PWPM 2022, Vol. XX
PROBLEMY WSPÓŁCZESNEGO PRAWA MIĘDZYNARODOWEGO, EUROPEJSKIEGO I PORÓWNAWCZEGO
REVIEW OF INTERNATIONAL, EUROPEAN AND COMPARATIVE LAW
ISSN 1730-4504

ARTYKUŁY / ARTICLES

DOI: 10.26106/3mp1-tm69

Unijny projekt regulacji sztucznej inteligencji a przeciwdziałanie próbom autorytarnego jej wykorzystywania przez władze publiczne

Jarosław Greser[1]
Doktor nauk prawnych, adiunkt w Szkole Nauk Ścisłych Uniwersytetu im. Adama Mickiewicza w Poznaniu
ORCID: 0000-0002-1021-6142; e-mail: greser@amu.edu.pl

Maria Dymitruk
Asystentka w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego
ORCID: 0000-0003-1003-9083; e-mail: maria.dymitruk@uwr.edu.pl

1. Wprowadzenie

Rozumienie pojęcia „sztuczna inteligencja" jest zróżnicowane[2]. Prężnie rozwijające się kierunki automatyzacji działań, których standardowe, tj. niezmechanizowane, wykonanie wymaga zaangażowania ludzkiej inteligencji, przyniosły liczne zmiany ekonomiczno-społeczne w niezliczonych branżach i obszarach aktywności

[1] Wkład do tekstu powstał w oparciu o badania prowadzone w ramach realizacji grantu „Cyberbezpieczeństwo urządzeń medycznego Internetu Rzeczy – perspektywa prawna" finansowanego ze środków Narodowego Centrum Nauki, nr umowy 2020/04/X/HS5/00135.

[2] Autorzy chcą uniknąć powielania w niniejszym artykule różnorodnego rozumienia pojęcia sztucznej inteligencji w naukach informatycznych lub w języku potocznym. Mnogość podejść badawczych oraz postępujący rozwój technologiczny praktycznie uniemożliwia stworzenie jednolitej i powszechnie akceptowanej definicji pojęcia sztucznej inteligencji. O czterech podstawowych naukowych sposobach jej definiowana zob. jednak: S. Russell, P. Norvig, *Artificial intelligence. A Modern Approach,* Upper Saddle River 2010, s. 1–2.

ludzkiej. Rozpatrywana często w kontekście korzyści i możliwości uzyskania przewagi konkurencyjnej przez podmioty ją wdrażające sztuczna inteligencja wymaga pogłębionej analizy również w zakresie rzeczywistych i potencjalnych sposobów jej wykorzystywania nie tylko przez osoby fizyczne i podmioty komercyjne, ale także przez władze publiczne. Działania sektora publicznego oparte na mechanizmach sztucznej inteligencji mogą być bowiem równie cenne z punktu widzenia rozwiązania palących kwestii społecznych czy efektywniejszej realizacji zadań publicznych, jak i niebezpieczne z perspektywy realizacji praw jednostki oraz zapewniania prawidłowego funkcjonowania społeczeństwa demokratycznego.

Unia Europejska stosunkowo wcześnie podjęła działania mające na celu utorowanie europejskiego podejścia do zagadnień sztucznej inteligencji. W 2012 r. Unia Europejska[3] rozpoczęła swoje zaangażowanie w prace nad analizą prawnych implikacji rozwoju sztucznej inteligencji[4], z czasem przesuwając ciężar aktywności nie tylko na współfinansowanie inicjatyw badawczych, ale także na działalność regulacyjną[5]. Pierwszymi efektami tego podejścia były: wydanie w dniu 16 lutego 2017 r. przez Parlament Europejski rezolucji zawierającej zalecenia dla Komisji Europejskiej w sprawie przepisów prawa cywilnego dotyczących robotyki[6] czy ustanowienie rozwoju sztucznej inteligencji częścią strategii w zakresie cyfryzacji europejskiego przemysłu i pełnego wykorzystania możliwości jednolitego rynku cyfrowego[7] oraz odnowionej strategii dotyczącej polityki przemysłowej UE[8],

[3] Dalej zamiennie UE lub Unia Europejska.

[4] Pierwsze działania UE opierały się na aktywnościach w ramach projektu naukowego o nazwie RoboLaw (*Regulating Emerging Technologies in Europe: Robotics Facing Law and Ethics*), mającego na celu weryfikację dopasowania unijnych ram prawnych do gwałtownego rozwoju automatyzacji wielu dziedzin życia.

[5] By być bardziej precyzyjnym, trzeba wskazać, że UE podjęła działalność przedregulacyjną, albowiem do dnia dzisiejszego nie mamy w Unii Europejskiej żadnego wiążącego aktu prawnego poświęconego *stricte* zagadnieniom sztucznej inteligencji.

[6] Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (Dz. Urz. UE C 252, s. 239–257). W późniejszym okresie Parlament Europejski wydał jeszcze szereg rezolucji związanych z zagadnieniami sztucznej inteligencji (m.in. dotyczących praw autorskich, odpowiedzialności, etyki, edukacji i kultury).

[7] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 19 kwietnia 2016 r., Cyfryzacja europejskiego przemysłu. Pełne wykorzystania możliwości jednolitego rynku cyfrowego, COM(2016) 180 final.

[8] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego, Komitetu Regionów i Europejskiego Banku Inwestycyjnego z dnia 13 września 2017 r., Inwestowanie w inteligentny, innowacyjny i zrównoważony przemysł. Odnowiona strategia dotycząca polityki przemysłowej UE, COM(2017) 479 final.

a następnie zapowiedź wielu aktywności badawczych i wdrożeniowych w komunikacie Komisji Europejskiej „Sztuczna inteligencja dla Europy" z dnia 25 kwietnia 2018 r.[9] oraz przygotowanie w kwietniu 2019 r. przez działającą przy Komisji Europejskiej grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji wytycznych w zakresie etyki dotyczących wiarygodnej sztucznej inteligencji[10]. Swoistym zebraniem dotychczasowych rozważań nad europejskim kierunkiem działań w obszarze sztucznej inteligencji była biała księga „Europejskie podejście do doskonałości"[11]. Jako dokument programowy. Księga wskazała główne zamierzenia Komisji Europejskiej z zakresu uporządkowania legislacji w obszarze sztucznej inteligencji. W dokumencie uwypuklono kwestię stworzenia w Europie takiego ekosystemu sztucznej inteligencji, który zapewni korzyści obywatelom i gospodarce również w zakresie działań władzy publicznej[12].

Niezmiennie w każdym z wymienionych dokumentów instytucje unijne podkreślały wagę takiego ukształtowania europejskiego podejścia do sztucznej inteligencji, które charakteryzować się będzie wdrażaniem odpowiednich zabezpieczeń w celu poszanowania podstawowych praw i wolności[13], rozwoju godnej zaufania i bezpiecznej sztucznej inteligencji[14] oraz respektowania wartości leżących u podstaw Unii Europejskiej[15], w tym również zasad praworządności[16]. Uwypuklenie akurat tych aspektów funkcjonowania mechanizmów sztucznej inteligencji na obszarze Unii Europejskiej czytelnie ukazuje chęć przeciwstawienia się podejściom pozostałych dwóch najważniejszych światowych graczy na polu sztucznej inteligencji: Chin oraz Stanów Zjednoczonych Ameryki Północnej. Unia Europejska zdaje się odcinać zarówno od czysto merkantylnego podejścia do sztucznej inteligencji, wyrażającego się w budowaniu rynkowej przewagi konkurencyjnej

---

9 Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 25 kwietnia 2018 r., Sztuczna inteligencja dla Europy, COM(2018) 237 final.

10 Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_PL.pdf (dostęp: 15.03.2022).

11 Komisja Europejska, Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania, COM(2020) 65 final, Bruksela, 19.02.2020 r., dalej: biała księga.

12 *Ibidem,* s. 2. Jednym z wyraźnie wskazanych w raporcie obszarów działań Unii Europejskiej pozostaje promowanie zastosowań sztucznej inteligencji przez sektor publiczny – zob. Section F. Promoting the adoption of AI by the public sector, *ibidem*, s. 8.

13 Zob. chociażby treść białej księgi, s. 2–3, 9–14, 17–19, 21– 22, 25.

14 *Ibidem,* s. 2–3, 9–10, 20–21, 23–25.

15 *Ibidem,* s. 1–3, 8, 10–11, 18–19, 23, 25.

16 *Ibidem,* s. 1.

za wszelką cenę, jak i od autorytarnych zapędów wykorzystywania sztucznej inteligencji jako narzędzia kontroli społecznej.

Ukoronowaniem dotychczasowych unijnych wysiłków (przed)regulacyjnych w obszarze sztucznej inteligencji pozostaje opublikowanie w dniu 21 kwietnia 2021 r. przez Komisję Europejską projektu rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji)[17]. Projekt ten wprowadzić miałby definicję legalną sztucznej inteligencji, rozwiewając istniejące wątpliwości definicyjne oraz ujednolicając – dotychczas rozbieżne – określenia sztucznej inteligencji pojawiające się w dokumentach unijnych. Zgodnie z projektowanym art. 3 pkt 1 aktu o sztucznej inteligencji „system sztucznej inteligencji" oznaczać miałby oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I do aktu, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję. Definicję ukuto więc poprzez odniesienie się do treści załącznika. W obecnym kształcie załącznik ten wśród technik i podejść z zakresu sztucznej inteligencji, o których mowa w art. 3 pkt 1 aktu o sztucznej inteligencji, wymienia: a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego; b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) oraz systemy ekspertowe; c) podejścia statystyczne, estymację bayesowską, metody wyszukiwania i optymalizacji.

Starając się zbudować neutralną pod względem technologicznym i mogącą podlegać regularnym uaktualnieniom nadążającym za rozwojem technologicznym[18] definicję sztucznej inteligencji, Komisja Europejska zdecydowała się na ujęcie w niej niezwykle szerokiego wachlarza podejść w efekcie zastosowania zarówno tradycyjnych technik opartych na logice typu *expert systems*, jak i zaawansowanych mechanizmów uczenia maszynowego (*machine learning*). Takie działanie odczytywać można jako zbyt rozległą próbę uchwycenia pojęcia sztucznej inteligencji, obejmującą – według niektórych niezasadnie – prawie każde tworzone współcześnie

[17] Projekt Komisji Europejskiej z dnia 21 kwietnia 2021 r. rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii, COM/2021/206 final, dalej: akt o sztucznej inteligencji lub rozporządzenie.

[18] Zgodnie z art. 4 aktu w sprawie sztucznej inteligencji Komisja Europejska jest uprawniona do zmiany wykazu technik i podejść wymienionych w załączniku I, aby uaktualnić ten wykaz z uwzględnieniem rozwoju sytuacji rynkowej i rozwoju technologicznego.

oprogramowanie[19]. Warto przy tym jednak podkreślić, że przedstawienie tak różnokierunkowej i wszechobejmującej definicji sztucznej inteligencji służy lepszemu zagwarantowaniu bezpieczeństwa jej funkcjonowania na obszarze Unii Europejskiej. Można bowiem twierdzić, że użycie (przykładowo) systemu oceny możliwości powrotu do przestępstwa[20] może wiązać się z bardzo różnymi rodzajami ryzyka dla obywatela Unii Europejskiej w zależności od tego, czy system ten jest prostym systemem regułowym (z definicji transparentnym), czy samouczącą się siecią neuronową (dotkniętą problemem „czarnej skrzynki"[21]). Należy jednak pamiętać, że efekt funkcjonowania systemu (profilowanie[22]) będzie z punktu widzenia jednostki w obydwu przypadkach identyczny: system oceni zebrane dane jej dotyczące i – w zależności od stopnia jego autonomiczności[23] – albo przekaże wynik ludzkiemu decydentowi (np. sędziemu decydującemu o zwolnieniu warunkowym), albo sam podejmie określone działania (np. automatycznie wyśle dodatkowy patrol policji w dany rejon miasta). Przyjęte przy projektowanym akcie prawnym podejście prawodawcy unijnego oparte jest na ocenie, czy dany sposób zastosowania AI stanowi zagrożenie dla praw i wolności jednostki, czy może oddziaływać na realizację zasad

[19] P. Glauner, *An Assessment of the AI Regulation Proposed by the European Commission*, „arXiv preprint" 2021, https://arxiv.org/pdf/2105.15133.pdf, s. 3–4 (dostęp: 15.03.2022).

[20] Niniejszy przykład odnosi się – co oczywiste – do szeroko dyskutowanych w doktrynie i mediach przykładów wykorzystania (zarówno w Europie, jak i w Stanach Zjednoczonych Ameryki Północnej) systemów automatycznej analizy ryzyka recydywy, które spotkały się z istotnym oporem społecznym oraz odpowiedzią organizacji broniących praw człowieka (zob. system COMPAS oraz HART).

[21] Problem „czarnej skrzynki" (*black box*) wiąże się z brakiem przejrzystości/wyjaśnialności zaawansowanych systemów uczenia maszynowego. W odpowiedzi na ten problem w literaturze przedmiotu postulowane stworzenie prawa jest do przejrzystości (interpretowalności, wyjaśnialności) – zob. M. Araszkiewicz, *Sztuczna Inteligencja i prawo do wyjaśnienia*, „Kwartalnik Trzeci Sektor" 2018, nr 4, s. 37.

[22] Definicja profilowania – zob. art. 4 pkt 4 rozporządzenia 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 (Dz. Urz. UE L 119, s. 1), dalej: RODO. Projekt aktu o sztucznej inteligencji wymienia systemy profilowania używane w celu ścigania przestępstw wysokiego ryzyka przez systemy sztucznej inteligencji, zob. załącznik III do projektu rozporządzenia, pkt 6 lit. e–g.

[23] Zwracamy uwagę na konieczność rozróżnienia pojęć „automatyczny" i „autonomiczny" w kontekście systemów technologicznych, różnicy pomiędzy nimi upatrując w zakresie ewentualnej samodzielnej „decyzyjności" takiego systemu. Umiejętność wykonania danego zadania przez system bez udziału człowieka czyni system „automatycznym". Z kolei system „autonomiczny" nie tylko automatyzuje dane czynności, ale dodatkowo jest w stanie samodzielnie podejmować określone decyzje (zamiast człowieka), np. autonomiczny pojazd samochodowy zdolny jest do przejęcia wszystkich obowiązków ludzkiego kierowcy bez jego bezpośredniej ingerencji.

demokratycznych lub w inny sposób wpływać na społeczeństwo. Kluczowe pozostaje więc to, jak system jest wykorzystywany: czy stanowi podstawę podejmowania decyzji wobec jednostki, a nie konkretnie jaka technologia się za nim kryje.

W kontekście publicznych zastosowań systemów sztucznej inteligencji zrodziła się swoista luka regulacyjna. Możliwości technologiczne oraz chęci władz niektórych państw, w tym również państw autorytarnych[24], do możliwie najszerszego wykorzystywania zaawansowanej technologii doprowadziły do momentu, w którym ewentualne nadużycia mogą być analizowane jedynie w oparciu o regulacje dotyczące praw człowieka. System ochrony prac człowieka często pozostaje narzędziem niewystarczającym, zbyt ogólnym i niezapewniającym odpowiednich mechanizmów wymuszania przestrzegania prawa, co czyni sztuczną inteligencję w rękach władz publicznych narzędziem potencjalnie niebezpiecznym[25]. Unijny akt o sztucznej inteligencji ma szansę stać się pierwszym narzędziem prawnym, które da obywatelom Unii Europejskich lepszą ochronę ich praw i interesów.

Pytanie badawcze, na które ma odpowiedzieć niniejszy artykuł, brzmi następująco: w jaki sposób projektowana regulacja unijna w zakresie sztucznej inteligencji kształtuje ramy prawne dla przeciwdziałania potencjalnemu autorytarnemu

[24] Przez państwo autorytarne rozumiemy państwo funkcjonujące w oparciu o rządy niespełniające standardów demokratycznych, w których występuje jeden silny ośrodek władzy, brak pluralizmu politycznego oraz ograniczenie możliwości kontroli władz przez obywateli. Zob. więcej na temat zagadnień terminologicznych i komparatystycznych w zakresie pojęć „demokracja", „dyktatura", „autorytaryzm" i „totalitaryzm" – R. Tokarczyk, *Demokracja a dyktatura, autorytaryzm, totalitaryzm. Komparatystyka relacji czterech pojęć*, „Acta Universitatis Wratislaviensis" nr 3039, Studia nad Faszyzmem i Zbrodniami Hitlerowskimi XXX, Wrocław 2008.

[25] Skuteczność systemu ochrony praw człowieka jest zależna od możliwości realnego egzekwowania ich przestrzegania. W przypadku państw autorytarnych z definicji jest to znacznie ograniczone lub niemożliwe m.in. ze względu na brak odpowiednich mechanizmów kontroli władzy czy brak niezawisłego sądownictwa. Na poziomie międzynarodowym problemem jest zaś bardzo ograniczona możliwość egzekwowalności stanowisk organów międzynarodowych wydanych w ramach systemu ONZ i systemów regionalnych. Nawet dysponujący najbardziej rozbudowanymi instrumentami w tym zakresie system europejski napotyka na brak realizacji swoich orzeczeń w krajach, takich jak Rosja. Ponadto, szczególnie w kontekście sztucznej inteligencji, na znaczeniu zyskuje zagadnienie odpowiedzialności za działania podmiotów niepaństwowych, w tym transnarodowych korporacji, które odgrywają wiodącą rolę w tworzeniu tej technologii. Na obecnym etapie rozwoju koncepcji praw człowieka nie ma wątpliwości, iż podmioty gospodarcze są adresatami tych praw, ale jednocześnie nie są adresatem sankcji przewidzianych w systemie praw człowieka. Zob. A. Młynarska-Sobaczewska, P. Radziewicz, *Horyzontalne oddziaływanie Konstytucji Rzeczypospolitej Polskiej oraz Konwencji o Ochronie Praw Człowieka i Podstawowych Wolnośc*i, Warszawa 2015; M. Nowak, *Introduction to the International Human Rights Regime*, Leiden–Boston 2003; N. Jagers, *Corporate Human Rights Obligations: In Search of Accountability*, Antwerpia, 2002.

wykorzystywaniu AI przez władze państwowe krajów członkowskich? Zadając takie pytanie badawcze, wyjaśnić wypada, że jedną z podstawowych wartości jednoczących państwa członkowskie pozostaje demokracja. Zgodnie z art. 2 Traktatu o Unii Europejskiej[26] Unia opiera się na wartościach poszanowania godności osoby ludzkiej, wolności, demokracji, równości, państwa prawnego, jak również poszanowania praw człowieka. Wartości demokratyczne jako wspólne wszystkim państwom członkowskim w teorii wykluczają zaistnienie autorytaryzmów w UE, jednocześnie współcześnie wyraźnie zauważalny pozostaje regres poszanowania demokracji w niektórych społeczeństwach unijnych, rosnące tendencje autorytarne władz niektórych państw członkowskich oraz zanik poważania dla podwalin ustrojów demokratycznych. Z tego względu stawianie pytania o potencjalnie autorytarny kierunek publicznego wykorzystywania technologii w krajach członkowskich nie pozostaje bezcelowe.

2. Wykorzystanie sztucznej inteligencji przez władze państw autorytarnych

Badania nad problemem wykorzystania sztucznej inteligencji przez państwa autorytarne są utrudnione ze względu na brak odpowiednich danych źródłowych, niezbędnych do analizy empirycznej tego zjawiska. Stosowane rozwiązania technologiczne, jak również szczegóły ich działania są objęte tajemnicą, ponieważ odnoszą się do kwestii bezpieczeństwa publicznego lub narodowego, a niejednokrotnie dodatkowo chronione są tajemnicą przedsiębiorstwa[27]. Niemniej jednak analiza dostępnych materiałów pozwala wyodrębnić kilka obszarów, w których są dowody na stosowanie sztucznej inteligencji w sposób wspierający narzędzia rządów autorytarnych, takie jak cenzura, kontrola na życiem osobistym jednostek czy tłumienie przejawów działalności opozycyjnej. W dalszej części pracy zostaną omówione dwa z nich: ustalanie tożsamości jednostek oraz predykcja zachowań osób fizycznych.

2.1. Ustalanie tożsamości

Systemy ustalania tożsamości osób opierają się na pobieraniu danych z sieci kamer zamontowanych w miejscach publicznych, takich jak ulice, pociągi czy lotniska, lub prywatnych, jak wnętrza biurowców, i porównywaniu ich z wizerunkami przechowanymi w bazach danych. Oficjalnym celem tej technologii jest podniesienie poziomu bezpieczeństwa publicznego poprzez zapobieżenie popełnianiu

[26] Dz. Urz. UE C 202 z 2016 r., s. 15, dalej: TUE.

[27] A. Gryszczyńska, *Struktura regulacji tajemnic ustawowo chronionych* [w:] *Jawność i jej ograniczenia. Struktura tajemnic*, red. A. Gryszczyńska, Warszawa 2016, s. 273–327.

przestępstw lub wykryciu ich sprawców. Sama technologia nadzoru przy pomocy kamer jest stosowana od dawna, ale połączenie jej z algorytmami sztucznej inteligencji prowadzi do uzyskania nowych możliwości. Jako przykład wskazuje się rozpoznanie i zatrzymanie przestępcy ukrywającego się w tłumie podczas święta piwa lub będącego jednym z 60 tysięcy gości na koncercie w Chinach[28]. Ze względu na swoje walory systemy te są stosowane nie tylko w państwach autorytarnych, ale również demokratycznych. Są doniesienia o ich wykorzystywaniu w Stanach Zjednoczonych[29], Niemczech[30] i Walii[31].

Liderem w rozwoju tej technologii są Chińczycy[32], którzy planują zainstalowanie do 2025 roku co najmniej 600 milionów kamer, z których większość będzie dostarczać dane do algorytmów sztucznej inteligencji działających w ramach projektu Niebiańska Sieć[33]. System ten już w chwili obecnej jest w stanie zidentyfikować w ciągu jednej sekundy każdego Chińczyka oraz każdą osobę, która przekroczyła chińską granicę, bez względu na to, czy określona osoba ma ubraną maskę[34], kapelusz lub okulary[35]. Trzeba zwrócić uwagę, że technologia ta nie ogranicza się do zbierania wizerunków twarzy, ale gromadzi i przetwarza inne dane biometryczne, takie jak sposób chodzenia, barwa głosu czy rodzaj artykulacji i wokalizacji, co pozwala na skanowanie rozmów telefonicznych w czasie rzeczywistym i identyfikację ich uczestników[36]. Ponadto możliwe jest ocenianie stanu emocjonalnego osób, których wizerunki są przetwarzane[37].

---

28 K. Strittmatter, *Chiny 5.0. Jak powstaje cyfrowa dyktatura*, Warszawa 2020, s. 222.

29 T. Ryan-Mosley, *The new lawsuit that shows facial recognition is officially a civil rights issue*, https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/?truid=c191724687e9f528673169436f1c3ccd&mc_cid=8fd0bb6e76&mc_eid=cd18e5bd72 (dostęp: 15.03.2022).

30 M. Fürstenau*, Niemcy. Kontrowersyjny projekt rozpoznawania twarzy*, https://p.dw.com/p/3S6R3 (dostęp: 15.03.2022).

31 *Walijska policja naruszyła prawo. Stosowanie technologii rozpoznawania twarzy nielegalne,* https://www.cyberdefence24.pl/walijska-policja-naruszyla-prawo-stosowanie-technologii-rozpoznawania-twarzy-nielegalne (dostęp: 15.03.2022).

32 Możliwości tej technologii i poziom jej ingerencji w życie prywatne obrazuje film z 2017 roku *Oczy ważki* wyreżyserowany przez Bing Xu. Składa się on z ujęć wybranych spośród 10 tysięcy godzin publicznie dostępnych nagrań z monitoringu miejsc publicznych w Chinach.

33 K. Strittmatter, *Chiny 5.0..., op. cit.,* s. 224.

34 M. Pollard, *Even mask-wearers can be ID'd, China facial recognition firm says*, „Reuters", 9.03.2020 https://www.reuters.com/article/us-health-coronavirus-facial-recognition-idUSKBN20W0WL (dostęp: 15.03.2022).

35 K. Strittmatter*, Chiny 5.0..., op. cit.*, s. 223, 239.

36 *Ibidem*, s. 248.

37 M. Szwoch, P. Pieniążek, *Detection of Face Position and Orientation Using Depth Data*, „Image Processing and Communications Challenges" 2015, nr 7, s. 239–251.

Oprócz wpływu na prywatność jednostek systemy te mogą naruszać prawa jednostek i wartości demokratyczne w inny sposób. Tytułem przykładu można wskazać dwa obszary. Pierwszym jest dyskryminacja, której źródłem jest błędna konstrukcja algorytmów sztucznej inteligencji. W literaturze wskazuje się, że na obecnym etapie rozwoju systemy identyfikacji mają niższe wskaźniki rozpoznawania osób o innym kolorze skóry niż biały[38] oraz znacząco słabsze parametry identyfikacji kobiet[39]. Ponadto istnieją liczne doniesienia o rasistowskich[40] i seksistowskich[41] efektach działania systemów rozpoznawania wizerunku. Skutkiem tego może być naruszenie prawa do bezpieczeństwa osobistego i domniemania niewinności, które były już odnotowywane, takie jak zatrzymanie przez policję osoby błędnie rozpoznanej przez komputer jako podejrzany[42].

Drugim obszarem, w którym algorytmy identyfikujące osoby stanowią zagrożenie dla wartości demokratycznych, jest tworzenie systemu braku zaufania społecznego charakterystycznego dla ustrojów państw autorytarnych i totalitarnych. Jednym ze sposób na jego osiągnięcie jest stworzenie atmosfery powszechnego szpiegowania i donosicielstwa. Przykładem realizacji tego celu przy pomocy nowoczesnych technologii jest chiński system Bystrych Oczu (*xueliang*). Program ten pozwala mieszkańcom na śledzenie obrazów z kamer w ich najbliższej okolicy i zawiadamiania policji, jeżeli dzieje się coś niebezpiecznego lub podejrzanego[43]. Zwraca się uwagę, że rozwiązanie to zarówno w nazwie, jak i założeniach odwołuje się do czasów Rewolucji Kulturalnej, w czasie której „cały naród nieustannie się szpiegował"[44]. Zjawisko to jest tym bardziej niebezpieczne, że ma objąć wszystkie przestrzenie publiczne w Chinach[45].

[38] Wyniki uzyskane w ramach projektu badawczego Gender Shades prowadzonego na Massachusetts Institute of Technology wskazują, że wszystkie badane programy mają największy stopień błędnych identyfikacji w przypadku kobiet o ciemnym kolorze skóry. Uśredniając, jest to 33,8% błędnych identyfikacji. J. Buolamwini, T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, „Proceedings of Machine Learning Research" 2018, nr 81, s. 1–15.

[39] We wskazanym wyżej badaniu stwierdzono, że 95,9% twarzy źle zinterpretowanych przez oprogramowanie Face++ było twarzami kobiet. *Ibidem,* s. 9.

[40] Zob. V. Eubanks, *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*, Nowy Jork 2018.

[41] C. Schwemmer, C. Knight, E.D. Bello-Pardo, S. Oklobdzija, M. Schoonvelde, J.W. Lockhart, *Diagnosing Gender Bias in Image Recognition Systems*, „Socius" 2020, nr 6, s. 1–17.

[42] T. Ryan-Mosley, *The new lawsuit…, op. cit.*

[43] *State of Surveillance: Government Documents Reveal New Evidence on China's Efforts to Monitor Its People,* https://www.chinafile.com/state-surveillance-china (dostęp: 14.06.2021).

[44] K. Strittmatter*, Chiny 5.0…, op. cit.*, s. 207.

[45] D. Gershgorn, *China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space*, https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015 (dostęp: 15.03.2022).

2.2. Analiza predykcyjna

Analiza predykcyjna to proces uzyskiwania informacji z istniejących zbiorów danych w celu przewidywania przyszłych zdarzeń i trendów[46]. Sztuczna inteligencja jest szczególnie przydatna w prowadzeniu działań tego rodzaju, co spowodowało, że są one szeroko wykorzystywane komercyjnie szczególnie w obszarach związanych z marketingiem i sprzedażą[47]. Jednocześnie można zaobserwować zwiększenie zainteresowania nimi przez władze publiczne, szczególnie w obszarach dostępu do usług publicznych i związanych z pracą organów ścigania. Wiążą się z tym różnorakie zagrożenia w sferze praw jednostek, w szczególności w zakresie dyskryminacji. W obszarze usług publicznych można przywołać przykłady algorytmów profilujących osoby bezrobotne.

Rozwiązania mające na celu przypisanie osób bezrobotnych do określonych grup i dzięki temu zróżnicowanie oferty wsparcia zostały wprowadzone do praktyki różnych państw europejskich w pierwszym dziesięcioleciu XXI wieku[48]. W Polsce kwestię tę regulowało rozporządzenie z 27 maja 2014 r.[49], które dzieliło bezrobotnych na trzy grupy w zależności od sytuacji socjoekonomicznej określonej osoby. Jednocześnie przypisanie do określonego profilu wyznaczało granice wsparcia, tym samym mogło prowadzić do dyskryminacji w dostępie do usług publicznych, szczególnie wobec wielu zastrzeżeń zgłaszanych w stosunku do metodologii, na której się opierał algorytm. Dotyczyły one zarówno zakresu zbieranych danych, jak i sposobu przypisywania wag poszczególnym informacjom[50]. Wskazuje się również na podręcznikowe błędy dotyczące konstrukcji algorytmu, w tym stosowanie pytań sugerujących odpowiedź, pomylenie kierunku zależności przyczynowo-skutkowych czy wreszcie brak predykcyjnego charakteru tego rozwiązania[51]. Przepis ten został

[46] C. Nyce, *Predictive Analytics White Paper*, American Institute for Chartered Property Casualty Underwriters/Insurance Institute of America, 2007, s. 1.

[47] M. Mariani, R. Perez-Vega, J. Wirtz, *AI in marketing, consumer research and psychology: A systematic literature review and research agenda*, „Psychology & Marketing" 2022, nr 39, s. 755–776.

[48] D. Przeklasa, *Koncepcja profilowania pomocy dla osób bezrobotnych jako nowy instrument poprawy jakości usług świadczonych przez powiatowe urzędy pracy*, „Internetowy Przegląd Prawniczy TBSP UJ" 2015, nr 4, s. 123–125.

[49] Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 14 maja 2014 r. w sprawie profilowania pomocy dla bezrobotnego (Dz.U. poz. 631). Rozporządzenie zostało uchylone w 2019 r.

[50] J. Niklas, *Co zawiera algorytm służący do profilowania w urzędach pracy?,* https://panoptykon.org/wiadomosc/co-zawiera-algorytm-sluzacy-do-profilowania-w-urzedach-pracy (dostęp: 15.03.2022).

[51] K. Sztandar-Sztanderska, M. Kotnarowski, M. Zieleńska, *Czy algorytmy wprowadzają w błąd? Metaanaliza algorytmu profilowania bezrobotnych stosowanego w Polsce*, „Studia Socjologiczne" 2021, nr 1, s. 108–109.

zaskarżony do Trybunału Konstytucyjnego przez Rzecznika Praw Obywatelskich i wyrokiem z 6 czerwca 2018 r. został uznany za niekonstytucyjny[52]. Trybunał wskazał na naruszenie prawa do sądu poprzez brak możliwości zaskarżenia decyzji działania algorytmu oraz regulowanie kwestii praw i wolności obywatelskich w akcie podustawowym. Tym samym nie rozstrzygnął on kwestii, czy takie działanie co do zasady jest dopuszczalne w świetle artykułu 51 Konstytucji, który wyznacza granice autonomii informacyjnej jednostki.

Analiza predykcyjna (*predictive analysis*) jest również stosowana w pracach organów ścigania. Obejmuje ona cztery obszary działań: metody przewidywania przestępstw, metody przewidywania, jakie osoby są zagrożone popełnieniem przestępstwa w przyszłości, metody przewidywania tożsamości sprawców oraz metody przewidywania ofiar przestępstw[53]. Działania takie budzą liczne obawy w zakresie równego traktowania obywateli. Są one pogłębiane przez potwierdzone przypadki dyskryminacyjnych zachowań, których źródłem była decyzja algorytmu. Szczególnie liczne przykłady pochodzą ze Stanów Zjednoczonych, gdzie – jak się wskazuje – źródłem takich zachowań są nie tylko błędy w konstrukcji algorytmów, w szczególności trenowanie ich na bazach danych umacniających rasistowskie stereotypy[54], ale również kultura organizacyjna organów ścigania, która przyzwala na takie zachowania[55], lub nawet celowe działania producentów umożliwiające działania dyskryminacyjne[56].

Porównując te dwie sytuacje, trzeba zauważyć, że narzędzie do profilowania bezrobotnych było stosunkowo mało skomplikowane i w swoim działaniu nie opierało się na mechanizmach uczenia maszynowego oraz pozwalało na ingerencje

---

52 Wyrok Trybunału Konstytucyjnego z 6 czerwca 2018 r., K 53/16, OTK-A 2018, poz. 38.

53 M. Dymitruk, *Legal Tech w organach ścigania* [w:] *Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym*, red. D. Szostek, Warszawa 2021.

54 W. Douglas Heaven, *Predictive policing algorithms are racist. They need to be dismantled*, „MIT Technology Review", 17.07.2020, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (dostęp: 15.03.2022).

55 A. Gelman, J. Fagan, A. Kiss, *An Analysis of the New York City Police Department's "Stop-and-Frisk" Policy in the Contex tof Claims of Racial Bias*, „Journal of the American Statistical Association" 2007, nr 479; J. Kołtunowicz, *Rasizm i seksizm w bazie MIT*, https://www.sztucznainteligencja.org.pl/rasizm-i-seksizm-w-bazie-mit/ (dostęp: 15.03.2022).

56 Należy zauważyć, że IBM w co najmniej jednym przypadku sprzedał system umożliwiający policji analizowanie obrazów z monitoringu według kryterium, którym jest kolor skóry. G. Joseph, K. Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color*, „The Intercept", 6.09.2018, https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/ (dostęp: 15.03.2022).

człowieka[57]. Skala problemów potęguje się jednak przy wykorzystaniu w pełni zautomatyzowanych algorytmów, których konstrukcja nie zawsze pozwala na wyjaśnienie, dlaczego określona decyzja została podjęta[58]. Trzeba podkreślić, że problem ten nie dotyczy tylko organów ścigania, ale również innych usług publicznych[59].

3. Aksjologiczne przesłanki regulacji AI

Celem Unii Europejskiej jest rozwój bezpiecznej, wiarygodnej i etycznej sztucznej inteligencji. Te trzy cechy podkreśla się zarówno w dokumentach o charakterze politycznym[60], jak i programowym[61] oraz w opracowaniach eksperckich[62]. Trzeba zauważyć, że takie podejście ogranicza potencjał rozwoju tej technologii ze względu na brak możliwości korzystania ze wszystkich źródeł danych, a tym samym osiągnięcia lepszego efektu w trenowaniu algorytmów. Wskazuje się, że takie podejście do systemów sztucznej inteligencji prowadzi do utraty przewag konkurencyjnych na rzecz Chin, gdzie praktyczne implementacje tej technologii nie napotykają barier w postaci norm prawnych lub etycznych[63]. Jednocześnie w UE nie toczyła się dyskusja, czy regulować tę technologię – stawianym obecnie pytaniem jest to, jak ją uregulować, żeby pogodzić rozwój sztucznej inteligencji ze standardami przyjętymi w Europie. Wskazuje się, że tworząc regulacje,

---

57 J. Niklas, *Co zawiera...*, *op. cit.*

58 Osobną kwestią podnoszoną w literaturze jest niedoreprezentacja badań prowadzonych poza Stanami Zjednoczonymi i krajami wysoko rozwiniętymi, co pozwala przyjąć, że opisy zagrożeń i błędów, które zostały przedstawione, są bardzo fragmentaryczne. Będzie to tym bardziej widoczne w przypadku państw autorytarnych, w których niezależna kontrola władzy jest niemożliwa. K. Sztandar-Sztanderska, M. Kotnarowski, M. Zieleńska, *Czy algorytmy wprowadzają...*, *op. cit*., s. 110.

59 A. Zagórna, *Bo algorytm był rasistowski*, https://www.sztucznainteligencja.org.pl/bo-algorytm-byl-rasistowski/ (dostęp: 15.03.2022).

60 *A Union that strives for more. My agenda for Europe by candidate for President of the European Commission Ursula von der Leyen. Political Guidelines For The Next European Commission 2019–2024*, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf (dostęp: 14.06.2021).

61 Komunikat Komisji z 19.2.2020 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Kształtowanie cyfrowej przyszłości Europy, COM(2020) 67 final; komunikat Komisji z 9.03.2021 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final.

62 Wytyczne w zakresie etyki..., *op. cit.,* s. 17–25.

63 K. Strittmatter, *Chiny 5.0...., op. cit.,* s. 232.

należy mieć na uwadze budowę zaufania użytkownika do systemu oraz konieczność zgodności regulacji z innymi normami prawa europejskiego, które chronią prawa jednostki.

Odnosząc się do problemu budowy zaufania, trzeba zauważyć, że kluczem do adaptacji nowej technologii i jej dalszego rozwoju jest jej akceptacja przez użytkowników[64]. Punktem wyjścia do niej jest przekonanie, że określona technologia przynosi więcej korzyści niż potencjalnych szkód. W przypadku sztucznej inteligencji poziom akceptacji zależy od celu, do którego jest ona wykorzystywana. Jak się wskazuje, systemy AI mogą wywoływać niezamierzone szkody nawet wówczas, gdy korzysta się z nich w dobrej wierze[65]. Jednocześnie kontrowersje związane z ochroną prywatności i brakiem przejrzystości powodują, że brak uwzględnienia zagadnień etycznych może prowadzić do oporu we wdrażaniu tej technologii lub jej całkowitego odrzucenia[66]. Jako rozwiązanie proponuje się mocne osadzenie sztucznej inteligencji w wartościach akceptowanych społecznie, co spowoduje zwiększenie zaufania, a tym samym większą akceptację proponowanych rozwiązań[67].

Argument odnoszący się do konieczności zapewnienia zgodności z prawem ma swój wymiar normatywny, który jest związany ze spójnością systemu prawa w wymiarze wertykalnym i horyzontalnym, ale stoją za nim również argumenty aksjologiczne. W teorii prawa od dawna podkreśla się, że norma uzasadniona w ten sposób ma wyższy poziom akceptacji przez jej adresatów[68]. Trzeba zauważyć, że transformacja Europejskiej Wspólnoty Gospodarczej w Unię Europejską związana jest ze zmianą w rozumieniu roli tych organizacji. O ile początkowo koncentrowano się przede wszystkim na zagadnieniach związanych z funkcjonowaniem gospodarki, to od lat 90. XX wieku można zauważyć, że poza kwestiami czysto gospodarczymi przywołuje się równolegle pewne wartości, takie jak prawa człowieka[69]. Ich źródłem jest godność osobowa rozumiana jako przynależna człowiekowi z samego faktu bycia

---

64 G. Tassey, *Technology Life Cycles* [w:] *Encyclopedia of Creativity*, *Invention, Innovation and Entrepreneurship*, red. E.G. Carayannis, New York 2013.

65 Wytyczne w zakresie etyki…, *op. cit*., s. 2.

66 Problem ten nie dotyczy wyłącznie sztucznej inteligencji, ale nowych technologii w ogólności. Por. J. Greser, *Etyczne problemy wdrażania medycznego Internetu Rzeczy*, „Prawo Mediów Elektronicznych" 2020, nr 3, s. 4–11.

67 E. Glikson, A. Williams Woolley, *Human Trust in Artificial Intelligence: Review of Empirical Research.* „Annals" 2020, nr 14, s. 627–660.

68 Z. Ziembiński, *Normy tetyczne a normy aksjologiczne w koncepcji Cz. Znamierowskiego*, „Studia Filozoficzne" 1963, nr 2, s. 87–112.

69 Normatywnie ta zmiana uwidocznia się w uchwaleniu w 1997 roku traktatu amsterdamskiego, choć wprowadzany przez niego zakres zmian i sposób redakcji tekstu był przedmiotem krytyki. C.H.Church, D. Phinnemore, *„Znikający" Traktat Amsterdamski*, „Studia Europejskie" 1998, nr 2, s. 48–49.

istotą ludzką[70]. Z tego prawa wypływają szczegółowe uprawnienia, wśród których można wymienić poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, wolność wypowiedzi i informacji czy zakaz dyskryminacji. Wskazuje się, że takie rozumienie praw jednostki stanowi swoiste DNA Unii Europejskiej[71], co znalazło swój wymiar normatywny w art. 2 TUE i Karcie praw podstawowych[72]. Na tej podstawie należy stwierdzić, że wszelkie normy w zakresie sztucznej inteligencji muszą być zgodne z tymi regulacjami. Takie jest również rozumienie prawodawcy, który podkreślił znaczenie standardów w zakresie praw człowieka w motywie 13 i 28 preambuły do projektu rozporządzenia. Jednocześnie wskazuje się, że problematyka ta nie jest odzwierciedlona w projekcie aktu o sztucznej inteligencji w dostatecznym stopniu, co powinno zostać skorygowane w drodze dalszych prac legislacyjnych[73].

4. Akt o sztucznej inteligencji jako potencjalne narzędzie ochrony przed nadużyciami władz publicznych

4.1. Planowany zakres zastosowania aktu o sztucznej inteligencji

Projekt aktu o sztucznej inteligencji już w początkowych przepisach świadomie zawęża zakres podmiotowy swojego zastosowania w odniesieniu do niektórych przejawów sprawowania władzy publicznej, wskazując w treści art. 2, że rozporządzenie w ogóle nie będzie miało zastosowania do: (a) systemów sztucznej inteligencji opracowanych lub wykorzystywanych wyłącznie do celów wojskowych oraz do (b) organów publicznych w państwie trzecim i organizacji międzynarodowych, jeżeli organy te lub organizacje wykorzystywać będą systemy sztucznej inteligencji w ramach umów międzynarodowych w zakresie egzekwowania prawa i współpracy sądowej zawartych z Unią lub z jednym państwem członkowskim bądź ich większą liczbą. Oznacza to, że z zakresu zastosowania przyszłego rozporządzenia umyka rozbudowany wachlarz militarnego wykorzystania sztucznej inteligencji, w szczególności zaś stosowania broni autonomicznej[74].

---

70 M. Nowicki, *Co to są prawa człowieka?, Szkoła praw człowieka – teksty wykładów zeszyt 1*, Warszawa 1998, s. 10; M. Piechowiak, *Filozofia praw człowieka. Prawa człowieka w świetle ich międzynarodowej ochrony*, Lublin 1999.

71 Wytyczne w zakresie etyki..., *op. cit*., s. 47.

72 Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 202 z 2016 r., s. 391).

73 *EROD i EIOD o projekcie aktu w sprawie sztucznej inteligencji,* https://uodo.gov.pl/pl/138/2090 (dostęp: 15.03.2022).

74 Zob. więcej F. Morgan, B. Boudreaux, A.J. Lohn, M. Ashby, Ch. Curriden, K. Klima, D. Grossman, *Military applications of artificial intelligence: ethical concerns in an uncertain world*, Santa Monica 2020.

Jednocześnie rozporządzenie wprowadzi cezurę czasową swojego obowiązywania. Zasadniczo akt o sztucznej inteligencji ma być stosowany po upływie 2 lat od dnia jego wejścia w życie[75]. Dodatkowo, zgodnie z art. 83 projektu rozporządzenia, nie będzie ono miało zastosowania do systemów, które wprowadzono do obrotu lub oddano do użytku przed upływem 12 miesięcy od daty rozpoczęcia stosowania przepisów, o ile zostały wymienione w załączniku IX, który odnosi się do systemów informatycznych związanych z migracją i polityką wizową, o ile systemy te nie zostaną znacząco zmienione. Dotyczy to również systemów sztucznej inteligencji wysokiego ryzyka, chyba że po dacie rozpoczęcia stosowania rozporządzenia ich projekt lub przeznaczenie tych systemów ulegną znaczącym zmianom.

Ponadto nie są objęte zakresem normowania rozporządzenia przypadki wykorzystania AI przez państwa nieczłonkowskie i organizacje międzynarodowe w obszarze egzekwowania prawa i współpracy sądowej, pod warunkiem zawarcia umowy międzynarodowej z co najmniej jednym państwem członkowskim lub UE[76]. Jako że w przypadku niepublicznych zastosowań AI Komisja Europejska zdecydowała się na bardzo szeroki zakres zastosowania rozporządzenia, tj. taki, który obejmuje każdy przypadek wprowadzenia do obrotu lub oddania do użytku systemu sztucznej inteligencji na terytorium Unii Europejskiej, niezależnie od tego, czy dostawca systemu ma siedzibę w Unii, czy w państwie trzecim[77], a także przypadki systemów sztucznej inteligencji, których dostawcy, a nawet użytkownicy znajdują się poza terytorium Unii Europejskiej, o ile tylko wyniki działania systemu są wykorzystywane w Unii[78]. Widać więc, że w pozornie szczelnym fundamencie rozporządzenia, jakim jest szeroki zakres terytorialny i podmiotowy zastosowania, dokonywany jest istotny wyłom właśnie w odniesieniu do publicznego wykorzystania AI. Oznacza to, że w razie przyjęcia obecnego brzmienia projektu rozporządzenia w Unii Europejskiej nie będzie istniał równy standard ochrony przed publicznymi i niepublicznymi zastosowaniami sztucznej inteligencji. Przyznać jednocześnie należy, że dominująca część publicznego wykorzystywania narzędzi sztucznej inteligencji przez władze państwowe będzie jednak podlegać regulacji projektowanego rozporządzenia. Warto jednak zwrócić uwagę, czy odbywać się to będzie na tych samych zasadach, jakie dotyczą podmiotów komercyjnych.

---

75 Art. 85 ust. 2 projektu rozporządzenia.

76 Art. 2 ust. 4 projektu rozporządzenia.

77 Projektowany art. 2 ust. 1 lit. a rozporządzenia.

78 Projektowany art. 2 ust. 1 lit. c rozporządzenia.

4.2. Zakazane sposoby wykorzystania systemów AI

Jak wyjaśniono w uzasadnieniu projektu rozporządzenia, systemy sztucznej inteligencji stwarzające niedopuszczalne ryzyko podlegają całkowitemu zakazowi wprowadzania do obrotu, oddawania do użytku lub wykorzystywania[79]. Zostały one wskazane w art. 5 i obejmują m.in. zakaz wykorzystywania systemów sztucznej inteligencji przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, kiedy to punktowa ocena społeczna prowadzi do jednego lub obu następujących skutków:

(i) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup w kontekstach społecznych, które nie są związane z kontekstami, w których pierwotnie wygenerowano lub zgromadzono dane,

(ii) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi[80].

Zakaz powyższy obejmuje więc systemy social scoringu, pod warunkiem wypełnienia przesłanek „krzywdzącego lub niekorzystnego traktowania"[81]. Systemy punktowej oceny zachowań społecznych przekładające się na negatywne konsekwencje dla jednostki będą więc, w zależności od skali wpływu na prawa i interesy jednostek lub społeczeństwa, albo podlegać całkowitemu zakazowi wykorzystywania, albo będą traktowane jako systemy wysokiego ryzyka[82], rodząc skutki opisane w tytule III projektu rozporządzenia.

Drugim, równie istotnym z analizowanego punktu widzenia zakazem pozostaje ten określony w art. 5 ust. 1 lit. d. Przepis ten wprowadza zakaz wykorzystywania systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni

[79] Projekt wprowadza podział dopuszczalnych systemów AI w zależności od potencjalnego wpływu na wartości Unii Europejskiej wynikającego z zakresu ich stosowania. Podział ten jest trójstopniowy i obejmuje systemy AI, które: (a) stwarzają ryzyko niedopuszczalne, (b) stwarzają ryzyko wysokie oraz (c) stwarzają ryzyko niskie lub minimalne.

[80] Projektowany art. 5 ust. 1 lit. c aktu o sztucznej inteligencji.

[81] Na niewystarczającą jasność pojęć użytych do definiowania zakazanych działań zwracają uwagę Michael Veale i Frederik Zuiderveen Borgesius. Zob. M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach*, „Computer Law Review International" 2021, nr 4, s. 100.

[82] Naszym zdaniem w kategorii dokonywania „oceny lub wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie zachowania społecznego/cech osobistych lub cech charakteru" mieszą się m.in. systemy wysokiego ryzyka określone w pkt 3–7 załącznika III do projektu rozporządzenia.

publicznej do celów egzekwowania prawa[83], chyba że ma zastosowanie któryś z przewidzianych wyjątków[84]. Projekt rozporządzenia wprowadza dodatkowe ograniczenia korzystania z owych wyjątków:

a) wymóg analizy pod kątem „charakteru sytuacji powodującej konieczność ewentualnego wykorzystania systemu, w szczególności powagę, prawdopodobieństwo i skalę szkody wyrządzonej w przypadku niewykorzystania systemu" oraz „konsekwencji wykorzystania systemu dla praw i wolności wszystkich zainteresowanych osób, w szczególności wagę, prawdopodobieństwo i skalę tych konsekwencji"[85],
b) wymóg zachowania niezbędnych i proporcjonalnych zabezpieczeń (w tym ograniczeń czasowych, geograficznych i osobowych) przy korzystaniu z dopuszczalnego wyjątku oraz
c) wymóg uzyskania uprzedniego zezwolenia organu sądowego lub niezależnego organu administracyjnego[86].

Pomimo otwarcia przez Komisję Europejską i tak niemałej furtki do stosowania systemów zdalnej identyfikacji biometrycznej, w tym m.in. systemów rozpoznawania twarzy, przez władze publiczne, przepis projektowanego art. 5 wprowadza jeszcze dalej idący przypadek dopuszczalności wykorzystania automatycznej identyfikacji biometrycznej i to bez uprzedniej kontroli organu sądowego lub niezależnego organu administracyjnego. Mowa tutaj o „nagłym przypadku". W takiej sytuacji o zezwolenie występuje się w trakcie lub nawet dopiero po zakończeniu wykorzystywania systemu[87]. Ponieważ projekt rozporządzenia w żadnym ze swoich postanowień nie wymaga wyraźnie przejrzystości ani nawet umiaru w odniesieniu do liczby i rodzaju wydanych zezwoleń na zdalną identyfikację biometryczną, słusznie podnosi się, że projekt rozporządzenia bardziej legitymizuje niż zakazuje inwigilacji na skalę populacyjną[88].

---

[83] Zgodnie z art. 3 pkt 41 aktu o sztucznej inteligencji „egzekwowanie prawa" oznacza działania prowadzone przez organy ścigania w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub egzekwowania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

[84] Wyjątkami tymi są: poszukiwanie ofiar przestępstw (w tym potencjalnych ofiar), zapobiegnięcie zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu oraz wykrywanie, lokalizowanie, identyfikowanie lub ściganie sprawcy niektórych przestępstw lub podejrzanego o popełnienie niektórych przestępstw – zob. art. 5 ust. 1 lit. c pkt i–iii aktu o sztucznej inteligencji.

[85] Art. 5 ust. 1 ust. 2 lit. a i b aktu o sztucznej inteligencji.

[86] Art. 5 ust. 3 zdanie pierwsze aktu o sztucznej inteligencji.

[87] Art. 5 ust. 3 zdanie drugie aktu o sztucznej inteligencji.

[88] M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft..., op. cit.*, s. 102.

Równie ważne jest, że zakaz wprowadzony ewentualnie przez art. 5 ust. 1 lit. d aktu o sztucznej inteligencji w ogóle nie dotyczyłby systemów identyfikujących nie w czasie rzeczywistym (tj. dokonujących oceny *ex post*). Oznacza to, że analiza materiałów z kamer CCTV przez władze publiczne kilka dni po nagraniu nie byłaby *ipso iure* zakazana. Co więcej, zakaz z art. 5 ust. 1 lit. d obejmowałby jedynie wykorzystywanie systemów identyfikujących „w celach egzekwowania prawa". Jeżeli więc identyfikacja biometryczna miałaby dotyczyć działań wymykających się definicji z art. 3 pkt 41 projektu, na przykład dotyczyłaby kwestii zdrowia publicznego), byłaby ona dopuszczalna. Powyższe również skłania do wniosku, że wejście w życie przepisów aktu o sztucznej inteligencji nie ukróci funkcjonowania systemów rozpoznawania twarzy w Unii Europejskiej, dając pole do nadużyć dla władz o zapędach autorytarnych.

4.3. Systemy wysokiego ryzyka

Komisja Europejska zaproponowała, aby na drugim miejscu pod względem rygorystyczności regulacji traktować systemy sztucznej inteligencji wysokiego ryzyka, które definiowane są dwojako: spełniają kumulatywnie obydwie przesłanki wymienione w art. 6 ust. 1 projektu rozporządzenia[89] albo wymienione zostały w załączniku nr III do projektu rozporządzenia. Załącznik nr III wśród systemów wysokiego ryzyka wymienia m.in.:

- systemy zdalnej identyfikacji biometrycznej (dokonywanej przez jakikolwiek podmiot, nie tylko podmiot publiczny), zarówno w czasie rzeczywistym, jak i *post factum*,
- systemy podejmujące decyzje o dostępie do instytucji edukacyjnych lub w celu oceny uczniów,
- systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy publiczne (lub w imieniu organów publicznych) w celu oceny kwalifikowalności osób fizycznych do świadczeń i usług publicznych, jak również w celu przyznawania, ograniczania, unieważniania lub żądania zwrotu takich świadczeń i usług,

[89] Przesłanki te są następujące: a) system sztucznej inteligencji jest przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II lub sam jest takim produktem; b) produkt, którego związanym z bezpieczeństwem elementem jest system sztucznej inteligencji, lub sam system sztucznej inteligencji jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II – ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku.

- systemy sztucznej inteligencji przeznaczone do wykorzystania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb ratunkowych w sytuacjach kryzysowych, w tym straży pożarnej i pomocy medycznej,
- systemy wykorzystywane przez organy ścigania: w celu automatycznej oceny ryzyka recydywy, jak poligrafy i podobne narzędzia, lub w celu wykrywania stanu emocjonalnego osoby fizycznej, do wykrywania deepfake'ów, do oceny wiarygodności dowodów, w celu profilowania osób fizycznych lub grup, do przeszukiwania zbiorów danych w celu zidentyfikowania wcześniej nieznanych wzorców i zależności,
- systemy sztucznej inteligencji, które mają służyć organowi sądowemu pomocą w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego.

Unia Europejska, stosując podejście oparte na analizie ryzyka, chce dopuścić funkcjonowanie na rynku europejskim systemów wysokiego ryzyka tylko pod warunkiem spełnienia stosownych wymogów określonych szczegółowo w projekcie rozporządzenia oraz pod warunkiem przeprowadzenia oceny zgodności *ex ante*. Klasyfikacja systemu sztucznej inteligencji jako systemu wysokiego ryzyka opiera się na analizie jego przeznaczenia, a zatem jej wynik zależy nie tylko od rodzaju algorytmu używanego w systemie, ale także od konkretnego celu i trybu wykorzystania samego systemu. Oceniając, czy system sztucznej inteligencji stanowi system wysokiego ryzyka, pod uwagę wziąć należy – zgodnie z brzmieniem art. 7 ust. 2 projektu rozporządzenia – m.in. jego przeznaczenie oraz zakres, w jakim wykorzystywanie systemu miało już niekorzystny wpływ na prawa podstawowe lub wzbudziło istotne obawy co do możliwości wystąpienia niekorzystnego wpływu. Ponadto trzeba uwzględnić potencjalny zakres szkody lub niekorzystnego wpływu, w szczególności pod względem ich nasilenia i możliwości oddziaływania na wiele osób czy ewentualną podległość osób potencjalnie poszkodowanych przez działanie systemu AI względem podmiotu go stosującego. Nierówny układ sił pomiędzy obywatelem jako podmiotem, wobec którego stosowany jest publiczny system AI, a organami władzy państwowej go wykorzystującymi, jak również częsty brak możliwości rezygnacji z zastosowania wyniku działania systemu AI przez obywatela oraz możliwość masowego wykorzystywania systemu wobec osób fizycznych skłaniać będzie do dokonania oceny większości wykorzystywanych przez władze publiczne systemów AI właśnie jako systemów wysokiego ryzyka.

Z aprobatą należy odnieść się do faktu, że zasadniczo Komisja Europejska zaproponowała w projekcie rozporządzenia tożsamy zakres obowiązków dla publicznych i niepublicznych podmiotów stosujących systemy AI wysokiego ryzyka. Zgodnie bowiem z brzmieniem projektowanego art. 16 w zw. z art. 3 pkt 2

obowiązki dostawców systemów sztucznej inteligencji wysokiego ryzyka są identyczne niezależnie od tego, czy podmiotem opracowującym system sztucznej inteligencji lub zlecającym jego opracowanie w celu wprowadzenia go do obrotu lub oddania go do użytku jest osoba fizyczna lub prawna, czy organ publiczny[90]. Odmienności pojawiają się dopiero w tytule IV projektu aktu na temat „obowiązków w zakresie przejrzystości w odniesieniu do określonych systemów sztucznej inteligencji". Zgodnie z art. 52 projektu rozporządzenia dostawcy zapewniają, aby systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi, a więc nie tylko systemy wysokiego ryzyka, projektowano i opracowywano w taki sposób, aby osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem sztucznej inteligencji. Obowiązek ten nie ma jednak zastosowania do systemów sztucznej inteligencji zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia dochodzeń/śledztw w związku z przestępstwami i ścigania ich sprawców. Od powyższej zasady wprowadzony został tylko jeden wyjątek: obowiązek informowania o interakcji z systemem obowiązuje wtedy, gdy systemy ten udostępnia się ogółowi społeczeństwa na potrzeby składania zawiadomień o popełnieniu przestępstwa. Identyczny w treści wyjątek na korzyść nietransparentnego wykorzystania systemów AI przez władze publiczne przewidziano w art. 52 ust. 2 w odniesieniu do systemów rozpoznawania emocji oraz systemów kategoryzacji biometrycznej, a w art. 52 ust. 3 – do tzw. deepfake'ów, tj. systemów sztucznej inteligencji, które generują obrazy, treści dźwiękowe lub treści wideo, które łudząco przypominają istniejące osoby, obiekty, miejsca lub inne podmioty lub zdarzenia, lub które tymi obrazami i treściami manipulują, przez co osoba będąca ich odbiorcą mogłaby niesłusznie uznać je za autentyczne lub prawdziwe.

4.4. Piaskownice regulacyjne

Specjalnym rozwiązaniem przewidzianym w projekcie rozporządzenia są „piaskownice regulacyjne" (*regulatory sandboxes*)[91]. Mają one na celu stworzenie kontrolowanego środowiska do testowania innowacyjnych technologii przez ograniczony czas, pod ścisłym nadzorem regulacyjnym, przed ich wprowadzeniem do

[90] Należą do nich między innymi: ustanawianie systemu zarządzania ryzykiem, odpowiednie zarządzanie danymi treningowymi, sporządzenie dokumentacji technicznej, rejestrowanie działania systemu, zapewnienie przejrzystości działania, zagwarantowanie stosownego nadzoru ludzkiego, uwzględnienie wymogów dokładności, solidności i cyberbezpieczeństwa (zob. przepisy projektowanego rozdziału II „Wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka").

[91] Zob. art. 53 i n. projektu aktu o sztucznej inteligencji.

obrotu lub oddaniem do użytku. Przyszłe istnienie piaskownic regulacyjnych ma na celu wspieranie innowacji w zakresie sztucznej inteligencji poprzez ustanowienie szans na przeprowadzanie odważnych eksperymentów i testów na etapie rozwoju systemów sztucznej inteligencji oraz zwiększenie pola manewru dla innowatorów. Piaskownice będą mogły być tworzone jedynie przez organy państw członkowskich lub przez Europejskiego Inspektora Ochrony Danych. Wśród celów przetwarzania danych osobowych w piaskownicach regulacyjnych projekt rozporządzenia wymienia m.in. zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych, egzekwowanie sankcji karnych, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom (art. 54 ust. 1 lit. a pkt i) oraz bezpieczeństwo publiczne i zdrowie publiczne (art. 54 ust. 1 lit. a pkt ii).

Trzeba zauważyć, że działalność podmiotów zainteresowanych opracowywaniem, testowaniem i walidacją innowacyjnych systemów sztucznej inteligencji w ramach piaskownicy regulacyjnej pozostaje pod kontrolą, obejmującą zarówno zgodność z wymogami rozporządzenia, prawem unijnym i prawem krajowym państwa członkowskiego objętego nadzorem w ramach piaskownicy, jak i konieczność podporządkowywania się wytycznym organu tworzącego piaskownicę, tj. organu państwa członkowskiego lub państw członkowskich albo Europejskiego Inspektora Ochrony Danych. Żaden projektowany przepis rozporządzenia nie wyklucza z kręgu potencjalnych beneficjentów piaskownicy regulacyjnej władz państwa członkowskiego ani podmiotów prywatnych, które chciałyby stworzyć określony system AI właśnie na potrzeby władz publicznych.

Odnosząc się do ewentualnej relacji pomiędzy próbami autorytarnego wykorzystania AI przez władze publiczne a piaskownicami regulacyjnymi, w pierwszej kolejności wskazać należy, że z definicji piaskownice te są środowiskiem kontrolowanym. Efekty działania systemów w nich funkcjonujących nie powinny (w razie niepowodzenia) przenikać na zewnątrz. Działania podejmowane w ramach piaskownic obejmują bowiem aktywność przed wprowadzeniem systemów do obrotu lub oddaniem do użytku, tj. okres poprzedzający swobodne funkcjonowanie systemu na terytorium Unii Europejskiej. W zamierzeniu prawodawcy unijnego niedopuszczalna byłaby więc sytuacja, w której organ państwa członkowskiego doprowadziłby do stworzenia w ramach piaskownicy regulacyjnej systemu niebezpiecznego, a następnie wprowadziłby go do ogólnego obrotu lub użytku. Prawodawca unijny przewidział bowiem pewne mechanizmy mające zapobiegać wykorzystaniu instytucji piaskownic regulacyjnych do wdrażania projektów stwarzających ryzyko autorytarnego wykorzystania przez państwa członkowskie. W motywie 72 projektowanego rozporządzenia wskazuje się na konieczność

ustanowienia wspólnych unijnych przepisów regulujących uruchamianie piaskownic regulacyjnych oraz ramy współpracy między odpowiednimi organami uczestniczącymi w nadzorze nad nimi. Dodatkowe wymagania wprowadzono w odniesieniu do systemów, których funkcjonowanie miałoby wiązać się z przetwarzaniem danych osobowych[92], obejmujące m.in. udział organów ochrony danych w działalności w ramach piaskownicy regulacyjnej.

Warto również podkreślić, że funkcjonowanie piaskownic regulacyjnych nie stoi na przeszkodzie wykonywaniu uprawnień nadzorczych i stosowania środków naprawczych[93], w tym również w ramach kompetencji organów nadzorczych ochrony danych osobowych na podstawie RODO, obejmujących możliwość nakładania administracyjnych kar pieniężnych na podstawie art. 83 RODO. Pamiętać przy tym należy, że organ nadzorczy RODO powinien pozostawać – zgodnie z przepisami rozporządzenia – niezależny od pozostałych władz publicznych państwa członkowskiego, w tym również (przykładowo) od organu władzy wykonawczej, który budowałby system w ramach piaskownicy regulacyjnej lub na którego zlecenie by się to odbywało.

Wszyscy uczestnicy korzystający z piaskownicy regulacyjnej (niezależnie od tego, czy są podmiotem prywatnym, czy publicznym) powinni zapewnić odpowiednie zabezpieczenia w celu ograniczenia ryzyka dla bezpieczeństwa i praw podstawowych, jakie może powstać w trakcie opracowywania produktów oraz prowadzenia eksperymentów w ramach piaskownicy regulacyjnej. Wykrycie istotnych zagrożeń dla zdrowa i bezpieczeństwa oraz dla praw podstawowych na etapie opracowywania i testowania takich systemów powoduje konieczność natychmiastowego zaradzenia tym zagrożeniom, a w przypadku ich nieusunięcia skutkuje zawieszeniem procesu opracowywania i testowania systemu, dopóki wspomniane zagrożenia nie zostaną wyeliminowane.

Projektowane przepisy rozporządzenia w sprawie sztucznej inteligencji nie są więc pozbawione zabezpieczeń przed sytuacjami nadużywania piaskownic regulacyjnych przez władze publiczne. W razie próby stworzenia w ich ramach systemów służących autorytarnemu wykorzystaniu AI w grę wchodzi również ponoszenie bezpośredniej odpowiedzialności danego podmiotu korzystającego z piaskownicy. Zgodnie z projektowanym brzmieniem art. 53 ust. 4 rozporządzenia ponosi on odpowiedzialność za wszelkie szkody wyrządzone osobom trzecim w wyniku eksperymentów prowadzonych w piaskownicy.

[92] Zob. projektowany art. 53 ust. 2 rozporządzenia oraz motyw 72 preambuły rozporządzenia.
[93] Zob. projektowany art. 53 ust. 3 rozporządzenia.

4.5. Sankcje

Projekt rozporządzenia przewiduje na wypadek nieprzestrzegania przewidzianych w nim zakazów i nakazów system administracyjnych kar finansowych, do wysokości nawet 30 milionów euro za pojedyncze naruszenie. Przepisy projektu różnicują jednak zasadniczo sytuację podmiotów publicznych i prywatnych dopuszczających się naruszenia, ponieważ na podstawie art. 71 ust. 7 krajom członkowskim została przyznana kompetencja do określenia w prawie krajowym, czy, a jeżeli tak – to w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim. Jest więc całkowicie możliwa sytuacja, w której państwo członkowskie, uchwalając przepisy wykonawcze do przyszłego rozporządzenia, nie przewidzi w ogóle możliwości ukarania własnych organów za nieprawidłowe wykorzystywanie systemów AI, włącznie z naruszeniem zakazu stosowania systemów wymienionych w art. 5 projektu. Czyni to stosowanie wymogów rozporządzenia do publicznych systemów AI rozwiązaniem iluzorycznym, a w najlepszym razie opartym na dobrej woli decydentów publicznych krajów członkowskich.

5. Podsumowanie

Choć skuteczność projektowanych przez Komisję Europejską rozwiązań prawnych zawartych w akcie o sztucznej inteligencji będzie można empirycznie zweryfikować dopiero po kilku latach jego obowiązywania na rynku unijnym, już teraz możliwe jest postawienie tezy, że z dużym prawdopodobieństwem prawodawca europejski nie zdecyduje się na stworzenie równego systemu nakazów i obowiązków wobec publicznych i niepublicznych dostawców AI. W efekcie spodziewać się należy, że władze państwowe co najmniej niektórych krajów członkowskich nie będą narzucać sobie tego samego poziomu wymogów w zakresie zastosowań sztucznej inteligencji, jakim obciążeni zostaną inni uczestnicy rynku. Relacje państwo – obywatel w zakresie AI mogą więc znacząco różnić się od relacji horyzontalnych pomiędzy wszystkimi niepublicznymi uczestnikami jednolitego rynku. Może to prowadzić do znaczącego odejścia od wyznaczonego przez akt o sztucznej inteligencji standardu postępowania z systemami AI. Przyczyną tego stanu rzeczy są:

1) stworzenie wielu wyjątków od planowanych regulacji (w tym zakazów z art. 5 projektu) na korzyść władz państwowych, w tym w szczególności w zakresie działań karno-policyjnych,
2) oparcie systemu sankcji pieniężnych dla podmiotów publicznych nieprzestrzegających wymogów rozporządzenia jedynie na dobrowolności (rozumianej jako krajowa swoboda ustawodawcza).

Biorąc więc pod uwagę szczególne cechy sztucznej inteligencji (takie jak na przykład efekt czarnej skrzynki, złożoność, zależność od jakości danych, zdolność do autonomicznych zachowań), udzielenie odpowiedzi na postawione w artykule pytanie badawcze brzmi: projektowana regulacja unijna aktu o sztucznej inteligencji nie kształtuje ram prawnych w sposób pewny przeciwdziałających potencjalnemu autorytarnego wykorzystaniu AI przez władze państwowe krajów członkowskich, w efekcie w sposób niewystarczający chroniąc obywateli UE przed pojawiającym się w tym zakresie ryzykiem.

Choć przyszła regulacja rozporządzenia tworzyć będzie prawdopodobnie pierwsze na świecie tak kompleksowe ramy prawne funkcjonowania sztucznej inteligencji w życiu osób fizycznych, dalece ryzykowne byłoby stawianie tezy, że będzie ona sama w sobie wystarczająco skutecznym narzędziem ochrony przez niedopuszczalnymi praktykami obejmującymi zautomatyzowaną kontrolę nad życiem społeczeństwa i jednostki czy istotną ingerencję w prywatność, życie osobiste, dostępność usług publicznych itd.[94]

Efektem tego stanu rzeczy będzie konieczność dalszego odwoływania się – w przypadkach ewentualnych naruszeń po stronie władz publicznych – do regulacji wynikających z systemu ochrony praw człowieka. Jak wskazano, nie jawią się one jako wystarczająco efektywne narzędzie ochrony interesów osób fizycznych w obliczu rozwoju sztucznej inteligencji. I choć podstawą unijnego podejścia do tego zagadnienia pozostaje perspektywa praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej, okazać się może, że ochrona ta będzie niedostateczna w przypadku prób przeciwdziałania autorytarnemu stosowaniu AI przez władze publiczne. Za często podkreślanym przesłaniem, że europejskie podejście do sztucznej inteligencji charakteryzuje się wdrażaniem odpowiednich zabezpieczeń w celu poszanowania podstawowych praw i wolności, rozwojem godnej zaufania i bezpiecznej sztucznej inteligencji oraz respektowaniem wartości leżących u podstaw Unii Europejskiej, w tym również zasad praworządności, nie poszło dotychczas stworzenie odpowiednich narzędzi prawnych zapewniających realizację wymienionych wyżej wartości i praw.

[94] Wśród zagrożonych rozwojem technologicznym w obszarze sztucznej inteligencji praw i wolności w literaturze przedmiotu wymienia się również m.in. wolność słowa czy prawa wyborcze – A. Podolska, Ł. Rąb, *(Re)wizja praw człowieka w dobie rozwoju nowych technologii. Między indywidualizmem a kolektywizmem* [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2021, s. 365.

Streszczenie

Sztuczna inteligencja należy do najdynamiczniej rozwijających się współcześnie technologii. Jest coraz szerzej wykorzystywana zarówno przez władze publiczne, jak i w zastosowaniach biznesowych w obszarze służby zdrowia, edukacji czy bezpieczeństwa. Budzi to obawy dotyczące możliwości występowania nadużyć lub naruszeń praw jednostki, tym bardziej że technologia ta nie podlega w obecnej chwili regulacjom. Problem zauważono w Unii Europejskiej i próbą odpowiedzi na niego jest projekt aktu o sztucznej inteligencji. W artykule odpowiadamy na pytanie, w jaki sposób projektowana regulacja unijna w zakresie sztucznej inteligencji kształtuje ramy prawne dla przeciwdziałania potencjalnemu autorytarnemu wykorzystywaniu AI przez władze państwowe krajów członkowskich. Wskazujemy możliwości potencjalnych naruszeń na przykładzie systemów służących ustalaniu tożsamości jednostek i analizie predykcyjnej ich zachowań. Ponadto opisujemy aksjologię regulacji, jej planowany zakres podmiotowy i przedmiotowy oraz przewidywane sankcje.

Słowa kluczowe: sztuczna inteligencja, AI Act, prawa podstawowe, prawa człowieka

EU Artificial Intelligence Act versus Authoritarian Tendencies in using AI by Public Authorities
Abstract

AI is one of the most dynamically developing technologies of today. It is increasingly more widely used both by public authorities and in business applications in the areas of health, education and security. This raises concerns about the possible abuses or violations of fundamental rights, especially as this technology is currently not regulated by law. The problem has been noted in the European Union and the draft of the Artificial Intelligence Act is an attempt to address it. This article poses a question how the proposed EU regulation establishes the legal framework to counteract potential authoritarian use of AI by Member State authorities. It identifies potential misuses by providing the examples of AI systems for identifying individuals and analysing predictive behaviour patterns. In addition, we describe the axiology of the regulation, its planned personal and material scope and the sanctions provided.

Key words: Artificial Intelligence, AI Act, fundamental rights, human rights