gromadzenie i przetwarzanie ich danych osobowych oraz o wpływie przetwarzania na te osoby⁴⁸. PIPL jeszcze większą ochroną prawną obejmuje sam wizerunek twarzy. Jest to szczególnie ważne w przypadku przetwarzania danych biometrycznych, takich jak ludzkie twarze, ponieważ są one zbierane i rozpoznawane w czasie rzeczywistym.

⁴⁴ S. Lee, *Coming into Focus: China's Facial Recognition Regulations*, Center for Strategic & International Studies, 04.05.2020, <https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations> [dostęp: 23.09.2021].

⁴⁵ *Ibidem*.

⁴⁶ M. Tan, *op. cit.*

⁴⁷ S. Lee, *op. cit.*

⁴⁸ R. Bird, J. Chiew, *China's first omnibus data protection law*, Freshfields, 15.01.2021, <https://digital.freshfields.com/post/102gorq/chinas-first-omnibus-data-protection-law> [dostęp: 23.09.2021].

stym w miejscach publicznych, przez co takie gromadzenie jest mniej odczuwalne. Należy więc zatroszczyć się o określenie rozsądnego zakresu przetwarzania, spełnienie obowiązku informacyjnego oraz uzyskanie zgody osoby zainteresowanej. Jako że wizerunek twarzy jest eksponowany w miejscach publicznych, ich niezauważalne przetwarzanie bez koniecznych ograniczeń prawnych może skutkować poważnymi konsekwencjami⁴⁹. Jak stanowi art. 26 PIPL, przetwarzanie takich danych powinno być możliwe wyłącznie, gdy odbywa się w sposób zgodny z odpowiednimi przepisami państwowymi oraz gdy jest konieczne do zapewnienia bezpieczeństwa narodowego, przy czym niezbędne jest również zainstalowanie wyraźnych znaków informacyjnych. Zebrane dane biometryczne nie mogą być publikowane ani udostępniane innym osobom, chyba że istnieje osobna zgoda danej osoby lub przepisy ustawowe lub administracyjne stanowią inaczej⁵⁰.

Poza zapewniającymi odpowiednią ochronę przepisami z zakresu danych osobowych Chińczycy potrzebują również odpowiednich wiążących regulacji odnoszących się bezpośrednio do kwestii technologicznych. Wraz z rozwojem technologii rosną również obawy osób, których ta technologia będzie dotyczyć. W lutym 2020 r. Chiny pokazały światu nowy system do rozpoznawania twarzy, który jest w stanie zidentyfikować twarz nawet w przypadku noszenia maseczki w związku z pandemią COVID-19. Obawy może budzić fakt, że od razu przyznano, że ten system ma nieznacznie niższy wskaźnik dokładności⁵¹. Dotychczasowe badania przeprowadzone w USA wskazują, że w 2020 r. średni próg dokładności tej technologii kształtował się na poziomie 99,97%⁵². Jednakże algorytm uczenia maszynowego rozpoznaje konkretne punkty na twarzy (teraz jest to co najmniej 68 takich punktów⁵³), z czego, jak wiadomo, w maseczce liczba tych punktów zmniejsza się o co najmniej połowę. Z tego powodu wzrasta również liczba błędów popełnianych przy rozpoznaniu twarzy. To może budzić obawy, szczególnie że technologia rozpoznawania twarzy jest w chińskiej przestrzeni publicznej coraz bardziej powszechna.

Wzrost świadomości oraz obaw chińskich obywateli o bezprawne przetwarzanie ich wizerunków twarzy, a także innych danych osobowych dobrze obrazuje pierwsza sprawa sądowa dotycząca wykorzystania technologii rozpoznawania twarzy w Chinach. Była ona związana ze sporem o rozsądny zakres zastosowania tej technologii⁵⁴, a doty-

⁴⁹ S. Ning, W. Han, J. Ke, L. Yunhan, P. Chi, Y. Minlv, Z. Ziqian, *Personal Information Protection Law (Draft): A New Data Regime*, China Law Insight, 11.11.2020, <https://www.chinalawinsight.com/2020/11/articles/compliance/personal-information-protection-law-draft-a-new-data-regime/> [dostęp: 23.09.2021].

⁵⁰ Art. 26 ustawy o ochronie danych osobowych, źródło tłumaczenia na angielski: <https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021> [dostęp: 23.09.2021].

⁵¹ S. Lee, *op. cit.*

⁵² *How Accurate is Facial Recognition Today?*, Rec Faces, 5.11.2020, <https://recfaces.com/articles/how-accurate-is-facial-recognition> [dostęp: 23.09.2021].

⁵³ *Ibidem*.

⁵⁴ S. Ning, W. Han, J. Ke, L. Yunhan, P. Chi, Y. Minlv, Z. Ziqian, *op. cit.*

czyła identyfikacji tożsamości przy wejściu do parku zoologicznego. W kwietniu 2019 r. Guo Bing, profesor prawa, nabył roczną kartę wstępu do parku Hangzhou Wildlife World. W momencie zakupu podał swoje dane osobowe oraz dostarczył zdjęcie. Za jego zgodą pobrane zostały również odciski palców, które stanowiły podstawę weryfikacji tożsamości przy wejściu do parku. Natomiast w lipcu ten system weryfikacji zastąpiono technologią rozpoznawania twarzy, w związku z czym profesor został poproszony o dostarczenie swojego wizerunku twarzy w celu aktywacji zakupionej wcześniej karty⁵⁵. Profesor stwierdził, że tym działaniem park „narusza prawo ochrony konsumentów poprzez przymusowe zbieranie indywidualnych danych gości”, po tym jak nagle uczynił rejestrację rozpoznawania twarzy obowiązkowym wymogiem przy wejściu dla zwiedzających⁵⁶. Powód nie wyraził więc na to zgody i poprosił o unieważnienie karty oraz zwrot poniesionej opłaty. Kiedy spotkał się z odmową, wniósł pozew do sądu, powołując się na naruszenie jego prywatności oraz złamanie przez Hangzhou Wildlife World Co. Ltd. postanowień umowy o świadczenie usług dostępu do parku⁵⁷. Guo Bing żądał również unieważnienia uchwały zarządu parku wprowadzającej nowy sposób weryfikacji, jako że procedura zbierania wizerunków twarzy odwiedzających naruszała według niego prawo do ochrony danych wrażliwych⁵⁸.

W dniu 20 listopada 2020 r. sąd wydał wyrok w I instancji, w którym orzekł o złamaniu umowy i nakazał Wildlife World zadośćuczynienie Guo Bingowi za utratę korzyści wynikających z umowy oraz koszty transportu w łącznej wysokości 1 038 RMB (ok. 500 zł), a także usunięcie danych wizerunku twarzy Guo Binga, które zostały dostarczone, gdy ubiegał się o roczne członkostwo⁵⁹. Sąd nie odniósł się jednak do wniosku o unieważnienie uchwały Zarządu, a więc nie wypowiedział się merytorycznie w kwestii naruszenia prawa do ochrony wrażliwych danych przez park⁶⁰. Zarówno Guo Bing, jak i Hangzhou Wildlife World odwołali się do sądu II instancji⁶¹.

Sąd II instancji uznał, że informacje biometryczne są wrażliwymi danymi osobowymi, a ich niewłaściwe wykorzystanie powoduje nieprzewidywalne zagrożenia dla prywatności ludzi, dlatego należy wprowadzić bardziej rygorystyczne przepisy⁶². Jed-

⁵⁵ M. Szmidt-Husarz, *Technologia rozpoznawania twarzy a ochrona danych osobowych w Chinach – sprawa prof. Guo Binga*, Chiny24, 16.12.2020, <https://chiny24.com/prawo/technologia-rozpoznawania-twarzy-a-ochrona-danych> [dostęp: 23.09.2021].

⁵⁶ K. Allen, *China facial recognition: Law professor sues wildlife park*, BBC, 8.11.2019, <https://www.bbc.com/news/world-asia-china-50324342> [dostęp: 23.09.2021].

⁵⁷ M. Szmidt-Husarz, *op. cit.*

⁵⁸ *Ibidem.*

⁵⁹ S. Qiao, C. Wang, D. Clark, *Zoo Loses the 'First Face Recognition Case' at Appeal*, Lexology, 22.04.2021, <https://www.lexology.com/library/detail.aspx?g=882322e8-fcb4-4f19-83c9-a4ff71d50e1d> [dostęp: 23.09.2021].

⁶⁰ M. Szmidt-Husarz, *op. cit.*

⁶¹ S. Qiao, C. Wang, D. Clark, *op. cit.*

⁶² *Ibidem.*

nakże ten sąd również nie unieważnił uchwały zarządu wprowadzającej sposób weryfikacji za pomocą wizerunku twarzy.

Ta jedna sprawa wystarczyła, aby wywołać powszechną dyskusję na temat ochrony danych osobowych, a tym bardziej danych biometrycznych w Chinach⁶³. Pomimo wprowadzonych niedawno regulacji nadal istnieje duża potrzeba, aby rząd bądź prywatne przedsiębiorstwa ustanowiły pewne standardy przetwarzania danych obywateli, które w odpowiedni sposób będą chronić obywateli. Możliwe, że lepszą ochronę dla obywateli zapewni wejście w życie PIPL. Kompleksowość tych regulacji wskazuje, że prywatne podmioty, takie jak np. wymieniony powyżej park, będą musiały spełnić wyższe wymagania, a tym samym zapewnić swoim klientom wyższy stopień ochrony prywatności oraz danych.

Sprawa Guo Binga i inne sprawy sądowe doprowadziły do wydania przez Najwyższy Sąd Ludowy 1 sierpnia 2021 r. dokumentu określającego wytyczne dotyczące stosowania technologii rozpoznawania twarzy oraz ochrony tożsamości i prywatności ludzi (*the Provisions on Several Issues on the Application of Law in Hearing Civil Cases Related to the Use of Facial Recognition Technology in Processing Personal Information*). Wydany dokument ma na celu ułatwienie sędziom rozstrzygania spraw wszczętych w związku z łamaniem praw poprzez stosowanie technologii rozpoznawania twarzy, a także ustanowienie pewnego standardu w tym zakresie wśród przedstawicieli władzy sądowniczej w całym kraju. Wytyczne są odpowiedzią na obawy obywateli o swoją prywatność i dane osobowe ze względu na przypadki nadużywania systemów FRT np. przez sklepy, które gromadziły dane konsumentów bez ich zgody⁶⁴.

Warto również wspomnieć, że w obliczu braków w legislacji ogólnokrajowej prywatne przedsiębiorstwa zajmujące się rozwojem technologii rozpoznawania twarzy uchwalają swoje tzw. miękkie prawo. Nie ma ono charakteru prawnie wiążącego, ale może stanowić pewne odniesienie dla chińskich władz, a także może pomóc w wypracowaniu standardów dla całej branży. Dwie główne inicjatywy są prowadzone odpowiednio przez Megvii i SenseTime⁶⁵. Dzięki ciągłym wysiłkom firm technologicznych w celu kierowania odpowiednim wykorzystaniem rozpoznawania twarzy standardy branżowe, pomimo braku wiążącej mocy prawnej w Chinach, mogą mieć kluczowe znaczenie w budowaniu zrównoważonego środowiska dla technologii rozpoznawania twarzy⁶⁶.

Oprócz niewiążących wytycznych przepisy regulujące technologię w Chinach w zasadzie nie istnieją. W tym zakresie chiński rząd bardziej skupia się na pokazaniu się na

⁶³ S. Lee, *op. cit.*

⁶⁴ *New rules to curb misuse of facial recognition tech*, ChinaDaily, 29.07.2021, http://english.court.gov.cn/2021-07/29/content_37545967.htm [dostęp: 23.09.2021].

⁶⁵ S. Lee, *op. cit.*

⁶⁶ *Ibidem*.

arenie międzynarodowej jako światowy lider w zakresie rozwoju SI. Największą rolę w regulacji technologii rozpoznawania twarzy pełnią więc aktualnie przepisy dotyczące danych osobowych, a przy tym danych biometrycznych. Zwraca jednak uwagę brak porządku w przyjętych przepisach, które często są bardzo fragmentaryczne. Sytuacja może jednak ulec zmianie po wejściu w życie ustawy o ochronie danych, której głównym celem jest kompleksowa regulacja danych osobowych. Może mieć też duże znaczenie dla FRT ze względu na ustanowienie ochrony dla danych biometrycznych. Co więcej, w związku z aktualnym brakiem regulacji firmy technologiczne przyjmują swoje własne wytyczne, które pomimo że nie są wiążące, to ustanawiają pewien standard działania dla branży.

4. Rozwój technologii rozpoznawania twarzy i przykłady jej zastosowania

Aby stworzyć odpowiednie środowisko do szybkiego rozwoju technologii w danym państwie czy regionie, potrzebne są trzy czynniki, a mianowicie: odpowiednia ilość dobrej jakości danych, duża moc obliczeniowa oraz dobrze wykształceni inżynierowie⁶⁷. Bardzo ważne jest też odpowiednie nastawienie władz państwowych do rozwoju technologicznego w danym kraju⁶⁸. W Chińskiej Republice Ludowej panują świetne warunki do rozwoju technologii. Chiński rząd wspiera ten rozwój ogromnymi nakładami finansowym. Jeśli chodzi o pozostałe czynniki, to Chiny mogą pochwalić się zarówno dostępem do dużej mocy obliczeniowej, jak i wykształconych inżynierów.

Jednakże to, co wyróżnia rozwój technologiczny w Chinach na tle międzynarodowym, to ogromne ilości danych, które produkuje chińskie społeczeństwo, a które są bardzo potrzebne do trenowania algorytmów uczenia głębokiego. „Data is the new oil”, jak powiedział w 2006 r. brytyjski matematyk Clive Humby, a jego wypowiedź stała się niezwykle popularna na całym świecie⁶⁹. Zgodnie z tym stwierdzeniem w obecnych czasach dane osobowe stały się niezwykle wartościowym „surowcem” i zastąpiły w tym zakresie ropę naftową. Natomiast w Chinach „dane to nie tylko nowa ropa naftowa”, ale również nowa tania siła robocza. Kraj ten przez wiele lat na świecie słynął ze swojej taniej siły roboczej, czyli osób, które pracowały za najniższe stawki w fabrykach, a jednocześnie nie miały zapewnionych żadnych praw pracowniczych oraz łamane były ich prawa człowieka⁷⁰. Obecnie taką taną siłą roboczą stali się chińscy obywatele, którzy

⁶⁷ K.F. Lee, *op. cit.*, s. 105-106.

⁶⁸ *Ibidem*, s. 84-87.

⁶⁹ A. Mavuduru, *Is Data Really the New Oil in the 21st Century?*, Towards Data Science, 12.12.2020, <https://towardsdatascience.com/is-data-really-the-new-oil-in-the-21st-century-17d014811b88> [dostęp: 23.09.2021].

⁷⁰ X. Lin, *A Dangerous Game: China's Big Data Advantage And How The U.S. Should Respond*, „Journal Of Law, Technology & Policy” 2020, no. 1, s. 256-258.

poprzez swoją aktywność cyfrową generują ogrom danych, które następnie są dowolnie wykorzystywane przez chiński rząd. Wynika to z tego, że chiński system prawny, pomimo coraz szerszej ochrony danych osobowych obywateli, nie tworzy wielu ograniczeń. Dane są wykorzystywane przez przedsiębiorstwa tworzące rozwiązania z zakresu chociażby SI, a te często wspierane są przez chiński rząd. Ustawa o cyberbezpieczeństwie z 2016 r. była szeroko krytykowana za swoją niejasność i przejawy protekcjonizmu handlowego. Co więcej, Chińczycy mniej dbają o swoje podstawowe prawa, takie jak prywatność, a bardziej zależy im na dobru wspólnym państwa, czyli szybszym rozwoju technologii, a w rezultacie – na rozwoju gospodarczym Chin. Przynajmniej taką oficjalną narrację przyjęły chińskie władze⁷¹. Z innych źródeł można wyczytać, że Chińczycy są jednak coraz bardziej zaniepokojeni niewystarczającym poziomem ochrony swoich danych⁷². Według sondażu przeprowadzonego przez *China Central Television* i *Tencent Research* prawie 80% respondentów uważa, że SI stanowi zagrożenie dla prywatności. Z danych *Internet Society of China* wynika, że 54% użytkowników Internetu w tym kraju obawia się naruszenia danych osobowych, określając takie przypadki jako „poważne”⁷³. Oficjalnie jednak są w stanie poświęcić swoje prawa dla państwa, a to stwarza pole do nadużyć i łamania praw pojedynczych obywateli w imię dobra wspólnego. Wszystkie wymienione czynniki sprawiają, że Chiny są idealnym środowiskiem do szybkiego rozwoju technologicznego. Chińskie władze otwarcie dążą do uczynienia swojego państwa światowym liderem technologicznym, o czym pisałam powyżej.

Skupiając się tylko na rozpoznawaniu twarzy, można dostrzec szerokie zastosowanie tej technologii na terytorium Chin. Stała się ona integralną częścią codziennego życia ludzi, zarówno w sektorze prywatnym, jak i publicznym. W przestrzeni publicznej jest ona używana w policyjnych systemach nadzoru oraz do kontroli ruchu drogowego⁷⁴, a także jest podstawową technologią używaną w tzw. *smart cities*. Na poziomie prywatnym używana jest ona do identyfikacji pracowników w biurach oraz klientów w sklepach, a także do uwierzytelniania użytkowników aplikacji mobilnych⁷⁵. Może być również częścią zabezpieczeń w domach. Wiele przedsiębiorstw i organizacji wykorzystuje rozpoznawanie twarzy w celu poprawy komfortu obsługi klienta i zwiększenia efektywności działalności gospodarczej⁷⁶. Co więcej, chińscy giganci cyfrowi, tacy jak Alibaba czy Tencent, dostarczający systemy płatności mobilnych, umożliwiają płacenie twarzą

⁷¹ K. Lucero, *op. cit.*, s. 109-110.

⁷² S. Lee, *op. cit.*

⁷³ K. Lucero, *op. cit.*, s. 113.

⁷⁴ M. Tan, *op. cit.*

⁷⁵ W. Knight, *China's AI Awakening. The West shouldn't fear China's artificial-intelligence revolution. It should copy it*, MIT Technology Review, 10.09.2017, <https://www.technologyreview.com/2017/10/10/148284/chinas-ai-awakening/> [dostęp: 23.09.2021].

⁷⁶ M. Tan, *op. cit.*

za zakupy w chińskich sklepach. Ponadto kamery mogą śledzić ludzi idących ulicą lub na stacjach transportu publicznego, identyfikować bezdomnych na ulicach i zwracać uwagę na to, kto z kim się spotyka, a nawet na jakie nabożeństwa uczęszcza. Za dowód na szybki rozwój tej technologii w Chinach może również posłużyć fakt, że w 2017 r. chińskie podmioty zgłosiły 530 wniosków na udzielenie patentów na narzędzia umożliwiające monitoring wideo, a więc ponad pięć razy więcej niż liczba podobnych wniosków złożonych przez podmioty amerykańskie⁷⁷.

Technologia rozpoznawania twarzy zaczyna być obecna w każdym aspekcie życia Chińczyków. Takie rozwiązanie ma swoje pozytywy oraz negatywy. Z pewnością w razie braku efektywnej ochrony prywatności oraz danych osobowych obywateli wykorzystanie tej technologii może bardzo łatwo posłużyć do nadużyć. Takim przykładem jest wprowadzenie systemu monitoringu biometrycznego na obszarze całego kraju. Gęsta sieć zamontowanych kamer śledzi wszystkie ruchy obywateli. Narzędzia te umożliwiają policji kontrolowanie populacji i zatrzymywanie podejrzanych, zanim jeszcze popełnią przestępstwo⁷⁸. Zapobieganie przestępstwom to niewątpliwy plus, ale z drugiej strony organy ścigania używały tego systemu do identyfikacji osób pokojowo protestujących oraz w celu tłumienia protestów w Hong Kongu w 2019 r., które organizowane były przeciwko autorytarnym chińskim rządóm⁷⁹. Protestujący stosowali różnego rodzaju środki, żeby kamery nie były w stanie zidentyfikować tożsamości – nosili kaski, a także maski i okulary na twarzach. Używali także laserowych długopisów, aby niemożliwe było zrobienie odpowiednich zdjęć twarzy⁸⁰. Jednakże system rozpoznawania twarzy w Hong Kongu to nie tylko wszechobecne kamery – każdy obywatel posiada również dowód osobisty wykorzystujący czipy, które przechowują dane biometryczne w postaci odcisków palców oraz zdjęcie. Zdjęcia wykonane na potrzeby dowodów osobistych wykorzystują rozpoznawanie twarzy w czasie rzeczywistym w celu potwierdzenia tożsamości osoby, a następnie są przechowywane w bazie danych przez Departament Imigracyjny⁸¹. Ta sytuacja pokazuje, że nadzór w Chinach ma charakter wielowymiarowy, na co wpływ ma wysoki poziom rozwoju technologii. Co prawda w prawie ochrony danych osobowych w Hong Kongu obowiązuje zasada o niegromadzeniu nadmiernej ilości danych, jednakże są od niej wyjątki dotyczące wykrywania lub przeciwdziałania przestępczości. W opisywanej sytuacji protestujący zostali uznani właśnie za przestępców.

⁷⁷ K. Lucero, *op. cit.*, s. 117.

⁷⁸ S. duPont, *On Facial Recognition, the U.S. Isn't China–Yet*, Lawfare, 18.06.2020, <https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet> [dostęp: 23.09.2021].

⁷⁹ R. Adams, *Hong Kong Protesters Are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched*, BuzzFeedNews, 17.08.2019, <https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers> [dostęp: 23.09.2021].

⁸⁰ *Ibidem*.

⁸¹ *Ibidem*.

Technologia rozpoznawania twarzy stanowi również jeden z najważniejszych elementów wprowadzonego w Chinach Systemu Zaufania Publicznego (*Social Scoring System*, dalej jako „SSS”), a więc systemu służącego do masowego nadzoru i inwigilacji społeczeństwa. Dzięki niemu obserwacja obywateli możliwa jest w czasie rzeczywistym poprzez umieszczone gęsto w każdym mieście kamery CCTV⁸². To narzędzie umożliwia szersze działanie niż sam monitoring biometryczny. SSS zakłada przyznanie Chińczykom (ale również przedsiębiorstwom) pewnej puli punktów na początek. Taka pula może być odpowiednio powiększana lub zmniejszana ze względu na poszczególne zachowania. Technologia rozpoznawania twarzy znacznie ułatwia w tym zakresie śledzenie poszczególnych aktywności obywateli oraz automatyczne przyznawanie bądź odejmowanie punktów.

Oficjalnie to narzędzie ma rozwiązać pewne społeczne problemy Chin, takie jak np. odbudowanie zaufania społecznego przez przywrócenie odpowiedzialności moralnej obywateli, przedsiębiorstw i instytucji rządowych⁸³. W rzeczywistości System Zaufania Publicznego to zestaw mechanizmów służących do wpływania na zachowania obywateli i organizacji poprzez ustalenie z góry listy zachowań pożądaných. Narzędzie będzie pozwalać na nagradzanie aktywności, które zostaną uznane za odpowiedzialne pod względem finansowym, ekonomicznym i społeczno-politycznym, a jednocześnie na karanie za zachowania uznane przez Partię za niegodne i niemoralne⁸⁴. Rząd utworzył już w tym celu dwie centralne bazy danych umożliwiające publiczne udostępnianie informacji⁸⁵.

SSS był na początku weryfikowany na poziomie poszczególnych miast. Przykładowo od listopada 2016 r. w Szanghaju testowana była aplikacja mobilna *Honest Shanghai*, która dzięki technologii rozpoznawania twarzy w ciągu doby przyznawała ocenę reputacji, w skali „bardzo dobry, dobry, zły”, opartą na danych rządowych⁸⁶. Planowane jest jednak wprowadzenie Systemu Zaufania Publicznego na terenie całego kraju. Pierwotnie rok 2020 był docelowym rokiem jego wdrożenia. Jednakże pandemia COVID-19 opóźniła ten proces. W styczniu 2021 r. Narodowa Komisja Rozwoju i Reform (*The National Development and Reform Commission*) opublikowała krajowe wytyczne dotyczące ra-

⁸² Technologia rozpoznawania twarzy pełni dla Systemu Zaufania Publicznego kluczową funkcję, gdyż jej implementacja do wszechobecnych kamer CCTV pozwala na natychmiastowe rozpoznanie osoby w przestrzeni publicznej. Wobec takiej osoby może zostać podjęte od razu odpowiednie działanie, np. w postaci odjęcia punktów z przyznanej puli.

⁸³ A.J. Wichura, *System Zaufania Społecznego – chiński patent na moralność*, Człowiek.info, 26.05.2019, <https://czlowiek.info/system-zaufania-spoecznego-chinski-patent-na-moralnosc/> [dostęp: 23.09.2021].

⁸⁴ K. Lucero, *op. cit.*, s. 116.

⁸⁵ *Ibidem*.

⁸⁶ A. J. Wichura, *op. cit.*

portowania w zakresie informacji społecznych pomiędzy prowincjami⁸⁷. Można się więc spodziewać pełnej implementacji już w tym roku.

Powyżej opisany system nadzoru społecznego jest w świetle chińskiej legislacji danoosobowej całkowicie dopuszczalny. Wprowadzanie nowych przepisów w teorii wzmacnia ochronę jednostek, ale jednocześnie zawierają one wiele wyjątków wyłączających ich stosowanie w odniesieniu do władz publicznych. Artykuł 26 najnowszej regulacji danoosobowej, czyli PIPL, przewiduje, że „Instalacja urządzeń do gromadzenia wizerunków lub rozpoznawania tożsamości w miejscach publicznych odbywa się w sposób wymagany do ochrony bezpieczeństwa publicznego i zgodnie z odpowiednimi przepisami państwowymi, przy czym należy zainstalować wyraźne znaki informacyjne”⁸⁸. Takie wyłączenie ustawowe wystarcza, aby każde użycie przez chińskie władze oprogramowania FRT w przestrzeni publicznej było uzasadnione.

Kolejnym zastosowaniem technologii rozpoznawania twarzy w Chinach, które budzi kontrowersje, jest wykorzystywanie jej do prześladowania grupy etnicznej Ujgurów. Ta muzułmańska mniejszość zamieszkująca północno-zachodni region Xinjiang stała się grupą doświadczalną dla szeroko zakrojonych chińskich operacji kontroli cyfrowej, w szczególności w dużej mierze została poddana wzmożonej inwigilacji i dyskryminacji⁸⁹. Zgodnie z medialnymi doniesieniami ponad milion Ujgurów oraz innych muzułmanów przebywa w chińskich obozach karnych, gdzie są poddawani indoktrynacji oraz zmuszani do wyzbycia się swojej religii. Reszta, przebywająca na względnej wolności, jest natomiast pod ciągłą obserwacją miejskich kamer⁹⁰. Kiedy w tym samym czasie w Europie toczy się dyskusja, jak sprawić, by algorytmy sztucznej inteligencji działały w sposób niedyskryminacyjny, w Chinach uczy się je, aby rozpoznawały mniejszości etniczne po kolorze skóry czy rysach twarzy⁹¹. Trudno powstrzymać się od porównania, że pomimo względnej wolności region Xinjiang otoczony jest wirtualną siatką, gdyż każde jego opuszczenie jest dokładnie śledzone. W innych regionach kraju algorytmy też są wytrenowane tak, aby rozpoznawać Ujgurów i informować o tym władze⁹². Celem takich działań jest uniemożliwienie osiedlenia się przedstawicieli tej mniejszości w innych częściach kraju, a tym bardziej stworzenie rodzin z Chińczykami.

⁸⁷ D. Donnelly, *An Introduction to the China Social Credit System*, 2021, NewHorizons, <https://nhglobalpartners.com/china-social-credit-system-explained/> [dostęp: 23.09.2021].

⁸⁸ Art. 26 ustawy o ochronie danych osobowych...

⁸⁹ N. Kobie, *The complicated truth about China's social credit system*, Wired, 07.06.2019, <https://www.wired.co.uk/article/china-social-credit-system-explained> [dostęp: 23.09.2021].

⁹⁰ P. Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, "The New York Times" 2019, <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> [dostęp: 23.09.2021].

⁹¹ *Ibidem*.

⁹² *Ibidem*.

W mieście Kaszgar informacje czerpane są z baz danych zawierających 68 miliardów rekordów, w tym tych dotyczących ruchu i aktywności ludzi. Dla porównania krajowy system natychmiastowego sprawdzania przeszłości kryminalnej FBI zawierał ok. 19 milionów rekordów na koniec 2018 r.⁹³ Co więcej, zintegrowana platforma bezpieczeństwa Chin gromadzi bezprecedensowe ilości danych na temat ponad 13 milionów osób należących do mniejszości etnicznych i religijnych w północno-zachodnim regionie Xinjiang⁹⁴. Pomimo tych informacji chiński rząd broni programu nadzoru, twierdząc, że poprawił on bezpieczeństwo w regionie oraz że obozy indoktrynacji w Xinjiang pełnią funkcję ośrodków szkolenia zawodowego⁹⁵.

Na przykładzie traktowania mniejszości Ujgurów łatwo zauważyć, że przy zastosowaniu technologii rozpoznawania twarzy w Chinach nie jest łamane jedynie prawo do prywatności, ale także i inne podstawowe prawa człowieka. Nietrudno odnieść wrażenie, że w regionie Xinjiang podstawowe wolności ludzi są ograniczane, a technologia w tym przypadku pomogła sprawić, że takie miasta jak Kaszgar stały się swoistymi gettami bez murów oraz bez żołnierzy, ale z systemem nadzoru, który pozwala władzy na obserwację obywateli przez całą dobę. Sytuacja nierealna z perspektywy UE, w Chinach jest rzeczywistością. Przykład ten pokazuje, do czego może doprowadzić stosowanie technologii rozpoznawania twarzy, jak i innych tego typu w przypadku braku odpowiednich narzędzi prawnych, które byłyby w stanie realnie zapobiec takim działaniom.

Jednak inwigilacja to nie wszystko, czego dopuszcza się chiński rząd. Ujgurzy stali się także grupą, na której można testować nowe możliwości FRT. W prowincji Xinjiang testowany jest aktualnie przez policję system służący do odczytywania z twarzy stanów emocjonalnych. Następnie przy użyciu algorytmów sztucznej inteligencji stwierdza się, czy zatrzymana osoba jest winna zarzucanego jej czynu⁹⁶. Nietrudno się domyślić, jak łatwo przy pomocy takiego oprogramowania niewłaściwie ocenić badanego człowieka. Uczący się system może wykazywać ogromny próg błędu, dlatego nigdy nie powinien być testowany w takich warunkach, a jego wyniki nie powinny stanowić jedyne go elementu decydującego o skazaniu człowieka.

⁹³ C. Buckley P. Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, "The New York Times" 2019, <https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html> [dostęp: 23.09.2021].

⁹⁴ K. Lucero, *op. cit.*, s. 117-118.

⁹⁵ C. Buckley P. Mozur, *op. cit.*

⁹⁶ U. Lesman, *Chińczycy testują AI na Ujgurach. Wskazuje: winny czy niewinny*, „Rzeczpospolita”, 27.05.2021, <https://cyfrowa.rp.pl/technologie/63698-chinczycy-testuja-ai-na-ujgurach-wskazuje-winny-czy-niewinny> [dostęp: 23.09.2021].

5. Zakończenie

Przeprowadzona analiza prowadzi do wniosków, że w zakresie ochrony danych osobowych w ostatnich latach wdrożono w Chinach duże reformy, z czym wiązało się wprowadzenie wielu nowych regulacji lub nowelizacja już istniejących. Aktualnie jesteśmy w trakcie doświadczania kolejnej zmiany, jaką jest implementacja pierwszej kompleksowej ustawy o ochronie danych, która zaczęła obowiązywać 1 listopada 2021 r. Jednakże na ten moment nie można powiedzieć, że regulacje danoosobowe przyznają odpowiedni poziom ochrony jednostkom. Należy jednak z uwagą przyglądać się wprowadzanym zmianom.

W Chinach następują również zmiany w zakresie regulacji samych technologii. Chiński plan rozwoju sztucznej inteligencji następnej generacji przewiduje, że Chiny staną się światowym liderem nie tylko w rozwoju sztucznej inteligencji do 2030 r., ale również w rozwoju przepisów oraz wytycznych dotyczących etyki w tym zakresie. Obecnie rozwijają się normy prawne dotyczące danych osobowych, a w szczególności danych biometrycznych, które ważne są w kontekście rozwoju technologii rozpoznawania twarzy. Pojawiają się też pierwsze, choć niewiążące standardy w zakresie wspierania rozwoju przemysłowego i promowania innowacji oraz wytyczne dotyczące etyki SI. Nie zmienia to jednak faktu, że regulacje nie nadążają za rozwojem technologii w Chinach – co nie stanowi wyjątku w porównaniu do innych regionów świata. Jednakże można wysnuć wniosek, że chińskie władze na pierwszym miejscu stawiają rozwój technologii, a dopiero na dalszym planie znajduje się zapewnienie swoim obywatelom odpowiedniego poziomu ochrony ich prawa do prywatności czy danych osobowych. Rezultatem takiego podejścia jest wysoko rozwinięta technologia rozpoznawania twarzy, która jest powszechnie stosowana.

W związku z powyższym przykład Chin pokazuje, że tak potężne narzędzie w niepowołanych rękach może stanowić zagrożenie dla obywateli. Chiński reżim wykorzystuje technologię rozpoznawania twarzy do inwigilacji oraz kontrolowania aktywności swoich obywateli. Jest także narzędziem do prześladowania i dyskryminacji mniejszości etnicznej Ujgurów zamieszkującej region Xinjiang. Zachowania te są uzasadniane zapewnieniem bezpieczeństwa narodowego, a przepisy prawne takie uzasadnienie przewidyują. Można sądzić, że w przypadku Chin dalsze rozwijanie tej technologii może przynieść więcej szkody niż pożytku dla prywatności oraz danych osobowych obywateli.

Bibliografia

Akty prawne

Civil Code of the People's Republic of China.

General Provisions of the Civil Law of the People's Republic of China.

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 119 z 4.05.2016 r., s. 1.

Ustawa o ochronie danych osobowych, źródło tłumaczenia na angielski: <https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021>.

Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane zasady dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM(2021) 206 final.

Literatura

Abu Gholeh M., Kuźnicka-Błaszowska D., *Ochrona danych osobowych w wybranych państwach Azji*, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2019, DOI: [10.34616/23.19.155](https://doi.org/10.34616/23.19.155).

Feng Y., *The future of China's personal data protection law: challenges and prospects*, "Asia Pacific Law Review" 2019, vol. 27, iss. 1.

Geller A., *How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective*, "GRUR International" 2020, vol. 69, no. 12.

Greenleaf G., *Asian Data Privacy Laws*, Oxford University Press 2014.

Lee K.F., *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata*, tłum. K. Hejwowski, Media Rodzina 2020.

Lin X., *A Dangerous Game: China's Big Data Advantage And How The U.S. Should Respond*, "Journal Of Law, Technology & Policy" 2020, no. 1.

Lucero K., *Artificial Intelligence Regulation and China's Future*, "Columbia Journal of Asian Law" 2019, vol. 33, no. 1.

Parasol M., *The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams*, "Computer Law & Security Review" 2018, no. 34.

Xue H., *Privacy and personal data protection in China: An update for the year end 2009*, "Computer Law & Security Review" 2010, no. 26.

Źródła internetowe

Adams R., *Hong Kong Protesters Are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched*, BuzzFeedNews, 17.08.2019, <https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers>.

Allen K., *China facial recognition: Law professor sues wildlife park*, BBC, 8.11.2019, <https://www.bbc.com/news/world-asia-china-50324342>.

- Bird R., Chiew J., *China's first omnibus data protection law*, Freshfields, 15.01.2021, <https://digital.freshfields.com/post/102gorq/chinas-first-omnibus-data-protection-law>.
- Bird R., *China "standardises" AI ethics*, Freshfields, 26.01.2021, <https://digital.freshfields.com/post/102gpfp/china-standardises-ai-ethics>.
- Buckley C., Mozur P., *How China Uses High-Tech Surveillance to Subdue Minorities*, "The New York Times" 2019, <https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html>.
- Chan M., Yue C., Gong J., Ke T., Zhang S., *The Gloves Are Off! China's Personal Information Protection Law was Passed and will Come into Effect on 1 November 2021*, Lexology, 23.08.2021, <https://www.lexology.com/library/detail.aspx?g=b11a28d4-a023-4af0-b7c3-d49ce8e80646>.
- Donnelly D., *An Introduction to the China Social Credit System*, New Horizons, 2021, <https://nhglobalpartners.com/china-social-credit-system-explained/>.
- duPont S., *On Facial Recognition, the U.S. Isn't China—Yet*, Lawfare, 18.06.2021, <https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet>.
- How Accurate is Facial Recognition Today?*, Rec Faces, 05.11.2020, <https://recfaces.com/articles/how-accurate-is-facial-recognition>.
- Kaja A., Luo Y., *Covington Artificial Intelligence Update: China's Vision for The Next Generation of AI*, Inside Privacy, 24.03.2018, <https://www.insideprivacy.com/artificial-intelligence/chinas-vision-for-the-next-generation-of-ai/>.
- Ke X., Liu V., Lao Y., Yu Z., *Analyzing China's PIPL and how it compares to the EU's GDPR*, IAPP, 24.08.2021, <https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/>.
- Knight W., *China's AI Awakening. The West shouldn't fear China's artificial-intelligence revolution. It should copy it*, MIT Technology Review, 10.10.2017, <https://www.technologyreview.com/2017/10/10/148284/chinas-ai-awakening/>.
- Kobie N., *The complicated truth about China's social credit system*, Wired, 07.06.2019, <https://www.wired.co.uk/article/china-social-credit-system-explained>.
- Lee S., *Coming into Focus: China's Facial Recognition Regulations*, Center for Strategic & International Studies, 04.05.2020, <https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations>.
- Lesman U., *Chinczycy testują AI na Ujgurach. Wskazuje: winny czy niewinny*, „Rzeczpospolita”, 27.05.2021, <https://cyfrowa.rp.pl/technologie/63698-chinczycy-testuja-ai-na-ujgurach-wskazuje-winny-czy-niewinny>.
- Mavuduru A., *Is Data Really the New Oil in the 21st Century?*, Towards Data Science, 12.12.2020, <https://towardsdatascience.com/is-data-really-the-new-oil-in-the-21st-century-17d014811b88>.
- Meng J., Fan W.S., *China strengthens its data protection legislation*, IAPP, 16.11.2016, <https://iapp.org/news/a/china-strengthens-its-data-protection-legislation/>.
- Mozur P., *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, "The New York Times" 2019, <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>.
- Murphy C., Li J., Liu C., Liu L., *China's New Data Law Gives Xi the Power to Shut Down Tech Firms*, Bloomberg, 11.06.2021, <https://www.bloomberg.com/news/articles/2021-06-10/china-passes-law-to-strengthen-control-over-tech-firms-data>.
- New rules to curb misuse of facial recognition tech*, China Daily, 29.07.2021, http://english.court.gov.cn/2021-07/29/content_37545967.htm.

- Ning S., Han W., Ke J., Yunhan L., Chi P., Minlv Y., Ziqian Z., *Personal Information Protection Law (Draft): A New Data Regime*, China Law Insight, 11.11.2020, <https://www.chinalawinsight.com/2020/11/articles/compliance/personal-information-protection-law-draft-a-new-data-regime/>.
- O'Meara S., *Will China lead the world in AI by 2030?*, "Nature", 21.08.2019, <https://www.nature.com/articles/d41586-019-02360-7>.
- Qiao S., Wang C., Clark D., *Zoo Loses the 'First Face Recognition Case' at Appeal*, Lexology, 22.04.2021, <https://www.lexology.com/library/detail.aspx?g=882322e8-fcb4-4f19-83c9-a4ff71d50e1d>.
- Robinson M., Lau N., Gong J., *China cybersecurity and data protection: Review of 2020 and outlook for 2021*, Lexology, 18.01.2021, <https://www.lexology.com/library/detail.aspx?g=44eee916-38fc-4132-8924-44377262ab4d>.
- Sheng J., Xu C., Tao E., *China Adopts New Data Security Law*, Pillsbury, 07.09.2021, <https://www.pillsburylaw.com/en/news-and-insights/china-adopts-new-data-security-law.html>.
- Szmidt-Husarz M., *Technologia rozpoznawania twarzy a ochrona danych osobowych w Chinach – sprawa prof. Guo Binga*, Chiny24, 16.12.2020, <https://chiny24.com/prawo/technologia-rozpoznawania-twarzy-a-ochrona-danych>.
- Tan M., *China: Facial recognition and its legal challenges*, OneTrust DataGuidance, 2020, <https://www.dataguidance.com/opinion/china-facial-recognition-and-its-legal-challenges>.
- Wichura A.J., *System Zaufania Społecznego – chiński patent na moralność*, Człowiek.info, 26.05.2019, <https://czlowiek.info/system-zaufania-spolecznego-chinski-patent-na-moralnosc/>.
- Yangfei Z., *Draft civil code emphasizes personality rights*, China Daily Hong Kong, 21.05.2020, <https://www.chinadailyhk.com/article/131295>.