REDAKCJA
AGNIESZKA FORTUNA
MARTYNA CZAPSKA

PRAWO PRZYSZŁOŚCI I PRZYSZŁOŚĆ PRAWA

JAK POGODZIĆ PRAWO I NOWE TECHNOLOGIE?

ARCHAEGRAPH
Wydawnictwo Naukowe

Prawo przyszłości i przyszłość prawa.
Jak pogodzić prawo i nowe technologie?

Redakcja

Agnieszka Fortuna
Martyna Czapska

REDAKCJA
AGNIESZKA FORTUNA
MARTYNA CZAPSKA

PRAWO PRZYSZŁOŚCI I PRZYSZŁOŚĆ PRAWA

JAK POGODZIĆ PRAWO I NOWE TECHNOLOGIE?

ARCHAEGRAPH
Wydawnictwo Naukowe

PARTNER
Baker McKenzie.

Redakcja
Agnieszka Fortuna
Martyna Czapska

Recenzja
dr hab. Ewa Galewska, prof. UWr
dr hab. Bogdan Fischer, prof. UP

Korekta redaktorska i skład
Karol Łukomiak

Projekt Okładki
Karol Łukomiak

ISBN: 978-83-67527-55-2

Wersja elektroniczna dostępna na stronie internetowej wydawcy:

www.archaegraph.pl

Główny Partner Monografii:

Kancelaria Baker McKenzie

ARCHAEGRAPH
Wydawnictwo Naukowe

ŁÓDŹ, KWIECIEŃ 2023

SPIS TREŚCI

MARTYNA CZAPSKA

PRAWO NOWYCH TECHNOLOGII - CZY TO MA SENS?

WSTĘP

Prawo nie nadąża za technologią. To fakt podkreślany często przez media[1]. Bardzo możliwe, że nigdy się to nie zmieni. Procesy legislacyjne trwają długo i są obwarowane licznymi krokami, obowiązkami, obostrzeniami, podczas gdy proces rozwoju technologicznego jest wolny od takich ograniczeń. Pomimo tego, dyskusja dotycząca prawnych aspektów różnego rodzaju technologii trwa i nie widać, żeby miała się w najbliższym czasie zakończyć. Bo czy przewidujemy zakończenie rozwoju technologii? Oczywiście nie, a prawo jako nauka społeczna, opisuje znaną nam rzeczywistość. Jeśli ona się zmienia, prawo powinno na to odpowiedzieć, a nie stanie się to inaczej niż poprzez osoby uprawiające tę dyscyplinę i poprzez procesy legislacyjne.

Technologii i zjawisk z nimi związanych, które wpływają lub potencjalnie mogą wpłynąć na krajobraz prawny jest wiele. W niniejszych rozważaniach skupiam się na jednej z nich, budzącej być może najwięcej emocji: sztucznej inteligencji[2].

---

[1] Kilka przykładów z ostatnich lat, tylko z polskich mediów: M. Bellon, *Potrafimy „wskrzeszać" aktorów, tymczasem prawo nie nadąża za technologią [WYWIAD]*, 15.04.2019, https://businessinsider.com.pl/technologie/prawo-a-rozwoj-technologii-czy-prawo-nadaza/5srtlnn, (dostęp: 20.02.2023); *Raport: prawo nie nadąża za rozwojem nowych technologii*, 24.06.2020, https://www.rp.pl/prawo-w-firmie/art8899381-raport-prawo-nie-nadaza-za-rozwojem-nowych-technologii, (dostęp: 20.02.2023); Ł. Kotkowski, *Prawo wciąż nie nadąża za nowymi technologiami. W tych obszarach pilnie potrzebujemy zmian*, 27.06.2022, https://spidersweb.pl/2022/06/prawo-nowe-technologie-2022.html, (dostęp: 20.02.2023)

[2] Dalej także jako „AI". Celowo nie wdaję się tutaj w kwestie definicyjne AI. Posługuję się przykładem tej technologii wyłącznie w celu zobrazowania generalnego zjawiska i odnalezienia odpowiedzi na pytanie, czy dziedzina taka jak prawo nowych technologii ma sens, biorąc pod uwagę rozdźwięk pomiędzy szybkością rozwoju technologicznego, a szybkością - czy też jej brakiem - w przypadku procesów legislacyjnych.

Intensywny rozwój sztucznej inteligencji trwa już od kilku lat, zwiększa się też stopień wykorzystania AI przez przedsiębiorców[3]. Wśród prognoz dotyczących AI w najbliższym czasie wymienia się między innymi następujące obszary i technologie, na które warto zwrócić szczególną uwagę: rozpoznawanie twarzy[4], opieka zdrowotna[5], prawa własności intelektualnej[6] czy ChatGPT[7]. Ta ostatnia technologia stała się przyczynkiem do napisania niniejszych rozważań.

CHATGPT, CZYLI KASANDRA PRZEMÓWIŁA

Jednym z najgłośniejszych, jeśli nie najgłośniejszym wydarzeniem w świecie sztucznej inteligencji, które odbiło się szerokim echem na całym świecie i we wszystkich środowiskach, nie tylko prawniczym czy informatycznym, była premiera ChatGPT. ChatGPT to chatbot, czyli program komputerowy służący do prowadzenia rozmowy, gdzie jednym z rozmówców jest program (komputer) a drugim - człowiek. Jak podają twórcy, ChatGPT jest nie tylko zdolny do prowadzenia rozmowy, ale też odpowiada na szczegółowe pytania, przyznaje się do błędów, kwestionuje błędne informacje czy odmawia udzielania odpowiedzi na „niestosowne" pytania[8]. Sposób działania i wytrenowania ChatGPT został dosyć szczegółowo opisany przez jego twórców[9]. W szkoleniu uczestniczyli ludzie - trenerzy sztucznej inteligencji, którzy na przykład tworzyli konwersacje, działając zarówno w imieniu człowieka, jak i AI[10].

Same chatboty istnieją na rynku już od dłuższego czasu, ale ChatGPT stał się popularny, mówiąc najprościej, z powodu swoich umiejętności - potrafi tworzyć złożone teksty, mniej lub bardziej poprawne, na zadany temat. Dla hasła „prawo a AI" ChatGPT pisze między innymi: „Prawo a sztuczna inteligencja to tematyka związana z zagadnieniami prawno-etycznymi dotyczącymi rozwoju i zastosowania sztucznej inteligencji (AI) w różnych dziedzinach

[3] Por. np. raport McKinsey & Company *The state of AI in 2022*, 6.12.2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review#/ (dostęp: 12.02.2023), z którego wynika przykładowo, że liczba przedsiębiorstw, które wdrożyły AI (w ten czy inny sposób) zwiększyła się ponad 2,5 razy w stosunku do poprzedniego badania.
[4] *AI in 2023: Key trends and developments*, 20.01.2023, https://www.dentons.com/en/insights/articles/2023/january/20/ai-in-2023-key-trends-and-developments, (dostęp: 12.02.2023).
[5] *Ibidem.*
[6] *Ibidem.*
[7] *AI Stocks To Watch in 2023,* 9.02.2023, https://www.dentons.com/en/insights/articles/2023/january/20/ai-in-2023-key-trends-and-developments, (dostęp: 12.2.2023),
[8] Por. opis na stronie projektu: https://openai.com/blog/chatgpt/, (dostęp: 15.02.2023).
[9] *Ibidem.*
[10] *Ibidem.*

życia, takich jak medycyna, przemysł, finanse, transport czy administracja publiczna. Wraz z postępem technologicznym i zwiększającym się wykorzystaniem sztucznej inteligencji, pojawiają się coraz większe wyzwania związane z ochroną prywatności, odpowiedzialnością za decyzje podejmowane przez algorytmy, a także z zapewnieniem bezpieczeństwa danych. Prawo a AI obejmuje m.in. kwestie dotyczące odpowiedzialności za szkody wyrządzone przez sztuczną inteligencję, zasad związanych z ochroną prywatności i ochroną danych osobowych, a także etyczne aspekty wykorzystania sztucznej inteligencji, takie jak dyskryminacja czy nierówności społeczne."

Jak widać, w odpowiedzi na proste zapytanie powstał dłuższy, logiczny i całkiem poprawny językowo tekst. Daje to szereg możliwości wykorzystania tej technologii, a nawet można powiedzieć, że pod pewnymi względami jest to kusząca perspektywa. I tak, od daty wydania ChatGPT (30.11.2022)[11] pojawiają się kolejne doniesienia o sposobach, na jakie można go wykorzystać. Te wiadomości mogą budzić skrajne emocje. ChatGPT „zda" między innymi egzamin lekarski w USA (UMSLE - United States Medical Licensing Exam)[12], „został" wybrany prezesem, który ma nadzorować codzienne operacje indyjskiego przedsiębiorstwa CS India[13] czy też „stawia" pierwsze kroki w odrabianiu prac domowych i pisaniu prac naukowych w sposób, który trudno odróżnić od tekstu napisanego ludzką ręką[14].

Naturalnie, nasza dziedzina nauki, prawo, również nie jest wolna od eksperymentów z ChatGPT i od czasu do czasu można przeczytać, że sztuczna inteligencja zdaje egzaminy prawnicze[15] , a ton tych doniesień bywa mocno

---

[11] https://openai.com/blog/chatgpt/, (dostęp: 17.02.2023).

[12] T. Hung, M. Cheatham, A. Medenilla, i in. *Performance of ChatGPT on USMLE: Potential for AI-assisted medical education using large language models*, PLOS Digital Health, 9.02.2023, https://doi.org/10.1371/journal.pdig.0000198, (dostęp: 17.02.2023). Autorzy badania określili ChatGPT „krokiem milowym" w rozwoju AI, jeśli chodzi o określone zastosowania w medycynie.

[13] *Nie lubisz swojego szefa? Spokojnie, zastąpi go ChatGPT. W Indiach już to robi,* 11.02.2023, https://geekweek.interia.pl/technologia/news-nie-lubisz-swojego-szefa-spokojnie-zastapi-go-chatgpt-w-indi,nId,6591483

[14] N. Frątczak, *ChatGPT odrabia lekcje, pisze magisterki, zwodzi nauczycieli. Wykończy szkołę?*, https://www.polityka.pl/tygodnikpolityka/spoleczenstwo/2201332,1,chatgpt-odrabia-lekcje--pisze-magisterki-zwodzi-nauczycieli-wykonczy-szkole.read, (dostęp: 17.02.2023).

[15] Por. np.: *Sztuczna inteligencja zdała egzaminy prawnicze i biznesowe na uczelniach. Popełniła też "zaskakujące błędy"*, 27.01.2023, https://tvn24.pl/biznes/tech/usa-sztuczna-inteligencja-zdala-egzaminy-prawnicze-i-biznesowe-na-uczelniach-6683939, (dostęp: 20.02.2023); *Sztuczna inteligencja zdaje egzaminy na uczelniach. ChatGPT zniszczy edukację?*, (dostp: 28.01.2023), https://cyfrowa.rp.pl/technologie/art37857871-sztuczna-inteligencja-zdaje-egzaminy-na -uczelniach-chatgpt-zniszczy-edukacje, dostęp: 20.02.2023; *ChatGPT idzie na studia? Zdał egzaminy do szkół prawniczych!*, 27.01.2023, https://geekweek.interia.pl/technologia/news-chatgpt -idzie-na-studia-zdal-egzaminy-do-szkol-prawniczych,nId,6560702, (dostęp: 20.01.2023).

alarmujący (bo zapewne AI wkrótce zastąpi prawników). Docierając do opisu przeprowadzonego eksperymentu (w warunkach amerykańskich) można przekonać się, że sztuczna inteligencja była w stanie uzyskać - w części polegającej na teście wielokrotnego wyboru - wyniki powyżej progu zdawalności, podczas gdy w innych się to nie udało[16].

CZY WARTO ZAJMOWAĆ SIĘ ASPEKTAMI PRAWNYMI OWYCH TECHNOLOGII - OTO JEST PYTANIE

Powrócę teraz do pytania, które postawiłam na samym początku, już w tytule tego tekstu. Czy dziedzina taka, jak prawo nowych technologii, ma w ogóle sens w świetle powyższego? Czy wydanie niniejszej monografii miało sens?

Prawo towarzyszy ludzkości od zawsze. Jednym z przykładów, istniejącym w powszechnej świadomości, jest Kodeks Hammurabiego pochodzącego z ok. XVII wieku p. n. e.[17], który wcale nie jest najstarszym źródłem prawa (inne odkryte spisy praw pochodzą np. z ok. 2400 r. p. n. e., jak np. kodeks Urukaginy, władcy Lagaszu[18]). Mówiąc w uproszczeniu: tam, gdzie jest społeczeństwo, prędzej czy później pojawią się pewne reguły dotyczące życia w nim co z kolei prowadzi do powstania prawa.

Co do technologii, posłużę się przykładem obszaru szeroko rozumianego prawa autorskiego, które jest mi najbliższe: w przypadku tej dziedziny prawa, można powiedzieć, że wynalazek druku (który utożsamiam na potrzeby wywodu z wydrukowaniem Biblii Gutenberga w latach 1452-1455) był przyczynkiem, a nawet kamieniem milowym w jej rozwoju. Nie trzeba było już przepisywać dzieł literackich, wystarczyło je skopiować. Nastała inna skala dystrybucji, zmienił się układ sił i możliwe zyski. Pojawiły się przywileje drukarskie, dając początek prawu autorskiemu[19], a w 1710 r. w Anglii wszedł w życie Statut Anny (znany też jako Statut Królowej Anny), o pełnym tytule: *An Act for the Encouragement of learning, by vesting the copies of printed books in the authors or purchaser or purchasers of such copies, during the times therein mentioned*, uznawany często za pierwszą ustawę prawnoautorską[20]. Jan Gutenberg wynalazł druk (użył ruchomej czcionki) w XV wieku, Statut Anny wszedł

[16] M. J. Bommarito, D. M. Katz, *GPT takes the Bar exam, 29.12.2022,* https://ssrn.com/abstract=4314839, (dostęp: 20.02.2023).
[17] M. Sczaniecki, oprac. K. Sójka-Zielińska, *Powszechna historia państwa prawa*, 2009, s. 34
[18] *Ibidem.*
[19] J. Barta, R. Markiewicz, *Prawo autorskie,* 21023, s. 18.
[20] *Ibidem.*

w życie ponad 250 lat później. Byłoby nieodpowiedzeniem gdyby stwierdzić, że nie stało się to od razu.

ODPOWIADAJĄC NA PYTANIE: TAK, WARTO

Statut Anny nie był natychmiastową (ani nawet bardzo szybką) konsekwencją wynalazku druku i jego upowszechnienia. Mimo to został jedną z podwalin prawa autorskiego, które towarzyszy nam do dzisiaj i którego rola wydaje się wręcz rosnąć, biorąc pod uwagę, że z rozwojem technologii wiąże się wytwarzanie różnego rodzaju przedmiotów własności intelektualnej.

Muszę jednak przyznać, że technologia rozwija się obecnie wielokrotnie szybciej niż kiedykolwiek, w tym w czasach Gutenberga i później. Nie sądzę, żeby można było porównywać szybkość rozwoju czcionek ruchomych wykorzystywanych w druku w czasach sprzed Statutu Anny do rozwoju technologii obecnie. Z pewnością odnalezienie się w nowej rzeczywistości z prawnego punktu widzenia jest ogromnym wyzwaniem. Czy prawo zacznie nadążać za rozwojem technologii w przewidywanym czasie? Nie sądzę, aby tak się stało.

Jednocześnie jednak prawo nie zniknie i w moim przekonaniu zawsze będzie towarzyszyć poszczególnym społeczeństwom, mniej lub bardziej nadążając za rzeczywistością. Rolą między innymi prawników jest badanie, interpretowanie, a w razie potrzeby - tworzenie prawa, które pozwoli regulować stosunki społeczne - w tym te związane z technologią - w sposób możliwie korzystny dla różnych graczy. Brzmi utopijnie, ale nie znaczy to, że nie mamy próbować dążyć do stanu optymalnego.

I dlatego moja odpowiedź na pytanie postawione w tytule niniejszych rozważań brzmi: tak, oczywiście. Dlatego z ogromną przyjemnością uczestniczyłam w pracach nad niniejszą monografią. Stanowi istotny wkład w dyskusję o prawnych aspektach nowych technologii. Zachęcam do uczestniczenia w tej dyskusji i zachęcam do lektury, która - jestem pewna - będzie interesująca dla Czytelnika.

CZĘŚĆ I.
OBRÓT CYWILNOPRAWNY

WIKTOR GAWŁOWICZ
UNIWERSYTET ŚLĄSKI W KATOWICACH

PODATKOWA KWALIFIKACJA EFEKTÓW PRACY TWÓRCZEJ SZTUCZNEJ INTELIGENCJ*I*

Abstrakt: Praca ma na celu właściwe przyporządkowanie efektów „pracy twórczej" sztucznej inteligencji do określonych pojęć występujących na gruncie prawa podatków dochodowych. Koncentruje się w tym zakresie na uldze badawczo-rozwojowej (ulga B+R) oraz 50% kosztach uzyskania przychodu z pracy twórczej (KUP 50%). Istotny element stanowi rozróżnienie sytuacji prawnej autora programu komputerowego od sytuacji prawnej badacza wykorzystującego program komputerowy w ramach działalności badawczo-rozwojowej. Praca przedstawia ogólne zasady rządzące ulgą B+R oraz KUP50%, zauważając znaczenie pojęć takich jak działalność twórcza i korzystanie przez twórców z praw autorskich, w perspektywie odpowiadających im pojęć na gruncie prawa autorskiego. Przedstawione konkluzje odnoszą się do możliwości uznania sztucznej inteligencji za koszt kwalifikowany ulgi B+R oraz możliwości uznania pracownika wykorzystującego sztuczną inteligencję za twórcę korzystającego z praw autorskich w rozumieniu KUP50%. Z punktu widzenia braku regulacji szczegółowej na gruncie prawa podatków dochodowych, konieczne jest dokładne opisanie określonych kwestii w umowie pomiędzy twórcą programu komputerowego oraz twórcą utworu powstającego z wykorzystaniem sztucznej inteligencji.

Słowa kluczowe: sztuczna inteligencja, , SI, działalność badawczo-rozwojowa, B+R, badania i rozwój, praca twórcza.

1. WSTĘP

Praca ma na celu rozważenie możliwości zastosowania preferencji podatkowych wskazanych w art. 4a pkt. 26, art 18d ustawy z dnia 15 lutego 1992 r.

o podatku dochodowym od osób prawnych[1] (dalej jako „CIT") oraz art. 5a pkt. 38, art. 26e, art. 22 ust. 9 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych[2] (dalej jako „PIT"), dotyczących więc ulgi z tytułu prowadzenia prac badawczo-rozwojowych (dalej jako: „ulga B+R") oraz 50% kosztów uzyskania przychodu z pracy twórczej (dalej jako „KUP 50%") do „działalności twórczej" sztucznej inteligencji. W sposób kolejny podejmując więc rozważania na temat samej ulgi B+R, uznawania sztucznej inteligencji za koszt kwalifikowany ulgi B+R, następnie KUP50%, uznawania pracownika za autora „pracy twórczej" sztucznej inteligencji, wreszcie problematyki korzystania przez twórców z praw autorskich do rezultatu „pracy twórczej" sztucznej inteligencji w rozumieniu KUP50%. Praca obejmuje stan prawny na dzień 30 grudnia 2021 roku, mając na względzie również przywołaną literaturę.

W tym celu, w pierwszej kolejności zauważyć należy czym jest sztuczna inteligencja. Algorytmy uczenia maszynowego albo szerzej sztuczna inteligencja będąca programem komputerowym korzystającym z tych algorytmów, bywa definiowana jako system, który pozwala na wykonywanie zadań wymagających procesu uczenia się i uwzględniania nowych okoliczności w toku rozwiązywania danego problemu i który może w różnym stopniu w zależności od konfiguracji – działać autonomicznie oraz wchodzić w interakcję z otoczeniem[3], jest efektem pracy człowieka. Wniosek ten prowadzi do konkluzji, że autor programu komputerowego w odniesieniu do komercjalizacji rozumianej jako wprowadzanie nowych produktów lub usług na rynek[4], jest podatnikiem podatków dochodowych tj. podlega obowiązkowi podatkowemu w odniesieniu do dochodów uzyskiwanych z komercjalizacji. Jest to jednak wniosek niepełny, ponieważ nie zawsze autor będzie w istocie tym podmiotem, który dany program komputerowy będzie komercjalizował.

Zgodnie ze stanowiskiem specjalnej komisji przy organach UE sztuczna inteligencja rozumiana jako systemy, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów[5] jest zdolna do samodzielnego gromadzenia i analizowania danych, a następnie wyciągania

[1] Dz. U. z 2021 r. poz. 1800 ze zm.
[2] Dz. U. z 2021 r. poz. 1128 ze zm.
[3] T. Zalewski, *Definicja sztucznej inteligencji* [w:] *Prawo Sztucznej Inteligencji*, Red. L. Lei, M. Świerczyński, Warszawa, 2020, s. 5.
[4] https://www.investopedia.com/terms/c/commercialization.asp, [dostęp: 21.05.2022].
[5] T. Zalewski, *Definicja sztucznej inteligencji* [w:] *Prawo Sztucznej Inteligencji*, Red. L. Lei, M. Świerczyński, Warszawa, 2020, s. 7.

z nich wniosków. „Praca" którą wykonuje sztuczna inteligencja, jest więc „pracą twórczą", prowadzącą do powstania nowej wiedzy o obserwowalnych zjawiskach. Wynika to z definicji pojęcia „działalność twórcza" występującej na gruncie prawa autorskiego. A. Michalak wskazuje, że uznanie danego rezultatu działalności człowieka za utwór możliwe jest tylko w przypadku spełnienia przez ów rezultat przesłanki twórczości, na którą składa się oryginalność (przejaw działalności twórczej) i indywidualność (indywidualny charakter tej działalności)[6].

Zgodnie z art. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[7] (dalej jako: „ustawa o prawie autorskim") przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór). Zgodnie zaś z art. 8 ustawy o prawie autorskim, prawo autorskie przysługuje twórcy, o ile ustawa nie stanowi inaczej. Domniemywa się, że twórcą jest osoba, której nazwisko w tym charakterze uwidoczniono na egzemplarzach utworu lub której autorstwo podano do publicznej wiadomości w jakikolwiek inny sposób w związku z rozpowszechnianiem utworu.

W procesie wykładni wskazanych przepisów konieczne jest rozróżnienie znaczenia określonych pojęć, zauważając, że za „przejaw działalności twórczej" uznać możemy ujawnienie wytworu umysłowości twórcy[8]. Za „indywidualny charakter" uznać możemy wytwór ludzkiego umysłu, który charakteryzuje się indywidualnością płynącą z osobowości twórcy[9]. Za „ustalenie w jakiejkolwiek postaci" uznać możemy uzewnętrznienie, nadające jakąś postać, możliwą do percepcji przez kogokolwiek poza twórcą[10]. „Niezależność od wartości, przeznaczenia i sposobu wyrażenia" to uniezależnienie istnienia utworu od jego wartości, przeznaczenia i sposobu wyrażenia. Zgodnie zaś z domniemaniem wyrażonym w art. 8 ustawy o prawie autorskim twórcą jest osoba, w nim wskazana, jeśli nie doszło do obalenia domniemania.

---

[6] A. Michalak, *art. 1* [w:] *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Red. A. Michalak, Warszawa, 2019, Legalis. https://sip.legalis.pl/document view.seam?documentId=mjxw62zogi3damrtgm4tmojoobqxalruhe3dcmzrgqza&refSource=guide1#tabs-metrical--info [dostęp: 22.05.2022].

[7] Dz.U. Nr 24, poz. 83

[8] E. Ferenc-Szydełko, *art. 1* [w:] *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Red. E. Ferenc-Szydełko, Warszawa, 2021, Legalis, https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damzqgy3tomroobqxalruhe3dcmzrgqza&refSource=guide1 [dostęp: 22.05.2022].

[9] Ibidem.

[10] Ibidem.

Utwór i autor w niniejszej pracy, oznaczają „utwór" w rozumieniu ustawy o prawie autorskim oraz „autora" rozumianego jako twórca w rozumieniu ustawy o prawie autorskim.

2. WPROWADZENIE DO ULGI BADAWCZO-ROZWOJOWEJ

Na gruncie CIT, zgodnie z art. 18d podatnik uzyskujący przychody inne niż przychody z zysków kapitałowych odlicza od podstawy opodatkowania ustalonej zgodnie z art. 18, koszty uzyskania przychodów poniesione na działalność badawczo-rozwojową, zwane dalej „kosztami kwalifikowanymi" (…)". Zgodnie z art. 4a ust. 1 pkt. 26 działalność badawczo-rozwojowa – oznacza działalność twórczą obejmującą badania naukowe lub prace rozwojowe, podejmowane w sposób systematyczny w celu zwiększenia zasobów wiedzy oraz wykorzystywania zasobów wiedzy do tworzenia nowych zastosowań". W zakresie definiowania badań naukowych i prac rozwojowych art. 4a ust. 1 pkt. 27 i 28 CIT odsyła do art. 4 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce[11] (dalej jako „ustawa prawo o szkolnictwie wyższym" lub „p.s.w.n."). Zgodnie z definicjami art. 4 ustawy prawo o szkolnictwie wyższym m.in.:

- badania aplikacyjne - prace mające na celu zdobycie nowej wiedzy oraz umiejętności, nastawione na opracowywanie nowych produktów, procesów lub usług lub wprowadzanie do nich znaczących ulepszeń;
- prace rozwojowe - działalnością obejmującą nabywanie, łączenie, kształtowanie i wykorzystywanie dostępnej aktualnie wiedzy i umiejętności, w tym w zakresie narzędzi informatycznych lub oprogramowania, do planowania produkcji oraz projektowania i tworzenia zmienionych, ulepszonych lub nowych produktów, procesów lub usług, z wyłączeniem działalności obejmującej rutynowe i okresowe zmiany wprowadzane do nich, nawet jeżeli takie zmiany mają charakter ulepszeń.

Wskazując na pracę Jakuba Jankowskiego pt. Ulgi w CIT z tytułu działalności innowacyjnej i inwestycyjnej[12], działalność B+R to działalność obejmująca badania naukowe lub prace rozwojowe, podejmowane w sposób

[11] Dz.U. z 2021 r. poz. 478 ze zm.
[12] J.Jankowski, *Ulgi w CIT z tytułu działalności innowacyjnej i inwestycyjnej*, Warszawa, 2020, Legalis, https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damrugyzdqmy [dostęp: 22.05.2022].

systematyczny w celu zwiększenia zasobów wiedzy oraz wykorzystania zasobów wiedzy do tworzenia nowych zastosowań[13]. Z powyższej definicji wynika, że działalność B+R musi mieć charakter twórczy, czyli tworzyć nowe i oryginalne rozwiązania, twórczość może przejawiać się opracowywaniem nowych koncepcji, narzędzi, rozwiązań niewystępujących dotychczas w praktyce gospodarczej podatnika lub na tyle innowacyjnych, że w znacznym stopniu odróżniają się od rozwiązań już u niego funkcjonujących. Twórczość należy odnosić do działalności w ramach własnej działalności – nie ma znaczenia czy podobne rozwiązanie (ulepszone procesy, usługi czy produkty) zostało już opracowane przez inny podmiot[14].

Wymóg „systematyczności" należy rozumieć jako działalność prowadzoną w sposób metodyczny, uporządkowany i zaplanowany[15]. Przesłanki tej nie będą spełniać prace o charakterze incydentalnym i jednorazowym, nawet jeśli trwały kilka lat[16]. „Systematyczność" to coś więcej niż tylko prowadzenie prac zgodnie z harmonogramem w ściśle wyznaczonych ramach czasowych. Konieczne jest również planowanie takich działań na przyszłość[17]. Dostępna dokumentacja podatnika powinna zawierać opis celu projektu B+R, jego przebieg oraz ostateczny wynik[18].

Działalność badawczo-rozwojowa powinna wiązać się z prowadzeniem badań naukowych lub prac rozwojowych. Badania naukowe to badania podstawowe lub aplikacyjne w rozumieniu ustawy prawo o szkolnictwie wyższym i nauce. W myśl jej przepisów badania podstawowe to prace empiryczne lub teoretyczne, mające przede wszystkim na celu zdobywanie nowej wiedzy o podstawach zjawisk i obserwowalnych faktów bez nastawienia na bezpośrednie zastosowanie komercyjne[19]. Badania aplikacyjne natomiast (dawniej badania przemysłowe) to prace mające na celu zdobycie nowej wiedzy oraz umiejętności, nastawione na opracowywanie nowych produktów, procesów lub usług, lub wprowadzanie do nich znaczących ulepszeń[20].

---

[13] Art. 4 pkt 26 CIT.
[14] J. Jankowski, *Ulgi w CIT…* op. cit. s. 2; Objaśnienia MF w sprawie IP Box, s. 12.
[15] J. Jankowski, *Ulgi w CIT* op. cit. s. 2; Objaśnienia MF w sprawie IP Box, s. 14.
[16] J. Jankowski, *Ulgi w CIT* op. cit. s. 2; P. Dudek, *Nie każdy skorzysta z ulgi B+R. Incydentalny projekt to nie prace rozwojowe*, DGP z 25.06.2019 r.
[17] J. Jankowski, *Ulgi w CIT* op. cit. s. 2; Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 19.06.2019 r., sygn. III SA/Wa 2257/18, LEX nr 2741286.
[18] J. Jankowski, *Ulgi w CIT…* op. cit. s. 2; OECD, *Podręcznik Frascati „Zalecenie dotyczące pozyskiwania i prezentowania danych z zakresu działalności badawczej i rozwojowej, pomiar działalności naukowo-technicznej i innowacyjnej*, Paryż, 2015.
[19] J. Jankowski, *Ulgi w CIT…* op. cit. s. 3; Art. 4 ust. 2 pkt. 1 p.s.w.n.
[20] J. Jankowski, *Ulgi w CIT…* op. cit. s. 3; Art. 4 ust. 2 pkt. 2 p.s.w.n.

Działalność B+R powinna być podejmowana w celu zwiększenia zasobów wiedzy oraz wykorzystania ich do tworzenia nowych zastosowań. Działalność B+R powinna koncentrować się na nowej wiedzy, a nie na nowych lub znacząco ulepszonych produktach lub procesach wynikających z zastosowania wiedzy[21]. Innymi słowy, działalność ta w fazie początkowej może bazować na istniejącej już wiedzy, jednakże połączenie w ramach prowadzonych badań istniejących zasobów wiedzy musi prowadzić do powstania „wartości dodanej". Ta „wartość dodana" to nowe koncepcje lub pomysły, które wzbogacają istniejącą wiedzę[22].

Może to być przykładowo:

1. zintegrowanie „podręcznika obsługi technicznej" bardzo złożonego systemu (np. pasażerskiego statku powietrznego) z dodatkowymi, właściwie skodyfikowanymi materiałami wynikającymi z praktycznego doświadczenia w zakresie codziennej obsługi technicznej, o ile przedsięwzięcie to zrealizowano w ramach projektu B+R; lub
2. systematyczne testy mające na celu stworzenie dokumentacji dla potencjalnych zastosowań reakcji chemicznych, która została już wdrożona w procesach produkcyjnych (istniejąca technologia) w celu uzyskania nowej cząsteczki[23].

Wynik prowadzonych prac B+R nie powinien być z góry możliwy do przewidzenia. Niepewność co do powodzenia prowadzonych badań jest istotną cechą działalności B+R. Uzyskana w ramach badań wiedza powinna być „przenośna", tj. inne podmioty powinny mieć możliwość odtworzenia jej wyników w ramach własnej działalności B+R[24]. Z zakresu prac B+R wyłączone są czynności o charakterze rutynowym. Do działalności B+R zaliczają się natomiast nowe metody opracowane w celu wykonywania pospolitych zadań[25]. Jak pokazuje jednak praktyka, konieczne jest, aby dochodziło do wzrostu efektywności, jakości lub bezpieczeństwa ich wykonywania. Na przykład, przetwarzanie danych nie jest działalnością badawczo-rozwojową chyba, że stanowi część projektu mającego na celu opracowanie nowych metod przetwarzania danych. Podobnie kształcenie zawodowe należy wyłączyć z zakresu działalności badawczo-rozwojowej, ale już nowe metody prowadzenia szkoleń mogą zostać zakwalifikowane jako działalność badawczo-rozwojowa.

[21] J. Jankowski, *Ulgi w CIT…* op. cit. s. 3; OECD, *Podręcznik Frascati…,* op. cit. s. 49.
[22] Ibidem.
[23] Ibidem.
[24] J. Jankowski, *Ulgi w CIT…* op. cit. s. 3; OECD, *Podręcznik Frascati…,* op. cit. s. 50.
[25] J. Jankowski, *Ulgi w CIT…* op. cit. s. 3; OECD, *Podręcznik Frascati…,* op. cit. s. 49.

Wreszcie nowa metoda rozwiazywania problemu, opracowana w ramach projektu, może być zaliczona do działalności badawczo-rozwojowej, jeśli wynik jest oryginalny i spełnione są pozostałe kryteria tej działalności[26].

W związku z powyższym, zauważając za Jakubem Jankowskim, działalność B+R w istocie powinna posiadać cechy takie jak twórczość, systematyczność, nieprzewidywalność, możliwość przeniesienia (transferu) oraz brak rutynowości[27].

3. SZTUCZNA INTELIGENCJA JAKO KOSZT KWALIFIKOWANY ULGI BADAWCZO-ROZWOJOWEJ

Jeżeli więc podatnik ma wykonywać działalność twórczą obejmującą badania naukowe lub prace rozwojowe, podejmowane w sposób systematyczny w celu zwiększenia zasobów wiedzy oraz wykorzystywania zasobów wiedzy do tworzenia nowych zastosowań, powinniśmy zadać sobie pytanie – czy będzie ją wykonywał, jeżeli działalność twórcza będzie realizowana przez algorytmy uczenia maszynowego?

Istotne w tym zakresie będzie zauważenie katalogu kosztów kwalifikowanych ulgi badawczo-rozwojowej określonego w art. 18d ust. 1-3 i 7 CIT, mając na względzie w szczególności kategorie takie jak: koszty pracy, materiały i surowce, sprzęt specjalistyczny, ekspertyzy, opinie i usługi doradcze, korzystanie z aparatury naukowo-badawczej, środki trwałe, wartości niematerialne i prawne. Odnoszące się do określonych kosztów kwalifikowanych, którymi są:

- Wynagrodzenia pracowników zatrudnionych w celu realizacji działalności badawczo-rozwojowej oraz związanych z nimi składek, na ubezpieczenia społeczne (finansowanych przez płatnika) w takiej części, w jakiej czas przeznaczony na realizację działalności badawczo-rozwojowej pozostaje w ogólnym czasie pracy pracownika w danym miesiącu;
- Wynagrodzenia osób zatrudnionych na podstawie umów zlecenia albo umów o dzieło związanych z nimi składek na ubezpieczenia społeczne (finansowane przez płatnika) w takiej części, w jakiej czas przeznaczony na realizację działalności badawczo-rozwojowej pozostaje w części czasu przeznaczonego na wykonanie usługi na podstawie umowy zlecenia lub umowy o dzieło w danym miesiącu;

[26] Objaśnienia MF w sprawie IP Box, s. 13 i 14.
[27] J. Jankowski, *Ulgi w CIT*… op. cit. s. 4.

- Nabycie materiałów i surowców bezpośrednio związanych z prowadzoną działalnością badawczo-rozwojową;
- Nabycie niebędącego środkami trwałymi sprzętu specjalistycznego wykorzystywanego bezpośrednio w prowadzonej działalności badawczo-rozwojowej, w szczególności naczyń i przyborów laboratoryjnych oraz urządzeń pomiarowych;
- Ekspertyzy, opinie, usługi doradcze i usługi równorzędne, świadczone lub wykonywane na podstawie umowy przez podmiot, o którym mowa w art. 7 ust. 1 pkt. 1, 2 i 4-8 ustawy prawo o szkolnictwie wyższym, a także nabycia od takiego podmiotu wyników prowadzonych przez niego badań naukowych, na potrzeby działalności badawczo-rozwojowej;
- Odpłatne korzystanie z aparatury naukowo-badawczej, wykorzystywanej wyłącznie w prowadzonej działalności badawczo-rozwojowej, jeżeli korzystanie wynika z umowy zawartej z podmiotem powiązanym w rozumieniu art. 11a ust. 1 pkt. 4 CIT;
- Nabycie usługi wykorzystania aparatury naukowo-badawczej wyłącznie na potrzeby prowadzonej działalności badawczo-rozwojowej, jeżeli zakup usługi nie wynika z umowy zawartej z podmiotem powiązanym z podatnikiem w rozumieniu art. 11a ust. 1 pkt. 4 CIT;
- Dokonywane w danym roku podatkowym, zaliczane do kosztów uzyskania przychodów, odpisy amortyzacyjne od środków trwałych oraz wartości niematerialnych i prawnych wykorzystywanych w prowadzonej działalności badawczo-rozwojowej, z wyłączeniem samochodów osobowych i budowli, budynków i lokali będących odrębną własnością;
- Określone koszty uzyskania i utrzymania patentu, prawa ochronnego na wzór użytkowy lub prawa z rejestracji wzoru przemysłowego, jeżeli zostały poniesione przez podatnika będącego mikroprzedsiębiorcą, małym lub średnim przedsiębiorcą w rozumieniu przepisów o swobodzie działalności gospodarczej[28].

W pierwszej kolejności, rozważyć należy możliwość uznania sztucznej inteligencji za aparaturę naukowo-badawczą. Zauważając, że przepisy CIT nie definiują pojęcia „aparatura naukowo-badawcza". W świetle wyjaśnień Głównego Urzędu Statystycznego, aparatura naukowo-badawcza to zestawy urządzeń badawczych, pomiarowych lub laboratoryjnych o małym stopniu

[28] Art. 18d ust. 1-3 i 7 ustawy o CIT.

uniwersalności i wysokich parametrach technicznych (zazwyczaj wyższych o kilka rzędów dokładności pomiaru w stosunku do typowej aparatury stosowanej dla celów produkcyjnych lub eksploatacyjnych). Do aparatury naukowo-badawczej nie zalicza się sprzętu komputerowego i innych urządzeń nie wykorzystywanych bezpośrednio do realizacji prac B+R. Dlatego np. w indywidualnej interpretacji podatkowej z dnia 14 czerwca 2018 r. Dyrektor Krajowej Administracji Skarbowej wskazał, że serwer nie ma znamion urządzenia o małym stopniu uniwersalności. Serwer jest urządzaniem powszechnym, dostępnym dla wszystkich. Nie można zatem zakwalifikować go do aparatury naukowo-badawczej[29]. Powyższe interpretować możemy w ten sposób, że co do zasady, sztuczna inteligencja rozumiana jako urządzenie (komputer lub serwer) nie będzie stanowiła aparatury naukowo-badawczej, chyba że będzie częścią specjalistycznych urządzeń o małym stopniu uniwersalności. Niewątpliwie jednak, nabycie majątkowych praw autorskich lub licencji do programu komputerowego sztucznej inteligencji będzie stanowiło nabycie wartości niematerialnych i prawnych mogących podlegać odpisom amortyzacyjnym.

W drugiej kolejności, celem analizy kwalifikowalności określonych kosztów można przyjąć wykorzystanie sztucznej inteligencji w procesach text and data mining (dalej jako: TDM), wykorzystywanych w prowadzonej działalności badawczo-rozwojowej. Zgodnie ze stanowiskiem E. Trapel, proces text and data mining (TDM) realizowany przez sztuczną inteligencja składa się z następujących etapów: 1) uzyskanie dostępu do danych i odpowiednie ich przygotowanie do procedury TDM; 2) pobranie danych i ich kopiowanie; 3) eksploracja polegająca na analizie i wyciągnięciu wniosków; 4) prezentowanie wyników i ich weryfikacja[30].

Uzyskanie dostępu do danych i odpowiednie ich przygotowanie do procedury TDM, możemy uznać za nabycie wartości niematerialnych i prawnych. W przypadku, jeśli nabycie zbioru danych nie będzie możliwe, koniecznym może być wynagrodzenie pracowników lub osób zatrudnionych na podstawie umów zlecenia albo umów o dzieło odpowiedzialnych za stworzenie

[29] Pismo z dnia 14.06.2018 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0111-KDIB1-3.4010.244.2018.1.MO, *Koszty wynajmu serwerów jako koszty kwalifikowane działalności badawczo-rozwojowej*, https://sip.lex.pl/#/guideline/185019296/0111-kdib-1-3-4010-244-2018-1-mo-koszty-wynajmu-serwerow-jako-koszty-kwalifikowane-dzialalnosci...?keyword=serwer&cm=URELATIONS [dostęp: 2022-05-22].

[30] E. Traple, *Granice eksploracji tekstów i danych na potrzeby maszynowego uczenia się przez systemy sztucznej inteligencji*, [w:] *Prawo Sztucznej Inteligencji i Nowych Technologii*, red. B. Fischer, A. Pązik, M. Świerczynski. Warszawa, 2021, s. 21.

odpowiedniego zbioru danych, względnie zamówienie określonego zbioru danych jako ekspertyzy, opinii, usługi doradczej lub usługi równorzędnej od jednostki naukowej w rozumieniu art. 7 ust. 1 pkt. 1, 2 i 4,8 ustawy prawo o szkolnictwie wyższym. Pobranie danych i ich kopiowanie, w zależności od tego czy konieczne będzie zaangażowanie pracy ludzi, stanowić może koszt wynagrodzenia pracowników lub osób zatrudnionych na podstawie umów zlecenia albo umów o dzieło. Jeśli sztuczna inteligencja będzie realizowała zadanie w sposób autonomiczny, kosztem kwalifikowanym będą jedynie odpisy amortyzacyjne od wartości niematerialnych i prawnych. W zakresie eksploracji polegającej na analizie i wyciągnięciu wniosków, jako pracy realizowanej przez program komputerowy bez wykorzystania pracy ludzi, kosztem kwalifikowanym będą jedynie odpisy amortyzacyjne od wartości niematerialnych i prawnych. Prezentowanie wyników i ich weryfikacja, co do zasady nie będzie stanowiło prac badawczo-rozwojowych mając na względzie jego przedwdrożeniowy charakter, a co za tym idzie brak możliwości uznania za badania aplikacyjne lub prace rozwojowe.

4. WPROWADZENIE DO 50% KOSZTÓW UZYSKANIA PRZYCHODU Z PRACY TWÓRCZEJ

Przepis art. 22 ust. 9 pkt. 3 PIT stanowi „Koszty uzyskania niektórych przychodów określa się: z tytułu korzystania przez twórców z praw autorskich i artystów wykonawców z praw pokrewnych, w rozumieniu odrębnych przepisów, lub rozporządzania przez nich tymi prawami – w wysokości 50 % uzyskanego przychodu, z zastrzeżeniem ust. 9a i 9b, z tym, że koszty te oblicza się od przychodu pomniejszonego o potrącone przez płatnika w danym miesiącu składki na ubezpieczenia emerytalne i rentowe oraz na ubezpieczenie chorobowe, o których mowa w art. 26 ust. 1 pkt. 2 lit. b, których podstawę wymiaru stanowi ten przychód".

Powołana regulacja nie zawiera ograniczenia podmiotowego do twórców uzyskujących przychody z praw majątkowych (art. 18 PIT). Oznacza to możliwość zastosowania przepisu również w stosunku do pracowników[31]. Zauważając za Jakubem Jankowskim, w odniesieniu do niektórych kategorii pracowników ustawodawca pozwala na podwyższenie kosztu podatkowego. Wówczas uznaje się, że wartość kosztów podatkowych wynosi 50% wartości wynagrodzenia pracownika[32]. Przedmiotowa preferencja choć dotyczy wy-

[31] J. Sekita, *Obowiązki płatników PIT w 2020 roku*, Warszawa 2020, s. 307.
[32] J. Jankowskio, *Ulgi w CIT*…, op. cit. s. 191.

nagrodzenia pracowników (osób fizycznych – podatników PIT), to jednak funkcjonalnie jest powiązana z przedsiębiorcami (często podatnikami CIT), którzy jako płatnicy, obliczają i pobierają z tego tytułu podatek dochodowy od osób fizycznych[33].

Zgodnie z art. 12 ust. 1 ustawy o prawie autorskim: „Jeżeli ustawa lub umowa o pracę nie stanowią inaczej, pracodawca, którego pracownik stworzył utwór w wyniku wykonywania obowiązków ze stosunku pracy, nabywa z chwilą przyjęcia utworu autorskie prawa majątkowe w granicach wynikających z celu umowy o pracę i zgodnego zamiaru stron". Szczególną regulację zawiera też art. 73 ust. 4 ustawy o prawie autorskim: „Prawa majątkowe do programu komputerowego stworzonego przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy przysługują pracodawcy, o ile umowa nie stanowi inaczej". Aby pracownik uzyskał przychód poddany kosztom autorskim, niezbędne jest zawarcie przez pracodawcę i pracownika umowy określającej odpłatne zbycie praw autorskich. Przejście na pracodawcę efektu pracy pracownika na podstawie ustawy, bez wyodrębnienia wynagrodzenia za zbycie praw autorskich (wynagrodzenie za świadczenie pracy, niezależnie od powstania lub braku powstania skutków prawno-autorskich) skutkuje potrąceniem kosztów uzyskania przychodów na zasadach ogólnych, o których jest mowa w art. 22 ust. 2 PIT[34].

Przepis art. 22 ust. 9 PIT jest stosowany przez pracodawcę (płatnika) w procesie obliczania zaliczek (wynika to z art. 32 ust. 2 PIT stanowiącego o poborze zaliczki od dochodu cyt. „po odliczeniu kosztów uzyskania w wysokości określonej w art. 22 ust. 2 pkt. 1 albo 3 lub w ust. 9 pkt. 1-3"). Znaczy to, że art. 22 ust. 10-10a PIT ustanawia możliwość potrącenia kosztów autorskich w wysokości kosztów rzeczywiście poniesionych, a nie wynikających z norm procentowych[35]. Norma art. 22 ust. 9 pkt. 3 PIT stanowi więc uprawnienie podatnika, nie powodujące samoistnie obowiązku płatnika w procesie kalkulacji zaliczek[36]. Pracodawca jako płatnik jest obowiązany zweryfikować

[33] Ibidem, s. 191.

[34] J. Sekita, *Obowiązki płatników PIT w 2020 roku*, Warszawa 2020, s. 307; Pismo z dnia 28.06.2019 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0113-KDIPT3.4011.238.2019.2.JR, *Zastosowanie 50% kosztów podatkowych do wynagrodzenia programisty*, https://sip.lex.pl/#/guideline/185052036?directHit=true&directHitQuery=0113-KDIPT3.4011.238.2019.2.JR [dostęp: 2022-05-22]; Pismo z dnia 13.03.2019 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0112-KDIL3-3.4011.14.2019.1.MM, *Zastosowanie 50% kosztów uzyskania przychodów do wynagrodzenia nauczyciela akademickiego*, https://sip.lex.pl/#/guideline/185039126?directHit=true&directHitQuery=0112-KDIL3-3.4011.14.2019.1.MM [dostęp: 2022-05-22].

[35] J. Sekita, *Obowiązki płatników*…, op. cit. s. 308.

[36] Art. 22 ust. 10 - 10a PIT.

przesłanki potrącenia kosztów autorskich (czy mamy do czynienia z działalnością twórczą skutkującą powstaniem prawa autorskiego)[37] oraz czy należy ono do katalogu praw objętych kosztami autorskimi. Płatnik nie może „cedować" na podatnika obowiązku prawnego weryfikacji tych okoliczności (wpływających na wysokość zaliczki), które wynikają z danych dostępnych płatnikowi i które mogą być poddane przez niego ocenie prawnej[38]. Jak wskazuje Dyrektor Krajowej Informacji Skarbowej „złożenie wniosku o wydanie interpretacji indywidualnej również nie jest w większości przypadków środkiem uzyskania bezpieczeństwa prawnego". Tryb interpretacyjny służy do „abstrakcyjnego" zastosowania przepisów, a nie stwierdzenia, czy dana twórczość ma charakter prawno-autorski lub czy jest twórczością np. publicystyczną[39].

Kolejne zagadnienie związane jest z dokumentowaniem faktu wykonania pracy twórczej i przeniesienia praw autorskich. W tym zakresie, J. Sekita wskazuje dwie linie interpretacyjne[40].

Pierwsza wiąże się z obowiązkiem prowadzenia ścisłej ewidencji czasu pracy twórczej (i wynikającej z tej ewidencji wartości przenoszonych praw autorskich) i „nietwórczej". Wymogiem zastosowania kosztów autorskich jest więc nie tylko odrębne wskazanie części wynagrodzenia przypadającego na rozporządzenie prawami autorskimi, ale także uzasadnienia właściwego przyporządkowania części wynagrodzenia do prac twórczych i rozporządzania ich efektami[41].

Druga linia interpretacyjna neguje konieczność prowadzenia ewidencji czasu pracy (twórczej i nietwórczej) jako bazy podziału wynagrodzenia. Może on nastąpić na podstawie innych kryteriów niż sam czas pracy. Jest to podejście prawidłowe, ponieważ sam czas pracy pracownika nie jest wyłącznym wyznacznikiem wartości efektów pracy. Pracodawca może w różny sposób wyceniać różne pola aktywności pracownika, ustalając wynagrodzenia

[37] Pismo z dnia 23.05.2019 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0115-KDIT2 1.4011.131.2019.1.DW, *50% kosztów uzyskania przychodów*, https://sip.lex.pl/#/guideline/185047066?directHit=true&directHitQuery=0115-KDIT2-1.4011.131.2019.1.DW [dostęp: 2022-05-22].

[38] J. Sekita, *Obowiązki płatników*…, s. 308.

[39] Pismo z dnia 9.11.2018 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0115-KDIT2-1.4011.330.2018.2.MN, *Działalność badawczo-rozwojowa w zakresie aplikacji i oprogramowania*, https://sip.lex.pl/#/guideline/185031124?directHit=true&directHitQuery=0115-KDIT2-1.4011.330.2018.2.MN [dostęp: 2022-05-22].

[40] J. Sekita, *Obowiązki płatników*…, s. 307.

[41] Pismo z dnia 21.12.2018 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0112-KDIL3-3.4011.378.2018.1.DS, *PIT w zakresie możliwości zastosowania 50% kosztów uzyskania przychodów*, https://sip.lex.pl/#/guideline/185034475?directHit=true&directHitQuery=0112-KDIL3-3.4011.378.2018.1.DS [dostęp: 2022-05-22].

za rozporządzenie prawami autorskimi zgodnie z wartością rynkową tych praw[42]. Kwota honorarium ma być wyznacznikiem rzeczywistej wartości utworu, stanowić odzwierciedlenie wartości rynkowej przekazanych praw autorskich. Tylko bowiem wyliczenia faktycznej wartości honorarium z tytułu przeniesienia praw autorskich lub rozporządzania tymi prawami pozwala na zastosowanie do tej wartości kosztów uzyskania przychodów w wysokości określonej w art. 22 ust. 9 pkt. 3 PIT[43].

Zgodnie z art. 22 ust. 9b PIT przepis ust. 9 pkt. 3 stosuje się do przychodów uzyskiwanych z tytułu:

1. Działalności twórczej w zakresie architektury, architektury wnętrz, architektury krajobrazu, inżynierii budowlanej, urbanistyki, literatury, sztuk plastycznych, wzornictwa przemysłowego, muzyki, fotografiki, twórczości audialnej i audiowizulanej, programów komputerowych, gier komputerowych, teatru, kostiumografii, scenografii, reżyserii, choreografii, lutnictwa artystycznego, sztuki ludowej i dziennikarstwa;
2. Działalności artystycznej w dziedzinie sztuki aktorskiej, estradowej, tanecznej i cyrkowej oraz w dziedzinie dyrygentury, wokalistyki i instrumentalistyki;
3. Produkcji audialnej i audiowizualnej;
4. Działalności publicystycznej;
5. Działalności muzealniczej w dziedzinie wystawienniczej, naukowej, popularyzatorskiej, edukacyjnej oraz wydawniczej;
6. Działalności konserwatorskiej;
7. Prawa zależnego, o którym mowa w art. 2 ust. 2 ustawy o prawie autorskim, do opracowania cudzego utworu w postaci tłumaczenia;
8. Działalności badawczo-rozwojowej, naukowej, naukowo-dydaktycznej, badawczej, badawczo-dydaktycznej oraz prowadzonej w uczelni działalności dydaktycznej".

Jeżeli jednak działalność twórcza pracownika należy do innych dziedzin, nawet jeżeli podlega ona ochronie prawno-autorskiej, art. 22 ust. 9 PIT nie ma zastosowania (w stosunku do wynagrodzenia stosowane są koszty wynikające

[42] J. Sekita, *Obowiązki płatników*…, op. cit., s. 312.
[43] Pismo z dnia 5.06.2019 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0114-KDIP3-3.4011.156.2019.2.AK, *Zastosowanie 50% kosztów podatkowych do wynagrodzenia programisty*, https://sip.lex.pl/#/guideline/185048567?directHit=true&directHitQuery=-0114-KDIP3-3.4011.156.2019.2.AK [dostęp: 2022-05-22].

z art. 22 ust. 2 PIT)[44]. Przepisy PIT nie wymieniają wprost kategorii umów, do których zastosowanie mogą mieć 50% koszty uzyskania przychodów. W przypadku art. 22 ust. 9 pkt. 1 i 2 PIT będą to zwykle umowy z podmiotami zewnętrznymi o przeniesienie prawa własności wynalazku bądź inne podobne. W odniesieniu natomiast do art. 22 ust. 9 pkt. 3 PIT będą to raczej umowa o pracę, umowa zlecenie lub umowa o dzieło[45].

5. PRACOWNIK JAKO AUTOR REZULTATU „PRACY TWÓRCZEJ" SZTUCZNEJ INTELIGENCJI

Sztuczna inteligencja rozumiana jako systemy inteligentnego uczenia się, może być wykorzystana w każdej z powyższych dziedzin. Zagadnieniem budzącym wątpliwości pozostaje jednak możliwość uznania pracownika za autora rezultatu „pracy twórczej" sztucznej inteligencji.

Kiedy utwory powstają jako rezultat „pracy twórczej" sztucznej inteligencji – czy twórcą będzie autor programu komputerowego? Kiedy z programu komputerowego w celu tworzenia nowych utworów będzie korzystał podmiot inny niż twórca programu komputerowego – czy stanie się twórcą utworów wytworzonych przez sztuczną inteligencję, pomimo tego, że nie jest autorem programu komputerowego?

Rozważyć można stosunki umowne będące podstawą do korzystania z majątkowych praw autorskich podmiotu będącego twórcą programu komputerowego. Przyjmując, że inaczej może wyglądać sytuacja podmiotu, na który przeniesiono majątkowe prawa autorskie do programu komputerowego niż podmiotu będącego stroną umowy licencyjnej, czy też podmiotu zlecającego wykonanie usługi na podstawie tzw. umowy SaaS (Software as a Service).

Zgodnie z wcześniejszymi rozważaniami, do powstania utworu konieczny jest element działalności twórczej człowieka, każdorazowo więc konieczne będzie zadanie sobie pytania - czy przesłanka twórczości występuje w odniesieniu do autora programu komputerowego czy też w odniesieniu do pracownika korzystającego z programu sztucznej inteligencji?

Istotne będzie również czy podmiot korzystający z majątkowych praw autorskich do programu komputerowego będzie korzystał z nich w ramach prac badawczo-rozwojowych lub też własnej działalności twórczej o indywidualnym charakterze, w wyniku której rezultat „pracy twórczej"

[44] J. Sekita, *Obowiązki płatników*…, op. cit. s. 320.
[45] J. Jankowski, *Ulgi w CIT*…, op. cit. s. 192.

sztucznej inteligencji stanie się jedynie częścią powstałego utworu. Konieczne w tym zakresie będzie odniesienie się do zagadnienia tzw. „prawa cytatu" określonego w art. 29 ustawy o prawie autorskim, bowiem w przypadku, jeśli przymiot działalności twórczej o indywidualnym charakterze spoczywał będzie po stronie autora programu komputerowego, to konieczne będzie wymienienie twórcy i źródła zapożyczenia[46]. Nawiązując do treści art. 43 ustawy o prawie autorskim, kwestie wynagrodzenia za korzystanie z utworu innego autora powinna rozstrzygać umowa przeniesienia majątkowych praw autorskich do programu komputerowego lub odpowiednio umowa licencyjna.

Zgodnie z art. 74 ust. 2 ustawy o prawie autorskim ochrona przyznana programowi komputerowemu obejmuje wszystkie formy jego wyrażenia. Na przykład, K. Gienas podnosi, że ochrona programu komputerowego nie jest uzależniona od przybranej przez niego formy wyrażenia[47]. Niewątpliwie jednak „formą wyrażenia programu komputerowego" nie będzie utwór tworzony z wykorzystaniem sztucznej inteligencji. Nie oznacza to jednak, że autorem rezultatu „pracy twórczej" sztucznej inteligencji, nie będzie autor programu komputerowego. Będzie nim, pod warunkiem, że rezultat będzie spełniał warunki uznania za utwór oraz np. dojdzie do ujawnienia autora zgodnie z art. 8 ust. 2 ustawy o prawie autorskim. Kwestie te, opisywać powinna umowa zawarta pomiędzy autorem programu komputerowego oraz podmiotem wykonującym działalność twórczą z wykorzystaniem sztucznej inteligencji.

Zgodnie jednak z powszechnie przyjmowanym poglądem, umowa nie może dotyczyć samego autorstwa utworu (nie można w umowie przesądzić kogo należy traktować jako twórcę)[48]. Przesądzenie kto jest twórcą programu komputerowego, jest szczególnie trudne, ponieważ jak zauważa K. Żok. cyt. „oprogramowanie powstaje w ramach złożonego, wieloetapowego procesu, angażującego nierzadko wiele osób. Po stronie kontrahenta zamawiającego

[46] A. Niewęgłowski *art. 29* [w:] *Prawo autorskie. Komentarz*, red. A. Niewęgłowski, Warszawa, 2021, LEX, https://sip.lex.pl/#/commentary/587871616/669056 [dostęp: 22.05.2022 r.].
[47] K. Gienas, *Art. 74* [w:] *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, red. E. Ferenc-Szydełko, Warszawa, 2021, Legalis, https://sip.legalis.pl/document view.seam?documentId=mjxw62zogi3damrtgm4tmojoobqxalruhe3dcmzwgy2q [dostęp: 22.05.2022];
[48] R. M. Sarbiński, *art. 8* [w:] *Prawo autorskie i prawa pokrewne*. Komentarz, red. W. Machała, Warszawa, 2019, LEX, https://sip.lex.pl/#/commentary/587792153/589593?keyword=umowa [dostęp: 04.06.2022 r.]; J. Barta, R. Markiewicz, *3. Podmiot praw autorskich* [w:] *Prawo autorskie*, red. J. Barta, R. Markiewicz, Warszawa, 2016, LEX, https://sip.lex.pl/#/monograph/369376704/290141/barta=-janusz-markiewicz-ryszard-prawo-autorskie?keyword-umowa&unitId=passage_8962 [dostęp: 04.06.2022 r.]; K. Żok, *2.4.3. Zakres podmiotowy* [w:] *Środki ochrony zamawiającego program komputerowy*, Warszawa, 2015, LEX, https://sip.lex.pl/#/monograph/369363031/282507/zok-krzysztof-srodki-ochrony-zamawiajacego-program-komputerowy?keyword=umowa&unitId=passage_4004 [dostęp: 04.06.2022 r.].

mogą zatem występować różne konfiguracje podmiotowe; w szczególności podmiot tworzący oprogramowanie może być twórcą sensu stricto programu komputerowego, pracodawcą twórcy, pochodnym nabywcą autorskich praw majątkowych do wyjściowego programu komputerowego albo licencjobiorcą wyjściowego programu komputerowego. Niewykluczone, że będzie on łączył kilka z tych statusów, będąc np. rzeczywistym twórcą podstawowej części oprogramowania oraz pracodawcą twórców dodatkowych modułów tego programu komputerowego[49]".

Istotne stanowisko, wyrażono w wyroku Sadu Najwyższego z dnia 5 kwietnia 2002 r.[50], na gruncie art. 70 ustawy o prawie autorskim, cyt. „Jakkolwiek w kwestii oceny skutków prawnych tego przepisu istniała różnica zdań co do tego, czy w danym wypadku nabycie praw majątkowych do utworu audiowizualnego należało traktować jako nabycie pierwotne, czy też jako wstąpienie z mocy ustawy w prawa innej osoby (cessio legis), to jednak oczywiste było to, iż dotyczył on wyłącznie sytuacji, w których w odniesieniu do określonej osoby w ogóle zasadnie można było mówić o istnieniu praw autorskich w rozumieniu art. 1 w związku z art. 8 ustawy o prawie autorskim i prawach pokrewnych[51]". W przywołanej sprawie uznano, że kierownika produkcji filmu reklamowego nie można uznać za współtwórcę utworu audiowizualnego w rozumieniu art. 69 ust. 1 w zw. z art. 1 ust. 1 i art. 8 ust. 1 ustawy o prawie autorskim, jeżeli w procesie powstawania tego utworu pełnił on względem współtwórców wyłącznie funkcje służebne (organizacyjno-administracyjne lub gospodarcze)[52]. Jak wskazał Sąd Najwyższy, cyt. „W rozpoznawanej sprawie jest poza sporem, że podatnik - Piotr D. zawarł z firmą "O.F." Sp. z o.o. umowy nazywane "umowami o dzieło", na podstawie których przyjął na siebie zobowiązanie do wykonania prac w charakterze kierownika produkcji przy realizacji filmów reklamowych. Z treści powyższych umów oraz z tzw. regulaminu grupy zdjęciowej, który stanowił ich integralną część, wynika przy tym, że zakres obowiązków i czynności kierownika produkcji

[49] K. Żok, *2.4.3. Zakres podmiotowy* [w:] *Środki ochrony zamawiającego program komputerowy*, Warszawa, 2015, LEX, https://sip.lex.pl/#/monograph/369363031/282507/zok-krzysztof-srodki-ochrony-zamawiajacego-program-komputerowy?keyword=umowa&unitId=passage_4004 [dostęp: 04.06.2022 r.].

[50] Wyrok wydano na skutek rewizji nadzwyczajnej złożonej przez Rzecznika Praw Obywatelskich od wyroku Naczelnego Sądu Administracyjnego wydanego w sprawie skargi podatników na decyzję izby skarbowej w przedmiocie określenia zaległości w podatku dochodowym do osób fizycznych za 1996 r., w związku z naruszeniem art. 22 ust. 9 pkt. 3 PIT (KUP 50%).

[51] Wyrok Sądu Najwyższego z dnia 5 kwietnia 2002 r., III RN 133/01, OSNP 2002, nr 12, poz. 281.

[52] Ibidem.

wskazywał jednoznacznie na ich służebny charakter względem rzeczywistych współtwórców uczestniczących w tworzeniu tych utworów audiowizualnych (kierownik produkcji sprawował bowiem funkcje organizacyjno-administracyjne i gospodarcze, a więc funkcje usługowe wobec twórców utworu audiowizualnego)"[53].

Powyższe prowadzi do wniosku, że niezależnie od stosunku prawnego stanowiącego podstawę korzystania z autorskich praw majątkowych do programu komputerowego, autor wykorzystujący program komputerowy do własnej działalności twórczej o indywidualnym charakterze, musi spełniać warunki określone w art. 1 ust. 1 i art. 8 ust. 1 ustawy o prawie autorskim, również w odniesieniu do rezultatu „pracy twórczej" sztucznej inteligencji. W przypadku pracownika, to pracodawca jako płatnik jest obowiązany zweryfikować przesłanki potrącenia kosztów autorskich (czy mamy do czynienia z działalnością twórczą skutkującą powstaniem prawa autorskiego)[54].

6. KORZYSTANIE PRZEZ TWÓRCÓW Z PRAW AUTORSKICH DO REZULTATU „PRACY TWÓRCZEJ" SZTUCZNEJ INTELIGENCJI

W odniesieniu do korzystania przez twórców z praw autorskich do rezultatu „pracy twórczej" sztucznej inteligencji, przepisy ustawy o podatku dochodowym od osób fizycznych nie definiują wskazanych pojęć. Jak pisze J. Sekita, ich ocena powinna być dokonana przede wszystkim przez pryzmat ich znaczenia językowego. Choć w wielu przypadkach ocena jest obarczona ryzykiem (np. stwierdzenie czy prowadzenie bloga firmowego jest działalnością publicystyczną – może tak być)[55]. W tym zakresie, wystąpienie z wnioskiem o wydanie indywidualnej interpretacji podatkowej jest ułomnym środkiem ochrony płatnika, gdyż organ podatkowy nie stwierdzi, czy konkretny efekt prac pracownika mieści się przedmiotowo w zakresie praw wymienionych w art. 22 ust. 9b PIT[56]. Istnieją jednak przykłady interpretacji, w których

[53] Ibidem.
[54] Pismo z dnia 23.05.2019 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0115-KDIT2 1.4011.131.2019.1.DW, *50% kosztów uzyskania przychodów*, https://sip.lex.pl/#/guideline/185047066?directHit=true&directHitQuery=0115-KDIT2-1.4011.131.2019.1.DW [dostęp: 2022-05-22].
[55] Pismo z dnia 19.09.2019 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0115-KDIT2-1.4011.296.2019.2.MN, *Opodatkowanie przychodu z tytułu przeniesienia autorskich praw majątkowych*, https://sip.lex.pl/#/guideline/185061781?directHit=true&directHitQuery=0115-KDIT2-1.4011.296.2019.2.MN [dostęp: 2022-05-22].
[56] J. Sekita, *Obowiązki płatników*…, op. cit. s. 320.

organ dokonuje ogólnej wykładni znaczenia pojęć wymienionych w art. 22 ust. 9b PIT, które mogą stanowić wskazówkę dla płatników. Dyrektor Krajowej Informacji Skarbowej w interpretacji indywidulanej z 28 czerwca 2019 r., wskazał np.: „sformułowanie działalność twórcza w zakresie programów komputerowych, zawarte w art. 22 ust. 9b pkt. 1 ustawy o podatku dochodowym od osób fizycznych dotyczy korzystania i rozporządzania prawami autorskimi do wszelkich utworów, które powstają w związku z działaniami podejmowanymi w celu stworzenia programów komputerowych. W tym znaczeniu, nie tylko kody źródłowe programów komputerowych wypełniają przesłanki z art. 22 ust. 9b pkt 1 omawianej ustawy, lecz także utwory powstałe w procesie tworzenia programu komputerowego, tj. kody źródłowe programów komputerowych i/lub aplikacji mobilnych i/lub webowych, plany i/lub prototypy systemów, bazy oraz struktury danych, strony internetowe, dokumentacja techniczna, publikacje naukowe, specyfikacje (w tym specyfikacje architektury projektowych rozwiązań informatycznych), plany, analizy, raporty oraz rekomendacje, projekty graficzne (np. interfejs użytkownika), materiały reklamowe i marketingowe, materiały audio-wideo, a także prezentacje”[57].

Korzystanie przez twórców z praw autorskich będzie w istocie więc uzależnione od tego co uznamy za rezultat pracy twórczej sztucznej inteligencji. Jeśli jednak płatnik dysponuje stosowną dokumentacją działalności twórczej o indywidualnym charakterze, rezultat działalności twórczej utrwalono, dokonano stosownej wyceny oraz możliwe jest udowodnienie autorstwa osiągającego dochód z tytułu korzystania z praw autorskich, to pod warunkiem zakwalifikowania działalności twórczej do jednej z dyscyplin wskazanych w art. 22 ust. 9b pkt. 1 PIT, płatnik będzie uprawniony do podwyższenia kosztów uzyskania przychodów pracownika zgodnie z art. 22 ust. 9 pkt. 3 PIT.

BIBLIOGRAFIA

Barta J., Markiewicz R., Prawo autorskie, Warszawa 2016

Dudek P., Nie każdy skorzysta z ulgi B+R. Incydentalny projekt to nie prace rozwojowe, Dziennik Gazeta Prawna z 25.06.2019 r.

Ferenc-Szydełko E., Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Warszawa 2021.

[57] Pismo z dnia 28.06.2019 r., wydane przez: Dyrektor Krajowej Informacji Skarbowej, 0114-KDIP3-3.4011.153.2019.2.PP, *50% kosztów uzyskania przychodu*, https://sip.lex.pl/#/guideline/185052156?directHit=true&directHitQuery=0114-KDIP3-3.4011.153.2019.2.PP [dostęp: 2022-05-22].

Fischer B., Pązik A., Świerczynski M., *Prawo Sztucznej Inteligencji i Nowych Technologii*. Warszawa 2021.

Jankowski J., Optymalizacja wypłat dla kadry menadżerskiej, Państwo i Prawo, 2014, Nr. 2.

Jankowski J., Ulgi w CIT z tytułu działalności innowacyjnej i inwestycyjnej, Warszawa 2020.

Lai L., Świerczyński M., Prawo Sztucznej Inteligencji, Warszawa 2020.

Małecki P., Mazurkiewicz M., CIT. Podatki i rachunkowość, Komentarz, Warszawa 2020.

Michalak A., Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Warszawa 2019.

Ministerstwo Finansów, Objaśnienia podatkowe z dnia 15 lipca 2019 r. dotyczące preferencyjnego opodatkowania dochodów wytwarzanych przez prawa własności intelektualnej – IP Box, Warszawa 2019.

Niewęgłowski A., Prawo autorskie. Komentarz, Warszawa 2021.

OECD, Podręcznik Frascati „Zalecenie dotyczące pozyskiwania i prezentowania danych z zakresu działalności badawczej i rozwojowej, pomiar działalności naukowo-technicznej i innowacyjnej", Paryż 2015.

Olchowicz I., Jamroży M., Rachunkowość podatkowa, analiza w zakresie podatku dochodowego od osób prawnych, Warszawa 2020.

Salamonowicz M., Treść i charakter prawny umowy o prace badawczo-rozwojowe, Warszawa 2018.

Sarbiński R.M., art. 8 [w:] Prawo autorskie i prawa pokrewne. Komentarz, red. W. Machała, Warszawa 2019.

Sekita J., Obowiązki płatników PIT w 2020 roku, Warszawa 2020.

Ziółkowski J., Koszty uzyskania przychodów w CIT, Warszawa 2021.

Ziółkowski J., Podatki dochodowe 2021, komentarz do zmian ujednolicone teksty ustaw, Warszawa 2021.

Żok K., Środki ochrony zamawiającego program komputerowy, Warszawa 2015.

TAX QUALIFICATION OF THE EFFECTS OF CREATIVE ARTIFICIAL INTELLIGENCE ACTIVITY

Abstract: The article aims to properly assign the effects of "creative work" of artificial intelligence to specific concepts occurring in the income tax law. It focuses in this scope on the research and development tax relief (R&D tax relief) and 50% tax-deductible costs corresponding to remuneration related to creative activities (KUP 50%). An important element is the distinction between the legal situation of the author of a computer program and the legal situation of a researcher using a computer program in research and development activity. The article presents the general rules governing the R&D tax relief and KUP 50% presenting the meaning of such terms as creative activity and the use of copyrights by authors in the perspective of the corresponding concepts under copyright law. The presented conclusions refer to the possibility to consider artificial intelligence as an eligible cost of R&D tax relief and the possibility to consider an employee using artificial intelligence as an author benefiting from copyright. In view of the lack of detailed regulations in the income tax law, it is necessary to carefully describe specific issues i n the agreement between the creator of a computer program and the creator of a work created with the use of artificial intelligence.

Key words: AI, artificial intelligence, research & development, R&D.

ALEKSANDRA SZULC
UNIWERSYTET ŚLĄSKI W KATOWICACH

JAK FINTECH PORADZI SOBIE W REALNYM OTOCZENIU PRAWNYM? ROZWIĄZANIA PIASKOWNIC REGULACYJNYCH JAKO ŚRODOWISKA TESTOWEGO DLA INNOWACJI FINANSOWYCH W EUROPIE I NA ŚWIECIE

Abstrakt: Częste zmiany krajobrazu innowacji i technologii finansowych zmusza dzisiejszego legislatora do szybkiej reakcji. Działania dostosowawcze systemu prawnego ukierunkowane na zamknięcie w ramy prawne i objęcie kontrolą aktywności nowych rozwiązań na rynku finansowym są czasochłonne i stanowią trudną do pokonania barierę dla ich wdrażania. Zadania w obszarze stabilizacji systemu finansowego i kontroli cyrkulacji pieniądza implikują szczególną ostrożność państwa w poruszaniu się po ekosystemie *fintech*, łączącym sferę finansową i technologiczną. Stosowanie wykładni rozszerzającej, czy *per analogiam* dla objęcia innowacji obowiązującymi przepisami prawa napotyka na ograniczenia przy nowatorskich produktach i start-upach. Jednocześnie brak możliwości sprawdzenia rozwiązania w otoczeniu regulacyjnym rynku generuje ryzyko dla przedsiębiorców oraz zniechęca potencjalnych inwestorów i interesariuszy do zaangażowania swoich środków w ich rozwój. Widoczna dysproporcjonalność między szybkością transformacji cyfrowej a tempem zmian legislacyjnych spowalnia postęp w zakresie budowania nowoczesnej oferty rynku. Dzisiejszy rynek wymaga od organów regulacyjnych przyjęcia proaktywnego stanowiska wiążącego się z bieżącym wsparciem i tworzeniem przyjaznego środowiska dla innowacji, szczególnie w obszarach silnie uregulowanych. Działania *ex ante* stanowią w trwającym wyścigu technologicznym element polityki państwa nastawionego na innowacyjność. W niniejszym artykule rozważania zostaną skoncentrowane na analizie eksperymentalnego podejścia do regulacji, polegającego na poddaniu testom innowacji finansowych w ściśle określonej przestrzeni i pod kontrolą organu nadzorującego i regulatora. Prócz omówienia złożoności ekosystemu *fintech* i zaprezentowania samego mechanizmu piaskownicy regulacyjnej, istotną część dyskursu zajmie analiza poszczególnych elementów *sandboxa* i rozwiązań wprowadzonych w tym obszarze przez krajowych regulatorów. W pracy zostaną podjęte również wątki związane z rolą legislatora i organów publicznych w obszarze implementacji *fintech.* Szanse powodzenia i możliwości w zakresie opracowania

i uruchomienia centralnej piaskownicy regulacyjnej dla rynku Unii Europejskiej to kolejny kluczowy element prezentowanej pracy.

Słowa kluczowe: fintech, innowacje finansowe, piaskownica regulacyjna, rynek finansowy, technologie finansowe, środowisko testowe, eksperyment prawny, współpraca transgraniczna, europejska piaskownica regulacyjna.

WPROWADZENIE

Dzisiejszy postęp technologiczny kontroluje transfer klasycznych usług z obszaru finansowania do środowiska cyfrowego przy jednoczesnej automatyzacji procesów minimalizujących udział czynnika ludzkiego. Kryzys finansowy *subprime* stał się granicą oddzielającą stary świat finansów od rzeczywistości rynkowej ukierunkowanej na innowacje, zwiększenie dostępności i efektywności usług w tym obszarze. Krajobraz pokryzysowy stał się przestrzenią niezwykle sprzyjającą dla nowych graczy – firm nastawionych na rozwój nowych technologii oraz dążących do naruszenia dynamiki konkurencji i dotychczasowej struktury usług finansowych[1]. Rynek i warunki konkurencji uległy zmianie, stawiając podwaliny pod rozwój nowych sposobów świadczenia usług i usprawnienia wdrożonych metod prowadzenia biznesu. Coraz większą popularność w XXI w. w ofertach dostawców na nowoczesnym rynku finansowym zyskują *fintechy* znajdujące się na styku finansowej strony gospodarki z obszarem technologicznym. W słowniku oksfordzkim zostały zdefiniowane jako „*programy komputerowe i inne technologie wykorzystywane w celu świadczenia usług bankowych i finansowych*"[2]. *Fintech* zasadniczo stanowi powszechnie stosowany na rynku akronim od *financial technology* (technologia finansowa) i obejmuje szerokie spektrum usług bazujących na rozwiązaniach ICT (*Information-Communication Technology*, technologia informacyjno-komunikacyjna)[3]. Początkowo ekosystem *fintech* postrzegało się jako domenę start-upów – dostawców nowych trendów w zakresie rozwiązań technologicznych w biznesie. Obecnie przedsiębiorstwa o długoletnim stażu na rynku, w tym tradycyjne banki, w codziennej działalności operacyjnej wykorzystują platformy

[1] H. Arslanian, F. Fischer, *The Future of Finance. The Impact of FinTech, AI, and Crypto on Financial Services*, Palgrave Macmillan, 2019, s. 25.
[2] https://www.oxfordlearnersdictionaries.com/definition/english/fintech (dostęp: 5.05.2022).
[3] R. Milic-Czerniak, *Rola fintechów w rozwoju innowacji finansowych*, Studia BAS, Nr 1(57) 2019, s. 41.

elektroniczne, Big Data[4], czy chmurę obliczeniową[5]. Można dokonać klasyfikacji technologii przynależących do obszaru *fintech* na:

a) bazowe, do których należą: bankowość elektroniczna, elektroniczne usługi płatnicze, robo-doradztwo[6], insur-tech[7],

b) wspierające, *inter alia,* technologia rozproszonych rejestrów (ang. Distributed Ledger Technology, DLT)[8], w tym blockchain[9], a także interfejsy API[10], sztuczna inteligencja[11] i machine learning[12] [13].

Przedmiotem badania, któremu zostało podporządkowane niniejsze opracowanie są rozwiązania piaskownic regulacyjnych w obszarze kreowania otoczenia prawnego dla innowacji finansowych w Europie i na świecie. Prymarnym celem tegoż dyskursu jest analiza, ocena i postawienie wniosków w zakresie wykorzystania środowisk testowych w ramach eksperymentalnego podejścia do regulacji jako narzędzi regulacyjnych w obszarze *fintech*. W pierwszej kolejności zostaną zaprezentowane metody tworzenia reżimu prawnego w dynamicznie zmieniającym się środowisku technologii finansowych, a następnie zostanie zobrazowana piaskownica regulacyjna jako

[4] Big data oznacza duże ilości danych, które można wygenerować, przeanalizować i w większym stopniu wykorzystywać przy pomocy narzędzi cyfrowych i systemów informatycznych.

[5] Chmura obliczeniowa (ang. cloud computing) to zdolność obliczeniowa zapewniająca dostęp sieciowy na żądanie do współdzielonej puli konfigurowalnych zasobów obliczeniowych, które można szybko udostępniać przy minimalnej interakcji z dostawcą; istnieją zasadniczo trzy modele: infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS), oprogramowanie jako usługa (SaaS); chmura obliczeniowa może być publiczna, prywatna lub hybrydowa (B. Nicoletti, *The Future of FinTech Integrating Finance and Technology in Financial Services*, Palgrave Macmillan, 2017, s. 284).

[6] Cyfrowe narzędzia doradztwa inwestycyjnego, które dopasowują konsumentów na podstawie ich osobistych preferencji do produktów finansowych, opiera się głównie na dwóch kluczowych elementach: informacjach wejściowych dostarczonych przez konsumenta oraz algorytmie (W. G. Ringe , C. Ruof, *A Regulatory Sandbox for Robo Advice,* EBI Working Paper Series, No. 26/2018, 02/05/2018, s. 4).

[7] Gałąź technologii finansowych z zakresu usług ubezpieczeniowych.

[8] Technologia rozproszonego rejestru stanowiąca bazę danych do rejestrowania informacji (danych) zdecentralizowanych i rozproszonych.

[9] Blockchain to rodzaj DLT z określonym zestawem funkcji, która polega na tym, że bloki tworzą łańcuch (H. Arslanian, F. Fischer, *op. cit.,* s. 114).

[10] Interfejs programowania aplikacji to zestaw reguł komunikacji między aplikacjami sieciowymi a elementami oprogramowania oraz wymiany informacji pomiędzy odrębnymi systemami.

[11] Sztuczną inteligencję (ang. Artificial Intelligence, AI) definiuje się jako system informatyczny, który wykonuje funkcje wymagające ludzkich możliwości (The World Bank Group, *Global Experiences from Regulatory Sandboxes*, Finance, Competitiveness & Innovation Global Practice, Fintech Note, No. 8, 2020, s. 63).

[12] Machine learning to metoda projektowania reguł rozwiązywania problemów, które wraz ze zdobywaniem doświadczenia automatycznie się ulepszają (*Ibidem*).

[13] Policy Department for Economic, Scientific and Quality of Life Policies*, Regulatory Sandboxes and Innovation Hubs for FinTech. Impact on innovation, financial stability and supervisory convergence*, Study requested by the ECON committee, September, 2020, s. 14-15.

przestrzeń eksperymentalna wraz z jej założeniami, poszczególnymi elementami i rodzajami. W dalszej kolejności zostanie przedstawiony i opisany przebieg eksperymentu od zaprojektowania po zakończenie testów wraz ze wskazaniem działań następujących po zamknięciu procesu. Przedmiotem rozważań będzie również relacja między regulatorem a uczestnikiem *sandboxa*, jak również współpraca transgraniczna między regulatorami i nadzorcami z różnych państw oraz koncepcja europejskiej piaskownicy regulacyjnej. Rozważania zamkną wnioski podsumowujące użycie środowiska testowego jako narzędzia regulacyjnego w obszarze *fintech*.

1. DZIAŁANIA USTAWODAWCY W OBSZARZE *FINTECH*

Stanowisko ustawodawcy wobec pojawienia się innowacji finansowych na rynku w zasadzie było dwojakie. Nieprzystosowanie tradycyjnych metod w zakresie stanowienia prawa w szybko zmieniającym się środowisku technologii finansowych niejednokrotnie decydowało o przyjęciu przez legislatora postawy biernego obserwatora. Takie stanowisko zasadniczo dominowało w pierwszej dekadzie XXI stulecia. Większą inicjatywę wykazywały banki komercyjne przesiewając masowy napływ innowacyjnych rozwiązań, eliminując z rynku projekty, których wprowadzenie w życie przełożyłoby się na wzrost ryzyka kredytowego i transakcyjnego[14]. Nowe metody świadczenia usług zostały zaadaptowane przez chłonny rynek, a prawodawca w drodze następczych działań legislacyjnych próbował wpasować je w istniejące ramy prawne bądź uwzględnić w nowelizacjach ustaw dotyczących rynku finansowego. Przyjęcie w doktrynie wykładni rozszerzającej, czy stosowanie interpretacji *per analogiam* dla objęcia innowacji obowiązującymi przepisami prawa napotykało limity w fluktuacyjnym i stale zmieniającym się ekosystemie *fintech*. Kierując się nadrzędną zasadą utrzymania stabilności finansowej prawodawcy narzucali kolejne obciążenia na dostawców finansowania i ich systemy zarządzania ryzykiem, wymuszając koncentrację zasobów wewnętrznych na działania dostosowawcze celem zachowania zgodności z obowiązującymi przepisami[15]. Restrykcyjność legislatora przy częstej wewnętrznej niespójności regulacji i nieadekwatności stosowanych przepisów przez lata stanowiła trudną do przezwyciężenia barierę dla implementacji innowacji. Zamknięcie w ścisłe ramy prawne i mnogość przepisów miały zatrzymać napływ na rynek finansowy

[14] Ł. Gębski, *FinTech i FinReg – nowe wyzwania dla systemu regulacji rynku finansowego w Polsce i na świecie*, Studia z polityki publicznej, Vol. 8, No. 1/2021, s. 143.
[15] H. Arslanian, F. Fischer, *op. cit.*, s. 26.

podmiotów nieregulowanych stanowiących konkurencję dla instytucji finansowych poddanych silnemu reżimowi prawnemu i systemowi monitorowania. *Rationale* ustawodawcy koncentrowało się wokół utrzymania kontroli nad aktywnością na rynku finansowym i względnie stabilnego poziomu ryzyka systemowego. Działania *ex-post* regulatora przyjmowały formę reaktywnego nadrabiania zaległości[16] i stanowiły zasadniczy element rzeczywistości prawnej początków innowacji finansowych.

Poszczególne krajowe systemy prawne porzucały apatyczną bądź restrykcyjną postawę na rzecz innowacyjnych modeli regulowania pewnych typów transakcji i metod świadczenia usług w obszarze finansów. Otworzył się dialog pomiędzy organami nadzorczymi a przedsiębiorstwami z branży *fintech* celem wypracowania rozwiązań efektywnych, godzących partykularne interesy i minimalizujących potencjalne ryzyko dla uczestników obrotu gospodarczego. Zasada proporcjonalności rządząca procedurą *ex ante,* poprzedzającą właściwą aktywność legislacyjną, sprowadza się do odnalezienia właściwej równowagi pomiędzy ograniczeniem swobody działalności gospodarczej a zapewnieniem bezpieczeństwa systemu finansowego i ochrony grupy docelowej, w szczególności konsumentów[17]. Znaczna część regulacji unijnych dotyczących wymogów dla świadczenia usług finansowych zawiera instrumenty wpisujące się w tą zasadę, tym samym pozostawiając pewien zakres uznania organowi nadzorczemu w obszarze licencjonowania innowacji finansowych[18].

Znaczące korzyści zaczęto upatrywać w eksperymentalnym podejściu do regulacji sprowadzającym się do metody „testuj i ucz się" (ang. "test-and-learn"), polegającym na przetestowaniu innowacyjnych rozwiązań w kontrolowanym środowisku opartym na ścisłych założeniach, w sposób bezpieczny i w warunkach ograniczonego ryzyka oraz wyciąganiu wniosków na przyszłość. Empiryczny reżim prawny wyróżniają trzy istotne elementy: temporalny charakter, implementacja metody prób i błędów oraz wielowymiarowa współpraca między organami publicznymi a interesariuszami ze sfery prywatnej[19].

---

[16] I. Jenik, K. Lauer, *Regulatory Sandboxes and Financial Inclusion*, CGAP Working Paper, October 2017, Washington, s. 1.

[17] J. Koleśnik, *Piaskownica regulacyjna jako akcelerator innowacyjności w polskim systemie bankowym*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Nr 475, Problemy ekonomii, polityki ekonomicznej i finansów publicznych, 2017, s. 92.

[18] Policy Department for Economic, Scientific and Quality of Life Policies, *op. cit.*, s. 35.

[19] L. Adomavičius, F. Pop, *Sandboxes for Responsible Artificial Intelligence*, September 2021, https://www.eipa.eu/publications/briefing/sandboxes-for-responsible-artificial-intelligence/ (dostęp: 07.05.2022).

2. PIASKOWNICA REGULACYJNA JAKO ŚRODOWISKO TESTOWE

Piaskownicę regulacyjną (ang. *regulatory sandbox*) można zdefiniować jako wyseparowane środowisko przeznaczone do testowania *fintech* bez ryzyka poniesienia konsekwencji prawnych w sytuacji niepowodzenia[20]. *Sandbox* ma na celu sprawdzenie, jak innowacja zachowa się w zaprojektowanych warunkach i jakie skutki implementacji w rzeczywistości rynkowej można przewidzieć. Odpowiednie zabezpieczenie konsumentów, przejrzyste wymogi dotyczące wejścia i wyjścia, jak również wstępnie zdefiniowany zakres[21] stanowią zestaw cech składających się na bezpieczną przestrzeń o jasnych i skończonych regułach gry. Intencją organizatora środowiska jest weryfikacja założeń innowacji finansowej, a uzyskane wyniki z przeprowadzonego testu posłużą jako baza dla ustawodawcy w odpowiednim dostosowaniu otoczenia prawnego, zamknięciu *fintech* w istniejące ramy prawne bądź odrzuceniu innowacji uznanych za zbyt ryzykowne lub nieprzygotowane w wystarczającym stopniu. Pomimo, iż motywacja regulatora zasadniczo jest wspólna w różnych modelach piaskownic regulacyjnych, może zostać obrany inny punkt koncentracji w opracowaniu wirtualnego środowiska testowego. Zasadniczo wyróżniamy cztery kategorie *regulatory sandbox* zważywszy na cele przyświecające ich implementacji:

a) ukierunkowane na daną politykę bądź regulację[22], których głównym celem jest *de facto* ich ewaluacja w warunkach kontrolowanych;
b) skoncentrowane na produkcie lub innowacjach[23], polegające na obniżeniu progu wejścia na rynek celem sprowadzenia inwestorów;
c) ukierunkowane tematycznie[24], czyli zawężone do danego typu produktu, innowacji, segmentu bądź polityki, celem przyspieszenia ich implementacji i wchłonięcia przez rynek;

[20] W. Szpringer, *1. Fintech – konkurencja a regulacja na rynku usług finansowych,* [w:] *Regulacje finansowe. Fintech - nowe instrumenty finansowe – resolution*, red. W. Rogowski, C.H. Beck, 2017, s. 13.
[21] W. G. Ringe, C. Ruof, *Regulating Fintech in the EU: the Case for a Guided Sandbox*, European Journal of Risk Regulation, 11 (2020), s. 606.
[22] Do piaskownic regulacyjnych ukierunkowanych na politykę lub regulację należą, *inter alia,* Korea Południowa, Serbia i Rosja (*Key Data from Regulatory Sandboxes across the Globe*, November 1, 2020, https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes-across-the-globe (dostęp: 2.05.2022)).
[23] Do piaskownic regulacyjnych skoncentrowanych na produkcie należą, *inter alia,* Hiszpania, Tajwan, Polska czy Norwegia (*Ibidem*).
[24] Do piaskownic regulacyjnych ukierunkowanych tematycznie należą, *inter alia,* Japonia i Malezja (*Ibidem*).

d) transgraniczne i wielojurysdykcyjne[25], opierające się na współpracy regulatorów w danej grupie państw i wsparciu przedsiębiorstw prowadzących działalność w tych regionach[26].

Należy w tym miejscu wskazać, iż w niektórych państwach utworzono dwie lub więcej piaskownic regulacyjnych, a założenia części istniejących *sandboxów* opierają się na realizacji mieszanych celów[27].

Regulatory sandbox stanowi sformalizowaną platformę opartą o podstawę prawną pozostającą w zależności od zakresu ustawowego upoważnienia udzielonemu danemu organowi. Należy nadmienić, iż do rzadkości należy uchwalanie w danym państwie ustawy szczególnej zamykającej piaskownicę regulacyjną w ścisłe ramy prawne[28]. Zasadniczo instytucja publiczna w ramach swoich kompetencji określonych przepisami ogólnymi dla rynku finansowego, w tym w odesłaniu do ustawowych celów powołania, organizuje przestrzeń eksperymentalną dla podmiotów regulowanych[29]. Podmiotem uprawnionym do opracowania, zarządzania i monitorowania przestrzeni eksperymentalnej jest w głównej mierze regulator[30] lub organ nadzorczy rynku finansowego, ale kompetencje w tym zakresie mogą zostać również powierzone agencji

[25] Transgraniczna piaskownica regulacyjna prowadzona jest m.in. w Kazachstanie (*Ibidem*).
[26] The World Bank Group, *op. cit.* s. 6.
[27] W Tajlandii prowadzone są dwie piaskownice regulacyjne, z których jedna została skoncentrowana na produkcie i realizacji polityki finansowej państwa, a drugą opracowano dla przeprowadzenia testów wyłącznie w odniesieniu do danego typu produktu i innowacji (*Key Data from Regulatory Sandboxes across the Globe*, *op. cit.*). Podobnie zostały skonstruowane *sandboxy* w Indiach, Indonezji, USA, czy Hong Kongu.
[28] Jedną z pierwszych znanych jurysdykcji, w których drogą ustawową zaadaptowano piaskownicę regulacyjną była Hiszpania (J. Kálmán, *Ex Ante Regulation? The Legal Nature of the Regulatory Sandboxes or How to Regulate before Regulation even Exists*, [in:] *European Financial Law in Times of Crisis of the European Union*, eds. G. Hulkó, R. Vybíral, Budapest 2019, s. 223).
[29] *Ibidem*. Wykorzystanie ogólnych uprawnień nadzorczych w celu uruchomienia piaskownic regulacyjnych przy braku uchwalenia nowych przepisów miało miejsce m.in. w Polsce, Wielkiej Brytani, Danii, Niderlandach i na Litwie (ESMA, EBA, EIOPA, *Report. FinTech: Regulatory sandboxes and innovation hubs*, JC 2018 74, s. 19).
[30] Przykładami w tym przypadku są: Financial Services Agency w Japonii będący jednocześnie agencją rządową i regulatorem rynku finansowego oraz Australian Securities and Investment Commission (Baker McKenzie, *A Guide to regulatory fintech sandboxes across Asia Pacific,* 2017, https://www.bakermckenzie.com/-/media/files/insight/publications/2018/01/qrg_ap_regulatoryfintech_jan18.pdf (dostęp 05.05.2022), s. 4).

rządowej, bankowi centralnemu[31], a także dwóm instytucjom jednocześnie odpowiedzialnym za powodzenie projektu[32].

Zasadniczo piaskownica regulacyjna swoją inaugurację wśród trendów w obszarze rozwiązań wspierających innowacje miała w 2015 r.[33] Od tego momentu rozpoczęła się zmasowana na skalę światową implementacja eksperymentalnego podejścia *pro-futuro* w zakresie aktywności legislacyjnej w wymiarze krajowym. Za prekursora *regulatory sandbox* należy uznać bezsprzecznie Financial Conduct Authority - organ nadzorujący brytyjski rynek finansowy[34]. Zaimplementowany model posłużył innym krajowym ustawodawcom otwierającym się na innowacje jako wzór dla własnych środowisk testowych. Rok później piaskownice regulacyjne zostały uruchomione w Australii, Hong Kongu, Indonezji, Malezji, Singapurze i Tajlandii[35].

3. BUDOWA ŚRODOWISKA TESTOWEGO I PRZEBIEG EKSPERYMENTU

Piaskownica regulacyjna zasadniczo opiera się na pięciu kluczowych czynnikach, których założenia składają się na specyfikę danego *sandboxa*. Pierwsze kryterium obejmuje kwestie związane z grupą podmiotów prywatnych, które mogą zostać dopuszczone do poddania ich innowacji ewaluacji pod nadzorem instytucji państwowej. Reżim środowiska testowego zezwala na testowanie produktów następujących grup podmiotów:

a) licencjonowanych i w inny sposób autoryzowanych, które prowadzą już działalność na rynku,
b) projektantów innowacyjnych rozwiązań nieobjętych obowiązującymi regulacjami,

[31] Przykładami banków centralnych, którym powierzono tą rolę są: Bank Negara Malaysia, Indyjski Bank Rezerw, Monetary Authority of Singapore, bank centralny Litwy i bank centralny Węgier (APEC Economic Committee, *FinTech Regulatory Sandboxes Capacity Building Summary Report*, APEC Project: EC 01 2020S, March 2021, s. 24; J. Kálmán, *op. cit.*, Annex 1.).
[32] W Niderlandach zarząd piaskownicy regulacyjnej powierzono jednocześnie organowi nadzoru finansowego - Autoriteit Financiële Markten oraz bankowi centralnemu - De Nederlandsche Bank (J. J. Goo, J.-Y. Heo, *The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation*, Journal of Open Innovation: Technology, Market, and Complexity, 6(2), 43, 18 June 2020, s. 6)
[33] I. Jeník, S. Duff, *How to build a regulatory sandbox. A Practical Guide for Policy Makers*, Technical Guide, CGAP, September 2020, s. 2.
[34] K. Marchewka-Bartkowiak, *Regulacyjne środowisko testowe (regulatory sandbox) – doświadczenia i perspektywy*, Studia BAS, Nr 1 (57), Innowacje i nowe technologie w finansach, 2019, s. 64.
[35] *Ibidem*, s. 66.

c) świadczących usługi niefinansowe, a współpracujących z podmiotami regulowanymi[36].

Warunkiem zezwolenia na udział w testach jest mieszczenie się wnioskodawcy w zakresie podmiotów poddanych kontroli, nadzorowi instytucji zarządzającej środowiskiem przy braku poddania wyłącznemu reżimowi innemu organowi lub partnerstwo z podmiotem spełniającym te warunki[37]. Organ zarządzający ustala również dodatkowe kryteria wejścia, w tym odwołujące się do motywacji wnioskodawcy i podstaw zgłoszenia udziału w testach. Niejednokrotnie restrykcje w przedmiocie dostępu do oprogramowania odnoszą się do innowacyjnego charakteru samego produktu czy usługi[38]. Przedmiotowe kryteria powinny wpisywać się w zasadę sprawiedliwości i transparentności procedury składania wniosków, co w tym kontekście oznacza, że warunki wstępu powinny być jasno określone i publicznie dostępne[39].

Środowisko testowe pozwala na redukcję zasad i ograniczeń panujących w realnym otoczeniu prawnym. Wpływ przepisów odnoszących się do świadczenia danego typu usługi czy wprowadzenia innowacji na rynek w *sandboxie* zostaje zminimalizowany. Stopień poluzowania obciążeń regulacyjnych zależy w głównej mierze od regulatora i nie zawsze jest on precyzyjnie określony w założeniach środowiska testowego[40]. Elastyczność regulatora w doborze zakresu poluzowania restrykcji prawnych podlega ograniczeniu w państwach członkowskich wspólnot międzynarodowych[41]. Należy podkreślić, że wymagane jest zachowanie pewnego minimum zgodności z regulacjami wykraczającymi poza gestię organu zarządzającego. Do bezwzględnie obowiązujących przepisów należą, *inter alia,* akty normatywne w przedmiocie przeciwdziałania praniu brudnych pieniędzy i finansowaniu terroryzmu[42] oraz przepisy *ius cogens* w zakresie ochrony konsumenckiej. Wyłączeniu nie podlegają również reguły odnoszące się do działalności licencjonowanej. Jeżeli świadczenie danego rodzaju usługi lub dostawa produktu spełnia przesłanki zakwalifikowania ich jako aktywności wymagającej zezwolenia odpowiedniego organu, przedsiębiorstwo będzie zobowiązane do złożenia wniosku o

[36] I. Jeník, S. Duff, *op. cit.*, s. 13.
[37] I. Jenik, K. Lauer, *op. cit.*, s. 3.
[38] Komisja Nadzoru Finansowego w Polsce wśród kryteriów wejścia cyfrowej piaskownicy regulacyjnej wymienia innowacyjny charakter produktu, którego warunek spełnia unikalność i istotny wkład rozwiązania dla ekosystemu *fintech* (K. Marchewka-Bartkowiak, *op. cit.*, s. 70).
[39] ESMA, EBA, EIOPA, *op. cit.,* s. 45.
[40] W. G. Ringe, C. Ruof, *A Regulatory Sandbox for Robo Advice*, *op. cit.*, s. 44.
[41] *Ibidem*, s. 45.
[42] I. Jeník, S. Duff, *op. cit.*, s. 13.

jego wydanie w zwykłej procedurze autoryzacyjnej na etapie przygotowania do udziału w testach[43]. Organizator może zgodnie z prawem krajowym zostać wyposażony w kompetencje do udzielenia temporalnej lub ograniczonej w zakresie licencji[44].

Zabezpieczenie realizacji praw konsumentów wchodzi w zakres obowiązku zapewnienia w piaskownicy tak zwanych "*safeguards*", minimalizujących ryzyko dla finalnych odbiorców usług[45]. Wprowadzone przez usługodawcę/dostawcę środki ostrożności powinny obejmować spektrum obowiązków informacyjnych adekwatnych do typów ryzyka związanego z innowacją[46]. Dalsze zabezpieczenia mają charakter finansowy. W przedmiotowy zakres wchodzą: ubezpieczenie, gwarancje bankowe, celowy funduszu gwarantujący zwrot poniesionych strat w sytuacji zakończenia projektu niepowodzeniem[47].

Drugie z kluczowych kryteriów obejmuje szerokie spektrum założeń związanych z wewnętrzną strukturą, funkcjami uczestników testów oraz procesami operacyjnymi[48]. Utworzenie i zarządzanie piaskownicą regulacyjną pochłania znaczną liczbę zasobów. Suma kosztów w większości przypadków przekracza projektowe założenia piaskownicy, co związane jest z niedoszacowaniem przez regulatora potrzebnych środków na jej uruchomienie[49]. Zważywszy na zaangażowane zasoby niezwykle istotne jest dopasowanie odpowiedniego modelu zarządzania i zaprojektowanie struktury *sandboxa* służącej realizacji wyznaczonych celów i postawionych założeń. Wśród najczęściej stosowanych formuł wymienić można utworzenie jednostki dedykowanej operacjom związanym z piaskownicą bądź powierzenie zadań w tym obszarze grupie stałych pracowników przy wykorzystaniu wiedzy eksperckiej regulatora i zewnętrznych specjalistów (model "*hub-and-spoke*")[50]. W zakresie struktury regulator może sięgnąć po formę piaskownicy wirtualnej - elektronicznej platformy symulującej warunki rynkowe bądź oprzeć *sandboxa* na modelu rzeczywistym, odbywającym się bezpośrednio na rynku przy udziale konsumentów.

[43] ESMA, EBA, EIOPA, *op. cit.*, s. 29.
[44] J. Kálmán, *op. cit.*, s. 223.
[45] W. G. Ringe, C. Ruof, *A Regulatory Sandbox for Robo Advice, op. cit.,* s. 41.
[46] I. Jenik, K. Lauer, *op. cit.*, s. 3.
[47] *Ibidem*; J. Kálmán, *op. cit.*, s. 223.
[48] I. Jeník, S. Duff, *op. cit.*, 12.
[49] The World Bank Group, *op. cit.*, s. 20.
[50] Zgodnie z badaniem ankietowym przeprowadzonym przez Bank Rozrachunków Międzynarodowych najczęściej wybieranym modelem jest utworzenie specjalistycznego zespołu dla krajowej piaskownicy regulacyjnej, zaś 28 % organizatorów nie posiada dedykowanej jednostki do obsługi *sandboxa* (*Ibidem*, s. 20-21).

Zarówno rodzaje przeprowadzonych testów, jak i parametry testowania powinny zostać ściśle określone wśród zasad organizacyjnych piaskownicy regulacyjnej. Plan testów zazwyczaj stanowi element propozycji rozwiązań przedłożonych przez uczestnika przy jednoczesnym spełnieniu niezbędnego minimum określonego w regulaminie *sandboxa.* Wymogi organizatora w tym obszarze zazwyczaj przyjmują postać otwartego katalogu działań pozwalających na ocenę innowacji finansowej pod kątem typowych cech, jakie powinien zawierać produkt finansowy wprowadzany na rynek regulowany. Do obligatoryjnych pozycji należą m.in. źródła finansowania, rodzaje zabezpieczeń, czy mechanizmy zarządzania ryzykiem. Dodatkowe parametry związane ze specyficznymi rodzajami ryzyka wskazanymi we wniosku aplikanta mogą zostać narzucone przez regulatora.

Na uczestniku ciąży obowiązek przekazywania organizatorowi wyników testów w formie regularnych raportów zgodnie z ustaloną częstotliwością. W dostarczonej grupie danych powinny znaleźć się wartości obliczonych wskaźników, dane statystyczne, informacje o danych rodzajach ryzyka i zaistniałych błędach, a także o wpłynięciu reklamacji od konsumentów[51].

Szereg piaskownic regulacyjnych przy różnorodności szczegółowych rozwiązań w zakresie nadzoru można sprowadzić do dwóch najczęściej zaimplementowanych modeli. Eksperymentalny wymiar środowiska testowego może opierać się na wyłączeniu stosowania pewnych zbiorów przepisów bądź upoważnieniu organów nadzorczych, lub których zakres kompetencji jest zawężony do jednej gałęzi rynku, do wprowadzenia regulacji w specyficznej dziedzinie związanej z eksperymentem (model decentralizacji)[52]. Pierwszy model polega na wprowadzeniu ograniczonej czasowo klauzuli odstępstwa i wyróżnia się następującymi elementami:

- obiektem testów jest wysoce-innowacyjny produkt,
- kwalifikacja prawna ewaluowanego *fintech* jest niezwykle utrudniona,
- organizator *sandboxa* wymaga od uczestnika spełnienia szeregu wymogów związanych z bazą testów, limitami transakcyjnymi, zabezpieczeniem praw konsumentów etc.,
- w środowisku testowym regulacje prawne za wyjątkiem przepisów *ius cogens* podlegają ograniczonemu stosowaniu[53].

[51] Baker McKenzie, *op. cit.*, s. 9.
[52] L. Adomavičius, F. Pop, *op. cit.*
[53] G. Leimüller, S. Wasserbacher-Schwarzer, *Regulatory Sandboxes. Analytical paper for BusinessEurope*, winnovation consulting gmbh Vienna, April 2020, s. 10.

Model zdecentralizowany charakteryzuje się brakiem klauzul eksperymentalnych i ograniczeń stosowania niektórych regulacji, a działania operatora piaskownicy skoncentrowane są na klasyfikacji *fintech* bądź wybrania grupy obowiązujących przepisów, które w drodze wykładni można zastosować do obiektu badań[54].

4. ZAKOŃCZENIE TESTÓW I DALSZE DZIAŁANIA

Okres trwania testów dla uczestników standardowo mieści się w przedziale od 6 do 12 miesięcy, czas ten może być w danym przypadku wydłużony bądź skrócony[55]. Odpowiednio zakreślony przez regulatora horyzont czasowy powinien wystarczyć dla zebrania bazy danych i zgromadzenia informacji stanowiących o spełnieniu przez badane innowacje wstępnych założeń i kryteriów kwalifikujących je do wprowadzenia na rynek finansowy. Z doświadczenia wdrożonych piaskownic regulacyjnych wynika, iż rok stanowi optymalny okres dla przeanalizowania skutków zaadaptowania innowacji w środowisku finansowym. Za daleko przesunięta granica czasowa rodzi ryzyko, iż proces, który ma mieć charakter wyłącznie testu w rzeczywistości zacznie przypominać licencję produktu bez spełnienia przesłanek dla jej udzielenia[56]. Dodatkowe ryzyko związane jest z nieefektywnym wykorzystaniem dostępnych środków i zasobów.

Piaskownica regulacyjna powinna mieć ściśle określone tzw. warunki wyjścia. Organizator *sandboxa* w swoich wachlarzu instrumentów kontroli dysponuje uprawnieniem do wycofania uczestnika testów w przypadku, *inter alia,* naruszeniu zasad, niewłaściwego postępowania, przekroczenia optymalnego poziomu ryzyka, czy w wyniku niezrealizowania założonych celów pomimo upływu ustalonego okresu trwania eksperymentu[57]. Prócz przymusowych przypadków "opuszczenia" piaskownicy, przedsiębiorstwa mają możliwość

[54] *Ibidem*, s. 10.
[55] W. G. Ringe, C. Ruof, *A Regulatory Sandbox for Robo Advice, op. cit.,* s. 44.
[56] The World Bank Group, *op. cit.* s. 22.
[57] W. G. Ringe, C. Ruof, *A Regulatory Sandbox for Robo Advice, op. cit.*, s. 46. W regulaminie piaskownicy wirtualnej uruchomionej przez Komisję Nadzoru Finansowego w Polsce, organizator może podjąć decyzję o wycofaniu uczestnika w przypadku braku współpracy podmiotu z administratorem, braku rozpoczęcia testów w wyznaczonej dacie, czy zaprzestaniu spełnienia kryteriów początkowych kwalifikujących udział w środowisku testowym (Regulamin udziału w testach w środowisku Piaskownicy Wirtualnej Urzędu Komisji Nadzoru Finansowego, Załącznik do zarządzenia nr 48/2020 Przewodniczącego Komisji Nadzoru Finansowego z dnia 25 listopada 2020 r., par. 11).

wycofania się ze środowiska testowego poprzez zakończenie działalności rynkowej bądź jej przesunięcie do sfery regulowanej[58].

Po zamknięciu fazy testowej organizator piaskownicy dokonuje ostatecznej ewaluacji na podstawie raportu końcowego sporządzonego przez przedsiębiorstwo uczestniczące w projekcie bądź wyznaczonego zewnętrznego audytora[59]. Kluczowym elementem oceny jest realizacja założonych celów dla poddania innowacji testom oraz analiza wyników przeprowadzonych testów. W modelu zdecentralizowanym to uczestnik dokonuje ostatecznego podsumowania osiągnięcia postawionych założeń i na nim spoczywa decyzja o złożeniu wniosku o wydanie licencji przez organ nadzoru[60]. Zakończenie okresu testowania z wynikiem pozytywnym w formule piaskownicy opartej na klauzuli odstępstwa wiąże się z implementacją innowacji do istniejących ram prawnych bądź uchwaleniem nowych przepisów umożliwiających jej wprowadzenie na rynek regulowany[61].

Pełne korzyści związane z implementacją piaskownicy regulacyjnej widoczne są na rynkach względnie dojrzałych o dynamicznym udziale technologii finansowych, które zdążyły już trwale zaznaczyć swoją obecność. Wprowadzenie tego mechanizmu w momencie, w którym aktywność *fintech* ma charakter sporadyczny wydaje się działaniem przedwczesnym, a inne narzędzia i rozwiązania wspierające innowacje mogą przynieść lepsze rezultaty[62]. Należy w tym miejscu podkreślić, iż opracowanie środowiska testowego wymaga zaangażowania ogromnej liczby zasobów i poniesienia znaczących kosztów, co przy niszowym rynku najpewniej okaże się być działaniem w gruncie rzeczy nieopłacalnym. Przyjęty system prawny w danym państwie, czy kontynentalny, anglosaski, bądź hybrydowy stanowiący połączenie elementów obu, nie przekłada się na ostateczny rezultat związany z poddaniem innowacji finansowych testom w kontrolowanym środowisku regulacyjnym[63].

5. RELACJA REGULATOR-UCZESTNIK

Piaskownicę regulacyjną można traktować jako rozwiniętą formę interakcji strony publicznej reprezentowanej przez nadzorcę i regulatora

[58] D. Zetzsche, R. P. Buckley, D. W. Arner et al., *Regulating a Revolution From Regulatory Sandboxes to Smart Regulation*, EBI Working Paper Series, No. 11, 2017, s. 38.
[59] I. Jeník, S. Duff, *op. cit.*, s. 18.
[60] Taki model został wprowadzony przez Komisję Nadzoru Finansowego dla polskich innowacji finansowych.
[61] G. Leimüller, S. Wasserbacher-Schwarzer, *op. cit.*, s. 10.
[62] The World Bank Group, *op. cit.*, s. 9.
[63] *Ibidem*, s. 10.

z interesariuszami, do których należą w głównej mierze usługodawca/dostawca (projektant innowacji finansowej). Udział w projekcie po stronie podmiotów regulowanych mogą wziąć także dostawcy technologii, organizacje badawcze i branżowe pozostające z nimi w relacji partnerstwa[64]. Częstokroć regulator przeprowadza nabór wśród instytucji finansowych do podjęcia się funkcji operatora piaskownicy. Rolę bieżącego prowadzenia *sandboxa* pod kontrolą regulatora może pełnić również grupa podmiotów regulowanych, przykładowo, banki komercyjne. W modelu rzeczywistym zaangażowana w procesie jest także grupa finalnych odbiorców usługi w ramach ustanowionych przez organizatora limitów. Ograniczenia w zakresie udziału konsumentów polegają częstokroć na określeniu górnej granicy liczby uczestników oraz maksymalnej ekspozycji na ryzyko na jednostkę i ogół odbiorców. Finalni odbiorcy innowacyjnego produktu powinni zostać poinformowani zarówno o udziale usługodawcy/dostawcy w piaskownicy regulacyjnej, jak i ryzykach związanych z *fintech* oraz o prawie, *inter alia,* do złożenia reklamacji, czy żądania rekompensaty w przypadku poniesienia szkody z winy przedsiębiorstwa[65].

Otwarta komunikacja na linii przedsiębiorstwo *fintech* - organizator umożliwia większą swobodę w obszarze wymianie informacji, w tym dotyczącej prawdopodobieństwa wystąpienia po stronie innowacji zagrożeń. Regulator ocenia możliwości zmniejszenia nadmiarowych obciążeń regulacyjnych i włączenia na pewnym etapie do komunikacji samego ustawodawcę.

Piaskownica regulacyjna generuje obopólne korzyści. Z jednej strony nadzorca bliżej zapoznaje się z poddanym testom innowacjom finansowym ułatwiając następcze opracowanie odpowiednich mechanizmów legislacyjnych, zaś podmiot prywatny otrzymuje możliwość zredukowania potencjalnego ryzyka związanego z wymogiem zgodności z obowiązującymi przepisami i sprawdzenia oczekiwań zarówno nadzorcy, jak i prawodawcy[66]. Każda ze stron dzieli się swoją ekspertyzą i wiedzą specjalistyczną na zasadzie *quid pro quo*. Podmiot publiczny otrzymuje dostęp do bazy wiedzy z obszaru innowacji finansowej, technologii i *know-how* rynkowego w zamian za zaznajomienie uczestników z niuansami procesu legislacyjnego i stosowania prawa.

[64] IDB, *Regulatory Sandboxes and Innovation Testbeds. A Look at International Experience in Latin America and the Caribbean. Final Raport*, 2020, https://publications.iadb.org/en/regulatory-sandboxes-and-innovation-testbeds-a-look-at-international-experience-in-latin-america-and-the-caribbean , s. 13 (dostęp: 05.05.2022).

[65] ESMA, EBA, EIOPA, *op. cit.*, s. 25.

[66] Policy Department for Economic, Scientific and Quality of Life Policies*, Regulatory Sandboxes and Innovation Hubs for FinTech. Impact on innovation, financial stability and supervisory convergence*, Study requested by the ECON committee, September 2020, s. 9.

Jedną z kluczowych korzyści dla dostawcy *fintech* wynikających ze współpracy z regulatorem jest niwelacja niepewności prawnej związanej z innowacją i przygotowanie do inicjacji postępowania w przedmiocie uzyskania zezwolenia na prowadzenie działalności regulowanej.

6. PIASKOWNICE TRANSGRANICZNE I EUROPEJSKI *REGULATORY SANDBOX*

Perspektywy innowacyjnych rozwiązań regulowania ekosystemu *fintech* związane są z coraz częściej z podejmowaną współpracą transgraniczną w obszarze kreowania ram regulacyjnych drogą eksperymentu prawnego. W ostatnich latach kooperacja krajowych regulatorów koncentruje się na działaniach koordynacyjnych w przedmiocie przeprowadzenia wspólnych testów w ramach istniejących piaskownic regulacyjnych[67].

Mnogość systemów piaskownic regulacyjnych i tym samym fragmentaryczność rynku unijnego stanowi barierę dla transgranicznego prowadzenia działalności w ramach innowacyjnych rozwiązań nie wpisujących się w reżim prawny w danym państwie i jednocześnie nie uwzględnionych w prawie międzynarodowym czy wspólnotowym. W granicach Unii Europejskiej kwestia problematyczna dotyka przede wszystkim usług finansowych typu *fintech* znajdujących się poza zakresem stosowania dyrektywy MIFID II[68]. Uzyskanie zezwolenia przez usługodawcę/dostawcę do prowadzenia działalności na rynku regulowanym w wyniku pomyślnego zakończenia testów jest ograniczone do terytorium państwa organu autoryzującego. Korzyść związaną ze współpracą transgraniczną w zakresie testowania innowacji finansowych stanowi uproszczenie umów licencyjnych i wzajemne uznawanie licencji, redukując tym samym obciążenia regulacyjne przedsiębiorstw dążących do zwiększania skali działalności[69]. Skuteczna implementacja tych rozwiązań może pociągnąć za sobą wzmocnienie przez ustawodawcę unijnego dźwigni proporcjonalności i zwiększenia elastyczności w procesie udzielania zezwoleń[70].

Innym zagrożeniem jest powstanie centralnych ośrodków innowacji odciągających inwestorów od krajowych rynków niskimi kryteriami wejścia, elastycznością regulatora i dalej posuniętym luzowaniem obciążeń regulacyjnych.

---

[67] *Ibidem*, s. 47.

[68] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE.

[69] The World Bank Group, *op. cit.*, s. 10.

[70] ESMA, EBA, EIOPA, *op. cit.*, s. 36.

Wskazane zjawisko, określane jako arbitralność regulacyjna i powiązany z nim "race-to-bottom"[71], różnicuje system ochrony konsumenckiej i narusza integralność Jednolitego Rynku[72].

Największe szanse zarówno w kontekście realizacji, jak i powodzenia implementacji innowacji finansowych wykazuje model tzw. kierowanej piaskownicy regulacyjnej. Charakteryzuje się szeroką interakcją pomiędzy organami unijnymi i krajowymi organizatorami piaskownicy, powierzeniem działalności operacyjnym tym ostatnim oraz wsparciem i kontrolą na poziomie wspólnotowym[73]. Możliwym rozwiązaniem jest także utworzenie pod kontrolą Komisji Europejskiej lub unijnego organu nadzoru platformy wymiany wiedzy i doświadczeń przy odgórnym zobowiązaniu państw członkowskich do współpracy i wzajemnej koordynacji działań celem ułatwienia uznania bądź uzyskania licencji i wprowadzenia innowacyjnego produktu na rynki zagraniczne. Kolejna opcja obejmuje uchwalenie dyrektywy lub rozporządzenia w przedmiocie *fintech* o charakterze transgranicznym, wprowadzających szereg standardów w obszarze, przykładowo, planu testów, zabezpieczenia konsumentów, czy niezbędne minimum w zakresie projektowania piaskownicy dla krajowych organizatorów *sandboxów*. Najbardziej miękkie rozwiązanie polega na opracowaniu wytycznych przez europejskie organy nadzoru dla operatorów krajowych, jednakże w tym przypadku nie prowadzi to do realnego postępu w realizacji celu w postaci utworzenia jednolitego, zharmonizowanego środowiska testowego dla innowacji finansowych.

Ostatnie działania na poziomie unijnym w zakresie innowacyjnych rozwiązań regulacyjnych zostały skoncentrowane na opracowaniu ram prawnych dla utworzenia *regulatory sandboxes* dla usług i produktów wykorzystujących technologię DLT, w szczególności blockchain, i sztuczną inteligencję. W pierwszym wskazanym obszarze Komisja Europejska otworzyła przetarg, 14 marca 2022 r. zaprosiła do składania ofert podmioty, które jako wykonawcy zewnętrzni wsparłyby Komisję w koordynacji i obsłudze europejskiej

[71] Zjawisko, w którym systemy prawne konkurują między sobą o pierwsze miejsce wśród najbardziej przychylnych jurysdykcji dla firm *fintech* poprzez m.in. maksymalnie możliwie obniżanie wymogów prawnych, obciążeń regulacyjnych, minimalizacji zakresu zabezpieczeń i procesu zarządzania ryzykiem.

[72] European Banking Authority, *Discussion Paper on the EBA's approach to financial technology (FinTech),* EBA/DP/2017/02, 4 August 2017, s. 45.

[73] W. G. Ringe, C. Ruof, *Regulating Fintech in the EU: the Case for a Guided Sandbox*, *op. cit.*, s. 605.

piaskownicy regulacyjnej[74]. W tym środowisku testowym podmioty prywatne we współpracy z regulatorami unijnymi i państw członkowskich dążyłyby do wypracowania ram prawnych dla tych innowacji. W przedmiocie transgranicznego świadczenia usług i oferowania rozwiązań wykorzystujących sztuczną inteligencję, obecnie trwają prace legislacyjne nad Rozporządzeniem Parlamentu Europejskiego i Rady ustanawiającym zharmonizowane przepisy dotyczące sztucznej inteligencji[75]. Regulacja ma na celu wprowadzenie jako jedno z instrumentów prawnych wspierających innowacyjność, piaskownic regulacyjnych jako rozwiązań w zakresie regulacji tej technologii na poziomie krajowym. W projektowanym art. 53 piaskownica została zdefiniowana jako "*kontrolowane środowisko ułatwiające opracowywanie, testowanie i walidację innowacyjnych systemów sztucznej inteligencji przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem ich do użytku zgodnie z określonym planem"*[76]. Ustawodawca unijny za istotne działanie realizujące cele regulacji uznaje uchwalenie na poziomie wspólnotowym reżimu prawnego dla uruchamiania *sandboxów* oraz założeń współpracy między organizatorami krajowymi. Regulacja zakłada obowiązek krajowych organizatorów koordynacji działań i kooperacji w ramach Europejskiej Rady ds. Sztucznej Inteligencji[77].

WNIOSKI

Piaskownica regulacyjna jako eksperymentalne podejście do tworzenia reżimu prawnego dla innowacji finansowych wykazuje szereg zewnętrznych korzyści. Dla podmiotów regulowanych o długiej historii na rynku stanowi impuls do wdrożenia koniecznych w dzisiejszych warunkach przyspieszonej cyfryzacji usług finansowych, działań transformacyjnych i nastawionych na zmianę dotychczasowych modeli biznesu. Dodatkowo jako nowoczesna forma komunikacji i współpracy na linii regulator-przedsiębiorstwo-ustawodawca,

[74] European Commission, *Regulatory sandbox for blockchain and legal advice for EBSI production phase,* https://digital-strategy.ec.europa.eu/funding/regulatory-sandbox-blockchain-and-legal-advice-ebsi-production-phase (dostęp 8.05.2022).

[75] Projekt 2021/0106 (COD) został utworzony dnia 21.4.2021 r., a obecnie prace nad nim znajdują się na etapie I czytania w Radzie Unii Europejskiej (Procedure 2021/0106/COD. COM (2021) 206: Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52021PC0206. (dostęp 8.05.2022)).

[76] Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w Sprawie Sztucznej Inteligencji) i zmieniające niektóre akty ustawodawcze Unii, Bruksela, dnia 21.04.2021 r., COM(2021) 206 finał, 2021/0106 (COD), art. 53 pkt 1.

[77] *Ibidem*, art. 53 pkt 5.

stanowi wyzwanie dla legislatorów krajowych pozostających w pozycji biernego obserwatora czy zdystansowanego nadzorcy i narzuca rewizję polityki licencjonowania działalności regulowanej[78]. Dla konsumentów *fintech* stanowi uzupełnienie oferty rynkowej o innowacyjne, bardziej efektywne i często tańsze produkty przy redukcji w warunkach kontrolowanego środowiska testowego potencjalnego ryzyka związanego z innowacją. Organ nadzorczy uzyskawszy od uczestników piaskownicy wiedzę ekspercką o wykorzystywanej nowoczesnej technologii, może ją zaadaptować w procesie rozwoju nowych metod nadzoru i poprawie efektywności działań kontrolnych[79].

Z wykorzystaniem piaskownicy regulacyjnej w celu dopasowania innowacji do istniejących ram prawnych bądź opracowania nowych przepisów prawnych wiążą się również zagrożenia. Obawy dotyczą nadmiernej koncentracji ustawodawcy i organów nadzorczych na jednym obszarze rynku finansowego, gamie produktów, czy bazie podmiotów wyróżniających się stosowaniem zaawansowanych technologii. Ustalenie priorytetów przy zaniedbaniu doświadczonych usługodawców i mniej innowacyjnych modeli biznesu może zniekształcać warunki konkurencji. Kolejny rodzaj ryzyka dotyczy nadmiernej sterowalności innowacji przez legislatora i selektywnym podejściu do stanowienia prawa[80]. Priorytetyzacja celów związanych z obsługą piaskownicy regulacyjnej może doprowadzić do przesunięcia na dalszy plan realizacji pozostałych celów z obszaru nadzoru rynku finansowego.

Obawy związane z instrumentem innowacyjności, jakim jest *sandbox,* dotykają także prywatnych podmiotów. Przedsiębiorstwo przyzwyczajone do kontrolowanych warunków środowiska testowego z poluzowaniem obciążeń regulacyjnych może mieć trudności z utrzymaniem optymalnego poziomu ryzyka związanego z produktem i dalszym spełnianiem wymogów dla *fintech*. Zagrożenie to dotyka także konsumentów, którzy jako finalni odbiorcy najbardziej odczują skutki niewystarczająco skontrolowanej innowacji.

[78] D. Zetzsche, R. P. Buckley, D. W. Arner et al., *op. cit.*, s. 38-39.
[79] W. G. Ringe, C. Ruof, *A Regulatory Sandbox for Robo Advice, op. cit.*, s. 49.
[80] K. Marchewka-Bartkowiak, *op. cit.*, s. 68.

BIBLIOGRAFIA

Adomavičius L., Pop F., *Sandboxes for Responsible Artificial Intelligence*, September 2021, https://www.eipa.eu/publications/briefing/sandboxes-for-responsible-artificial-intelligence/.

APEC Economic Committee, *FinTech Regulatory Sandboxes Capacity Building Summary Report*, APEC Project: EC 01 2020S, March 2021.

Arslanian H., Fischer F., *The Future of Finance. The Impact of FinTech, AI, and Crypto on Financial Services*, Palgrave Macmillan, 2019.

Baker McKenzie, *A Guide to regulatory fintech sandboxes across Asia Pacific*, 2017, https://www.bakermckenzie.com/-/media/files/insight/publications/2018/01/qrg_ap_regulatoryfintech_jan18.pdf.

ESMA, EBA, EIOPA, *Report. FinTech: Regulatory sandboxes and innovation hubs*, JC 2018 74.

European Banking Authority, *Discussion Paper on the EBA's approach to financial technology (FinTech)*, EBA/DP/2017/02, 4 August 2017.

European Commission, *Regulatory sandbox for blockchain and legal advice for EBSI production phase,* https://digital-strategy.ec.europa.eu/funding/regulatory-sandbox-blockchain-and-legal-advice-ebsi-production-phase.

Gębski Ł., *FinTech i FinReg – nowe wyzwania dla systemu regulacji rynku finansowego w Polsce i na świecie*, Studia z polityki publicznej, Vol. 8, No. 1/2021.

Goo J. J., Heo J.-Y., *The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation*, Journal of Open Innovation: Technology, Market, and Complexity, 6(2), 43, 18 June 2020.

IDB, *Regulatory Sandboxes and Innovation Testbeds. A Look at International Experience in Latin America and the Caribbean. Final Raport*, 2020, https://publications.iadb.org/en/regulatory-sandboxes-and-innovation-testbeds-a-look-at-international-experience-in-latin-america-and-the-caribbean.

Jeník I., Duff S., *How to build a regulatory sandbox. A Practical Guide for Policy Makers*, Technical Guide, CGAP, September 2020.

Jenik I., Lauer K., *Regulatory Sandboxes and Financial Inclusion*, CGAP Working Paper, October 2017, Washington.

Kálmán J., *Ex Ante Regulation? The Legal Nature of the Regulatory Sandboxes or How to Regulate before Regulation even Exists*, [in:] *European Financial Law in Times of Crisis of the European Union*, eds. G. Hulkó, R. Vybíral, Budapest 2019, pp. 215–225.

Key Data from Regulatory Sandboxes across the Globe, November 1, 2020, https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes-across-the-globe.

Koleśnik J., *Piaskownica regulacyjna jako akcelerator innowacyjności w polskim systemie bankowym*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Nr 475, Problemy ekonomii, polityki ekonomicznej i finansów publicznych, 2017, s. 90-99.

Leimüller G., Wasserbacher-Schwarzer S., *Regulatory Sandboxes. Analytical paper for BusinessEurope*, winnovation consulting gmbh Vienna, April 2020.

Marchewka-Bartkowiak K., *Regulacyjne środowisko testowe (regulatory sandbox) – doświadczenia i perspektywy*, Studia BAS, Nr 1 (57), Innowacje i nowe technologie w finansach, 2019, s. 61 - 75.

Milic-Czerniak R., *Rola fintechów w rozwoju innowacji finansowych*, Studia BAS, Nr 1(57) 2019, s. 37–60.

Nicoletti B., *The Future of FinTech Integrating Finance and Technology in Financial Services,* Palgrave Macmillan, 2017.

Policy Department for Economic, Scientific and Quality of Life Policies*, Regulatory Sandboxes and Innovation Hubs for FinTech. Impact on innovation, financial stability and supervisory convergence*, Study requested by the ECON committee, September 2020.

Procedure 2021/0106/COD. COM (2021) 206: Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52021PC0206.

Regulamin udziału w testach w środowisku Piaskownicy Wirtualnej Urzędu Komisji Nadzoru Finansowego, Załącznik do zarządzenia nr 48/2020 Przewodniczącego Komisji Nadzoru Finansowego z dnia 25 listopada 2020 r.

Ringe W. G., Ruof C., *A Regulatory Sandbox for Robo Advice*, EBI Working Paper Series, No. 26/2018, 02/05/2018.

Ringe W. G., Ruof C., *Regulating Fintech in the EU: the Case for a Guided Sandbox*, European Journal of Risk Regulation, 11 (2020), pp. 604–629.

Szpringer W., *1. Fintech – konkurencja a regulacja na rynku usług finansowych,* [w:] *Regulacje finansowe. Fintech - nowe instrumenty finansowe – resolution*, red. W. Rogowski, C.H. Beck, 2017.

The World Bank Group, *Global Experiences from Regulatory Sandboxes*, Finance, Competitiveness & Innovation Global Practice, Fintech Note, No. 8, 2020.

Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w Sprawie Sztucznej Inteligencji) i zmieniające niektóre akty ustawodawcze Unii, Bruksela, dnia 21.4.2021 r., COM(2021) 206 final, 2021/0106 (COD).

Zetzsche D., Buckley R. P., Arner D. W. et al., *Regulating a Revolution From Regulatory Sandboxes to Smart Regulation*, EBI Working Paper Series, No. 11, 2017.

HOW WILL FINTECH COPE IN A REAL LEGAL ENVIRONMENT? REGULATORY SANDBOX SOLUTIONS AS A TEST ENVIRONMENT FOR FINANCIAL INNOVATION IN EUROPE AND THE WORLD

Abstract: The frequent changes in the landscape of innovation and financial technology are forcing today's legislator to react quickly. Adjustment of the legal system aimed at closing the legal framework and controlling the activity of new solutions on the financial market is time-consuming and constitutes a barrier to their implementation that is difficult to overcome. Tasks in the area of stabilizing the financial system and controlling money circulation imply a special caution of the state in navigating the *fintech* ecosystem, which connects the financial and technological spheres. The application of a broad interpretation, or by analogy, to cover innovation with the applicable legal regulations, encounters limitations in the case of innovative products and start-ups. At the same time, the inability to verify the solution in the regulatory environment of the market generates a risk for entrepreneurs and discourages potential investors and stakeholders from engaging their resources in their development. The visible disproportionality between the speed of digital transformation and the pace of legislative changes slows down the progress in building a modern market offer. Today's market requires regulators to take a proactive stance in supporting and creating an innovation-friendly environment on an on-going basis, especially in highly regulated areas. *Ex ante* actions in technological race are part of the state policy focused on innovation. In this article, considerations will be focused on the analysis of an experimental approach to regulation, which consists in testing financial innovation in a well-defined space and

under the control of a supervisory authority and regulator. Apart from discussing the complexity of the *fintech* ecosystem and presenting the regulatory sandbox itself, a significant part of the discourse will be devoted to the analysis of individual elements of the sandbox and the solutions introduced in this area by national regulators. The work will also address issues related to the role of the legislator and public authorities in the field of *fintech* implementation. The chances of success and the possibilities of developing and launching a central regulatory sandbox for the European Union market are another key element of the presented work.

Keywords: fintech, financial innovation, regulatory sandbox, financial market, financial technologies, test environment, legal experiment, cross-border cooperation, European regulatory sandbox.

SZYMON SKALSKI
UNIWERSYTET JAGIELLOŃSKI

ROLA SZTUCZNEJ INTELIGENCJI W INŻYNIERII SPOŁECZNEJ JAKO PODSTAWA DO OKREŚLENIA WADLIWOŚCI OŚWIADCZENIA WOLI W POSTACI BŁĘDU

Streszczenie: Celem tej pracy, jest wskazanie kluczowych zagadnień z perspektywy prawa prywatnego w perspektywie szerszego wykorzystania technologii *deepfake.* Przyjęta metodologia zakładać będzie scharakteryzowanie relewantnych zagadnień prawnych wskazywanych zarówno przez doktrynę jak i orzecznictwo i odniesienie ich do specyfiki technologicznej wykorzystania wygenerowanych przy pomocy sztucznych sieci neuronowych, fałszywych wizerunków ludzi. Pytania, na które udzielona zostanie odpowiedź w tekście opierają się na wspomnianej analizie. Dodatkowym elementem jest również uwzględnienie praktycznych przykładów wykorzystania technologii *deepfake* zarówno w kontekście prawnokarnym jak i prywatnoprawnym. Efektem tej pracy ma być analiza i ewaluacja obecnie funkcjonujących w porządku prawnym rozwiązań pod kątem efektywności. Celem regulacji wad oświadczeń woli, jest bowiem ochrona podmiotów prawa cywilnego w konkretnych stanach faktycznych. Mechanizmem, który to umożliwia jest instytucja uchylenia się od skutków wadliwie złożonego oświadczenia woli. Należy zatem udzielić odpowiedzi na pytanie, czy w stanach faktycznych, w których do manipulacji stanem wiedzy kontrahenta użyty został *deepfake,* ochrona zapewniana przez tę regulację jest wystarczająca. Poczynione zostaną również uwagi w zakresie prawa konsumenckiego i szerszej perspektywy legislacyjnej. Będą one efektem analizy społecznych i ekonomicznych skutków wykorzystania *deepfake* a w szczególności negatywnego wpływu tej technologii na szeroko pojęte zaufanie społeczne i bezpieczeństwo obrotu. Wspomniana ewaluacja ma posłużyć do stwierdzenia, czy w obecnym systemie istnieją niedające się pominąć luki, i w jakim zakresie konieczna jest interwencja unijnego i krajowego prawodawcy.

Słowa kluczowe: błąd, podstęp, *deepfake,* wady oświadczeń woli, konsument

1. KWESTIE WSTĘPNE

Praktyka kontraktowa niewątpliwie kieruje się w stronę coraz dalej idącej digitalizacji procesów zarówno zawierania, jak i wykonywania umów. Wiąże się to nierozerwalnie z przeniesieniem kolejnych sfer życia do sieci. Sytuacji konsumenta w XXI w. zdecydowanie bliżej jest do scenariusza, w którym osoba fizyczna korzystając z rozwiązań z zakresu *internet of things* (dalej „IoT"), wypowiadając słowa do swojego zegarka zawiera umowę sprzedaży cyfrowych aktywów z mieszkańcem innego kontynentu. Powoli z obrotu wypierane będą transakcje zawierane w sklepie, gdzie rozmówcą kupującego będzie fizycznie obecny sprzedawca, na rzecz rozwiązań coraz bardziej „zdigitalizowanych". Z perspektywy legislacyjnej musi się to wiązać z daleko idąca zmianą wielu regulacji, co dotyczy szczególnie perspektywy konsumenckiej oraz małych i średnich przedsiębiorców. Mniejsze podmioty wchodzące w interakcję z podmiotami z sektora BigTech [1]znajdują się w tak znaczącej dysproporcji, jak chodzi o pozycję na rynku, że kwestie ochrony ich statusu muszą być stale redefiniowane i dostosowywane. Jedną z konsekwencji digitalizacji jest zwiększone prawdopodobieństwo wykorzystania czyjegoś wizerunku, który dzięki portalom społecznościowym i cyberatakom może być łatwy do zdobycia, do celów niezgodnych z wolą osoby, której wizerunek jest wykorzystywany.

Najbardziej widowiskowym sposobem wykorzystania w ten sposób czyjegoś wizerunku jest bez wątpienia *deepfake.* O ile szczegółowa analiza tego pojęcia będzie przedmiotem dalszych rozważań wskazać można, iż chodzi tutaj o „obraz lub nagranie, które zostało przekonująco zmienione i zmanipulowane w celu fałszywego przedstawienia kogoś jako robiącego lub mówiącego coś, co w rzeczywistości nie zostało zrobione lub powiedziane"[2]. Zjawisko to z oczywistych względów budzić musi obawę, szczególnie w zakresie, w jakim dotyczy zagadnień związanych z kwestiami składania oświadczeń woli. W poniższej pracy podjęta zostanie próba rozważenia możliwości stosowania obecnie istniejących regulacji do sytuacji faktycznych, w których wykorzystany został *deepfake*. Zagadnienie omówione zostanie na podstawie trzech scenariuszy, w których technologia *deepfake* może być wykorzystana do imitowania obrazu i dźwięku w celu wywołania skutków w sferze obowiązków i uprawnień kontrahentów.

[1] https://en.wikipedia.org/wiki/Big_Tech, dostęp: 21.05.2022.
[2] https://www.merriam-webster.com/dictionary/deepfake, dostęp: 21.05.2022.

Metoda przyjęta w poniższej pracy zakładać będzie analizę przesłanek błędu i relewantnych z punktu widzenia tych rozważań sporów na gruncie regulacji błędu i podstępu w polskim prawie cywilnym. Podjęta zostanie również próba ukucia definicji *deepfake,* która pozwoli na dalszą dyskusję w sposób, który pozbawiony będzie zbędnych niedomówień. Kontynuacją tych rozważań będzie wskazanie potencjalnych stanów faktycznych, w których wykorzystanie technologii *deepfake* może oznaczać wadliwość oświadczenia woli złożonego przez którąś ze stron.

Już w tym miejscu wskazać można kluczową dla poniższej pracy ideę, jaką jest uporządkowanie dyskursu. W tym zakresie postawić należy tezę, zgodnie z którą *deepfake* jako taki nie ma na uznanie za spełnione, w dowolnym stanie faktycznym, przesłanek błędu. Jedynie wpływ tej technologii na stan wiedzy podmiotów w obrocie cywilnoprawnym będzie relewantny z perspektywy regulacji wad oświadczeń woli. Pozwoli to na pewne oderwanie się od szczegółów stojących za samą technologią i przyjęcie pragmatycznego, opartego na aspektach relewantnych prawnie, podejścia.

Omówić również, należy społeczną wagę szerszego wykorzystania technologii *deepfake*. Oświadczenie woli, w sferze społecznej jest zdarzeniem o niedającej się pominąć doniosłości[3]. W szczególności konieczne jest tutaj wprowadzenie pojęcia społecznego zaufania, które znajduje się na pograniczu prawa[4], socjologii[5] i filozofii[6]. Wskazać można na dwie potencjalne definicje zaufania w tym kontekście. Zgodnie z pierwszą wiąże się zaufanie z chęcią współpracy pomimo niepewności co do pewnych okoliczności faktycznych, zgodnie zaś z drugą wyróżnić można, w pewien sposób, wiążący charakter zaufania. Podsumować drugi nurt definicyjny można zdaniem: „Ufam ci, ponieważ twój interes pokrywa się z moim, czyli to znaczy, że masz interes w tym, aby zaspokoić moje zaufanie”[7]. Wskazać należy, że o ile definicja pierwsza ma pewne wady[8], nie można odmówić jej istotności pod kątem omawianego zagadnienia. Dla ogólno-społecznego wymiaru technologii *deepfake* szczególnie ważne będzie rozważenie kwestii swoistej kalkulacji ryzyka związanego z niepewnością. Społeczny koszt, szerszego wykorzystania technologii *deepfake* może wiązać się

[3] M. Królikowski, *Błąd jako wada oświadczenia woli strony umowy,* Wrocław 2014, s. 4.
[4] A. Frąckowiak-Adamska, *Granice wzajemnego zaufania w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości*, EPS 2014, nr 2, s. 4-19.
[5] R.C. Mayer, J.H. Davis, F.D. Schoorman, *An integrative model of organizational trust,* Academy of Management Review 1995, 20 (3), s. 709–734.
[6] N. Daukas, *Epistemic Trust and Social Location,* Episteme 2006, 3(1–2), s. 109–124.
[7] F. Herros, H. Criado *The State and the Development of Social Trust*, International Political Science Review 2008, Vol. 29, No. 1, s. 53.
[8] F. Herros, H. Criado, *ibidem*, s. 54.

w dużej mierze ze znacznym utrudnieniem oceny prawdziwości, przykładowego video, na którym uwieczniony jest człowiek.

Struktura poniższej pracy przedstawia się następująco. W pierwszej kolejności zdefiniowane zostaną kluczowe techniczne aspekty powiązane z technologią *deepfake.* O ile zgodzić się należy z tezą, że szczegóły technologiczne nie zawsze przeważać będą w dyskusjach doktrynalnych, to ważne jest, aby poznać choćby ogólne założenia wybranej technologii. Błąd w postaci zignorowania aspektów technicznych danego konceptu może prowadzić do daleko idących konsekwencji legislacyjnych i praktycznych, co daje się zaobserwować na poziomie unijnym, gdzie debata m.in. na temat definicji sztucznej inteligencji stanowi główny punkt dyskusji w procedowanym Akcie o Sztucznej Inteligencji[9]. Pozostałe części artykułu będą omawiały szczegółowe zagadnienia, jakie pojawiają się na styku technologii i przepisów o wadach oświadczenia woli. Poniższy wywód zamknie krótka refleksja o konsekwencjach płynących dla bezpieczeństwa obrotu.

Celem pracy będzie zatem kompleksowe omówienie problematyki błędu w rozumieniu cywilistycznym w kontekście rozwijających się technologii pozwalających na imitowanie dźwięku i obrazu. Nacisk położony zostanie na wyjaśnienie najistotniejszych zagadnień z perspektywy bezpieczeństwa uczestników obrotu na coraz szybciej rozwijającym się rynku nowych technologii, który w dzisiejszych czasach trudno odseparować od jakiejkolwiek gałęzi gospodarki.

2. *DEEPFAKE*

Koncepcja określana jako *deepfake* pojawiła się relatywnie niedawno. Jako jej źródło wskazać można plagę komputerowo wygenerowanych filmów pornograficznych, w których wykorzystano wizerunki znanych aktorek. Termin *deepfake* pochodzi od połączenia słów *deep,* który pochodzi od określenia *deeplearning* oraz *fake,* co nawiązuje do sztucznego, fałszywego charakteru wygenerowanych treści.

Wykorzystanie słowa *deeplearning,* skierować musi wyjaśnienia w kierunku koncepcji sztucznych sieci neuronowych. O ile uznać należy, że sam *deeplearning* stanowi bardzo szeroką kategorią rozwiązań z zakresu uczenia maszynowego często pozostających poza zakresem tego, co określamy jako *deepfake*, to tak ukształtowane nawiązanie w samej nazwie konstrukcji, utrwaliło

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, dostęp: 21.05.2022.

się już w języku i nie wydaje się możliwe doprecyzowanie tego stwierdzenia. Z perspektywy *deepfake,* kluczowe są rozwiązania technologiczne spod szyldu wspomnianych, sztucznych sieci neuronowych. Z perspektywy wywodu prawniczego wystarczy stwierdzenie, iż jest to technologia oparta na rozwiązaniach imitujących funkcjonowanie mózgu[10]. Najważniejszą cechą tej technologii, również z perspektywy deepfake jest zdolność do adaptacji, uczenia się, uogólniania i/lub grupowania lub porządkowania danych[11]. O ile uznać należy, że skutki wykorzystania *deepfake* najdalej idące konsekwencje, szczególnie społecznie, mają z perspektywy prawa karnego, to nie można wykluczyć możliwości szerszego wykorzystania tej technologii. Jednym z takich przykładów wykorzystania jest *deepfake* wykorzystany do sztucznego wygenerowania głosu CEO jednej z brytyjskich firm sektora energetycznego. Stan faktyczny wyglądał następująco:

Według raportu opublikowanego w The Wall Street Journal[12] dyrektor generalny niewymienionej z nazwy brytyjskiej firmy energetycznej wierzył, że rozmawia przez telefon ze swoim szefem, dyrektorem generalnym niemieckiej spółki matki, kiedy wykonywał polecenie natychmiastowego przelania 220 000 euro na konto bankowe węgierskiego dostawcy.

W rzeczywistości głos należał do oszusta, który wykorzystał technologię sztucznej inteligencji do podrobienia niemieckiego dyrektora generalnego. Rüdiger Kirsch z Euler Hermes Group SA, firmy ubezpieczeniowej, podzielił się tą informacją z WSJ. Wyjaśnił, że prezes rozpoznał subtelny niemiecki akcent w głosie swojego szefa, a co więcej, że głos ten przenosił "melodię" tego człowieka[13].

Powyższy stan faktyczny musi być alarmujący z perspektywy praktyki obrotu. Wraz z rozwojem technologii z zakresu sztucznej inteligencji, coraz łatwiejsze będzie generowanie wiarygodnych wizerunków osób i podejmowanie prób składania w ten sposób oświadczeń woli. Skutkiem takich działań będzie obniżenie poziomu bezpieczeństwa obrotu na niespotykanym poziomie. Skoro w obrocie cyfrowym, gdzie zawieramy ustnie umowy np. w czasie

[10] C. Woodford, *How Neural Networks Work - A Simple Introduction*, Explain that Stuff, June 17, 2020, http://www.explainthatstuff.com/introduction-to-neural-networks.html, dostęp: 20.05.2022.

[11] B. Krose, P. van der Smagt, *An Introduction to Neural Networks, November* 1996, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.18.493., dostępu: 20.05.2022.

[12] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, dostęp: 20.05.2022.

[13] https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/, dostęp: 20.05.2022.

wideokonferencji, nigdy nie będziemy mogli być pewni, czy rozmawiamy z człowiekiem, czy wygenerowanym przez sztuczną sieć neuronową obrazem.

Zarówno regulator unijny, jak i krajowy będzie musiał odpowiedzieć na pytania, stawiane przez kolejne dalece inwazyjne rozwiązanie technologiczne. Co jednak istotne i co stanowi jedną z racji napisania tej pracy, zanim rozpoczęty zostanie proces tworzenia regulacji szczegółowo regulujących kwestię *deepfake,* rozważyć należy możliwość stosowania istniejących już instytucji. Wady oświadczeń woli w tym wypadku są najbardziej naturalnym wyborem, biorąc pod uwagę okoliczności wykorzystywania wygenerowanych obrazów i głosu.

3. BŁĄD- WĘZŁOWE ZAGADNIENIA PRAWNE

Dla klarowności wywodu konieczne jest wskazanie na istotne, z perspektywy omawianego zagadnienia, elementy konstrukcji prawnej błędu w polskim prawie cywilnym. Szczególna uwaga zostanie poświęcona problematyce stosunku regulacji art., 84 k.c.[14] do art. 86 k.c. tj. regulacji błędu do podstępu. Obydwa przepisy mają duże znaczenie dla omawianego zagadnienia, szczególnie biorąc pod uwagę fakt daleko idącego skomplikowania stanów faktycznych, w których w szerokim zakresie wykorzystywane są rozwiązania z zakresu nowych technologii.

Dla porządku, wskazać można na potoczne rozumienie błędu, zgodnie z którym za błąd uznamy mylne wyobrażenie o faktach[15]. Rozumieć należy to zatem jako taki stan wiedzy/przekonania, który uznać należy wedle obiektywnych kryteriów za sprzeczny z rzeczywistością. Co istotne i warte zauważenia już w tym momencie, zaznaczyć można, iż każdorazowo, gdy podmiot, nie wiedząc czy rozmawia z człowiekiem składać będzie oświadczenie woli (nie rozstrzygając w tym miejscu czy jest to dopuszczalne) wygenerowanemu za pomocą *deepfake* obrazowi, będziemy mieli do czynienia z takiego rodzaju błędem. Jednak zarówno dla tej, jak i każdego prawniczego opracowania tej problematyki kluczowe będzie pojęcie błędu prawnie relewantnego, tak jak rozumie się go na gruncie art. 84 k.c.

Mylne wyobrażenie o rzeczywistości występować musi w chwili składania oświadczenia woli[16]. Wskazać należy, że zgodnie z ugruntowanym

[14] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2020 r. poz. 1740 z późn. zm.).
[15] R. Strugała, [w:] E. Gniewek (red.), *Komentarz do art. 84 kodeksu cywilnego*, Warszawa 2019, art. 86 nb. 4.
[16] M. Królikowski, *op.cit,* s. 130.

w polskiej doktrynie pojęciem błędu musi spełniać on trzy kluczowe przesłanki, aby zastosować można było art. 84 k.c.:

a) błąd dotyczyć musi treści czynności prawnej;
b) musi być istotny;
c) oraz musi być następstwem określonych zachowań kontrahenta.

O ile przedmiotem tej pracy, jest analiza bardzo wąskiego wycinka stanów faktycznych, do których może mieć zastosowanie regulacja błędu, to warto na wstępie wskazać na przyjmowane w doktrynie rozumienie tych przesłanek. Szczególnie istotne może okazać się to w perspektywie przesłanki trzeciej, w której mowa jest o „zachowaniu" kontrahenta. W poniższym tekście konieczne będzie udzielenie odpowiedzi na pytanie, czy możliwe jest stwierdzenie, iż o zachowaniu mówić można w sytuacji wykorzystania technologii *deepfake.*

Krótką charakterystykę przesłanek błędu rozpocząć należy, od zagadnienia ukierunkowania błędu na treść czynności prawnej. Przede wszystkim zwrócić tu uwagę należy na dalece nieostry charakter tej przesłanki[17]. Na użytek tej pracy, pominąć można rozbudowany katalog opracowań doktrynalnych tej przesłanki w zakresie tzw. motywu, który to koncept jest szeroko przez doktrynę krytykowany[18]. Szczególnie istotne z perspektywy poniższych rozważań będzie przeanalizowanie zakresu pojęcia treści czynności prawnej pod kątem elementów stanowiących część konstrukcji technicznej i koncepcyjnej *deepfake.* W obecnej doktrynie wskazuje się na konieczność wykładania tej przesłanki możliwie szeroko. Przemawia za tym szereg argumentów, zarówno historycznych, materialno-prawnych oraz procesowych. Wskazać należy tutaj na zmianę kształtu tego przepisu w stosunku do poprzednio obowiązującej regulacji Kodeksu zobowiązań[19]. Decyzja ustawodawcy o zastąpieniu pojęcia „treści oświadczenia woli" pojęciem „treści czynności prawnej" może być uznana za przejaw woli rozszerzenia możliwości stosowania tego przepisu[20]. Nie analizując dogłębnie tej argumentacji, stwierdzić należy, iż rozszerzenie tej przesłanki pozwala również na ograniczenie pewnej przypadkowości w stosowaniu tej regulacji (względy materialno-prawne) jak i pozwala lepiej

[17] M. Królikowski, *op. cit.*, s. 150.
[18] Z. Radwański, (red.), *System Prawa Prywatnego, Tom II*, Warszawa 2019, s. 398.
[19] Rozporządzenie Prezydenta Rzeczypospolitej z dnia 27 października 1933 r. Kodeks zobowiązań (Dz. U. Nr 82, poz. 598 z późn. zm.).
[20] B. Lewaszkiewicz-Petrykowska, *Wady oświadczenia woli w polskim prawie cywilnym*, Wydawnictwo Prawnicze, Warszawa 1973, s. 110.

chronić składającego oświadczenie pod wpływem błędnego przekonania o okolicznościach w danym stanie faktycznym (względy procesowe)[21].

Wskazać należy zatem, że treścią czynności prawnej jest treść stosunku prawnego powstającego w wyniku dokonania czynności prawnej, czyli prawa i obowiązki stron tego stosunku[22]. Co szczególnie interesujące z perspektywy tej pracy, przywołać należy zapatrywania doktryny w zakresie błędu co do okoliczności powiązanych z podmiotami zawierającymi umowę, wynika to z oczywiście z typowego celu, w jakim tworzone są *deepfake.*

Istotne będzie więc tutaj zauważenie, iż za błąd co do czynności prawnej uznać należy także błąd co do kwalifikacji osoby, która spełnić ma świadczenie. Taka sytuacja wystąpi, gdy osoba ta podawać się będzie przykładowo za lekarza lub prawnika, nie posiadając w tym zakresie odpowiednich uprawnień. O ile taka wykładnia art. 84 k.c. nie podlega dyskusji, zastanowić się należy, nad dalej idącymi interpretacjami.

Za M. Gutowskim przywołać należy w tym miejscu tzw. model minimum treści czynności prawnej, zgodnie z którym czynność prawna powinna określać, przynajmniej:

1. podmiot dokonujący czynności;
2. przedmiot czynności;
3. wolę wywołania określonych skutków prawnych;
4. ewentualnie inne elementy nakazane normami regulującymi dany typ czynności[23].

Uznać więc należy, że każdorazowo badając błąd co do treści czynności prawnej, rozważyć można kwestię przekonań w zakresie charakteru podmiotowego stron umowy. W orzecznictwie został również wyrażony pogląd, zgodnie z którym „[j]eżeli u podstaw konstrukcji błędu jako wady oświadczenia woli leży założenie, że stanowi on mylne wyobrażenie strony umowy (błądzącego) o rzeczywistym stanie rzeczy (nieodpowiadające rzeczywistości), to na pewno mylne wyobrażenie powoda o tym, że pozwany jest producentem danego rodzaju towaru, należy do treści czynności prawnej w rozumieniu art. 84 § 1 k.c. Odpowiedni status faktyczny lub prawny partnera umowy może bowiem przesadzać o jej treści i konsekwencjach prawnych”[24].

[21] M. Królikowski, *op.cit*, s. 154.
[22] P. Sobolewski, *Art. 84 KC,* red. K. Osajda, W. Borysiak, 2021.
[23] M. Gutowski, *Kodeks cywilny. Tom I. Komentarz do art. 84 KC*, 2021, Legalis, nb. 11.
[24] Wyrok SN z 6.04.2017 r., IV CSK 371/16, LEX nr 2312227.

Jako ostatnie przywołać można najogólniej ujęte stanowisko, zgodnie z którym błąd dotyczyć może osoby kontrahenta *vel* strony czynności prawnej[25]. Podsumowując zatem powyższe rozważania, stwierdzić należy, iż kryterium podmiotowe przy badaniu treści czynności prawnej pod kątem błędu, występuje i może stanowić podstawę do uznania tej przesłanki stosowania art. 84 k.c. za spełnioną. Oczywistym jest jednak to, iż każdorazowo w danym stanie faktycznym konieczne będzie przeanalizowanie, czy ta przesłanka została spełniona. Jest to szczególnie istotne przy rozwiązaniach nowatorskich z perspektywy praktyki obrotu, jakim bez wątpienia jest *deepfake.*

Kolejną przesłanką błędu, którą należy uszczegółowić pod kątem przeprowadzanych w tej pracy rozważań, jest istotność błędu. Już w tym miejscu powiedzieć można, że ta przesłanka również stanowić może pole do interesujących rozważań na gruncie stanu faktycznego, w którym jedna ze stron korzysta z rozwiązania technologicznego w postaci *deepfake.* Szczególnie ważne będzie przeanalizowanie często przyjmowanego w doktrynie poglądu w zakresie dualnego charakteru tej przesłanki[26]. Dualny charakter zakłada wyróżnienie przesłanki subiektywnej i obiektywnej. Przesłankę subiektywną, sprowadzić można do pytania, czy w konkretnym stanie faktycznym *errans* zawarłby umowę o istniejącej treści, gdyby nie był w błędzie. Przesłanka obiektywna zakłada analizę stanu faktycznego pod kątem zachowania modelowego uczestnika obrotu i kieruje się tym samym kryterium co przesłanka subiektywna. Na gruncie tego opracowania, przyjęty zostanie pogląd o relewantności przesłanki subiektywnej na gruncie obecnej regulacji, aczkolwiek wskazać można na pewne głosy krytyczne w tym zakresie[27].

Trzecią przesłanką, stosowania art. 84 k.c. jest konieczność powiązania błędu po stronie jednej ze stron z zachowaniem kontrahenta. Wskazać można dla porządku, że w ramach tej pracy pozostawiona bez szerszej analizy pozostanie kwestia odpłatności jako przesłanki stosowania regulacji art. 84 k.c., problemy i spory doktrynalne pojawiające się na gruncie tej przesłanki, nie są bowiem (na ogół) relewantne z perspektywy wykorzystania technologii *deepfake*. Dla metodologii przyjętej w tej pracy najbardziej wartościowym sposobem analizy tej przesłanki będzie wyliczenie stanów faktycznych, co do których zgodzić się należy, iż mówić będziemy o zachowaniu kontrahenta wywołującym błąd. Pozwoli to w dalszej części pracy w sposób systematyczny

[25] Z. Radwański, *op. cit.*, s. 395; J. Strzebinczyk, [w:] E. Gniewek, P. Machnikowski, *Komentarz KC*, 2016, s. 234.
[26] M. Królikowski, *op.cit*, s. 64.
[27] Tak np. B. Lewaszkiewicz-Petrykowska, *Wady*, s. 115.

skorzystać z tak stworzonej matrycy do oceny hipotetycznych stanów faktycznych pod kątem dopuszczalności stosowania regulacji art. 84 k.c.

1) Po pierwsze wskazać można na najbardziej intuicyjną formę wywołania błędu przeze kontrahenta, jaką jest złożenie fałszywego zapewnienia[28]. Scharakteryzować można tę okoliczność jako taki przekaz informacji pomiędzy kontrahentami, który wywołuje u jednej ze stron błędne przeświadczenie co do rzeczywistego stanu rzeczy. Odnosząc już w tym miejscu zagadnienie fałszywego zapewnienia do *deepfake*, stwierdzić należy, że zakwalifikowanie takiego stanu faktycznego z perspektywy art. 84 k.c. jest dalece problematyczne. W szczególności wskazać należy tutaj na konieczność klaryfikacji pewnych zagadnień technologicznych i uwzględnienia konkretnego stanu faktycznego co zostanie uczynione w dalszej części analizy.

2) Wskazać można również na konieczność stosowania testu *sine qua non* do oceny. Ta przesłanka w kontekście zdigitalizowanego obrotu nabiera szczególnego znaczenia, jako że w dobie szumu informacyjnego utrudniającego ustalenie dokładnego stanu wiedzy na daną chwilę, może okazać się problematyczne stwierdzenie, czy konkretne zapewnienie było w danym momencie fałszywe.

3) Co istotne szczególnie w kontekście *deepfake* fałszywe zapewnienie nie musi być elementem inicjującym powstanie błędnego przekonania po stronie jednego z kontrahentów. Przyjąć należy, że może również stanowić element utwierdzenia kontrahenta w błędnym przekonaniu. Podobne rozumowanie uznać należy za właściwe, również co do wykorzystania osoby trzeciej do przekazania fałszywej informacji. Z perspektywy rozważań przedstawionych w tej pracy dodać można również, iż nie będzie miało tym bardziej znaczenia skorzystanie z algorytmu. Pozwala na to w pewnym zakresie zastosowanie rozumowania *a maiori ad minus.* Skoro bowiem dopuszczamy zakwalifikowanie jako okoliczności spełniającej tę przesłankę sytuacji, w której kontrahent posługuje się osobą trzecią do wywołania błędu u *erransa,* tym bardziej powinniśmy uznać za możliwe na gruncie tej przesłanki, posłużenie się algorytmem sztucznej inteligencji, czy szeroko pojętym *deepfake* do wywołania błędu.

Powyższe, skrótowe omówienie przesłanek błędu stanowi wprowadzenie do problematyki omówionej w dalszej części pracy. Celem tego wyliczenia było wskazanie istotnych problemów i zarysowanie pola do dalszych rozważań, nie zaś kompleksowe omówienie tej problematyki.

[28] M. Królikowski, *op.cit*, s. 64.

4. PODSTĘP

Zagadnieniem, które powiązać należy z problematyką błędu, jest niewątpliwie regulacja art. 86 k.c. Zgodzić się należy z poglądem wyrażanym w orzecznictwie i przyjmowanym przez doktrynę, zgodnie z którym podstęp stanowi szczególną, kwalifikowaną formę błędu[29]. Stwierdzić należy, że szczególnie w przypadku analizy prowadzonej w sposób taki jak w poniższej pracy, każdorazowo należy przeanalizować, czy jeżeli rozważamy stosowanie przepisów o błędzie, to czy w danym stanie faktycznym, nie byłoby możliwe uznanie zachowania stron za spełniające przesłanki podstępu.

Należy więc przywołać przesłanki stosowania art. 86 k.c. Po pierwsze wskazać można na pewną dwoistość w rozumieniu podstępu. Wskazuje się bowiem w doktrynie na wewnętrzny (mentalny, psychiczny) aspekt podstępu oraz zewnętrzny (materialny) pod postacią określonego zachowania[30].

Dla dalszych rozważań kluczowe będzie stwierdzenie, iż błąd wywołany podstępnie pozwala na skorzystanie z ochrony przewidzianej przez ustawodawcę dla wadliwie złożonych oświadczeń woli, a właściwie *erransa* nawet jeśli nie zostaną spełnione przesłanki istotności i treści.

Na użytek definicji w tym opracowaniu przywołać można stwierdzenie Sądu Najwyższego, zgodnie z którym, „Kodeks cywilny nie zawiera definicji podstępu, o którym mowa w art. 86 k.c., dlatego należy kierować się potocznym znaczeniem tego pojęcia. Powszechnie przyjmuje się, że działanie podstępne polega na świadomym wywołaniu u drugiej osoby mylnego wyobrażenia o rzeczywistym stanie rzeczy po to, aby skłonić ją do dokonania określonej czynności prawnej. Działanie podstępne jest zawsze naganne z punktu widzenia ocen etycznych, gdyż zakłóca w niedopuszczalny sposób proces decyzyjny innej osoby, doprowadzając tę osobę na podstawie zasugerowanych jej fałszywych przesłanek rozumowania do dokonania określonej czynności prawnej”[31].

5. *DEEPFAKE JAKO STRONA UMOWY*

W tym momencie powinno wydawać się oczywiste, że główną płaszczyzną interpretacyjną dla większości stanów faktycznych, w których wykorzystywany jest *deepfake,* musi być analizowana z perspektywy błędu co do osoby. Wskazać również należy, że istnieje istotna różnica pomiędzy dotychczas

[29] Postanowienie SN z 18.04.2013 r., II CSK 497/12, LEX nr 1324270.
[30] P. Sobolewski, *op. cit.*
[31] Wyrok SN z 9.09.2004 r., II CK 498/03, LEX nr 137573.

analizowanymi w orzecznictwie przypadkami[32] a kazusem wykorzystania *deepfake* do wywołania błędnego przekonania o rzeczywistości po stronie *erransa.*

Przypomnieć można wskazaną powyżej metodologię, zgodnie z którą konkretny przypadek wykorzystania omawianej technologii przeanalizować należy z perspektywy przesłanek błędu i podstępu. Wpierw jednak warto doprecyzować stan faktyczny będący przedmiotem zainteresowania. Warta przywołania będzie tutaj sytuacja, w której jedna ze stron wykorzystuje technologię *deepfake,* tj. generuje obraz i dźwięk innej osoby w taki sposób, aby wywołać błędne przekonanie po stronie swojego kontrahenta. Jako przykład można tu podać sytuację, gdy podajemy się za znaną drugiej stronie osobę w rozmowie telefonicznej lub w czasie wideokonferencji. Celem takiego działania, może być zawarcie umowy sprzedaży samochodu za uprzednią wpłatą określonej kwoty na rachunek kontrahenta korzystającego z *deepfake.*

Kluczową kwestią jest tutaj określenie, czy dochodzi w powyższym stanie faktycznym do zawarcia umowy, a jeśli tak to kto będzie uznany za jej stronę. Wydaje się, że z perspektywy klasycznej triady, jaką wykorzystuje się do analizy umowy tj. zawarcie, ważność i skuteczność brak tutaj dalej idących problemów. Problematyczne jest jednak tutaj określenie, kto będzie stroną takiej umowy. Strona korzystająca z *deepfake* posługuje się nim w celu złożenia oświadczenia woli, sam algorytm nie ma żadnych „aspiracji" do uznania go za samodzielny podmiot zdolny do bycia stroną złożenia w danej sytuacji skutecznego oświadczenia woli. Rozważyć należy w ramach zbiorczej kategorii imitowania za pomocą *deepfake* strony umowy następujący stan faktyczny. Możliwa bowiem jest sytuacja, w której ktoś generując *deepfake* ma na celu zawarcie umowy, co do której wie, że druga strona nie zawarłaby jej z nim bez wpłynięcia na jej stan wiedzy. Jako przykład można podać tutaj podszywanie się pod wykwalifikowanego pracownika takiego jak: inżynier, lekarz, prawnik czy broker ubezpieczeniowy. Co jednak istotne, uznać należy, że nie ma w takiej sytuacji mowy o konsensie, a w konsekwencji niedopuszczalne byłoby twierdzenie, że w ogóle zawarta została umowa. Brak bowiem jakichkolwiek podstaw do twierdzenia, iż zakresem zgodnego oświadczenia woli objęte może być zawarcie umowy z inną osoba niż ta, której tożsamość objęta jest naszą wiedzą w momencie składania tego oświadczenia.

[32] Zob. Uchwała SN z 23.09.1992 r., III CZP 105/92, PPH 1993, nr 7, poz. 16; Wyrok SN z 10.12.2004 r., III CK 40/04, LEX nr 399725; Wyrok SN z 9.06.2006 r., IV CSK 169/05, LEX nr 187058.

Wskazać należy, że jeśli przyjmiemy powyżej przedstawione stanowisko brak jest również podstaw do stosowania art. 86 k.c. Podstęp, o ile jak podkreślono powyżej jest kwalifikowaną formą błędu, nie może być wykorzystywany jako podstawa do uznania wadliwości określonego oświadczenia woli w sytuacji, gdy do czynności prawnej w ogóle nie dochodzi. Jak bowiem zostało wskazane w powyższej argumentacji, w tak ukształtowanym stanie faktycznym trudno jest mówić o konsensie, *ergo* o dokonaniu czynności prawnej w postaci umowy.

6. *DEEPFAKE* JAKO ELEMENT UWIARYGADNIAJĄCY

Równie istotnym stanem faktycznym, jest wykorzystanie *deepfake* do wpłynięcia na stan wiedzy kontrahenta w inny sposób niż podszywanie się pod określoną osobę. Źródłem tego przykładu jest konstatacja, zgodnie z którą na fakt zawarcia lub niezawarcia określonej umowy może mieć wpływ wiele czynników zarówno wewnętrznych, jak i zewnętrznych. Jednym z tych czynników, szczególnie istotnym z perspektywy kalkulacji kosztu zawarcia i wykonania umowy, jest przekonanie o pewnych cechach przedmiotu umowy. Najprostszym przykładem jest umowa sprzedaży określonej rzeczy ruchomej, co do której jedna ze stron nie ma kwalifikacji do oceny jej parametrów, zaś druga nie posiada cech, którymi mogłaby przekonać drugą stronę o prawdziwości swoich zapewnień. Strona wykorzystująca technologię *deepfake* może wygenerować obraz i głos znanego drugiej stronie eksperta w tej dziedzinie, który wypowiadać się może pochlebnie o określonym produkcie. W ten sposób, doprowadzić może do zmiany w przekonaniach drugiej strony w stopniu tak znacznym, że umowa zostanie zawarta.

Podejmując się analizy tego stanu faktycznego przez pryzmat przesłanek błędu, wskazać można na kilka interesujących, niespotykanych w dotychczasowych opracowaniach aspektów.

1) Przede wszystkim należy zauważyć, że rozpatrując tę sytuację pod kątem błędu co do treści czynności prawnej, ocena nie nastręcza dużych problemów. Wskazać należy, że skoro *deepfake* został wykorzystany do zmiany postrzegania cech danej rzeczy, która jest przedmiotem umowy oraz przyjmujemy założenie, iż owo zapewnienie jest fałszywe, to powiązanie błędu z treścią czynności prawnej będzie w powyższym stanie oczywiste. Powtórzyć można również, za poglądem przyjmowanym w doktrynie, że *deepfake* może zostać wykorzystany nie tylko do stworzenia błędnego przekonania, ale również

do jego pogłębienia, w sytuacji, gdy błędne przeświadczenie po stronie *erransa* już istnieje[33].

2) W zakresie istotności błędu przywołać należy ponownie dualny charakter tej przesłanki. Zgodnie ze wskazanymi powyżej poglądami doktryny wskazać należy na przesłankę subiektywną i obiektywną. Przesłanką subiektywną istotności błędu jest fakt, iż okoliczność, której dotyczy błąd, jest czynnikiem decydującym w procesie podejmowania decyzji o złożeniu określonego oświadczenia woli. Uznać należy, że gdy wygenerowany wizerunek, ma na celu zmianę określonego przekonania o przedmiocie umowy po stronie kontrahenta, to co do zasady przesłanka subiektywna istotności błędu będzie spełniona w większości stanów faktycznych. W ramach przesłanki obiektywnej stwierdzić należy, czy z perspektywy rozsądnego uczestnika obrotu umowa taka nie powinna zostać zawarta. Co do zasady uznać należy, że o ile zapewnienie składane za pomocą *deepfake* jest fałszywe, to przesłanka ta zostanie zrealizowana. Tym samym uznać należy, że w większości przypadków spełnione zostaną również przesłanki istotności błędu.

3) Ostatnią ze wskazywanych na początku pracy przesłanek jest powiązanie powstania błędnego przekonania u jednej ze stron z zachowaniem kontrahenta. Przesłanka ta na pierwszy rzut oka wydawać się może problematyczna. Jeżeli bowiem spojrzeć na całą sytuację z pewnego oddalenia to łatwo ulec wrażeniu, iż to nie kontrahent składa fałszywe zapewnienie a algorytm, za pomocą którego wygenerowany został *deepfake.* Taka ocena stanu faktycznego byłaby jednak błędna. Wydaje się, że biorąc pod uwagę obecny etap zaawansowania algorytmów, ciężko jest mówić o tak daleko idącym zakresie autonomiczności, który pozwoliłby na tak swobodne funkcjonowanie algorytmu w obrocie. Dużo bliższe prawdzie będzie uznanie, iż posługiwanie się przez jedną ze stron algorytmem do wywołania u *erransa* błędnego przekonania, jest przejawem działania tej strony.

Tym samym stwierdzić należy, że powyższy stan faktyczny jest kluczowy z perspektywy oceny zjawiska *deepfake* przez pryzmat wad oświadczeń woli. O ile w pierwszym przytoczonym przykładzie, dalece utrudnione będzie doszukiwanie się możliwości zastosowania ochrony, jaką daje instytucja uchylenia się od skutków wadliwie złożonego oświadczenia woli, to w drugim przytoczonym kazusie takich wątpliwości jest już dużo mniej. Wydaje się, że dopóki *deepfake* nie zostanie wykorzystany do podszywania się pod określoną osobę, *ergo* nie będzie mogło być mowy o stosunku zobowiązaniowym,

[33] M. Królikowski, *op.cit*, s. 171.

to ochrona w postaci wad oświadczeń woli i możliwości skorzystania z uprawnienia przyznanego w art. 88 k.c. stanowi wystarczające źródło ochrony dla podmiotów funkcjonujących w obrocie.

Wskazać można dodatkowo, iż w przedstawionym stanie faktycznym skorzystanie z art. 86 k.c. nie powinno stanowić problemu. Konieczne będzie jedynie każdorazowe wykazanie podstępnego charakteru działania drugiej strony. Odwołując się do definicji przywołanej we wcześniejszych rozważaniach, zauważyć w tym miejscu można jedynie, że ciężko wyobrazić sobie stan faktyczny, w którym ktoś korzysta z *deepfake* w sposób nieświadomy. Choć w nielicznych stanach faktycznych prawdopodobnie można by analizować kwestie świadomości w zakresie wywoływania błędnego przekonania. Nie ma to jednak dużego znaczenia z perspektywy teoretycznej, w tym miejscu wystarczająca będzie uwaga o możliwości skorzystania, w większości stanów faktycznych, również z regulacji art. 86 k.c. jako podstawy do uchylenia się od skutków wadliwie złożonego oświadczenia woli.

7. BEZPIECZEŃSTWO OBROTU

Dla kompletności wywodu rozważyć należy również kazus, w którym podmiot posługuje się technologią *deepfake* do wywołania błędnego przekonania u bliżej nieokreślonej grupy osób. Wygenerowane obrazy znanych lekarzy mogą skutecznie zachęcić rzesze konsumentów do zakupu szkodliwych suplementów, zaś wzbudzający zaufanie członek elity finansowej ma duże szanse na kontrolowanie zainteresowania określonymi instrumentami finansowymi na rynku. Zatem wykorzystanie *deepfake* do podszycia się pod taką osobę i publiczne złożenie fałszywych zapewnień może być metodą na uzyskanie dużych korzyści majątkowych z tego tytułu. W tym miejscu wskazać można, iż poza zakresem tego opracowania pozostaje kwestia kwalifikowania takich praktyk z perspektywy prawa karnego.

Wskazać można również, iż zgodnie z rozważaniami wskazanymi powyżej wiele sytuacji, w których wykorzystywany jest *deepfake* nie będzie podlegało ocenie z perspektywy wad oświadczeń woli. W szczególności zwrócić należy tutaj uwagę, na kazusy wykorzystania tej technologii w sposób niepowiązany lub powiązany w niewielkim stopniu z dokonywaną czynnością. Ta uwaga, będzie relewantna szczególnie w sytuacji, gdy podmiot niepowiązany ze stroną transakcji wygenerował *deepfake,* który wpłynął na stan wiedzy drugiej strony. Możliwe będzie jednak tutaj, po analizie przesłanek tego przepisu, stosowanie regulacji art. 86 par. 2 k.c.

Przyjąć należy, że z perspektywy pojedynczej transakcji możliwe będzie co do zasady wykorzystanie uwag wskazanych powyżej w zakresie dwóch przywołanych stanów faktycznych. Osobnego rozważenia wymaga jednak zagadnienia szerszego kontekstu bezpieczeństwa obrotu a w szczególności tzw. zbiorowego interesu konsumentów.

Ponownie podkreślić należy skalę problemu, jaki może spowodować upowszechnienie się stosowania rozwiązań *deepfake* w obrocie. Prawdopodobieństwo przekonania uczestnika obrotu do niekorzystnego rozporządzenia swoim majątkiem wskutek fałszywego zapewnienia złożonego za pomocą algorytmu jest bardzo duże. Wynika ono przede wszystkim z wszechstronności tej technologii i możliwości, jakie ona daje. Najbardziej przemawiającym do szerokiej publiki przykładem jest generowanie wizerunków osób znanych. Jednak z perspektywy biznesu, wskazać można na zagrożenie podszywania się pod ekspertów w danej branży, a także właścicieli korporacji czy innych znaczących podmiotów rynkowych. W tym zakresie wskazać należy, że ochrona zapewniana przez analizowane reguły prawa prywatnego może okazać się niewystarczająca, szczególnie, jeśli uwzględnimy szerszy kontekst gospodarczy. Biorąc pod uwagę obecne „trendy" regulacyjne na poziomie unijnym, spodziewać się można w przyszłości doprecyzowania tej kwestii na poziomie regulacyjnym przez unijnego regulatora.

Na ten moment wskazać można jedynie na reguły związane z praktykami naruszającymi zbiorowy interes konsumentów. Ustawodawca definiuje praktyki naruszające zbiorowy interes konsumentów w art. 24 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów[34]. Wskazuje się na dwa składniki tej regulacji: klauzulę generalną i przykładowe wyliczenie czterech grup praktyk[35]. Za sprzeczne z klauzulą generalną uznaje się bezprawne lub sprzeczne z dobrymi obyczajami działanie przedsiębiorcy godzące w zbiorowe interesy konsumentów. Wyliczenie grup praktyk obejmuje na ten moment: naruszanie obowiązku udzielania konsumentom rzetelnej, prawdziwej i pełnej informacji, nieuczciwe praktyki rynkowe lub czyny nieuczciwej konkurencji oraz proponowanie konsumentom nabycia usług finansowych, które nie odpowiadają potrzebom tych konsumentów ustalonym z uwzględnieniem dostępnych przedsiębiorcy informacji w zakresie cech tych konsumentów lub proponowanie nabycia tych usług w sposób nieadekwatny do ich charakteru.

[34] Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2021 r. poz. 275).

[35] A. Wędrychowska-Karpińska, A. Wiercińska-Krużewska, [w:] *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, wyd. II, red. A. Stawicki, E. Stawicki, Warszawa 2016, art. 24.

Za wskazaniami doktryny stwierdzić należy zatem, że zakaz wspomnianych praktyk odnosi się do sytuacji, gdy:

a) praktyka jest działaniem lub zaniechaniem przedsiębiorcy,
b) praktyka jest sprzeczna z prawem

lub

c) praktyka jest sprzeczna z dobrymi obyczajami,
d) praktyka godzi w zbiorowy interes konsumentów[36].

Na gruncie tego opracowania, brak jest miejsca do szczegółowej i rozbudowanej analizy wpływu technologii *deepfake* na sytuację ogólnospołeczną i ekonomiczną z perspektywy konsumentów. Wskazać jednak należy, iż szerokie wykorzystanie tego rodzaju rozwiązań do wprowadzania w błąd grup odbiorców, którzy spełniają definicję konsumenta, stanowiłoby z dużym prawdopodobieństwem zarówno praktykę sprzeczną z dobrymi obyczajami, jak i godzącą w zbiorowy interes konsumentów. Wskazać bowiem można, iż zgodnie z szeroko rozumianymi dobrymi obyczajami obrotu gospodarczego, wprowadzanie kontrahentów w błąd na szeroką skalę przy użyciu nowatorskich rozwiązań technologicznych, często nieznanych szerszej grupie odbiorców, stanowi jawne naruszenie takich zasad. Mówić tu można prawdopodobnie zarówno o regułach uczciwości kupieckiej, jak i szeroko rozumianej dbałości o podwyższanie wspólnego poziomu bezpieczeństwa. Takie praktyki, jeśli ich celem będzie doprowadzanie do niekorzystnego rozporządzania majątkiem, w oczywisty sposób naruszać będą również ekonomiczny interes konsumentów.

Stwierdzić można również, że prawdopodobnie takie praktyki uznane zostałyby za sprzeczne z prawem. Nie można jednak odgórnie założyć sprzeczności z prawem każdego rozwiązania opartego na *deepfake*. Prowadzić by to mogło do absurdalnych wniosków, szczególnie w świetle wielu przykładów wykorzystania tej technologii w sytuacjach, w których ciężko doszukiwać się złych intencji[37].

[36] Ibidem.
[37] https://www.knowledgenile.com/blogs/applications-of-deepfake-technology-positives-and-dangers/, dostęp: 22.05.2022.

8. KONKLUZJE

Podsumowując, stwierdzić należy, że *deepfake* już teraz stanowi wyzwanie dla unijnego i krajowego porządku prawnego. Kluczowa jednak w tym aspekcie jest perspektywa nadchodzących lat. Wraz z rozwojem sztucznej inteligencji, a w szczególności sztucznych sieci neuronowych, zakres i możliwości wykorzystania rozwiązań stanowiących temat tej pracy jedynie wzrosną. Porządki prawne muszą przygotować się na czynniki technologiczne, które mogą prowadzić nie tylko do obniżenia zaufania społecznego i bezpieczeństwa obrotu, ale do całkowitej destabilizacji systemów.

Celem tej pracy było zbadanie użyteczności ochrony, jaką ustawodawca przewidział dla przypadków złożenia wadliwego oświadczenia woli w perspektywie rozpowszechnienia się technologii *deepfake.* Skonkludować należy, po przeanalizowanie potencjalnych stanów faktycznych, iż ochrona ta, przynajmniej w jakiejś części, może być uznana za wystarczającą.

Wnioski z przeprowadzonej analizy poprowadzić można dwutorowo. Z jednej strony powiedzieć można jasno, że wykorzystanie *deepfake* do wpłynięcia na stan wiedzy *erransa* w sposób, który powoduje powstanie błędnego przekonania o rzeczywistości, będzie podlegał ochronie na podstawie istniejących regulacji[38]. Z drugiej zaś strony stwierdzić należy, że szerszy kontekst społeczny i gospodarczy rysuje się zdecydowanie mniej optymistycznie. Konieczne jest w tym zakresie odniesienie się ustawodawcy unijnego i krajowego do wskazanych w tej i innych pracach zagadnień, aby zapewnić zadowalający poziom ochrony zarówno konsumentów jak i wszystkich uczestników obrotu.

BIBLIOGRAFIA

Daukas N., *Epistemic Trust and Social Location,* Episteme 2006, 3(1–2).

Frąckowiak-Adamska A., *Granice wzajemnego zaufania w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości*, EPS 2014, nr 2.

Gutowski M., *Kodeks cywilny. Tom I. Komentarz do art. 84 KC*, 2021.

Herros F., Criado H., *The State and the Development of Social Trust*, International Political Science Review 2008, Vol. 29, No. 1.

[38] Ibidem.

Krose B., van der Smagt P., *An Introduction to Neural Networks*, November 1996.

Królikowski M., *Błąd jako wada oświadczenia woli strony umowy,* Wrocław 2014.

Lewaszkiewicz-Petrykowska B., *Wady oświadczenia woli w polskim prawie cywilnym,* Wydawnictwo Prawnicze, Warszawa, 1973.

Mayer R.C., Davis J.H., Schoorman F.D., *An integrative model of organizational trust,* Academy of Management Review 1995, 20(3).

Radwański Z. (red.), *System Prawa Prywatnego, Tom II*, Warszawa 2019.

Sobolewski P., *Art. 84 KC,* red. K. Osajda, W. Borysiak 2021.

Strugała R., [w:] E. Gniewek (red.), *Komentarz do art. 84 kodeksu cywilnego*, Warszawa 2019.

Woodford C., *How Neural Networks Work - A Simple Introduction, Explain that Stuff*, June 17, 2020.

Wędrychowska-Karpińska A., Wiercińska-Krużewska A., [w:] *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, wyd. II, red. A. Stawicki, E. Stawicki, Warszawa 2016.

Ziobroń A., *Deepfake a prawo karne. Uwagi de lege lata i de lege ferenda dotyczące fałszywej pornografii* [w:] *Wyzwania dla państwa prawa i gospodarki w dobie pandemii*, Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne 2021, Tom 37.

Źródła internetowe:

https://www.knowledgenile.com/blogs/applications-of-deepfake-technology-positives-and-dangers/, dostęp: 22.05.2022.

https://en.wikipedia.org/wiki/Big_Tech, dostęp: 21.05.2022.

https://www.merriam-webster.com/dictionary/deepfake, dostęp: 21.05.2022.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, dostęp: 21.05.2022.

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, dostęp: 20.05.2022.

https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/, dostęp: 20.05.2022.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN SOCIAL ENGINEERING AS A BASIS FOR DETERMINING THE DEFECTIVENESS OF A STATEMENT OF INTENT IN THE FORM OF AN ERROR

Abstract: The purpose of this work is to identify key issues from the perspective of private law in the wider use of deepfake technology. The adopted methodology will assume the characterization of relevant legal issues indicated both by doctrine and jurisprudence and relating them to the technological specifics of using false images of people generated with the help of artificial neural networks. The questions which will be answered in the text are based on the above mentioned analysis. An additional element is also the inclusion of practical examples of the use of deepfake technology both in the criminal and private law context. The result of this work is to analyze and evaluate the current solutions in the legal order in terms of their effectiveness. The purpose of regulating defects in declarations of will is to protect civil law entities in specific factual situations. A mechanism that makes it possible is the institution of evading the effects of a defectively made declaration of will. Therefore, it is necessary to answer the question whether in factual situations, in which deepfake was used to manipulate the state of knowledge of the contracting party, the protection provided by this regulation is sufficient. Observations will also be made with regard to consumer law and the broader legislative perspective. They will be the result of analysis of social and economic consequences of the use of deepfake, in particular the negative impact of this technology on the broader public trust an+d security of trade. This evaluation will be used to determine whether there are any unavoidable gaps in the current system and to what extent the EU and national legislators need to intervene.

Key words: error, deceit, deepfake, defect in declaration of intent, consumer

IZABELLA BEDNARZ
UNIWERSYTET WARSZAWSKI

CODE IS LAW, CZYLI ANALIZA PRAWNA *SMART CONTRACTS*

Abstrakt: Artykuł stanowi zwięzłą analizę prawną pojęcia smart kontraktu w polskim porządku prawnym z odwołaniem się do kultury prawnej common law. W pierwszej części o charakterze wprowadzającym omówione zostaną pojęcia w kolejności od najbardziej ogólnego, czyli blockchainu, do meritum artykułu, czyli smart kontraktu. Zamierzam pokrótce przedstawić czym jest blockchain, jaki jest jego cel oraz zastosowania, jak możemy go sklasyfikować i jaki ma związek z omawianym przez nas tematem. Kolejnym punktem wprowadzenia będzie przedstawienie platformy Ethereum oraz jej związku z koncepcją smart contracts. Przytoczone zostaną również związany z tą dziedziną język programowania Solidity, choć ze względu na tematykę i krąg odbiorców, bez głębszej analizy. Chciałabym również wyróżnić typy smart kontraktów, szczególnie zwracając uwagę na DAO, czyli decentralized autonomous organization. W ten sposób zamierzam pokazać różnorodność oraz możliwości technologii, jaką jest smart kontrakt. Po zagadnieniach wstępnych nastąpi płynne przejście do drugiej, analitycznej, a nie opisowej, części opracowania. Będzie to analiza smart kontraktów na gruncie prawa polskiego. Ową analizę zamierzam rozpocząć od klasyfikacji samego smart kontraktu. Będzie to wyjście od polskiej próby zdefiniowania zagadnienia. Kolejnym krokiem będzie próba zestawienia polskiego rozumienia umowy ze smart kontraktem. Zamierzam przytoczyć kilka istniejących w doktrynie argumentów, jednak przede wszystkim skupić się na smart kontrakcie jako sposobie zawarcia umowy oraz wiążących się z tym ograniczeń. Nierozłączne z taką analizą będzie uwzględnienie pojęcia czynności prawnej. Następnie zostanie omówiona zależność pomiędzy smart kontraktem a wzorcem umownym. Dalsza analiza będzie systematycznie zgodna z procesem zawierania i wykonania umowy. Zacznie się ona od wykładni smart kontraktu w kontekście oświadczenia woli. Omówiona zostanie także problematyka związana z samowykonalnością oraz niezmienialnością smart kontraktu. W podsumowaniu zawarte zostaną wnioski co do obecnego statusu prawnego smart kontraktów w polskim porządku prawnym, a także pokrótce możliwości, jaką ten typ kontraktu ze sobą niesie. Zostanie również rozstrzygnięte to, jak pojęcie *Code is law* ma się do rzeczywistości.

Słowa kluczowe: blockchain, DAO, ethereum, inteligentny kontrakt, oświadczenie woli, prawo nowych technologii, smart kontrakt, technologia rozproszonego rejestru, umowa, wzorzec umowy.

1. *IS CODE LAW*?[1]

Zarówno w literaturze prawniczej, jak i tej ze świata nowych technologii spotykamy się z pytaniem: czy kod komputerowy może zastąpić prawo? *Is Code Law*? Już w 1998 roku twórca hasła "Code is law", Lawrence Lessig zauważył jedną istotną analogię pomiędzy tymi dwoma światami, kodem i prawem. Jest to ich zdolność kreacyjna, regulacyjna. Można powiedzieć, że prawo również jest kodem, kreującym stosunki społeczne. Nic więc dziwnego, że pojawił się pomysł połączenia tych dwóch, opornych dotychczas na współpracę, dziedzin. Pojawiła się nawet koncepcja wyparcia prawa przez jurysdykcję cyfrową, na ten moment jednak nie trzeba się tego obawiać. Niniejsze opracowanie w wystarczający sposób pokaże, że świat nie jest jeszcze gotowy na rezygnację z prawa, które to nie powinno stanowić przeszkody, a wręcz przeciwnie, powinno być instrumentem stopniowo cyfryzującym rzeczywistość.

Jednym z takich narzędzi, stopniowo cyfryzujących naszą rzeczywistość, jest smart kontrakt. Niniejszy artykuł stanowi szczegółową jego analizę, opierając się głównie na polskim porządku prawnym, ale też nawiązując do innych jurysdykcji. Podejście komparatystyczne wydaje się bowiem konieczne w przypadku stosunkowo nowych instytucji oraz w obliczu globalizacji stosunków handlowych. Celem artykułu jest lepsze zrozumienie smart kontraktu przez prawników, a w tym celu konieczne jest odpowiednie wprowadzenie, uwzględniające czynniki technologiczne.

Nowe technologie stanowią nie lada wyzwanie dla prawników. Dzieje się tak ze względu na specyfikę obu tych nauk, tj. prawa i nowych technologii, cechujących się rozwiniętą terminologią i kompleksowością. Regulacja prawna w zakresie nowych technologii wymaga analizy tych zjawisk, a literatura nie została jeszcze w pełni rozwinięta na potrzeby wprowadzenia w nowy, choć popularny temat. Powoli jednak się to zmienia, dlatego też pozwolę sobie przytoczyć, w mojej ocenie przystępne, zagadnienia podstawowe dotyczące *blockchainu* jako zjawiska, przed wprowadzeniem w temat niniejszego opracowania, tj. smart kontraktów.

2. BLOCKCHAIN

Blockchain, a dawniej w literaturze *block chain* pisane oddzielnie, już etymologicznie opisuje nam swoją naturę. Tłumacząc termin dosłownie,

[1] Nazwa artykułu autorstwa Tian Ma, https://legal-tech.blog/is-code-la dostęp: 06.06.2022.

jest to "łańcuch bloków", które to określenie było podejmowane w polskiej praktyce, jednak nie zwalczyło swojego angielskiego pierwowzoru i raczej nie jest obecnie spotykane w nomenklaturze. Jest zaś powszechnie stosowane w próbach definicji samego *blockchainu*.

Taką na przykład definicję proponuje Krzysztof Piech[2]: "to rozproszona baza danych, która zawiera stale rosnącą ilość informacji (rekordów) pogrupowanych w bloki i powiązanych ze sobą w taki sposób, że każdy następny blok zawiera oznaczenie czasu (timestamp), kiedy został stworzony oraz link do poprzedniego bloku, będący zaszyfrowanym "streszczeniem" (hash) jego zawartości".

Wyjaśnienia wymaga termin *hash,* czy też w wersji spolszczonej *hasz*. Autor proponuje tutaj "krótki ciąg znaków przyporządkowany do dowolnie dużego zbioru danych za pomocą funkcji mieszającej (haszującej)". Do zapisu wykorzystano przy tym system szesnastkowy, o wiele bardziej czytelny dla człowieka niż układ binarny. Hashe cechują się odpornością na kolizję (zmiany kodu) i jednokierunkowością, oznaczającą, iż nie istnieje możliwość poznania danych jedynie na podstawie samej wartości skrótu. Pozyskiwanie nowych hashów jest widoczne w przypadku tzw. "kopalni bitcoinów". Kryptowaluta bitcoin zapoczątkowała zresztą zainteresowanie blockchainem, jednak krzywdzące jest ograniczanie tego zjawiska wyłącznie do pieniądza cyfrowego. By lepiej zrozumieć zastosowanie tej technologii, należy poznać jej naturę.

2.2 Cechy *blockchainu*

Za cechę immanentną blockchainu przyjmuje się jego nierozerwalność - dokonanie jakiejkolwiek zmiany w zapisach historycznych jest możliwe tylko przy zmianie całej historii transakcji. Pojawiła się wprawdzie koncepcja korygowalnych blockchainów, czego przykładem jest blockchain firmy Accenture. Takie rozwiązanie nie wywołuje jednak entuzjazmu środowiska. Wskazuje się w takim wypadku na konieczność wystąpienia zaufanej osoby trzeciej, co kłóci się z ideą blockchainu. Blockchain opiera się bowiem na braku centralnej instytucji uwierzytelniającej (ang. trusted third party), którą w obrocie są banki. Owa "samodzielność" polega na zasadzie *peer-to-peer* (P2P), czyli "modelu komunikacji w sieci komputerowej, w której zadania rozdzielona są pomiędzy równe sobie pod względem uprawnień osoby (węzły)".

[2] K. Piech, *Leksykon pojęć na temat technologii blockchain i kryptowalut*, s. 5.

Kolejną, związaną z P2P, cechą modelu jest jego decentralizacja, czy inaczej technologia rozproszonego rejestru lub w wersji angielskiej DLT (*Distributed ledger technologies*). Blockchain umożliwia globalny zasięg swoich transakcji. Oczywiście skala, z jakiej korzystać można z decentralizacji jest zależna od modelu blockchainu, który przyjmiemy.

Wszystkie powyższe cechy są możliwe dzięki zaufaniu opartemu nie na zasobach ludzkich, a na kryptografii. Wszelkie transakcje są weryfikowane przed dodaniem do łańcucha bloków, a następnie zabezpieczane kodem. O bezpieczeństwo dbają kolektywnie wszyscy użytkownicy przy zachowaniu anonimowości i transparentności danych. Taki zabieg w zasadzie uniemożliwia ataki hackerskie, gdyż wymagałoby to włamanie do każdego bloku w danym łańcuchu.

2.3 Klasyfikacja *blockchainu*

W kontekście blockchainu zaczyna mówić się o ładzie (governance). Dzieje się tak, gdyż otwarty system poza możliwościami powoduje także zagrożenia, w tym kumulacji zasobów. Nie wszędzie pożądana jest również anonimowość. W związku z tym mówi się o wyodrębnieniu dwóch modeli blockchainu, czyli publicznego i prywatnego.

Anonimowość, umożliwiona przez daleko idącą kryptografię, jest wykorzystywana przez model publiczny. Można tu mówić o klasycznym i znanym w praktyce blockchainie, np. tym wykorzystywanym przy kryptowalutach. Pozwala on na analizę i zawieranie transakcji wszystkim zainteresowanym w ramach sieci.

Model ten nie sprawdzi się jednak, gdzie ze względu na sytuację gospodarczą, zaufanie pomiędzy kontrahentami jest niezbędne *a priori*. Taką możliwość daje nam model prywatny, polegający na odpowiednim zarządzaniu prywatnością. Jest najczęściej tworzony przez konsorcja oraz ustalone grupy uczestników.

Wyróżnia się również podział ze względu na licencjonowanie blockchainów[3] oraz różne warianty związane z obiema tymi klasyfikacjami. Możemy na przykład wyobrazić sobie sytuację, w której ograniczenie podmiotów zachodzi tylko co do ich typów, ale nie jest weryfikowany (lub weryfikacja ta jest znacznie ograniczona) indywidualnie. Jest to model publiczno-licencjonowany.

[3] K. Ciupa, *Warianty zastosowania koncepcji blockchain a modele ich doboru,* Studia i prace. Kolegium zarządzania i finansów. Zeszyt naukowy 173/2019 s. 89-110.

Te różnice będą miały istotny wpływ na ochronę danych i wymienione wyżej cechy blockchainu. W najbardziej surowym wydaniu, czyli takim, w którym nie ma wyjątków dla nierozerwalności, P2P, decentralizacji czy kryptografii, mówimy o pełnym modelu publicznym. Rezygnacja ze stężenia którejkolwiek z podanych cech prowadzi nas do wyboru alternatywnego modelu blockchainu.

3. ETHEREUM

Możliwości kodu programistycznego poszerzają się przy każdym projekcie. Kod ten może przewidywać wszystko, co jest w stanie objąć język programowania. Dzięki temu blockchain znajduje rozmaite zastosowania. Na tym tle wyróżnia się Ethereum, czyli platforma, która wystartowała w 2015 r. Jej fenomen opiera się na umożliwieniu użytkownikom (programistom) tworzenie własnych aplikacji, w tym *smart kontraktów*. W tym celu stworzono nawet specjalnie język programowania o nazwie Solidity, który służyć ma właśnie do tworzenia umów. Na ten moment jest on ciągle najpopularniejszym językiem programowania przeznaczonym do tego celu, jednak wciąż powstają nowe, takie jak Serpent, LLL czy Vyper.

Platforma Ethereum to ogromny mechanizm (EVM - Ethereum Virtual Machine), który udostępnia środowisko wykonywania kodu, gdzie posługujemy się nie tylko odrębnymi językami programowania, ale też walutą (ETH - ether) oraz koncepcją paliwa (gas), czyli "surowca", który ogranicza ilość zawieranych transakcji, tak aby zablokować uruchomienie pętli[4]. Łańcuch bloków, podobnie jak w przypadku m.in. bitcoina, jest jawny.

4. DAO

DAO (Decentralised Autonomous Organisation) jest to niematerialna forma organizacji, realizowana poprzez użycie smart kontraktu, która jest w stanie realizować swoje cele za pomocą kodu programistycznego. Omówienie jej w tej części opracowania nie jest przypadkowe, gdyż po pierwsze koncepcja ta jest związana z rozwojem i reformacją platformy Ethereum, a po drugie pokazuje potencjał inteligentnych kontraktów, jak i możliwości (oraz ryzyka) samego DAO.

[4] Więcej na ten temat: G. Wood, *Ethereum: A secure decentralised generalised transaction ledger,* https://ethereum.github.io/yellowpaper/paper.pdf dostęp: 06.06.2022.

DAO mogą być tworzone dla różnych celów, najczęściej ekonomicznych. Upodabnia je to do spółek handlowych. Dzieje się tak, gdyż celem takiej formy organizacji jest zrealizowanie przedsięwzięcia przez grupę osób. Ze względu na wielość podmiotów, DAO jest znacznie bardziej skomplikowane niż typowe, pierwotne smart kontrakty. Co więcej DAO mogą być otwarte na nowe podmioty. Od zwykłej spółki odróżnia je natomiast "pewność kodu", czyli zaufanie oparte na szyfrowaniu. Jacek Czarnecki wyróżnia podmioty biorące udział w transakcji DAO[5]:

- posiadacze tokenów, którzy mogą mieć wpływ na działania DAO oraz czerpać z nich zyski, podobni do znanych nam ze spółek kapitałowych akcjonariuszy;
- autorzy kodu, czyli znawcy konstrukcji, którzy niekoniecznie muszą angażować się w implementację DAO;
- regulatorzy, czyli zainteresowane instytucje publiczne, szczególnie kontrolne;
- kontraktorzy, czyli osoby, które wchodzą w kooperację z DAO;
- wyrocznie (oracles), które to dostarczają różnego rodzaju dane ze świata zewnętrznego;
- inni, tj. platforma i jej twórcy, kuratorzy, itp.

Należy jednak podkreślić, iż na ten moment prawo polskie nie wyposaża DAO w zdolność prawną, co znacznie ogranicza kompetencje takiego tworu wobec spółek handlowych, a szczególnie spółek kapitałowych. Transakcje zawierane przez DAO w naszej rzeczywistości prawnej będą bowiem transakcjami zawieranymi bezpośrednio przez jego członków. Rodzi to konieczność transparentności, co po pierwsze mija się z celem DAO, a po drugie może być niemożliwe do osiągnięcia przez wielość podmiotów. Na ten moment najrozsądniejsze wydaje się funkcjonalne połączenie DAO z rzeczywistą spółką handlową. W przyszłości jednak prawdopodobnie pojawi się konieczność uregulowania DAO, żeby ta mogła spełniać swoją funkcję, wyposażając użytkowników w szeroką gamę możliwości.

Problem braku regulacji nie jest niestety jedynym ryzykiem związanym z DAO. Reprezentatywna dla tej formy organizacja o nazwie The DAO niechlubnie zasłynęła dokonanym na niej atakiem hakerskim w 2016 roku,

[5] J. Czarnecki, *Czym są inteligentne kontrakty i DAO*, [w:] *Blockchain, inteligentne kontrakty i DAO*, 2016, https://wardynski.com.pl/publikacje/opracowania/blockchain-inteligentne-kontrakty-i-dao, dostęp: 06.06.2022.

w wyniku którego z platformy wypłynęły środki o wartości 50 milionów dolarów. Hakerzy wykorzystali tzw. furtkę w kodzie, której nie dostrzegli sami twórcy platformy. W związku ze specyfiką samego DAO, jak i szerzej pojętego smart kontraktu, pojawiło się pytanie, czy takie działanie jest w ogóle bezprawne. Smart kontrakty nie mogą być przecież sfałszowane i nie podlegają kontroli instytucjonalnej, są autonomiczne. Tak też argumentuje swoje działanie sam Napastnik (The attacker) w liście otwartym do społeczności Ethereum, zawierając w nim zresztą zwięzłą analizę prawną[6].

Taka interpretacja nie spodobała się oczywiście użytkownikom platformy. Działanie hakera zostało po części odwrócone poprzez stworzenie nowego blockchaina, zawierającego modyfikację The DAO, która miała przywrócić stan poprzedni, tak jakby atak nigdy się nie wydarzył. Na takie rozwiązanie zgodziło się 90% użytkowników, w efekcie czego funkcjonują obok siebie dwie sieci, jednak waluta starego (oryginalnego) blockchainu reprezentuje znacznie mniejszą wartość[7]. Działanie to było w gruncie rzeczy powtórzeniem działania Napastnika. Nasuwa to wątpliwości co do autonomicznego charakteru The DAO, gdyż w gruncie rzeczy zgodzono się na społeczną kontrolę instytucji. Pokazuje to przywiązanie społeczeństwa do idei słuszności, w kontraście do zaufania "nieomylnym" algorytmom.

Oczywiście takiej sytuacji dało się uniknąć już na momencie programowania platformy. Należy jednak pamiętać, że autorem kodu jest człowiek, który nie jest w stanie przewidzieć wszystkich możliwości oprogramowania. Podobnie zresztą działa prawo, gdyż ustawodawca nie jest w stanie przewidzieć wszystkich skutków wprowadzanej przez siebie regulacji. Nie zawsze jest to jednak proste. Co ważne, pomimo załamania zaufania do DAO, wcale nie zmalała ich popularność. Z sytuacji wyciągnięto wnioski, które przyczyniły się do ulepszenia mechanizmu. Być może zbyt szybko chciano wprowadzić tak rozbudowaną instytucję, nie przewidując błędów, a dopiero ucząc się na nich. Nie należy jednak zniechęcać się przez to do samych smart kontraktów.

5. SMART KONTRAKT

W celach niniejszego opracowania przyjęty został termin zapożyczony z angielskiego, tj. smart kontrakt (*smart contract*), chociaż w literaturze

[6] List w języku angielskim: https://pastebin.com/CcGUBgDG dostęp: 04.06.2022 r.
[7] Więcej na ten temat: A. Kraińska, *Co historia The DAO mówi o prawie,* [w:] *Blockchain, inteligentne kontrakty i DAO*, 2016, https://wardynski.com.pl/publikacje/opracowania/blockchain-inteligentne-kontrakty-i-dao dostęp na dzień 06.06.2022.

spotykane są jak najbardziej typowo polskie odpowiedniki jak inteligentna umowa, czy lingwistyczny kompromis, tj. inteligentny kontrakt.

Autorem pojęcia (*smart contract*) jest Nick Szabo, który koncepcję smart kontraktu przedstawił już w 1997 r[8]. Jako prototyp nowej instytucji podaje on automaty sprzedające (*vending-machine*). Smart kontrakty miałyby się jednak, w przeciwieństwie do nich, opierać na blockchainie. Wśród cech charakterystycznych N. Szabo wymienia także algorytmiczny charakter w postaci kodu programistycznego, zabezpieczenie (najczęściej kryptograficzne), a przede wszystkim samowykonalność, automatyzm i autonomia, które to mają zapewnić oszczędność czasu oraz zasobów ludzkich. Zbudowaną na tej podstawie definicję smart kontraktu należy traktować jako idealną i docelową postać. Na przestrzeni lat, również w efekcie praktyki, pojawiły się jednak różne przeszkody w tak dosłownym rozumieniu smart kontraktu, między innymi wskazany wyżej atak hakerski na The DAO, który niejako wymusił odejście od zasady autonomii. Należy również dodać, iż blockchain nie jest obecnie jedyną (choć pozostaje najbardziej popularną) opcją zastosowania smart kontraktu.

Kompromisową w mojej opinii definicję wprowadziło ustawodawstwo Malty, według którego smart kontrakt jest porozumieniem technologicznym, składającym się z protokołu komputerowego lub z umowy zawartej w całości lub części w elektronicznej formie, która jest możliwa do zautomatyzowania oraz egzekwowania przez kod komputerowy, pomimo, że niektóre elementy mogą wymagać ingerencji człowieka i jego kontroli, a które mogą być egzekwowane zwykłymi metodami prawnymi lub poprzez zmieszanie obu tych metod[9]. Jest to bardzo praktyczne, choć również niepokojąco szerokie pojęcie smart kontraktu, co skłania nas wobec kolejnych zagadnień, a mianowicie szerokiego i wąskiego pojęcia smart kontraktu.

Wąskie rozumienie jest rozumieniem jak najbardziej zbliżonym do pierwowzoru wskazanego przez N. Szabo. Wszystkie cechy są przy tym rozumiane ściśle, tzn., że nie ma miejsca na dopuszczanie osób trzecich, a wywołane skutki są nieodwracalne. Możemy sobie wyobrazić funkcjonowanie takich kontraktów w przypadku umów krótkoterminowych, dyskretnych. Zbyt daleko idące będzie jednak definiowanie tym sposobem smart kontraktu w przypadku umów skomplikowanych, długoterminowych, a tym bardziej

[8] N. Szabo, *Smart Contract: Formalizing and Securing Relationships on Public Networks,* https://firstmonday.org/ojs/index.php/fm/article/view/548/469, dostęp: 06.06.2022.

[9] *Chapter 590 Virtual Financial Assets*, 1st November, 2018, https://legislation.mt/eli/cap/590/eng/pdf dostęp: 06.06.2022.

w przypadku organizacji (czego przykład widzieliśmy już wyżej). Na tym etapie najbezpieczniejsze byłoby jednak stosowanie definicji szerszej, np. takiej jak w ustawodawstwie maltańskim. Należy jednak uważać, by definicja nie była też zbyt szeroka, gdyż wtedy traci na znaczeniu cała innowacyjność smart kontraktu. Nie powinniśmy na przykład ograniczać definicji do jej elektronicznego charakteru (czego przykładem byłyby zakupy przez internet), czy automatyzmu (funkcjonującego w przypadku automatów sprzedających).

Klasyfikacja blockchainu wiąże się bezpośrednio z możliwościami różnicowania smart kontraktów. Możemy wyróżnić bowiem smart kontrakt publiczny i prywatny. W związku z tym pozostają inne cechy, jak globalizacja kontraktu (jego otwartość na kontrahentów), jego anonimowość czy prawo właściwe do jego stosowania. Ze względu na naturę *blockchainu*, który nadal pozostaje główną metodą zapisywania smart kontraktów, nie powinniśmy ograniczać się do jego wąskiej definicji, a wręcz przeciwnie, powinniśmy skupić się na jej elastyczności, pamiętając przy tym o możliwościach, jakie daje nam sam *blockchain*.

5.1 Czy smart kontrakt jest umową?

Jedną z podstawowych kwestii na gruncie prawa polskiego jest rozstrzygnięcie pytania, czy smart kontrakt jest umową. Właściwsze byłoby może jednak opisanie stosunku pomiędzy umową a smart kontraktem, gdyż zrównanie ich wynika raczej z błędnej wykładni językowej w połączeniu z anglosaskim pochodzeniem.

W związku z tym zagadnieniem powstały dwie koncepcje: monistyczna, utożsamiająca smart kontrakt z umową cywilnoprawną oraz dualistyczna, rozdzielająca oba te pojęcia. Należy podkreślić, że rozumienie smart kontraktu jako umowy będzie inaczej rozpatrywane na gruncie różnych porządków prawnych. Możemy sobie wyobrazić utożsamianie umowy ze smart kontraktem na gruncie common law, wydaje się to jednak nieakceptowalne w naszej kulturze prawnej. Przypomnijmy, że umowa to zgodne oświadczenia woli stron wywołania określonych skutków prawnych[10]. Istota smart kontraktu nie polega jednak na jego treści. Smart kontrakt staje się smart kontraktem w momencie, gdy kod już jest ustalony, natomiast treść umowy, czyli owe zgodne oświadczenia woli są ustalane wcześniej. Innymi słowy, kod jest ustalany pod treść umowy, jest subsydiarny. Możemy sobie wyobrazić, że kod

[10] A. Wolter, J. Ignatowicz, K. Stefaniuk, *Prawo cywilne. Zarys części ogólnej*, Warszawa 2018.

może być wprawdzie stworzony wcześniej, ale to strony decydują się na jego zastosowanie poprzez zgodne oświadczenia woli. Treść kodu programistycznego powinna się przy tym pokrywać z treścią zawartej umowy. Takie rozumienie smart kontraktu jest oczywiście nie samą umową, a jej formą, dokumentem czy instrumentem egzekwującym jej treść. Możemy sobie wprawdzie wyobrazić sytuację, w której smart kontrakt zaczyna niejako "żyć własnym życiem", jednak nigdy nie będzie to oderwane od kodu, którego treść ustaliły strony lub na którą się zgodziły. Wybór formy zawarcia umowy jest przy tym jednym z przejawów swobody umów (art. 353 Kodeksu Cywilnego).

Podsumowując, możemy nazwać smart kontrakt umową w takim samym zakresie, w jakim umową nazywamy podpisaną przez strony kartkę papieru uzgadniającą treść stosunku prawnego. Sam smart kontrakt nie jest jednak umową w rozumieniu Kodeksu Cywilnego i nie powinien być z nią utożsamiany w takiej formie, z jaką aktualnie się spotykamy.

Rozwiązaniem, które idealnie wpasowuje się w nasze rozważania jest model kontraktu ricardiańskiego (*Ricardian contract*), wymyślony przez Iana Grigga. Polega on na stworzeniu dokumentu, który jednocześnie zawiera treść w języku prawniczym oraz te same postanowienia zapisane w języku programowania. Taki zabieg eliminuje ryzyko niezrozumienia kodu programowego przez zwykłego człowieka będącego kontrahentem. Model ricardiański może wprawdzie być zastosowany w przypadku smart kontraktu, jednak nie zawsze będą to pojęcia tożsame. Szczególnie przy wąskim rozumieniu smart kontraktu, kontrakt ricardiański będzie rozumiany raczej jako jego przystępniejsza alternatywa[11].

Na drodze dokonanych definicji i analizy należałoby również dopuścić możliwość dokonania jednostronnej czynności prawnej za pomocą smart kontraktu. Niestety ten przypadek to kolejny dowód tego, jak bardzo nazwa ta może być myląca. Nie wydaje się jednak, by wielość podmiotów była cechą konstytutywną smart kontraktu, a należałoby się tutaj skupić na jego samowykonalności, niezmienialności i automatyzmie. Możnaby na przykład wyobrazić sobie samowykonalny testament. Być może przy spopularyzowaniu takich rozwiązań należałoby pomyśleć o zmianie nomenklatury lub stworzyć termin odrębny.

[11] Takie stanowisko wyraża: https://learn.bybit.com/defi/how-are-ricardian-contracts-different-from-smart-contracts/?fbclid=IwAR1goahtyQzqEY-2Wym5fmwm1I6v6JBxuHPmgR7r4CV9kSNVmZ_XJV56K-0, dostęp: 06.06.2022.

5.2 Smart kontrakt jako wzorzec umowny

Specyfika smart kontraktu, a także jego specjalistyczny język w postaci kodu programistycznego sprawia, że forma ta stanowi idealny materiał na wzorzec umowny, przez który rozumie się "klauzulę umowną (zbiór klauzul), która została przygotowana z góry na użytek przyszłych umów, opracowana jednostronnie przez podmiot zamierzający wzorzec stosować"[12]. Bardzo często w przypadku umów zawieranych przez użycie wzorca umownego, stroną, która pozostaje bez wpływu na treść jest konsument. Ze względu na jego status, ale również ze względu na możliwość nadużyć przez zastosowanie wzorca umownego, przysługuje mu spora ochrona. Jej konieczność jest dodatkowo widoczna w specjalistycznym języku smart kontraktu, niezrozumiałego dla przeciętnego człowieka.

Ochrona konsumenta opiera się na szeregu przepisów. Po pierwsze będzie to art. 384 k.c., zgodnie z którym konsument jest związany tylko tymi postanowieniami wzorca umownego, o których został przez przedsiębiorcę poinformowany przed zawarciem umowy, pod warunkiem, że przedmiot umowy nie należy do drobnych, bieżących spraw życia codziennego. Na przedsiębiorcy spoczywa więc obowiązek wytłumaczenia skutków, jakie niesie za sobą dany kontrakt.

Po drugie, przedsiębiorcę ogranicza zakaz zastosowania niedozwolonych klauzul umownych, czyli postanowień nieuzgodnionych indywidualnie z konsumentem, jeżeli kształtują one jego prawa i obowiązki w sposób sprzeczny z dobrymi obyczajami, rażąco naruszając jego interesy. Przepis ten nie będzie jednak dotyczył jednoznacznie sformułowanych postanowień określających główne świadczenie stron.

Dalsze elementy ochrony pojawią się na etapie wykonania lub wygaśnięcia umowy (pkt 4.4.).

5.3 Oświadczenie woli

Wiemy już, że oświadczenie woli nie jest elementem samego smart kontraktu, a raczej elementem zewnętrznym. Jego charakter nie pozostaje jednak bez znaczenia przy wykładni smart kontraktu już na etapie jego wykonania

[12] K. Pietrzykowski, *Kodeks cywilny. Tom I. Komentarz do art. 1-449*, C.H. Beck, Warszawa 2020.

(które ma charakter samodzielny), a tym bardziej w przypadku ewentualnego błędu w kodzie programistycznym.

Należałoby zacząć od kwestii elementarnej, a mianowicie tego, że przyjęta obecnie koncepcja oświadczenia woli w Kodeksie Cywilnym przemawia za przejawem, a nie aktem woli, którego uznanie ujawnia się tak naprawdę tylko jako jeden z czynników mogących czynność unieważnić (mowa tutaj o błędach oświadczenia woli). Można zatem powiedzieć, że to prawo związuje strony węzłem prawnym, a czynnik psychologiczny jest tutaj pomijany.

Ma to duże znaczenie dla osiąganych skutków prawnych. I tutaj jednak, pomimo samowykonalności, nie jest to zjawisko tak nowe, jak mogłoby się wydawać. Należy przypomnieć, że czynność prawna wywołuje nie tylko skutki w niej wyrażone, lecz również te, które wynikają z ustawy, z zasad współżycia społecznego i z ustalonych zwyczajów. Wywoływane skutki nie są więc tożsame z tymi wyrażonymi w oświadczeniu woli, a wyrażenie zamiaru dokonania określonej czynności prawnej niejako implikuje nam skutki dodatkowe. Strony godzą się ponadto na samowykonanie umowy i jej automatyzm, więc do momentu zmiany zdania (z prawa do którego strony rezygnują) właściwie nie powinny wyniknąć spory, dopóki w grę nie wchodzą błędy oświadczenia woli, czy inne szczególne sytuacje. Innymi słowy, godząc się na zawarcie smart kontraktu, strony akceptują taką formę stosunku prawnego i godzą się na związane z nią skutki i ryzyka. Prawo powinno jednak przewidywać mechanizm na powstrzymanie wykonania umowy w związku z jej nieważnością czy bezskutecznością. W szczególności dodać należy, iż strony nie mogą wyłączyć między sobą wspomnianych przepisów *ius cogens*, a wykonanie takiej umowy nie może rodzić skutków prawnych. Koncepcja jurysdykcji cyfrowej brzmi co prawda kusząco, jednak na ten moment jest nieakceptowalna. Do istotnych dla postaci smart kontraktu przepisów powszechnie obowiązujących należy między innymi niemożność złożenia tzw. oferty wieczystej, to znaczy takiej, w wyniku której powstaje niekończące się zobowiązanie. Co więcej, w przypadku zobowiązań o charakterze ciągłym, zawartych na czas nieoznaczony, możliwe jest jej wypowiedzenie w każdej chwili.

I w przypadku błędu w kodzie można odnieść się do szeroko pojętej doktryny prawa cywilnego, nie tylko tej związanej z tematem niniejszego opracowania. Należy skupić się na elemencie zaufania i rozważyć, kiedy zostanie on naruszony. Takim przypadkiem byłaby sytuacja, w której jedna ze stron błąd spostrzega, ale nie informuje o tym drugiej. Takiej osobie nie przysługuje wtedy ochrona.

W doktrynie zauważa się również pewne analogie pomiędzy charakterem smart kontraktu, a cywilnoprawną instytucją pełnomocnika. Błąd w kodzie programistycznym mógłby być przy tym rozstrzygany jako przekroczenie zakresu umocowania. Oczywiście jest to raczej uwaga teoretyczna i nie powinna być na ten moment stosowana, gdyż jest to interpretacja zbyt szeroka (nadaje pełnomocnictwo programowi, co Kodeks Cywilny kategorycznie wyklucza, ograniczając grupę podmiotów uprawnionych do wykonywania pełnomocnictwa do osób fizycznych).

5.4 Niezmienialność i automatyzm w wykonaniu smart kontraktu

Typowe cechy smart kontraktu potrafią być jego błogosławieństwem i przekleństwem. W drodze regulacji powinny być ostrożnie wyważone dwie wartości: idea smart kontraktu (jego cechy konstytutywne) oraz ochrona kontrahentów (nawet jeśli przed samymi sobą). Wiele szczegółowych przepisów przewiduje taką ochronę, np. wspomniane już przepisy związane ze wzorcami umownymi. Innym przykładem może być również prawo konsumenta do odstąpienia od umowy zawartej na odległość. Na mocy jednak naszej dotychczasowej analizy należy wskazać, iż że względu na dualizm pojęcia smart kontraktu, możemy doszukiwać się możliwości jego zmiany poprzez zmianę stosunku zobowiązaniowego, bez zmiany kodu programistycznego. Innymi słowy możemy doprowadzić do sytuacji, w której kod pozostanie co prawda niezmieniony, jednak zmieni się sytuacja prawna podmiotów. Jest to najdalej idąca ochrona w przypadku smart kontraktów, gdyż stanowi całkowite oderwanie treści kodu programistycznego od wiążącego strony stosunku prawnego.

Należy pamiętać, że samowykonalność umowy nie przesądza o braku wad jej przedmiotu[13]. Dlatego też prawo w przypadku smart kontraktów powinno być wyższą instancją dla kodu programistycznego. Nie możemy przyjąć, że choć umowa zawarta przez strony może być nieważna bądź bezskuteczna, to w rzeczywistości dojdzie do jej wykonania. Wprowadziłoby to ogromne zagrożenie dla obrotu prawnego, kreując równocześnie równoległy obrót cyfrowy. Zarówno prawo, jak i twórcy kodów używanych przez smart kontrakty, powinni przyjąć mechanizm wzajemnego oddziałowywania w przypadku kolizji na rzecz prawa, ale także dla dobra kontrahentów, których zamiarem było przecież zawiązanie stosunku prawnego właśnie za pomocą smart kontraktu.

[13] M. Pecyna, A. Behan, *Smart contracts - Nowa technologia prawa umów?,* Transformacje prawa prywatnego 3/2020.

5.5 Amerykańskie ujęcie smart kontraktu - wzmianka

Należałoby pokrótce wyjaśnić, jak traktuje smart kontrakty prawo kraju, w którym jest to zjawisko najbardziej powszechne. Kolejnym powodem jest oczywiście również zastosowanie rozwiązań anglosaskich w transakcjach międzynarodowych. Dodatkowo, chociaż prawo federalne Stanów Zjednoczonych raczej milczy, pojawiły się pierwsze regulacje stanowe w kwestii smart kontraktów. Co więcej, regulacje te nie są jednakowe. Wśród najważniejszych, regulowanych kwestii wymienić można m.in. wprowadzenie definicji legalnych pojęć związanych z blockchainem (Nevada, Arizona, Tennessee), wprowadzenie rejestru kryptograficznego w rejestrach państwowych (Kolorado), ustanowienie zespołu odpowiedzialnego za rozwój i kontrolę technologii blockchainu (Connecticut, Wirginia i Hawaje), czy licencjonowanie działalności związanej np. z kryptowalutami (Alabama)[14].

Tematyka smart kontraktu jest rozwinięta w amerykańskiej literaturze prawniczej znacznie bardziej niż w polskiej. Wielokrotnie był tam też poruszany temat smart kontraktu jako umowy, jednak z innymi wnioskami. Jak już wcześniej zostało wspomniane, wynika to z odmienności kultury prawnej. Żeby dana czynność została uznana za umowę, muszą pojawić się następujące elementy: oferta, przyjęcie oferty, świadczenie oraz zamiar stworzenia stosunku prawnego. Można stwierdzić, że jest to podejście bardziej formalne (przy czym łatwiejsze do osiągnięcia) niż to przewidziane w polskim Kodeksie Cywilnym. Jednak amerykańska jurysprudencja nie jest jednogłośna co do uznania smart kontraktu jako umowy cywilnoprawnej. W szczególności pojawiają się głosy o niezależności smart kontraktu od prawa w ogóle, w imię wyższości jurysdykcji cyfrowej. Bezsprzeczne jest jednak raczej to, że wszystko, co spełnia powyższe przesłanki umowy, umową jest. A to jest w przypadku smart kontraktu wykonalne.

Uznawaniu smart kontraktu w niektórych państwach za umowę (szczególnie kultury anglosaskiej), a odmienne stanowisko w innych (głównie reprezentujących system prawa kontynentalnego), jak słusznie zauważył Alexandros A. Papantoniou[15], może poważnie zakłócić porządek międzynarodowego prawa prywatnego. Bowiem, jak zobaczyliśmy na przykładzie Polski i Stanów

[14] Legislacja związana z technologią blockchain do 2018 r. dostępna na: https://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx dostęp: 06.06.2022.

[15] A. A. Papantoniou, *Smart contracts in the new era of contract law,* Digital Law Journal, 1(4). s. 8-24.

Zjednoczonych, definicje umów, na pozór podobne, szczególnie dla osób bez wykształcenia prawniczego, zdecydowanie się różnią.

6. *LAW BECOMES CODE*

Od wynalezienia smart kontraktu minęło już dwadzieścia pięć lat, co w dobie nowych technologii stanowi ogrom czasu. Myśl ta przeszła sporą ewolucję, choć nadal pojawiają się głosy przywiązane do pierwotnej, idealnej koncepcji, gdzie kod programistyczny rzeczywiście jest silniejszy niż prawo. Można jednak powiedzieć, że w tym przypadku pomysłowość przesadnie wyprzedziła rzeczywistość. Na gruncie prawa polskiego nie można bowiem po pierwsze uznać wyższości smart kontraktu nad prawem, a po drugie nie można uznać go jako umowę, a jedynie jako sposób jej wykonania. Inaczej jest w przypadku prawa Stanów Zjednoczonych, choć i tam koncepcja Code is law nie przyjęła się w swojej idealistycznej wersji.

Nie stanowi to natomiast przeszkody, by z pierwotnej idei smart kontraktu czerpać pełnymi garściami w celu usprawnienia obecnej praktyki umów. Co więcej, w przypadku smart kontraktów należy przyjąć zasadą odwrotną niż *Code is law*, gdyż to nie kod staje się prawem, a prawo, poprzez swoją stopniową cyfryzację, staje się kodem. To prawo jest jednak podstawą stosunków społecznych, nawet jeśli zaczyna zmieniać swoją formę.

BIBLIOGRAFIA

Bekhta A., *Blockchain: Możliwości i wyzwania dla sektora publicznego, E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego*, Wrocław 2021.

Cong L.W., He Z., *Blockchain Disruption and Smart Contracts*, SSRN Electronic Journal 2017.

Hulicki M., *Istota uznania prawnego smart kontraktu w świetle rozwiązań amerykańskich* [w:] Człowiek w cyberprzestrzeni 1/2018.

Kowacz K., Wielgus K., *Smart kontrakty w prawie umów*, Wydawnictwo Księgarnia Akademicka, Kraków 2021.

Krzemińska M., Rzeszutek M., *Stosowanie smart kontraktów w obrocie konsumenckim - wybrane problemy* [w:] Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2021, nr 6(10).

Pecyna M., Behan A., *Smart contracts - Nowa technologia prawa umów?,* [w:] Transformacje prawa prywatnego 3/2020.

Papantoniou A. A., *Smart contracts in the new era of contract law*. Digital Law Journal, 1(4).

Raskin M., *The law and legality of smart contracts*, Georgetown Law Technology Review 2017, nr 1:2, s. 305–340.

Wolter A., Ignatowicz J., Stefaniuk K., *Prawo cywilne. Zarys części ogólnej*, Wolters Kluwer, Warszawa 2018.

Źródła internetowe:

Grigg I., *Financial Cryptography in 7 layers*, https://iang.org/papers/fc7.html, dostęp: 06.06.2022.

Kraińska A., Kuchta R., Prokurat J., Rutkowski P., *Blockchain, inteligentne kontrakty i DAO*, 2016, https://wardynski.com.pl/publikacje/opracowania/blockchain-inteligentne-kontrakty-i-dao, dostęp: 06.06.2022.

Ma T., *Is code a law?*, https://legal-tech.blog/is-code-law, dostęp: 06.06.2022.

Morton H., *Blockchain State Legislation*, https://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx, dostęp: 06.06.2022.

Nagaraj K., Maguire E., *Securing the chain*, KPMG International, https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/09/realizing-blockchains-potential.pdf, dostęp: 06.06.2022.

Nakamoto S., Bitcoin: *Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, dostęp: 06.06.2022.

Waloszek M., *Prawo a inteligentne kontrakty* https://lawmore.pl/prawo-a-inteligentne-kontrakty/, dostęp: 06.06.2022.

DLA Piper, *Smart Contracts: Is the Law Ready?*, https://www.dlapiper.com/~/media/files/people/tank-margo/smart-contracts-is-the-law-ready-web.pdf?la=en&hash=003897A104F6A74DD9FC1C2E0FE2A4F16ADE500F, dostęp: 06.06.2022.

Cryptocurrency Laws and Regulations by State, https://pro.bloomberglaw.com/brief/cryptocurrency-laws-and-regulations-by-state/, dostęp: 06.06.2022.

CODE IS LAW, OR LEGAL ANALYSIS OF SMART CONTRACTS

Abstract: The article is a concise legal analysis of the concept of smart contract in the Polish legal system with reference to the common law legal culture. In the introductory part will be discussed the concepts in order from the most general, that is blockchain, to the substance of the article, that is smart contract. I am going to briefly introduce what blockchain is, what is its purpose and applications, how we can classify it and how it relates to the topic we are discussing. The next point of introduction will be to present the Ethereum platform and its relation to the smart contracts concept. The related programming language Solidity will also be cited, although due to the topic and audience, without a deeper analysis. I would also like to distinguish the types of smart contracts, specifically highlighting DAO, or decentralized autonomous organization. In this way, I intend to show the diversity and possibilities of the technology that is the smart contract. After the introductory issues, there will be a smooth transition to the second, analytical, rather than descriptive, part of the paper. This will be the analysis of smart contracts under Polish law. I intend to start this analysis with a classification of the smart contract itself. This will start from the Polish attempt to define the issue. The next step will be an attempt to compile the Polish understanding of the contract with the smart contract. I intend to cite a number of doctrinal arguments, but first and foremost to focus on the smart contract as a form of contracting and its limitations. Inherent in such an analysis will be consideration of the concept of a legal transaction. Next to discuss will be the relationship between the smart contract and the patterns of contract. Further analysis will systematically follow the process of contract creation and execution. It will begin with the interpretation of the smart contract in the context of a declaration of intent. The self-executing and unalterable nature of the smart contract will also be discussed. In summary, conclusions will be drawn as to the current legal status of smart contracts in the Polish legal system, as well as briefly the opportunities this type of contract brings with it. It will also address how the concept of *Code is law* relates to reality.

Key words: blockchain, contract, DAO, distributed ledger technologies, ethereum, new technology law, smart contract, model contract.

ZOFIA FLACZYŃSKA
UNIWERSYTET WROCŁAWSKI

ROLA PIASKOWNIC REGULACYJNYCH (*REGULATORY SANDBOXES*) JAKO POMOSTU POMIĘDZY NOWYMI TECHNOLOGIAMI A PRAWEM PRZYSZŁOŚCI NA PRZYKŁADZIE SEKTORÓW RYNKU FINANSOWEGO

Abstrakt: Ograniczenia prawne motywowane koniecznością zapewnienia bezpieczeństwa rynku finansowego stanowią istotną przeszkodę, z jaką borykają się przedsiębiorcy z branży technologii finansowych (fintech). Odpowiedź na potrzebę znalezienia kompromisu między innowacyjnym rynkiem finansowym a reżimem regulacyjnym oferuje koncepcja piaskownicy regulacyjnej (*regulatory sandbox*). Pojęcie to, nieznajdujące podstawy normatywnej w przepisach, zostało wypracowane dosyć jednolicie na gruncie praktyki organów nadzoru oraz w literaturze przedmiotu. Jest to środowisko testowe, w którym przedsiębiorca wyłoniony w procesie naboru, pod nadzorem regulatora może wypróbować innowacyjne pomysły przed wprowadzeniem ich na rynek. Doświadczenia funkcjonujących piaskownic pokazują, że z takiej formy wsparcia korzystają zarówno start-upy, jak i podmioty już usytuowane na rynku. Istotną korzyścią dla organ nadzoru jest możliwość pozyskania informacji na temat potrzeb biznesowych i pożądanych zmian regulacyjnych. Za przykłady efektywnie działających piaskownic mogą posłużyć utworzona w 2016 r. brytyjska piaskownica regulacyjna, a także piaskownice azjatyckie. Na uwagę zasługują działania podjęte w tym zakresie przez Komisję Nadzoru Finansowego, jak również podejmowane próby wprowadzenia koncepcji *regulatory sandbox* w polskim sektorze energetycznym.

Słowa klucze: Piaskownica regulacyjna, *regulatory sandbox,* rynek finansowy, organ nadzoru, fintech, Komisja Nadzoru Finansowego, KNF

1. WPROWADZENIE

Nowe technologie odgrywają coraz istotniejszą rolę w kolejnych sektorach gospodarki, stawiając tym samym wyzwanie obowiązującym wymogom regulacyjnym. Niczym w soczewce, zderzenie nowych technologii z nienadążającym za nimi prawem można dostrzec w systemie finansowym. Ograniczenia prawne motywowane koniecznością zapewnienia bezpieczeństwa rynku finansowego i jego uczestników stanowią istotną przeszkodę, z jaką borykają się przedsiębiorcy z branży technologii finansowych (powszechnie określanych jako fintech). Odpowiedź na potrzebę znalezienia kompromisu między innowacyjnym rynkiem finansowym a reżimem regulacyjnym oferuje koncepcja piaskownicy regulacyjnej (zwanej dalej również *regulatory sandbox* lub piaskownicą). W niniejszym tekście dokonana zostanie analiza mechanizmu *regulatory sandbox* jako uniwersalnego sposobu na złagodzenie barier regulacyjnych na rynku finansowym, tak aby móc pogodzić wdrażane innowacyjne produkty i usługi z obowiązującym prawem lub wskazać pożądane kierunki jego zmiany. Jednocześnie zarysowany zostanie potencjał, jaki kryje w sobie koncepcja piaskownicy regulacyjnej również w innych sektorach gospodarki, na przykładzie polskiej energetyki.

Zagadnienie fintech przekracza ramy niniejszego opracowania, toteż na jego potrzeby autorka posługuje się definicją pojęcia proponowaną przez Financial Stability Board ("technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services")[1].

2. PRZEREGULOWANIE SYSTEMU FINANSOWEGO JAKO PRZYCZYNEK DO ROZWOJU PIASKOWNIC REGULACYJNYCH

Punktem wyjścia dla rozważań na temat koncepcji piaskownicy regulacyjnej jest próba krytycznego spojrzenia na światowy nurt wyznaczania ram regulacyjnych dla rynku finansowego. Globalny kryzys finansowy

[1] Za: A. Butor-Keler, *The role of regulatory sandboxes in the development of innovations on the financial services market: the case of the United Kingdom*, Ekonomia i Prawo. Economics and Law 2020, Volume 19, Issue 4, s.622. Szeroko na temat fintech piszą również: M. Nowakowski, *FINTECH - technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*,,Warszawa 2020, LEX, czy W.Rogowski, *Regulacje finansowe. FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017, Legalis, A.Gorgol, *Teoretycznei i praktyczne aspekty prawa finansowego. Problemy, koncepcje, wyzwania i rozwiązania*, Warszawa 2020, Legalis.

zapoczątkowany w 2007 r. w Stanach Zjednoczonych Ameryki Północnej (dalej jako Stany Zjednoczone) na rynku kredytów hipotecznych stanowił niewątpliwie przełomowy moment w historii systemu finansowego. Nienależycie nadzorowane instytucje rynku finansowego wykorzystywały swoją pozycję, określaną w literaturze przedmiotu jako „zbyt duże by upaść" (*too big to fail*, TBTF)[2], by nadużywać zaufania rynku, konsumentów, organów nadzoru, organów władzy publicznej i podejmować nadmierne ryzyko (postawa określana w literaturze jako *moral hazard*). Zagrożenie stabilności finansowej, a w dalszej perspektywie gospodarki, zmusiło amerykańskie władze do podjęcia radykalnych kroków w celu dofinansowania kolejnych zagrożonych utratą płynności finansowej i upadłością podmiotów. Wobec pogłębiającego się kryzysu finansowego, w ślad za Stanami Zjednoczonymi poszły inne państwa. Jak zauważa K. Marchewka-Bartkowiak, krokiem zwyczajowo podejmowanym przez władze publiczne na drodze do ustabilizowania rynków finansowych w obliczu kryzysu jest wprowadzenie bardziej restrykcyjnych przepisów normujących funkcjonowanie rynków finansowych oraz działalności jego uczestników[3]. Na poparcie tej tezy warto wspomnieć o całościowej reformie prawa rynków finansowych Unii Europejskiej (dalej jako UE), obejmującej wprowadzenie nowego modelu nadzoru makroostrożnościowego, wcielenie w życie unii bankowej oraz regulowanie kolejnych obszarów sektora finansowego, jak chociażby usług płatniczych.

Konsekwencją podejmowania działań w celu ochrony stabilności systemu finansowego stało się jednak „przeregulowanie" sektora finansowego, określane również w literaturze jako tsunami regulacyjne czy inflacja prawa finansowego wynikająca ze znacznej ilości nowelizacji przepisów[4]. Systematycznie zwiększany nadzór nad działalnością podmiotów rynku finansowego oraz obowiązek stałego monitorowania i dostosowywania się do zmieniającego się otoczenia regulacyjnego doprowadził do istotnego ograniczenia możliwości rozwoju rynku finansowego, jak również pewności prawa finansowego. Jednocześnie nie sposób nie doceniać roli reglamentacji systemu finansowego, polegającej na konieczności uzyskania wymaganym prawem zezwoleń lub

[2] Doktrynę TBTF charakteryzuje przykładowo M.Kozińska w: *Przymusowa restrukturyzacja banków w Unii Europejskiej*, Warszawa 2018, s. 33 i n.

[3] K. Marchewka-Bartkowiak, *Nowe rozwiązania regulacyjne – RIA, sandbox, compliance, RegTech – w świetle procesu „inflacji" prawa finansowego*, Studia Biura Analiz Sejmowych 2018, nr 1 (53), s. 135.

[4] Ibidem, s. 136. Autorka przytacza w artykule statystyki opracowane przez firmy consultingowe, dotyczące liczby zmian legislacyjnych na przełomie lat w kontekście niestabilności prawa rynków finansowych.

licencji przez podmioty rozpoczynające działalność finansową. Bariery licencyjne stoją na straży stabilności sektora ważnego dla całej gospodarki i chronią konsumentów[5].

Zarysowane powyżej spostrzeżenia dotyczące kondycji otoczenia regulacyjnego systemu finansowego stanowiły przyczynek do podjęcia działań przez nadzorców krajowych rynków finansowych w celu ułatwienia rozwoju rynku finansowego, przy jednoczesnym ograniczeniu ryzyka destabilizacji i legislacyjnej „inflacji". Interesującym rozwiązaniem pozwalającym na nawiązanie współpracy między przedsiębiorcami i nadzorcami w zakresie kształtowania rynku finansowego przyszłości jest koncepcja piaskownicy regulacyjnej – *regulatory sandbox.*

3. ISTOTA I CECHY PIASKOWNICY REGULACYJNEJ

Pojęcie piaskownicy regulacyjnej jako termin nieznajdujący podstawy normatywnej w przepisach prawa krajowego ani międzynarodowego, zostało wypracowane dosyć jednolicie na gruncie praktyki organów nadzoru oraz w literaturze przedmiotu. W. Rogowski zauważa, że termin *regulatory sandbox* opisuje „dość prostą koncepcję – stworzenia wydzielonego, bezpiecznego środowiska, w którym można eksperymentować bez ponoszenia prawnych konsekwencji porażki"[6]. Owo eksperymentowanie polega na testowaniu przez przedsiębiorców innowacyjnych rozwiązań przy wykorzystaniu nowych technologii (tytułem przykładu – sztuczna inteligencja czy technologia rozproszonego rejestru, które to, jednakże zagadnienia przekraczają ramy niniejszego opracowania) pod nadzorem organu nadzoru nad rynkiem reglamentowanym – a jednocześnie we współpracy z nadzorcą. Założeniem piaskownicy regulacyjnej jest obniżenie barier wejścia na rynek nadzorowany z jednej strony i pozyskanie przez organ nadzoru wiedzy na temat modeli biznesowych i potencjalnych kierunków rozwoju rynku z drugiej strony. Nadzór nad rynkiem – w omawianym przypadku - finansowym wiąże się z wymogiem posiadania licencji lub zezwolenia. Uczestnictwo w piaskownicy regulacyjnej pozwala odroczyć momentu przejścia procesu autoryzacyjnego. Regulacyjna piaskownica to pomysł opierający się na zniesieniu barier, ale w bardzo małej skali[7].

[5] W. Rogowski, *Regulacje finansowe. FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017, Legalis.
[6] Ibidem.
[7] Ibidem.

Zdaniem Bazylejskiego Komitetu Nadzoru Bankowego – atrybutem piaskownicy regulacyjnej jest również korzystanie ze swobody decyzyjnej przez organ nadzoru finansowego wobec uczestników lub przyszłych uczestników rynku finansowego[8].

Warto w tym miejscu odwołać się do sposobu definiowania *regulatory sandboxes* przez praktyków. Brytyjski organ nadzoru nad rynkiem finansowym – *Financial Conduct Authority* (FCA) jako światowy pionier w zakresie wdrażania koncepcji finansowej piaskownicy regulacyjnej, stosuje wobec niej określenie „*safe space*", przestrzeń zapewniającą jednocześnie próbowanie nowych technologii przez przedsiębiorców fintech oraz należytą ochronę konsumentów i samego systemu finansowego[9].

Na temat *regulatory sandboxes* stanowisko zajęła również Specjalna Rzecznik Sekretarza Generalnego ONZ ds. finansowania rozwoju sprzyjającego włączeniu społecznemu (dalej jako UNSGSA)[10], posługując się następującą definicją piaskownic: *sandboxes are, at their core, formal regulatory programs that allow market participants to test new fnancial services or business models with live customers, subject to certain safeguards and oversight*[11]. W opublikowanym w 2019 r. raporcie UNSGSA dotyczącym stosowania innowacji w celu wzmocnienia inkluzyjności systemu finansowego, przedstawione zostały dwa główne modele funkcjonowania piaskownic regulacyjnych: *product testing sandboxes, policy testing sandboxes* oraz *multi jurisdictional sandboxes*. Nazwy poszczególnych modeli wskazują na odrębne cele im przyświecające. Zadaniem *product testing sandboxes* jest wypróbowanie innowacyjnych produktów lub usług w bezpiecznych warunkach, przed wprowadzeniem ich na rynek i związaną z tym koniecznością dochowania wszelkich wymogów regulacyjnych. Z kolei w *policy testing sandbox,* większy akcent kładzie się na weryfikację obowiązujących przepisów pod kątem sprzyjania rozwojowi innowacyjności rynku finansowego. Rezultatem funkcjonowania piaskownicy w tym modelu powinno być zasygnalizowanie przez nadzorcę potrzeby nowelizacji

[8] *Sound Practices Implications of fintech developments for banks and bank supervisors*, Basel Committee on Banking Supervision, February 2018, s. 41, https://www.bis.org/bcbs/publ/d431.pdf (dostęp: 01.06.2022).

[9] *Regulatory Sandbox Lessons Learned Report*, Financial Conduct Authority, October 2017, s. 3, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf (dostęp: 19.05.2022).; H.J. Allen, *Regulatory Sandboxes*, The George Washington Law Review 2019, vol. 87 no. 3, s. 596.

[10] Funkcję tę pełni Jej Wysokość Maxima, królowa Niderlandów.

[11] *Early Lessons on Regulatory Innovations to Enable Inclusive Fintech. Innovation Offices, Regulatory Sandboxes and RegTech*, The FinTech WorkingGroup, UNSGSA, 2019, s. 26, https://www.unsgsa.org/sites/default/files/resources-files/2020-09/UNSGSA_Report_2019_Final-compressed.pdf (dostęp: 26.05.2022).

przepisów, a dalszej perspektywie – ustanowienie przez właściwe władze prawa przyjaznego nowym technologiom[12].

Zdaniem K. Marchewki-Bartkowiak, koncepcja piaskownicy regulacyjnej wpisuje się w model oceny skutków regulacji rynku finansowego zarówno na poziomie *ex ante*, jak i *ex post*.[13] Nawiązanie współpracy z przedsiębiorcą fintech przed wprowadzeniem nowego produktu lub usługi na rynek pozwala nadzorcy poznać i przewidzieć potencjalne bariery dla rozwoju innowacyjności, ale również zagrożenia dla stabilności systemu i praw konsumentów wynikające z niezgodności nowych produktów i usług z obowiązującymi przepisami.

Kluczowymi cechami piaskownicy regulacyjnej są zatem: minimalizacja wymogów stawianych wobec przedsiębiorców z branży fintech podczas testowania, udział w teście określonej grupy konsumentów oraz bieżący nadzór i możliwość współpracy ze strony organu nadzoru[14]. Utworzenie piaskownicy regulacyjnej nie wymaga adekwatnych zmian legislacyjnych – dotychczasowe doświadczenia organów nadzoru wykazały, że *regulatory sandboxes* są wdrażane w zakresie ogólnie przysługujących nadzorcom uprawnień. W odniesieniu do omawianej w dalszej części opracowania polskiej piaskownicy regulacyjnej warto nadmienić, że rodzimy ustawodawca zdecydował się ustanowić bardziej uszczegółowione zadanie polskiego nadzorcy nad rynkiem finansowym, realizowane właśnie poprzez *regulatory sandbox.*

4. DZIAŁALNOŚĆ REGULATORY SANDBOXES – WYBRANE PRZYKŁADY ZE ŚWIATA

Piaskownice regulacyjne funkcjonują obecnie w ponad 30 państwach, na rynkach finansowych charakteryzujących się różnym stopniem dynamiki[15]. Uzasadniony wydaje się zatem pogląd o uniwersalnym charakterze koncepcji *regulatory sandbox*, możliwym do zastosowania w różnych porządkach prawnych i ramach regulacyjnych systemów finansowych. Poniżej poświęcono uwagę pierwszym wdrożonym modelom piaskownicy regulacyjnej – począwszy od brytyjskiego *regulatory sandbox*, przez przykłady nieco odmiennych modeli azjatyckich piaskownic, po prognozy co do amerykańskiego *regulatory sandbox.* Na uwagę zasługuje także koncepcja polskiej piaskownicy

[12] Ibidem, s. 27.
[13] K. Marchewka-Bartkowiak*, Nowe rozwiązania…,* s. 142.
[14] H.J. Allen, *op. cit.,* s. 580.
[15] Dane aktualne na 2019 r. przedstawiające zestawienie funkcjonujących oraz planowanych piaskownicy znajduje się w *Early Lessons*…, s. 52 i n.

regulacyjnej, która przeszła w ciągu kilku lat znaczną modyfikację. W kolejnej części pracy przedstawiono także przewidywania co do utworzenia unijnej *regulatory sandbox*.

4.1. Piaskownica regulacyjna w Wielkiej Brytanii – pierwsze na świecie regulatory sandbox

Wspominany już brytyjski organ nadzoru nad rynkiem finansowym – FCA – jest organem władzy odpowiedzialnym za zapewnienie ochrony konsumentów, konkurencji i integralności brytyjskiego rynku finansowego[16]. Idąc za H.J. Allen można uznać, że inauguracja pierwszej piaskownicy regulacyjnej dla rynku finansowego przez FCA dała stolicy Wielkiej Brytanii miano światowej stolicy fintechów (*fintech hub*)[17].

Już w listopadzie 2015 r. FCA wyraziło pozytywne stanowisko w sprawie utworzenia piaskownicy regulacyjnej, wykazując takie potencjalne korzyści jak minimalizacja czasu i kosztów wdrażania innowacji na rynku finansowym, zwiększenie inkluzyjności rynku finansowego poprzez wsparcie małych przedsiębiorców lub start-upów we wprowadzaniu swoich produktów i usług, zacieśnienie współpracy organu nadzoru z przedsiębiorcami w celu wypracowania satysfakcjonujących rozwiązań. Raport podsumowujący analizę możliwości utworzenia brytyjskego *regulatory sandbox* stanowił efekt prac FCA zleconych przez Skarb Państwa Jej Królewskiej Mości (*Her Majesty's Treasury*) po sukcesach odniesionych w ramach funkcjonującej innej formie wsparcia brytyjskiego rynku usług finansowych – *Innovation Hub*[18]. Pierwsza brytyjska finansowa piaskownica regulacyjna - i zarazem pierwsza na świecie - powstała w 2016 r.[19] Jej idea funkcjonowania opiera się na współpracy uczestnika piaskownicy z przydzielonym mu z ramienia nadzorcy koordynatorem. Koordynator (*case officer*) wspiera podmiot w dostosowaniu projektowanego produktu lub usługi do wymogów regulacyjnych. Stały kontakt organu nadzoru z innowacyjnym przedsiębiorcą pozwala lepiej zrozumieć jego cele i potrzeby związane z nowym produktem. W konsekwencji możliwe jest wskazanie uczestnikowi piaskownicy właściwego sposobu na wprowadzenie nowego produktu na rynek finansowy z jednoczesnym uwzględnieniem obowiązujących

[16] Financial Services and Markets Act, 2000, c. 8, § 1B(3).
[17] H.J. Allen, *op.cit.*, s. 580,
[18] *Regulatory Sandbox*, Financial Conduct Authority, November 2015, s.2, https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf (dostęp: 20.05.2022).
[19] Oficjalna strona internetowa brytyjskiej piaskownicy regulacyjnej - https://www.fca.org.uk/firms/innovation/regulatory-sandbox (dostęp: 01.06.2022).

ram regulacyjnych – albo zidentyfikowanie obszarów legislacji, które należałoby dostosować do zmieniającej się rzeczywistości na rynku finansowym[20].

Brytyjski organ nadzoru przewidział szereg dodatkowych „narzędzi" (*tools*), które mają służyć efektywnej działalności *regulatory sandbox*. Należy do nich możliwość wydania przez nadzorcę opinii dotyczącej możliwości wprowadzenia innowacyjnego produktu lub usługi na rynek pod kątem otoczenia regulacyjnego. W tym miejscu warto zwrócić uwagę na dalsze kroki, jakie może podjąć FCA w sytuacji, gdy negatywnie zaopiniuje testowany produkt lub usługę. Organ nadzoru dysponuje narzędziem *waiver*, czyli możliwością modyfikacji odstąpienia od stosowania przepisu, którego dyspozycji uczestnik piaskownicy nie jest w stanie dopełnić. Powyższe wymaga uściślenia dwóch kwestii. Złagodzenie reżimu regulacyjnego następuje jedynie w środowisku testowym piaskownicy i na potrzeby wypróbowania nowych technologii wykorzystanych w produkcie lub usłudze. Z oczywistych względów natury ustrojowej, organ nadzoru nie posiada kompetencji uchylania przepisów powszechnie obowiązujących. Może jednak zastosować kolejne "narzędzie" i zaniechać orzeczenia o stosowaniu środków nadzorczych wobec podmiotu naruszającego przepisy, jeżeli podmiot ten współpracuje w otwarty sposób z organem nadzoru, przestrzega ustalonych podczas testów w piaskownicy regulacyjnej i prowadzi działalność zgodnie z przepisami o prawach konsumenta[21].

Przewidziane przez nadzorcę odstępstwa od obowiązujących ram regulacyjnych zdają się stanowić o tyle istotne ułatwienie, że podmioty aplikujące do brytyjskiej piaskownicy mają obowiązek posiadania wymaganym prawem zezwoleń lub wpisu do rejestru na prowadzenie działalności na brytyjskim rynku finansowym. Pomyślne przejście przez autoryzację FCA stanowi jedno z kryteriów wyboru do cyklu piaskownicy regulacyjnej. Organ nadzoru oferuje, poza tym uproszczoną formę zezwolenia, ograniczoną jedynie do potrzeb funkcjonowania w środowisku testowym w ramach piaskownicy regulacyjnej.

Brytyjski nadzorca chętnie dzieli się informacjami dotyczącymi funkcjonowania piaskownicy, warto więc poświęcić uwagę specyfice *regulatory sandbox* oraz imponującym statystykom. Do pierwszej połowy 2021 r., nabór do kolejnych cykli piaskownicy (tzw. *cohorts*) odbywał się dwa razy do roku (tym samym każdy cykl piaskownicy trwał 6 miesięcy), natomiast od sierpnia 2021 r. możliwe jest składanie wniosków przez cały rok. W dotychczas przeprowadzonych 7 *cohorts* umożliwiono przetestowanie swoich usług

[20] *Regulatory Sandbox Lessons*…s. 4.

[21] *Call for Input: Cross Sector Sandbox*, Financial Conduct Authority, May 2019, s. 7, https://www.fca.org.uk/publication/call-for-input/call-for-input-cross-sector-sandbox.pdf (dostęp: 23.05.2022).

łącznie ponad 150 podmiotom spełniającym kryteria wyboru spośród około 500 przedłożonych wniosków. Już pierwsza odsłona piaskownicy została okrzyknięta sukcesem w obliczu 69 zgłoszeń, z których FCA zaakceptował 24 podmioty, zaś testy odbyło 18 z nich. W największą liczbę aplikacji obfitował rok 2019[22].

Obszerna grupa uczestników różnych rozmiarów, szeroki przekrój wykorzystywanych technologii oraz proponowanych innowacji pozwoliła brytyjskiemu nadzorcy na sformułowanie w specjalnym raporcie interesujących i pozytywnych wniosków na temat skuteczności piaskownicy regulacyjnej już po odbyciu dwóch pierwszych cykli na przełomie 2016 i 2017 r. Niewątpliwą zaletą dostrzeganą przez uczestników piaskownicy był wzrost świadomości prawnej na temat obowiązujących ram regulacyjnych oraz minimalizacja kosztów związanych z zapewnieniem zgodności nowych produktów:

> "Direct feedback from firms both during testing and following testing in their final reports indicates that this aspect of the sandbox programme is valuable in helping them to understand how the regulatory framework applies to them, accelerating their route to market and reducing expenditure on external regulatory consultants"[23].

Współpraca z organem nadzoru postrzegana jest pozytywnie przez podmioty zewnętrzne, na przykład potencjalnych inwestorów, co przekłada się na zwiększone możliwości pozyskania kapitału na rozwój innowacyjnych usług. Powyższe posiada szczególną wartość dla *start-upów* oraz przedsiębiorców we wczesnej fazie rozwoju. Według statystyk FCA, około 40% podmiotów, które ukończyły pierwszy cykl piaskownicy regulacyjnej, pozyskało wsparcie inwestorów jeszcze w trakcie współpracy z nadzorcą w ramach *regulatory sandbox*[24].

Przedsiębiorcy docenili możliwość przetestowania w rzeczywistych (a zarazem ograniczonych, próbnych) warunkach zarówno wykorzystywanych technologii pod kątem cyberbezpieczeństwa i zgodności z obowiązującymi przepisami, jak i sprawdzenia potencjalnego odbioru przez konsumentów. Bieżąca weryfikacja proponowanego modelu biznesowego pod kątem zgodności z obowiązującym prawem oraz otwartości grupy odbiorców na nowy produkt pozwala odpowiednio wcześnie reagować na potrzeby rynkowe i potencjalne zagrożenia[25].

---

[22] Przegląd uczestników poszczególnych *cohorts* oraz opisy produktów i usług znajdują się na stronie FCA: https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms (dostęp: 24.05.2022).
[23] *Regulatory Sandbox Lessons*…s. 5.
[24] Ibidem, s. 6.
[25] Ibidem, s. 9.

O sukcesie brytyjskiej piaskownicy może świadczyć także różnorodność podmiotów, które zdecydowały się współpracować z FCA. Należą do nich podmioty nadzorowane o ugruntowanej pozycji – na przykład brytyjski bank o globalnym znaczeniu - HSBC, testujący w pierwszym *cohort* aplikację wspierającą klientów banku w zarządzaniu swoim budżetem czy też Lloyds Banking Group (jedna z największych brytyjskich instytucji finansowych), który ulepszał usługę telefonicznej i elektronicznej obsługi klientów w swoich oddziałach. Jednocześnie w piaskownicy wzięli udział mniejsi przedsiębiorcy i start-upy oferujące innowacyjne rozwiązania. Z podsumowania opublikowanego przez FCA wynika, że testowane od pierwszego cyklu produkty i usługi wywodzą się z takich obszarów jak zielone finanse, otwarta bankowość, identyfikacja i weryfikacja klienta (Know Your Customer), płatności oparte na technologii blockchain czy też włączenie finansowe[26].

4.2. Azja Południowo-Wschodnia i Australia – wypracowanie odmiennego modelu *regulatory sandbox* oraz reagowanie na zmienne potrzeby rynku finansowego

Szeroko zakrojone działania na rzecz rozwoju innowacyjnego rynku finansowego oraz zmniejszania barier do jego dostępu zostały podjęte przez właściwe władze nadzorcze państw z rejonu Azji Południowo – Wschodniej oraz z Australii niedługo po utworzeniu pierwszego, brytyjskiego *regulatory sandbox*. Poniżej opisane zostały wybrane pionierskie nad Pacyfikiem inicjatywy piaskownic regulacyjnych, wykorzystujące odmienne rozwiązania od brytyjskiego pierwowzoru.

Pierwsza piaskownica regulacyjna w Azji Południowo-Wschodniej powstała jesienią 2016 r. w Singapurze. Tamtejszy organ nadzoru nad rynkiem finansowym – *Monetary Authority of Singapore* (dalej jako MAS) – przewidział odmienny od brytyjskiego sposób funkcjonowania piaskownicy regulacyjnej. Do *regulatory sandbox* dopuszczane są również podmioty nieposiadające stosownego zezwolenia na działalność na rynku finansowym. Okres działalności w ramach piaskownicy jest czasem na dopełnienie formalności przed organem nadzoru celem późniejszego funkcjonowania na singapurskim rynku finansowym jako podmiot regulowany, po uzyskaniu wymaganego prawem zezwolenia. W przeciwieństwie do FCA, singapurski organ nadzoru od początku

[26] https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms (dostęp: 01.06.2022).

prowadzi ciągły nabór do piaskownicy. Podmioty zainteresowane wsparciem ze strony MAS powinny przedłożyć nadzorcy pisemne zgłoszenie według określonego wzoru. Po zakończeniu działalności w środowisku testowym (czas trwania ustalany jest indywidualnie), podmiot spełniający wszystkie przepisane prawem wymogi może wprowadzić innowacyjne usługi i produkty na rynek. Nie sposób nie wspomnieć o strategicznym położeniu Singapuru w centralnej części regionu, które pozwala przedsiębiorcom na ekspansję na sąsiednie rynki zbytu, w tym rynki finansowe. Podmiot fintech zainteresowany oferowaniem nowo wypróbowanych usług poza Singapurem powinien mieć więc na uwadze możliwe dodatkowe obowiązki licencyjne i regulacyjne obowiązujące w porządkach prawnych innych państw [27].

Odmienny model, zakładający funkcjonowanie odrębnych piaskownic regulacyjnych dla poszczególnych kategorii podmiotów i tym samym nadzorowanie przez różne organy władzy, został zastosowany w Hong Kongu. Banki nadzorowane przez the *Hong Kong Monetary Authority* (dalej jako HKMA) mogą od września 2016 r. testować innowacyjne rozwiązania w prowadzonej przez tego nadzorcę piaskownicy zwanej *the Fintech Supervisory Sandbox*[28]. Podmiotom prowadzącym działalność ubezpieczeniową dedykowano *insurtech sandbox* pod nadzorem *the Hong Kong Insurance Authority* (dalej jako IA). Z kolei *the Hong Kong Securities and Future Commission* (dalej jako SFC) prowadzi piaskownicę dla pozostałych podmiotów przez nią regulowanych, w tym start-upów. W ramach każdej z piaskownic przewidziano szczegółowe wymogi dotyczące aplikacji oraz – co dla zainteresowanych podmiotów najistotniejsze – mniejszą restrykcyjność wobec uczestników w zakresie spełniania wymogów prowadzenia działalności na rynku finansowym. Nadzorcy prowadzą ciągły nabór do piaskownic, a okres funkcjonowania ustalany jest indywidualnie dla poszczególnych podmiotów. Po „opuszczeniu" piaskownicy, jej uczestnicy są obowiązani dopełnić wszelkich przewidzianych wymogów regulacyjnych – *regulatory sandboxes* nie służą bowiem do obejścia obowiązującego prawa rynków finansowych[29].

Model singapurski, łagodzący reżim regulacyjny wobec kandydatów na uczestników piaskownicy regulacyjnej wprowadził pod koniec 2016 r. australijski organ nadzoru nad rynkiem finansowym – *Australian Securities and*

[27] *A Guide to Regulatory FinTech Sandboxes Across Asia-Pacific*, Baker McKenzie 2017, s. 7, https://www.bakermckenzie.com/-/media/files/insight/publications/2018/01/qrg_ap_regulatoryfintech_jan18.pdf?la=en (dostęp: 23.05.2022)

[28] https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/ (dostęp: 24.05.2022).

[29] *A Guide to Regulatory*…, s.4-5.

Investments Commision (dalej jako ASIC). Podmioty aplikujące do *regulatory sandbox* mogą notyfikować ASIC chęć skorzystania ze zwolnienia z obowiązku uzyskania zezwolenia na prowadzenie działalności regulowanej na okres 12 miesięcy, czyli przewidywalny okres funkcjonowania podmiotu w ramach piaskownicy regulacyjnej. Prawo do skorzystania z wyłączenia obowiązku licencyjnego wymaga, jednakże spełnienia wymogów dotyczących liczby klientów detalicznych, ekspozycji finansowej, przestrzegania prawa konsumentów czy posiadania procedur polubownego rozstrzygania sporów. Po zakończeniu działania w ramach piaskownicy aktualizuje się w pełni obowiązek posiadania Australian *financial services licence* lub *Australian credit licence*, toteż uczestnicy piaskownicy zobligowani są zawnioskować do organu nadzoru o wydanie stosownego zezwolenia w ciągu 12 miesięcy od pomyślnej aplikacji do piaskownicy[30]. Możliwość testowania nowych innowacyjnych produktów i usług oraz wprowadzania ich na rynek bez konieczności uprzedniego ubiegania się o licencję znacznie przyspiesza rozwój podmiotów z branży fintech. Przewidziane preferencyjne warunki aplikowania do australijskiej piaskownicy nie przełożyły się jednak na wysokie zainteresowanie podmiotów fintech[31], w przeciwieństwie do pozostałych piaskownic w regionie. Z możliwości testowania innowacji finansowych skorzystało raptem 7 podmiotów, dlatego od 1 września 2020 r. w Australii funkcjonuje wzmocniona piaskownica regulacyjna (*enhanced regulatory sandbox*, dalej jako ERS), która zastąpiła pierwotny koncept australijskiej piaskownicy i stanowiła odpowiedź na rozwój *regulatory sandboxes* w sąsiednich państwach.

Analiza powyższych przykładów pozwala wysnuć wniosek o pozytywnym efekcie funkcjonowania kilku piaskownic w regionie. Z jednej strony przedsiębiorcy mogą wybrać wśród konkurencyjnych modeli funkcjonowania *regulatory sandboxes*, z drugiej zaś strony poszczególne władze nadzorcze zmuszone są do weryfikacji dotychczasowych efektów działania piaskownic oraz ich aktywnej modernizacji. Reformę australijskiej piaskownicy poprzedziły działania podjęte przez MAC oraz HKMA: w Singapurze utworzona została piaskownica *Sandbox Express* dedykowana określonej grupie fintech, natomiast w Hong Kongu funkcjonuje trzecia już odsłona piaskownicy, *The*

[30] Ibidem, s. 2-3.

[31] H.J. Allen, *op.cit.*, s. 598; Więcej informacji na temat reglamentacji dostępu do rynku finansowego w Australii na stronie internetowej ASIC: https://asic.gov.au/for-finance-professionals/afs-licensees/, (dostęp 23.05.2022) oraz *Regulatory Guide 257: Testing Fintech Products and Services Without Holding an AFS or Credit Licence*, AUSTL. SEC. & INV. COMM'N 20 (2017), https://download.asic.gov.au/media/ 4420907/rg257-published-23-august-2017.pdf, (dostęp 23.05.2022)

Fintech Supervisory Sandbox 3.0.[32]. Niewątpliwie schemat funkcjonowania brytyjskiej piaskownicy wywarł znaczący wpływ na kształt południowoazjatyckich *regulatory sandboxes*, jak trafnie jednak zauważyła K. Marchewka-Bartkowiak – „poszczególne państwa dostosowują organizację piaskownic regulacyjnych do swoich doświadczeń, prawodawstwa oraz specyfiki rynku"[33].

4.3. Stany Zjednoczone – pierwsze piaskownice regulacyjne wobec głosów sceptycyzmu

Godnym podkreślenia jest fakt, że Stanach Zjednoczonych nie powstał do tej pory *regulatory sandbox* na poziomie federalnym, co może budzić zaskoczenie zważywszy na genezę wzmacniania reżimu regulacyjnego nad rynkiem finansowym, a także wysoką pozycję Stanów Zjednoczonych na światowej mapie fintech i sprzyjające warunki do rozwoju nowych technologii[34].

W amerykańskiej literaturze przedmiotu pojawiają się sceptyczne głosy dotyczące tworzenia *regulatory sandboxes*. Tytułem przykładu, H.J. Allen podnosi konieczność poświęcenia większej uwagi zagadnieniu piaskownic regulacyjnych oraz krytycznego nań spojrzenia. Profesor American University Washington College of Law wyraża sceptycyzm wobec wprowadzania *regulatory sandboxes* w Stanach Zjednoczonych jako sposobu na promocję innowacyjności finansowej. Piaskownice powinny być areną edukacji dla organu nadzoru i sposobem na obniżenie barier regulacyjnych dla podmiotów innowacyjnych, nie zaś kanałem promocji nowych technologii i innowacji[35]. Potencjalne zagrożenie dla skuteczności działań podejmowanych w ramach piaskownicy regulacyjnej z perspektywy całego systemu finansowego, a także ryzyko spowalniania rozwoju innowacyjności rynku przez *regulatory sandboxes* w obrazowy

[32] A.N. Didenko, *Why Australia needs a better model for its enhanced fintech sandbox*, The FinReg Blog, Global Financial Markets Center Duke University School of Law, 26.07.2021, https://sites.law.duke.edu/thefinregblog/2021/07/26/why-australia-needs-a-better-model-for-its-enhanced-fintech-sandbox/ (dostęp: 23.05.2022). Więcej na temat Singapur Sandbox Express w wytycznych opublikowanych przez singapurskiego nadzorcę w styczniu 2022 r.: *Singapur Sandbox Express Guidelines,* Monetary Authority of Singapore, 1 January 2022,https://www.mas.gov.sg/-/media/MAS-Media-Library/development/Regulatory-Sandbox/Sandbox-Express/Sandbox-Express-Guidelines-1-Jan-2022.pdf?la=en&hash=08F99C6216499DFCED58489B5C0B3C8A8139CC57 (dostęp: 24.05.2022).

[33] K. Marchewka-Bartkowiak, *Regulacyjne środowisko testowe (regulatory sandbox) – doświadczenia i perspektywy*, Studia Biura Analiz Sejmowych 2019, nr 1 (57), s. 66.

[34] Pośród 5 globalnych „ekosystemów fintech" (*fintech ecosystems*), dwa znajdują się w Stanach Zjednoczonych: Dolina Krzemowa oraz Nowy Jork. Pozostałe miejsca sprzyjające rozwojowi fintech to Londyn, Singapur i Pekin. Dane za 2020 r., https://startupgenome.com/article/global-top-20-fintech-ranking-2020 (dostęp: 25.05.2022).

[35] H.J. Allen, *op.cit.*, s. 581.

sposób przedstawiła w 2018 r. H.M. Peirce z Komisji Papierów Wartościowych i Giełd Stanów Zjednoczonych (dalej jako SEC). Idei piaskownicy, w której nadzorca niczym rodzic siada wraz z podmiotem innowacyjnym i jego „zabawkami", przeciwstawiła koncepcję „regulatory beach" z organem nadzoru jako ratownikiem czuwającym nad bezpieczeństwem innowatorów-plażowiczów, pozostawiając im jednak wolną rękę w podejmowaniu decyzji[36].

Niezależnie od biernej jak dotąd postawy władz federalnych i krytycznych głosów literatury, na poziomie stanowym od 2018 r. tworzone są piaskownice regulacyjne mające na celu zwiększenie atrakcyjności lokowania działalności podmiotów fintech w poszczególnych stanach. Pionierem w zakresie amerykańskich *regulatory sandboxes* okazała się Arizona, której gubernator już w marcu 2018 r. podpisał nowelizację prawa stanowego z inicjatywy Prokuratora Generalnego stanu Arizona, Marka Brnovicha. Na wzór australijskiej piaskownicy, podmioty biorące udział w inicjatywie nie podlegają przez okres 2 lat (z możliwością przedłużenia o kolejny jeden rok) obowiązującym wymogom wobec uczestników rynku finansowego. Kolejne stanowe piaskownice regulacyjne zostały unormowane w Kentucky, Nevadzie, Utah, Vermont, Wyoming, Wirginii Zachodniej, na Florydzie, Hawajach oraz w 2021 r. w Karolinie Północnej. W 2022 r. przewidywane jest uchwalenie przepisów umożliwiających powstanie piaskownicy w Tennesee[37]. Innowacyjnym podejściem do koncepcji tworzenia bezpiecznych środowisk testowych pochwalić się może stan Utah, w którym w marcu 2021 r. powstał pierwszy w Stanach Zjednoczonych *regulatory sandbox* nieograniczony jedynie do rynku usług finansowych, a dedykowany wspieraniu innowacyjności także w innych sektorach gospodarki[38].

4.4. Polska – dwie odsłony piaskownicy regulacyjnej Komisji Nadzoru Finansowego

Punktem wyjścia dla przedstawienia tematyki polskiej finansowej piaskownicy regulacyjnej powinien być zamiar ustawodawcy ukierunkowany na powierzenie organowi nadzoru nad rynkiem finansowym (Komisji Nadzoru

[36] H.M. Peirce, *Beaches and Bitcoin: remarks before the Medici Conference,* Los Angeles 2018, https://www.sec.gov/news/speech/speech-peirce-050218 (dostęp 20.05.2022 r).
[37] P.Gleason, *Regulatory Sandboxes Give States An Edge Attracting Innovation And Investment*, Forbes, 31.12.2021 r., https://www.forbes.com/sites/patrickgleason/2021/12/31/regulatory-sandboxes-give-states-an-edge-attracting-innovation-and-investment/?sh=43188f457003 (dostęp: 23.05.2022).
[38] https://le.utah.gov/~2021/bills/static/HB0217.html (dostęp: 23.05.2022).

Finansowego, dalej jako KNF lub Komisja) zadania wspierania rozwoju innowacyjności rynku finansowego. Zadanie to zostało sformułowane w art. 4 ust.1 lit.3a ustawy o nadzorze nad rynkiem finansowym[39] (u.n.r.f.), dodanym na mocy ustawy z 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw[40]. Jak zauważa B.Wojno, nowe zadanie nadzorcy należy rozpatrywać przez pryzmat celów nadzoru wyliczonych w art. 2 u.n.r.f., a więc zapewnienia prawidłowego funkcjonowania rynku, jego stabilności, bezpieczeństwa, zapewnienia zaufania do rynku finansowego oraz ochrony interesów jego uczestników[41]. Idąc za B.Wojno należy pamiętać o tym, że:

> „innowacyjność rynku nie powinna być postrzegana jako dobro samo w sobie, które KNF winna mieć na uwadze, lecz powinna być postrzegana przez pryzmat celów nadzoru"[42].

W konsekwencji, organ nadzoru powinien wspierać innowacyjny rozwój, który przyczyni się do wykorzystania takich celów. Na poparcie powyższego warto wskazać jedno z kryteriów naboru do powstałej w 2018 r. Piaskownicy regulacyjnej KNF, tzn. wskazanie, w jaki sposób projekt lub usługa w perspektywie ma przyczynić się do rozwoju rynku finansowego. Koncepcja piaskownicy regulacyjnej stanowi obok systemu wsparcia doradczego (*innovation hub*) oraz przedstawiania opinii w procesie legislacyjnym dotyczącym rynku finansowego zespół niewładczych form działania KNF[43].

Komisja w 2016 r. rozpoczęła analizę potrzeb polskiego rynku finansowego w zakresie wspierania rozwoju innowacji. W tym celu powstał zespół roboczy ds. innowacji finansowych (FinTech), w skład, którego weszli przedstawiciele środowiska biznesu, nauki i prawa. W niniejszej pracy nie ma miejsca na analizę postulatów i wniosków przedstawionych w ramach pracy zespołu, kluczowym jest jednak wskazanie, że między innymi w wyniku prac zespołu FinTech, w Urzędzie KNF powstał w 2018 r. specjalny Departament

[39] T.j. Dz.U. z 2022 r., poz. 660 ze zm.
[40] Dz.U. z 2018 r. poz. 1075.
[41] B. Wojno [w:] M. Wierzbowski, L. Sobolewski, P. Wajda (red.), *Prawo rynku kapitałowego. Komentarz*, wyd. 3, Warszawa 2018, Legalis.
[42] Ibidem.
[43] Ibidem. Na marginesie warto wspomnieć o władczej, sformalizowanej formie realizacji zadania z art. 4 ust.1 pkt 3a u.n.r.f., czyli unormowanej w art. 11b tejże ustawy możliwości wydania na wniosek podmiotu wiążącej interpretacji w indywidualnej sprawie dotyczącej produktów i usług, które mają prowadzić do zwiększenia innowacyjności rynku finansowego.

Innowacji Finansowych odpowiedzialny za wsparcie sektora fintech[44]. Również w tym samym roku działalność zapoczątkowała polska piaskownica regulacyjna – początkowo pod nazwą Piaskownicy regulacyjnej KNF, a od 2020 r. - Piaskownica Wirtualna o nieco innym profilu działalności niż jej prekursorka.

Informacje dotyczące zakresu przedmiotowego i podmiotowego polskiej piaskownicy zostały opublikowane na stronie internetowej Komisji. Piaskownica dedykowana jest start-upom, czyli podmiotom planującym rozpocząć działalność na rynku finansowym i oferującym innowacyjny produkt lub usługę opartą na nowoczesnej technologii, jak również podmiotom nadzorowanym, które chcą rozszerzyć oferowane już rozwiązania i wprowadzić nowy model usług[45]. Wartym wspomnienia kryterium wyboru podmiotów testujących przez KNF jest innowacyjny charakter rozwiązania polegający na określonej unikalności rynkowej rozwiązania. Organ nadzoru oczekuje od instytucji finansowych, że testowane przez nich usługi lub produkty będą stanowiły realny wkład w rozwój sektora innowacji finansowych w Polsce. Kolejną przesłanką pozytywną jest realna potrzeba udziału podmiotu w piaskownicy, spowodowana zbyt wysokimi kosztami związanymi z tradycyjnym sposobem wprowadzenia nowego produktu na rynek lub luką prawną ograniczającą owo wdrożenie[46]. Warto dodać, że wymienione przesłanki stanowią szczególny katalog wymogów stawianych pretendentom do piaskownicy regulacyjnej, niespotykany w innych krajach europejskich[47].

Polski nadzorca wybrał pośrednie rozwiązanie pomiędzy brytyjskim a singapurskim modelem piaskownicy, określając czas trwania testów od 3 do 9 miesięcy, przy czym w uzasadnionych przypadkach dopuszczalne jest przedłużenie okresu do 12 miesięcy. Użytkownik piaskownicy ma możliwość wyboru jednego z dwóch wariantów środowiska testowego: wirtualny albo rzeczywisty. Każdy z nich różni się sposobem pozyskiwania informacji zwrotnej na temat testowanego produktu lub usługi. W wirtualnym wariancie wykorzystywane są zanonimizowane dane, podczas gdy piaskownica w wersji

[44] J. Byrski, M. Synowiec, *Wybrane instrumenty wpływające na rozwój prawa innowacji finansowych (FinTech)*, Dodatek MOP 2020, nr 20 s. 80.
[45] *Urząd KNF uruchamia Piaskownicę regulacyjną KNF*, 25.10.2018 r., https://www.knf.gov.pl/dla_rynku/fin_tech/aktualnosci?articleId=63540&p_id=18, (dostęp 25.05.2022).
[46] K. Marchewka-Bartkowiak, *Regulacyjne środowisko…*,s. 70.
[47] *Report: Fintech: Regulatory Sandboxes and Innovation Hubs*, European Banking Authority, European Securities and Markets' Authority, European Insurance and Occupational Pensions Authority, 2018, s. 23., https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/154a7ccb-06de-4514-a1e3-0d063b5edb46/JC%202018%2074%20Joint%20Report%20on%20Regulatory%20Sandboxes%20and%20Innovation%20Hubs.pdf (dostęp: 01.06.2022).

rzeczywistej opiera się na testowaniu produktu lub usługi na oznaczonej grupie klientów, którzy wyrazili zgodę na udział w teście i przekazują opinie na temat udostępnionych ich do testowania innowacyjnych rozwiązań. Komisja dokonuje wyboru operatora piaskownicy, czyli uczestnika rynku finansowego, który koordynuje funkcjonowanie piaskownicy oraz udostępnia uczestnikom piaskownicy odpowiednio bazę zanonimizowanych danych albo bazę swoich klientów – testerów. Zakres podmiotowy operatora polskiego *regulatory sandbox* zawężony został do banków, akceleratorów, fundacji oraz innych organizacji pozarządowych. Obiektywizm i rzetelność prowadzenia piaskownicy zapewnić ma wyłączenie możliwości pobierania od uczestników piaskownicy opłat za prowadzenie środowiska testowego. Powyższe odgrywa istotne znaczenie szczególnie dla start-upów fintech, które w uczestnictwie w piaskownicy upatrują szansę na zminimalizowanie kosztów wprowadzenia innowacyjnego produktu lub usługi na rynek, a także – co pokazały doświadczenia uczestników brytyjskiej piaskownicy – szybszego pozyskania finansowania. To ostatnie udział w Piaskownicy regulacyjnej KNF wręcz miał ułatwić, ponieważ operatorzy mogli nabyć akcje lub udziały w podmiocie testującym. W wyniku naboru na operatora pierwszej polskiej piaskownicy regulacyjnej, KNF wyłonił osiem podmiotów: cztery banki, fundację oraz dwie spółki z sektora fintech. Każdy z operatorów odpowiadać miał za inny obszar działalności piaskownicy oraz formy wsparcia jej uczestników w procesie testowania nowoczesnych produktów i usług[48].

W tym miejscu należy wskazać, że w 2020 r. nastąpiła znacząca modyfikacja modelu działania polskiego *regulatory sandbox.* Nowa – Piaskownica Wirtualna funkcjonująca w ramach programu Innovation Hub, dedykowana jest węższemu gronu podmiotów: *start-upom* jak i podmiotom już funkcjonującym na rynku finansowym w sektorze usług bankowych. Dotychczasowe założenia i wymogi piaskownicy regulacyjnej wykorzystane zostały w Programie Innovation Hub[49]. Piaskownica przewiduje możliwość wypróbowania rozwiązań technologicznych bazujących interfejsie Open API, zgodnym ze standardem Polish API[50] poprzez symulowanie usług płatniczych przewidzianych

[48] Operatorami Piaskownicy regulacyjnej KNF zostali: PKO Bank Polski SA, Huge Thing Sp. z o.o., D-RAFT SA (The Heart), Alior Bank SA, Fundacja Rozwoju Przedsiębiorczości BusinessCaddy, Bank Pekao SA, Bank Handlowy w Warszawie SA, Bank BGŻ BNP Paribas SA. Zob. E.Machewka-Bartkowiak, , *Regulacyjne środowisko…,* s. 69-70; R.Tomaszewski, *Znamy pierwszych operatorów piaskownicy regulacyjnej,* 16.11.2018 r., https://fintek.pl/znamy-dwoch-pierwszych-operatorow-piaskownicy-regulacyjnej/ (dostęp: 27.05.2022).

[49] https://www.knf.gov.pl/dla_rynku/fin_tech/Innovation_Hub (dostęp: 27.05.2022).

[50] Więcej na temat standardu Polish API: https://polishapi.org (dostęp: 30.05.2022).

w dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (tzw. dyrektywa PSD2)[51]. Co ciekawe, udział w piaskownicy nie obliguje do późniejszego ubiegania się o licencję.[52] Sam program piaskownicy trwa do 90 dni, z możliwością przedłużenia o kolejne 30 dni. Okres ten jest wyjątkowo krótki w porównaniu do czasu trwania piaskownic w innych państwach. Można mieć z tego względu obawy co do uzyskania pożądanych efektów w tak krótkim okresie. Piaskownicę moderuje Administrator, czyli Urząd KNF, który udziela wsparcia uczestnikom i nadzoruje przebieg testów. Po zakończeniu działalności w piaskownicy, uczestnik samodzielnie podejmuje analizę przeprowadzonych badań i decyduje, czy przejść proces licencyjny KNF oraz wprowadzić nową usługę na rynek finansowy.

Polska piaskownica regulacyjna zdążyła przejść długą drogę, zmieniwszy w międzyczasie swój kształt i stając się ostatecznie Piaskownicą Wirtualną o ograniczonym zakresie działania oraz wsparcia dla uczestników. Na wymierne korzyści z działalności polskiego *regulatory sandbox* trzeba jeszcze poczekać i mieć jednocześnie nadzieję, że pierwotny pomysł na jego funkcjonowanie zostanie jeszcze w przyszłości wykorzystany.

5. UNIA EUROPEJSKA WOBEC KONCEPCJI PIASKOWNICY REGULACYJNEJ

Potrzeba odnalezienia kompromisu pomiędzy ochroną stabilności systemu finansowego oraz utworzeniem korzystnego środowiska do rozwoju nowych technologii w sektorze finansowym została dostrzeżona również w kontekście prawa UE. Unijni nadzorcy pozytywnie odnoszą się do koncepcji rozwoju krajowych piaskownic regulacyjnych. Również podejmowane inicjatywy dla rozwoju nowych technologii w UE przemawiają za otwartością wspólnoty na unijnego rynku finansowego w XXI wiek – przykład może stanowić pierwszy unijny plan działania w sprawie technologii finansowej przedstawiony przez Komisję Europejską w marcu 2018 r. czy też nowy pakiet funkcjonujący od września 2020 r.[53]

[51] https://www.knf.gov.pl/dla_rynku/fin_tech/Piaskownica_Wirtualna (dostęp: 27.05.2022).
[52] Zarządzenie nr 48/2020 Przewodniczącego Komisji Nadzoru Finansowego z dnia 25 listopada 2020 r. w sprawie ustalenia Regulaminu udziału w testach w środowisku Piaskownicy Wirtualnej Urzędu Komisji Nadzoru Finansowego, https://www.knf.gov.pl/knf/pl/komponenty/img/Regulaminu_udzialu_w_testach_w_srodowisku_Piaskownicy_Wirtualnej_UKNF.pdf (dostęp: 18.05.2022).
[53] https://www.consilium.europa.eu/pl/policies/digital-finance/ (dostęp 01.06.2022)

Unijne otoczenie regulacyjne zmienia się dynamicznie, dążąc do unormowania kolejnych przejawów wykorzystania nowych technologii w rynku finansowym[54]. Nad możliwością utworzenia unijnej piaskownicy regulacyjnej pozwalającej na łatwiejszy dostęp do rynku finansowego przy zapewnieniu jego bezpieczeństwa zastanawiają się W.Ringe i C.Ruof[55]. Autorzy analizując konstrukcję *regulatory sandbox*, podkreślają zwłaszcza jedną z korzyści, jaką jest:

> "a mutual » learning process « that on the one hand allows regulators to better assess the risks that are connected with respective fintech firms, and on the other enables fintechs to benefit from the regulator's expertise in applying the legal framework"[56].

Z założenia, sposób funkcjonowania europejskiej piaskownicy regulacyjnej zależałby od przyjętego dla niej kształtu. Jak wskazują W.Ringe i C.Ruof, najmniej prawdopodobnym wariantem jest *regulatory sandbox* utworzony na poziomie unijnym i koordynowany przez unijnego nadzorcę, np. Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (dalej jako ESMA). Powyższe wymagałoby bowiem nowelizacji Traktatu o funkcjonowaniu Unii Europejskiej[57] celem wzmocnienia kompetencji UE w zakresie sprawowania nadzoru nad rynkami finansowymi państw członkowskich. Innym pomysłem jest harmonizacja sposobu funkcjonowania piaskownic regulacyjnych z pozostawieniem krajowym nadzorcom swobody co do wyboru środków. W odniesieniu do tego pomysłu trzeba zwrócić uwagę na wciąż występujące różnice w rozwoju rynków finansowych państw członkowskich, tym samym decyzja o utworzeniu piaskownicy powinna leżeć w gestii nadzorców krajowych, po analizie realnego zapotrzebowania na wsparcie fintech w tej formie. Ostatnia przedstawiona przez autorów propozycja opiera się na koncepcji prowadzenia *regulatory sandboxes* przez państwa członkowskie z udziałem instytucji unijnych jako koordynatorów[58]. Mechanizm ten, nazwany przez autorów „*guided sandbox*", pozwoliłby rozwijać działalność piaskownic w obowiązującym stanie prawnym i dodatkowo stanowiłoby arenę do wymiany cennych

[54] Przykładowo szeroko omawiany w środowisku naukowym projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynku kryptoaktywów, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020PC0593 (dostęp: 01.06.2022).

[55] W. Ringe i C. Ruof, *Regulating FinTech in the EU: the Case for a Guided Sandbox*, European Journal for Risk Regulation, 2020, Volume 11, issue 3, Cambridge University Press, s. 604, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/regulating-fintech-in-the-eu-the-case-for-a-guided-sandbox/3EE71CEEB3BC22E57A1BF08023073A6F, (dostęp 27.05.2022).

[56] Ibidem, s.606.

[57] Dz.Urz. UE C 202 z 7 lipca 2016 r.

[58] W. Ringe i C.Ruof, *op.cit.,* s. 620.

informacji i doświadczeń pomiędzy krajowymi nadzorcami oraz instytucjami UE[59]. Istotną rolę w organizowaniu i prowadzeniu *guided sandboxes* odgrywałoby wówczas regulacyjne *soft law* europejskich urzędów nadzoru.

W odniesieniu do podejmowanych działań przez UE w zakresie rozwoju piaskownic regulacyjnych – póki co krajowych – warto wskazać na obserwacje poczynione przez Europejski Urząd Nadzoru Bankowego (dalej jako EBA), ESMA oraz Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych podsumowane w raporcie „FinTech: regulatory sandboxes and innovation hubs" opublikowanym w 2018 r.[60] Z raportu wynika, że funkcjonujące na dzień publikacji pięć piaskownic regulacyjnych w państwach członkowskich UE opiera się na podobnych założeniach, jak również wszystkie piaskownice dopuszczają udział przedsiębiorców różnej wielkości i doświadczeniu na rynku finansowym. Dostrzeżone zostały pozytywne aspekty działalności *regulatory sandboxes,* ale również konieczność zachowania transparentności w zakresie działania piaskownicy i zapewnienia warunków uczciwej konkurencji między podmiotami rynku finansowego[61].

6. MOŻLIWOŚĆ WYKORZYSTANIA POTENCJAŁU REGULATORY SANDBOX NA INNYCH RYNKACH REGLAMENTOWANYCH – PRZYKŁAD PROJEKTOWANEJ POLSKIEJ ENERGETYCZNEJ PIASKOWNICY REGULACYJNEJ

Korzyści płynące ze współpracy przedsiębiorców oraz regulatorów w ramach bezpiecznego środowiska testowego powoli dostrzegane są również w innych branżach, newralgicznych z punktu widzenia bezpieczeństwa gospodarki i ochrony konsumentów. Godnym uwagi rodzimym przykładem próby wykorzystania *regulatory sandbox* jako środka do zwiększenia innowacyjności innego rynku niż finansowy, jest projekt utworzenia piaskownicy regulacyjnej przez Prezesa Urzędu Regulacji Energetyki (dalej jako URE).

Działania mające na celu zwiększenie innowacyjności sektora energetyki odnawialnej podjęło polskie Ministerstwo Klimatu i Środowiska. Trudno oprzeć się wrażeniu, że inspiracją dla polskich władz był projekty testowania innowacyjnych rozwiązań w sektorze energetyki prowadzone w krajach

[59] Ibidem, s. 622-623.
[60] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/154a7ccb-06de-4514-a1e3-0d063b5edb46/JC%202018%2074%20Joint%20Report%20on%20Regulatory%20Sandboxes%20and%20Innovation%20Hubs.pdf (dostęp: 01.06.2022).
[61] Ibidem, s. 36.

Europy Zachodniej, przykładowo niemiecki projekt Delta polegający testowaniu rozwiązań sprzyjających transformacji energetycznej w miastach[62].

W dniu 30 kwietnia 2021 r. przedłożono projekt nowelizacji ustawy - Prawo energetyczne oraz ustawy o odnawialnych źródłach energii (dalej jako ustawa)[63]. Projekt przepisów znajduje się obecnie na etapie konsultacji publicznych. Projektodawcy proponują uregulowanie na poziomie ustawowym koncepcji piaskownic regulacyjnych w sektorze energetyki. Energetyczne *regulatory sandbox* rozumiane jest analogicznie jak w przypadku rynku finansowego. Jak wynika z uzasadnienia do projektu nowelizacji, organ nadzoru nad rynkiem energetycznym – Prezes URE uzyskać ma prawo do odstępowania od przepisów wskazanych w decyzjach adresowanych do uczestników rynku energetycznego, w ramach realizacji projektu wdrażania innowacyjnych technologii, usług, produktów w sektorze energetycznym[64]. Stosownie do projektowanego art. 24b ust.2 ustawy, odstępstwa mogą dotyczyć warunków dostępu do sieci, korzystania z sieci i instalacji, a także warunków uzyskania koncesji na prowadzenie działalności[65]. Korzyści dla podmiotów innowacyjnych, nadzorców oraz odbiorców usług płynące z funkcjonowania piaskownic regulacyjnych na rynku finansowym dostały dostrzeżone przez polskie Ministerstwo Klimatu i Środowiska, toteż wzorem państw Europy Zachodniej (m.in. Francja, Holandia, Niemcy) proponowane jest rozszerzenie kompetencji Prezesa o możliwość udzielania odstępstw w drodze decyzji, po spełnieniu przez wnioskujący podmiot warunków wskazanych w ustawie. Decyzja o zastosowaniu odstępstw ma być wydawana na okres do 3 lat, z możliwością jednokrotnego przedłużenia o maksymalnie kolejne 3 lata. Nowe przepisy mają zobowiązać regulatora energetycznego do regularnego ogłaszania naboru projektów, ms które uczestnicy sektora będą mogli wnioskować o udzielenie odstępstwa[66].

---

[62] Więcej na ten temat w: https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2021/05/20210511-Reallabore-der-Energiewende-DELTA-geht-in-Darmstadt-an-den-Start.html; strona internetowa programu: https://delta-darmstadt.de (dostęp: 02.06.2022).

63 Numer z wykazu: UC74, https://legislacja.rcl.gov.pl/docs//2/12347450/12792158/12792159/dokument505837.pdf (dostęp: 01.06.2022).

[64] Uzasadnienie do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz ustawy o odnawialnych źródłach energii (UC 74), s. 3, https://legislacja.rcl.gov.pl/docs//2/12347450/12792152/12792153/dokument505829.pdf (dostęp 15.05.2022)

[65] Projekt ustawy z dnia 30 kwietnia 2021 r. o zmianie ustawy Prawo energetyczne oraz ustawy o odnawialnych źródłach energii (UC 74), s. 56, https://legislacja.rcl.gov.pl/docs//2/12347450/12792152/12792153/dokument505827.pdf (dostęp: 15.05.2022).

[66] Na marginesie warto wskazać, że projektowane przepisy zostały poddane analizie przez M.Będkowskiego-Kozioła w: *Piaskownice regulacyjne w energetyce – kilka uwag w odniesieniu do projektowanych rozwiązań prawnych*, Energetyka rozproszona 2022, nr 7, s. 19.

Analiza projektowanych przepisów pozwala zauważyć, że proponowany mechanizm wspierania innowacyjności sektora energetycznego różni się od finansowych piaskownic regulacyjnych. Nie zakłada bowiem systemowego wsparcia ani procedury testowania nowych produktów i usług (co, zważywszy na specyfikę branży energetycznej, może stanowić wyzwanie dla np. bezpieczeństwa dostaw energii). Można pokusić się o stwierdzenie, że terminem „piaskownicy regulacyjnej" nieco na wyrost określono kolejny rodzaj postępowania administracyjnego przed Prezesem URE. Jest to władczy środek działania energetycznego nadzorcy, odmienny od sposobu działania nadzorców rynku finansowego w ramach nadzorowanych przez nich *regulatory sandboxes* i – jak wynika z projektowanych przepisów – pozbawiony istotnego dla idei piaskownic elementu współpracy i wymiany doświadczeń przedsiębiorcy z regulatorem.

7. PODSUMOWANIE I WNIOSKI

Podsumowanie powyższej analizy zacząć należy od spostrzeżenia, że dotychczas regulatory sandbox nie doczekał się definicji normatywnej. Z tego względu, poszczególne organy nadzoru oraz przedstawiciele literatury posługują się mniej więcej jednolitym sposobem rozumienia tego pojęcia. Uniwersalna idea piaskownicy regulacyjnej uzupełniana szczegółowymi wymogami przez krajowych nadzorców, w zależności od dostrzeżonych potrzeb rynku finansowego oraz przedsiębiorców.

Spojrzenie na koncepcję piaskownicy regulacyjnej jako środka do znoszenia barier dostępu do rynków finansowych pozwala dostrzec istotne znaczenie dla zwalczania wykluczenia finansowego oraz przyspieszenia rozwoju systemu finansowego w krajach rozwijających się. Spośród korzyści płynących ze stosowania *regulatory sandboxes*, dla rozwoju innowacyjnego rynku finansowego szczególnie istotna wydaje się możliwość wymiany wiedzy pomiędzy przedsiębiorcami-uczestnikami rynku finansowego a organem nadzoru w zakresie rozwoju nowych technologii przydatnych w świadczeniu usług finansowych oraz ochrony stabilności systemu finansowego i konsumentów.

Zgodzić się trzeba ze spostrzeżeniami poczynionymi przez FCA na temat pozytywnego wpływu funkcjonowania piaskownicy regulacyjnej na cały rynek, bowiem uczestnictwo w regulatory sandbox pozwala zmniejszyć koszty wprowadzania nowych produktów na rynek, jest doceniane przez potencjalnych inwestorów, a ponadto wzrasta świadomość prawna uczestników rynku dzięki bieżącej wymianie informacji z organem nadzoru. Jednocześnie

podkreślić trzeba, że utworzenie przez organ nadzoru piaskownicy regulacyjnej jest dopiero pierwszym krokiem na drodze do tworzenia atrakcyjnego środowiska dla nowych technologii . Nie każdy *regulatory sandbox* powtórzy sukces brytyjskiej piaskownicy, dlatego też konieczne jest otwarte podejście nadzorcy do ewentualnych zmian oraz badania zapotrzebowania przedsiębiorców – dobrym przykładem może być australijska piaskownica regulacyjna. Interesującym i wartym dalszej obserwacji modelem piaskownicy jest Piaskownica Wirtualna prowadzona przez Urząd KNF, dedykowana jedynie rozwojowi usług płatniczych.

Konsekwencją pozytywnego przyjęcie regulatory sandbox w obszarze rynku finansowego jest stopniowa transpozycja owej koncepcji współpracy przedsiębiorców z regulatorami do innych sektorów gospodarki objętych reglamentacją. W tym miejscu również warto mieć na uwadze projektowane przepisy normujące działalność polskiej energetycznej piaskownicy regulacyjnej.

Zasadne zdaje się podkreślenie, że na nadzorcy spoczywa obowiązek zapewnienia bezpiecznych warunków testowania innowacyjnych produktów i usług, jak również poddania pod analizę obowiązujących ram prawnych pod kątem ewentualnych zmian przepisów, tak aby testowane usługi finansowe mogły przyczynić się do rozwoju nowoczesnego systemu finansowego. Jednocześnie należy zgodzić się z poglądem, że piaskownice regulacyjne powinny stanowić jeden z wielu środków wykorzystywanych przez organy nadzoru do znoszenia barier przeregulowanego systemu finansowego. Konieczna jest analiza ex ante możliwych kierunków rozwoju rynku oraz potencjalnych rezultatów i spodziewanych korzyści po trzech stronach środowiska testowego: przedsiębiorców, nadzorcy i przyszłych użytkowników innowacyjnych produktów oraz usług. Owa współpraca oraz badanie *ex post* wypracowanych rozwiązań przez nadzorcę powinny stanowić podwaliny pod przegląd obowiązujących ram prawnych oraz – w razie dostrzeżonej potrzeby – zasygnalizowanie ustawodawcy niezbędnych zmian legislacyjnych.

BIBLIOGRAFIA

Allen H.J., *Regulatory Sandboxes*, The George Washington Law Review 2019, vol. 87 no. 3.

Będkowski-Kozioł M., *Piaskownice regulacyjne w energetyce – kilka uwag w odniesieniu do projektowanych rozwiązań prawnych*, Energetyka rozproszona 2022, nr 7.

Butor – Keler A., *The role of regulatory sandboxes in the development of innovations on the financial services market: the case of the United Kingdom*, Ekonomia i Prawo. Economics and Law 2020, Volume 19, Issue 4.

Byrski J., Synowiec M., *Wybrane instrumenty wpływające na rozwój prawa innowacji finansowych (FinTech*), Dodatek MOP 2020, nr 20.

Didenko A.N., *Why Australia needs a better model for its enhanced fintech sandbox*, The FinReg Blog, Global Financial Markets Center Duke University School of Law, 26.07.2021, https://sites.law.duke.edu/thefinregblog/2021/07/26/why-australia-needs-a-better-model-for-its-enhanced-fintech-sandbox/ (dostęp: 23.05.2022).

Gleason P., *Regulatory Sandboxes Give States An Edge Attracting Innovation And Investment*, Forbes, 31.12.2021 r. https://www.forbes.com/sites/patrickgleason/2021/12/31/regulatory-sandboxes-give-states-an-edge-attracting-innovation-and-investment/?sh=43188f457003 (dostęp: 23.05.2022 r).

Gorgol A., *Teoretyczne i praktyczne aspekty prawa finansowego. Problemy, koncepcje, wyzwania i rozwiązania*, Warszawa 2020, Legalis.

Kozińska M., *Przymusowa restrukturyzacja banków w Unii Europejskiej*, Warszawa 2018.

Marchewka-Bartkowiak K., *Nowe rozwiązania regulacyjne – RIA, sandbox, compliance, RegTech – w świetle procesu „inflacji" prawa finansowego*, Studia Biura Analiz Sejmowych 2018, nr 1 (53).

Marchewka-Bartkowiak K., *Regulacyjne środowisko testowe (regulatory sandbox) – doświadczenia i perspektywy*, Studia Biura Analiz Sejmowych 2019, nr 1 (57).

Nowakowski M., *FINTECH - technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych,*,Warszawa 2020, LEX.

Peirce H.M., *Beaches and Bitcoin: remarks before the Medici Conference,* Los Angeles 2018, https://www.sec.gov/news/speech/speech-peirce-050218 (dostęp 20.05.2022 r).

Ringe W., Ruof C., *Regulating FinTech in the EU: the Case for a Guided Sandbox*, European Journal for Risk Regulation, 2020, Volume 11, Issue 3, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/regulating-fintech-in-the-eu-the-case-for-a-guided-sandbox/3EE71CEEB3BC22E57A1BF08023073A6F, (dostęp 27.05.2022).

Rogowski W., *Regulacje finansowe. FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017, Legalis.

Tomaszewski R., *Znamy pierwszych operatorów piaskownicy regulacyjnej*, 16.11.2018 r., https://fintek.pl/znamy-dwoch-pierwszych-operatorow-piaskownicy-regulacyjnej/ (dostęp: 27.05.2022).

Wojno B. [w:] M. Wierzbowski, L. Sobolewski, P. Wajda (red.), *Prawo rynku kapitałowego. Komentarz*, wyd. 3, Warszawa 2018, Legalis.

A Guide to Regulatory FinTech Sandboxes Across Asia-Pacific, Baker McKenzie 2017, https://www.bakermckenzie.com/-/media/files/insight/publications/2018/01/qrg_ap_regulatoryfintech_jan18.pdf?la=en (dostęp: 23.05.2022).

Call for Input: Cross Sector Sandbox, Financial Conduct Authority, May 2019, https://www.fca.org.uk/publication/call-for-input/call-for-input-cross-sector-sandbox.pdf (dostęp: 23.05.2022).

Early Lessons on Regulatory Innovations to Enable Inclusive Fintech. Innovation Offices, Regulatory Sandboxes and RegTech, The FinTech WorkingGroup, UNSGSA, 2019, https://www.unsgsa.org/sites/default/files/resources-files/2020-09/UNSGSA_Report_2019_Final-compressed.pdf (dostęp: 26.05.2022).

Financial Services and Markets Act, 2000, c. 8, § 1B(3).

Sound Practices Implications of fintech developments for banks and bank supervisors, Basel Committee on Banking Supervision, February 2018, https://www.bis.org/bcbs/publ/d431.pdf (dostęp: 01.06.2022).

Oficjalna strona internetowa brytyjskiej piaskownicy regulacyjnej - https://www.fca.org.uk/firms/innovation/regulatory-sandbox (dostęp: 01.06.2022).

Regulatory Sandbox Lessons Learned Report, Financial Conduct Authority, October 2017, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf (dostęp: 19.05.2022).

Regulatory Sandbox, Financial Conduct Authority, November 2015, https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf (dostęp: 20.05.2022).

Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynku kryptoaktywów, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020PC0593 (dostęp: 01.06.2022).

Projekt ustawy z dnia 30 kwietnia 2021 r. o zmianie ustawy Prawo energetyczne oraz ustawy o odnawialnych źródłach energii (UC74), https://legislacja.rcl.gov.pl/docs//2/12347450/12792152/12792153/dokument505827.pdf (dostęp: 15.05.2022).

Report: Fintech: Regulatory Sandboxes and Innovation Hubs, European Banking Authority, European Securities and Markets Authority, European Insurance and Occupational Pensions Authority, 2018, 23https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/154a7ccb-06de-4514-a1e3-0d063b5edb46/JC%202018%2074%20Joint%20Report%20on%20Regulatory%20Sandboxes%20and%20Innovation%20Hubs.pdf (dostęp: 01.06.2022).

Singapur Sandbox Express Guidelines, Monetary Authority of Singapore, 1 January 2022, https://www.mas.gov.sg/-/media/MAS-Media-Library/development/Regulatory-Sandbox/Sandbox-Express/Sandbox-Express-Guidelines-1-Jan-2022.pdf?la=en&hash=08F99C6216499DFCED58489B5C0B3C8A8139CC57 (dostęp: 24.05.2022).

Urząd KNF uruchamia Piaskownicę regulacyjną KNF, 25.10.2018 r., https://www.knf.gov.pl/dla_rynku/fin_tech/aktualnosci?articleId=63540&p_id=18, (dostęp: 25.05.2022).

Uzasadnienie do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz ustawy o odnawialnych źródłach energii (UC 74), https://legislacja.rcl.gov.pl/docs//2/12347450/12792152/12792153/dokument505829.pdf (dostęp 15.05.2022).

Zarządzenie nr 48/2020 Przewodniczącego Komisji Nadzoru Finansowego z dnia 25 listopada 2020 r. w sprawie ustalenia Regulaminu udziału w testach w środowisku Piaskownicy Wirtualnej Urzędu Komisji Nadzoru Finansowego, https://www.knf.gov.pl/knf/pl/komponenty/img/Regulaminu_udzialu_w_testach_w_srodowisku_Piaskownicy_Wirtualnej_UKNF.pdf (dostęp: 18.05.2022).

Ustawa z dnia 26 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. Dz.U. z 2022 r., poz. 660 ze zm.).

Ustawa z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. z 2018 r. poz. 1075).

https://startupgenome.com/article/global-top-20-fintech-ranking-2020 (dostęp: 25.05.2022)

https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms (dostęp: 24.05.2022).

https://le.utah.gov/~2021/bills/static/HB0217.html (dostęp: 23.05.2022).

https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/ (dostęp: 24.05.2022).

https://asic.gov.au/for-finance-professionals/afs-licensees/ (dostęp: 23.05.2022 r).

Regulatory Guide 257: Testing Fintech Products and Services Without Holding an AFS or Credit Licence, AUSTL. SEC. & INV. COMM'N 20 (2017), https://download.asic.gov.au/media/ 4420907/rg257-published-23-august-2017.pdf (dostęp: 23.05.2022).

https://www.knf.gov.pl/dla_rynku/fin_tech/Innovation_Hub (dostęp: 27.05.2022).

https://www.knf.gov.pl/dla_rynku/fin_tech/Piaskownica_Wirtualna (dostęp: 27.05.2022).

https://www.consilium.europa.eu/pl/policies/digital-finance/ (dostęp: 01.06.2022).

https://polishapi.org (dostęp: 30.05.2022).

THE ROLE OF REGULATORY SANDBOXES AS A BRIDGE BETWEEN NEW TECHNOLOGIES AND THE LAW OF THE FUTURE: THE CASE OF FINANCIAL SERVICES MARKET

Summary: Legal limitations which ensure safety of the financial market are challenging for financial technology (fintech) entrepreneurs. The idea of regulatory sandbox offers a compromise between the innovative financial market and the regulatory regime. Despite of lacking legal definition, the meaning of regulatory sandbox has been developed quite uniformly by supervisory authorities and in legal literature. A regulatory sandbox is a testing environment in which an entrepreneur selected in the recruitment process, under the supervision of the regulator, can try out innovative ideas before they are brought on the market. Start-ups as well as long-experienced companies are eager to cooperate with the supervisors. Crucial for the latter ones is the possibility

of obtaining information concerning business needs and regulatory changes expectations. The British regulatory sandbox established in 2016, as well as some Asian sandboxes serve as an example of effectively operating sandboxes. Worth to mention are actions taken by the Polish Financial Supervision Authority in order to establish financial regulatory sandbox, as well as governmental attempts to create regulatory sandbox in the Polish energy sector.

Keywords: Regulatory sandbox, financial market, supervisory authority, fintech, the Polish Financial Supervision Authority, KNF.

ANNA DĄBKOWSKA, BEATA SKRZYŃSKA
UNIWERSYTET WARSZAWSKI

WYZWANIA I PROBLEMY PRAWNE ZWIĄZANE Z HIGH-FREQUENCY TRADING

Streszczenie: High-frequency trading (dalej: „HFT") jest zupełnie nowym zjawiskiem, swego rodzaju przesłanką postępu technologicznego XXI w. High-frequency trading jest jedną z postaci handlu algorytmicznego. Inaczej można określić go mianem handlu wysokich częstotliwości, który polega głównie na składaniu w jak najkrótszym czasie (zazwyczaj mili- lub nawet nanosekundach) wielu zleceń, przy jednoczesnym osiąganiu niewielkich zysków z każdej operacji. Algorytmy HFT służą głównie analizowaniu poziomów cen i pozycji w czasie trwania sesji. Zazwyczaj transakcje są optymalizowane w trakcie trwania sesji, bez pozostawiania otwartej pozycji na kolejny dzień. System podejmuje decyzje znacznie szybciej niż byłby w stanie jakikolwiek człowiek. Rosnąca popularność HFT jest wynikiem postępującej automatyzacji i coraz większego znaczenia nowych technologii w większości sektorów rynku, w tym na rynku papierów wartościowych. Rola człowieka jest ograniczona - jego zadanie kończy się na zaprogramowaniu algorytmu, na którym bazuje system. Pomimo wielu zalet z automatycznymi systemami transakcyjnymi związane są również zagrożenia, takie jak możliwość popełniania przy ich użyciu przestępstwa manipulacji rynkowej oraz powodowanie nadmiernej niestabilności kursów. Z tego powodu wielu inwestorów wyraża sceptyczne podejście wobec systemów HFT, które nierzadko obarczane są winą za powodowanie krachów na giełdzie. Dodatkowo, jak podkreśliła K. Ochocińska, „komputeryzacja i automatyzacja doprowadza do coraz większej zależności pomiędzy giełdami w skali światowej i szybszego przenoszenia się zjawiska kryzysów"[1]. Celem poniższego artykułu jest przede wszystkim przybliżenie Czytelnikowi zjawiska HFT oraz zarysowanie najważniejszych wątpliwości, które się z nim wiążą, między innymi związanych z możliwością składania oświadczeń woli przez AI. Przedstawione zostały także rozwiązania, które wprowadzono w celu ochrony inwestorów przed manipulacjami rynkowymi.

Słowa kluczowe: High-frequency trading, handel algorytmiczny, handel wyskich częstotliwości, HFT, manipulacje rynkowe, oświadczenie woli, AI

[1] K. Ochocińska, *Wpływ unijnej regulacji handlu algorytmicznego na polskie prawo giełdowe,* MOP 2018, Nr 8.

1. WPROWADZENIE

Postępujący rozwój nowych technologii i sztucznej inteligencji odgrywa coraz istotniejszą rolę zarówno we wszystkich dziedzinach gospodarki, jak i w życiu codziennym. Korzystanie z automatyzacji i samouczących się algorytmów staje się powszechne, co nie eliminuje licznych wątpliwości, które spowodowane są coraz mniejszą kontrolą człowieka nad najróżniejszymi zjawiskami. Wspomniane kwestie nie omijają także prawa. Rozwój *artificial intelligence* (dalej: AI) wywiera wpływ zarówno na tworzenie, jak i stosowanie prawa, czego dowodem są m.in. próby uregulowania najbardziej problematycznych kwestii na poziomie unijnym (Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji[2]). Wśród problemów, z jakimi muszą zmierzyć się dzisiejsi prawodawcy, znajduje się m.in. zagadnienie odpowiedzialności karnej i cywilnej za decyzje podejmowane przez sztuczną inteligencję, a także podmioty praw autorskich do utworów stworzonych przez AI.

Do dziedzin prawa, dla których nowe technologie (w tym także sztuczna inteligencja) mogą okazać się szczególnie użyteczne, należy z pewnością prawo rynków kapitałowych. Obrót giełdowy, zwłaszcza obrót instrumentami finansowymi, od wielu lat korzysta z postępującej informatyzacji. Dowodem na to jest zdematerializowanie akcji, a także obsługiwanie procesów transakcyjnych przez zaawansowane oprogramowania komputerowe[3]. Wspomniane wyżej wątpliwości co do roli człowieka w procesach sterowanych przez technologie dotyczą również giełdy. Wśród ponoszonych problemów wskazuje się zwłaszcza na decyzyjność jednostki, a co za tym idzie - wpływ inwestora na losy inwestycji. Do najbardziej kontrowersyjnych zjawisk na giełdzie, które są powiązane z wykorzystaniem nowych technologii, należy High Frequency Trading, którego specyfika i wątpliwości prawne zostaną zarysowane w poniższym opracowaniu.

2. DEFINICJA HIGH FREQUENCY TRADING

Jak już zostało wspomniane, giełda z całą pewnością należy do tych obszarów, na które sztuczna inteligencja i postęp technologiczny ma znaczący

[2] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206&from=PL (dostęp: 6.06.2022)

[3] J. Buko, M. Rozwałka, *Wpływ rozwoju technologii teleinformatycznych na funkcjonowanie warszawskiej Giełdy Papierów Wartościowych*, Ekonomiczne Problemy Usług, 2016/123, s. 19.

wpływ. Wydaje się, że wykorzystanie algorytmów i sztucznych sieci neuronowych (a więc mechanizmów zbliżonych do ludzkiego systemu nerwowego, zdolnych do samodzielnej nauki) może zwiększyć szanse na udane inwestycje. Skoro sztuczna inteligencja jest w stanie bez udziału człowieka wyciągać wnioski, uzyskując nierzadko lepsze wyniki niż ludzki umysł, to być może uzyska lepsze efekty podczas analizy zjawisk na giełdzie, a następnie - skuteczniej inwestując pieniądze. Na powyższych założeniach opiera się mechanizm High Frequency Trading (handel wysokich częstotliwości). Podanie jednoznacznej definicji HFT nie jest łatwe, ale można zwrócić uwagę na kilka kluczowych kwestii.

Po pierwsze, handel algorytmiczny jest procesem transakcyjnym, który może być wykonany ręcznie, może być też częściowo zautomatyzowany lub całkowicie zautomatyzowany. Handel algorytmiczny można ogólnie podzielić na dwie kategorie:

1. *Algorithmic execution* (wykonanie za pośrednictwem algorytmów), która to polega na tym, że człowiek podejmuje decyzję wyboru instrumentu finansowego, a algorytmy określają sposób wykonania transakcji. Przykładem są strategie uzależnione od przedziału czasowego (*Time Weighted Average Price* – TWAP) czy obserwowanego obrotu (*Volume Weighted Average Price* – VWAP). Jest to często stosowana kategoria algorytmów dla większych wartości nominalnych.
2. *Algorithmic trade decision-making* (algorytmiczne podejmowanie decyzji transakcyjnych), która to polega na budowaniu modeli dokonujących wstępnej analizy informacji (makroekonomicznej, sektorowej czy mikrostrukturalnej). Decydują one o tym, które instrumenty podlegają transakcji. Następny krok może być analogiczny do poprzedniej kategorii, tj. określone są warunki, według których są realizowane transakcje. Należy jednak pamiętać, że decyzje dotyczące realizacji transakcji nie zawsze *de facto* wiążą się z faktyczną realizacją. Często celem jest składanie i anulowanie składanych zleceń, nie dochodząc tym samym do realizacji transakcji[4].

High Frequency Trading jest odmianą handlu algorytmicznego (ang. *algorithmic trading*), który zgodnie z ustawą z 29.07.2005 o obrocie instrumentami finansowymi[5] polega na nabywaniu lub zbywaniu instrumentów

[4] BIS, *High-frequency trading in the foreign exchange market*, Basel 2011, www.bis.org/publ/mktc05.htm (dostęp: 6.06.2022).
[5] t.j. Dz.U. z 2022 r. poz. 861 ze zm.

finansowych przy pomocy algorytmu komputerowego, który ustala indywidualne parametry zlecenia, przy czym następuje to bez udziału człowieka lub przy jego ograniczonym udziale. Innymi więc słowy handel algorytmiczny wykorzystuje komputery do przeprowadzenia zestawu instrukcji dotyczących zawarcia transakcji, jednocześnie powodując zyski z prędkością i częstotliwością niemożliwą do osiągnięcia przez człowieka. Algorytm będący podstawą do zawieranych w ten sposób transakcji w ułamku sekundy generuje informacje o tym, czy, w co i za ile warto zainwestować[6].

Po drugie, HFT odróżnia od innych transakcji handlu algorytmicznego bardzo duża liczba zleceń w tym samym czasie, przy jednoczesnym osiąganiu niewielkich zysków[7]. Dokładne częstotliwości są trudne do odmierzenia, określane są najczęściej w milisekundach[8]. Natomiast zysk liczony jest w kwotach często nieprzekraczających nawet ułamka groszy[9].

Zwrócić należy w tym miejscu uwagę na definicję legalną HFT, znajdującą się we wspomnianej już ustawie o obrocie instrumentami finansowymi. Zgodnie z art. 3 pkt 2c jest to handel algorytmiczny, w którym:

1. są wykorzystywane systemy teleinformatyczne (umożliwiające skrócenie czasu przesłania zlecenia do systemu jego wykonania i analizujące dane z rynku finansowego);
2. występuje duża liczba komunikatów wysyłanych w dniu obrotu do systemu obrotu instrumentami finansowymi (ocena spełnienia kryteriów ,,dużej liczby komunikatów" następuje przez odniesienie do Rozporządzenia 2017/565[10]).

Podsumowując wymienione powyżej charakterystyczne cechy HFT, można wskazać przede wszystkim, że handel wysokich częstotliwości jest odmianą handlu algorytmicznego, a więc polega na nabywaniu lub zbywaniu instrumentów finansowych za pomocą algorytmu komputerowego, przy jednoczesnym ograniczonym udziale człowieku albo jego braku. Od innych

[6] https://businessinsider.com.pl/gospodarka/makroekonomia/czym-jest-handel-algorytmiczny/0l8hy35 (dostęp: 22.05.2022).
[7] https://businessinsider.com.pl/gospodarka/makroekonomia/hft-co-to-jest/v3w5bx1 (dostęp: 22.05.2022).
[8] C. J. Lenczewski Martins, *Zastosowanie drapieżnych strategii w handlu o wysokiej częstotliwości*, Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia, 2017/4, s. 207.
[9] https://businessinsider.com.pl/gospodarka/makroekonomia/hft-co-to-jest/v3w5bx1 (dostęp: 23.05.2022).
[10] Rozporządzenie delegowane Komisji (UE) 2017/565 uzupełniające Dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy (Dz.Urz.UE.L 2017 Nr 87, str. 1).

rodzajów handlu algorytmicznego odróżnia się przede wszystkim częstotliwością zleceń (bardzo wysoka) i wysokością pojedynczego zysku (bardzo niska).

3. WĄTPLIWOŚCI ZWIĄZANE Z HFT

High frequency trading, tak jak wiele innych rozwiązań technologicznych, wywołuje liczne wątpliwości i obawy. Charakterystyczne cechy HFT, takie jak bardzo duża ilość zleceń, dokonywanie ich w bardzo krótkim odstępie czasu, a zwłaszcza brak kontroli człowieka nad składaniem zleceń przez algorytm sprawiają, że HFT postrzega się jako przyczynę występowania błyskawicznych krachów na giełdzie (*Flash Crash*), a także wskazuje się na możliwość popełniania przy ich użyciu przestępstwa manipulacji rynkowej[11].

Poza wątpliwościami występującymi wśród uczestników rynku, którzy przede wszystkim obawiają się wpływu HFT na losy ich inwestycji, należy wskazać także na problemy prawne, które polegają zwłaszcza na określeniu, kto składa oświadczenia woli w przypadku dokonywania transakcji przez algorytmy.

4. FLASH CRASH

Flash Crash to zjawisko występujące na giełdzie, które polega na nagłym, gwałtownym krachu. Zazwyczaj trwa bardzo krótko, kilkadziesiąt sekund lub minutę. Zwiastowane jest przez brak zleceń na danym walorze, natomiast po wystąpieniu tego epizodu następuje odrabianie strat. Krach na giełdzie to moment, który wywołuje strach inwestorów, ponieważ zazwyczaj prowadzi do sprzedaży posiadanych papierów wartościowych. Zauważono, że najczęściej zjawisko *Flash Crash* dotyczy akcji spółek finansowych, znacznie rzadziej problem pojawia się w przypadku papierów emitowanych przez spółki przemysłowe i handlowe. Pierwszy *Flash Crash* odnotowany został 6 maja 2010 r., znanym przypadkiem jest także krach na giełdzie w 2013 r., spowodowany informacją o rzekomym zamachu na Biały Dom. Intensywne załamania dotyczą zwłaszcza rynków kryptowalut, ale występują także na rynkach surowców, zwłaszcza srebra.

Przyczyna pojawiania się *Flash Crash* jest jak na razie niewyjaśniona. Badaniem powodów występowania zjawiska zajęło się wiele uczelni na całym świecie. Istnieją dwie dominujące teorie. Pierwsza z nich przyczynę upatruje

[11] K. Ochocińska, *op. cit.*, s. 430.

w złożeniu jednego, dużego zlecenia. Według pierwszej *Flash Crash* powodowany jest przez błędy w algorytmach - zwłaszcza tych wykorzystywanych w *high frequency trading*. Druga przyczynę upatruje w złożeniu jednego, dużego zlecenia.

Transakcje HFT podejmowane są w bardzo krótkim czasie. To właśnie w tym ułamku sekundy może wystąpić błąd popełniony przez algorytm. Nawet najlepiej napisane algorytmy obarczone są ryzykiem pomyłki. Możliwość popełnienia błędu przez maszynę, która składa transakcje właściwie bez kontroli człowieka, wywołuje wiele wątpliwości wśród uczestników rynku.

Według najnowszych badań jednak to jednak złożenie jednego, bardzo dużego zlecenia najczęściej prowadzi do wystąpienia *Flash Crash*. Oznacza to, że za pojawienie się omawianego krachu na giełdzie odpowiedzialny jest czynnik ludzki. Takie zdarzenie może wystąpić także przez pomyłkę – przykładowo inwestor zamiast złożyć zlecenie na 20 milionów, omyłkowo (wpisując błędną kwotę na arkuszu) składa na 20 miliardów, co powoduje gwałtowną reakcję i spadek notowań na giełdzie.

Chociaż najwięcej obaw budzi wykorzystywań maszyn, algorytmów i sztucznej inteligencji, które nie są na bieżąco kontrolowane przez człowieka, okazuje się, że w przypadku *Flash Crash* większym ryzykiem obarczone są transakcje dokonywane bezpośrednio przez człowieka. Potwierdzają to badacze z Uniwersytetu w Duisburgu-Essen, którzy w artykule ,,Impact and recovery process of mini flash crashes: An empirical study"[12] stwierdzili, że za 60% błyskawicznych krachów odpowiadają pojedyncze, bardzo duże zlecenie składane przez człowieka. Liczne, bardzo drobne transakcje dokonywane w ramach *high frequency trading* odgrywają mniejsze znaczenie w wywoływaniu *Flash Crash*.

5."DRAPIEŻNOŚĆ" STRATEGII SYSTEMU HFT

Jak sama nazwa wskazuje, większość strategii HFT opiera się na składaniu i realizacji zleceń w dużych częstotliwościach, co wiąże się też z wywoływaniem dużych zmian cenowych na rynku. Taki efekt dotyczy wielu strategii drapieżnych, przy czym niekoniecznie musi występować duża płynność na danym instrumencie finansowym. Przykładem może być generowanie fałszywego obrazu arkusza zleceń, co zachęca inne podmioty do podejmo-

[12] Braun T., Fiegen J.A., Wagner D.C., Krause S.M., Guhr T., *Impact and recovery process of mini flash crashes: An empirical study*. PLoS ONE, 2018/13(5), https://doi.org/10.1371/journal.pone.0196920 (dostęp: 6.06.2022).

wania określonych działań. Oczywiście może to mieć znamiona manipulacji, ale ze względu na wysokie częstotliwości zleceń, jest to trudno uchwytne.

Potencjalne ofiary strategii drapieżnych obawiają się przede wszystkim możliwego wymuszenia zamknięcia pozycji czy też połączenia tych działań ze zjawiskiem zwanym *hot potato*. Zjawisko to po raz pierwszy zostało określone w 1999 r. przez Evansa i Lyonsa. Jego specyfika polega na tym, że dealerzy walutowi przerzucają się między swoimi pozycjami, dążąc do tego, by przed jego końcem nie posiadać żadnych otwartych pozycji. Może to być szczególnie dotkliwe dla osób, które mają wyznaczone poziomy zlecenia *stop-loss*. Podmioty HFT wiedząc o tym, doprowadzają ceny do takiego poziomu, aby w szczególności tego typu zlecenia zostały zrealizowane. Inną wrażliwą sytuacją może być dążenie do tego, by nie posiadać pozycji otwartej pod koniec dnia, który powinien być rozumiany różnie w zależności od rynku, którego dotyczy. Podmioty HFT wiedząc o tym, mogą doprowadzić do pogorszenia cen przez okresowe występowanie zjawiska *hot potato*[13]. Oehmke i Brunnermeier podkreślają, że taka obawa nie jest związana jedynie z zamknięciem pozycji, ale też ze zmniejszeniem wartości instytucji finansowych poprzez likwidację długoterminowych inwestycji. Odróżnia się bowiem zamknięcie pozycji krótkoterminowej od długoterminowej. W przypadku znaczącej zmiany cenowej może właśnie w konsekwencji dojść nie tylko do zamknięcia krótkoterminowych pozycji, lecz także do zlikwidowania długoterminowych inwestycji. Doprowadza to do tego, że instytucja ponosi istotne straty, zatem zmniejsza się wartość[14].

Co ciekawe, techniki drapieżne często mylnie są uznawane za manipulację cen. Występują w dużej ilości i wielu odmianach. Ich specyfika polega na tym, że niektóre z nich mogą być zastosowane szybciej na rynku kapitałowym niż np. walutowym i odwrotnie. Wynika to przede wszystkim ze sposobu konstrukcji pewnych technik, ilości występujących podmiotów czy płynności instrumentów finansowych.

Jeżeli chodzi o same techniki, możemy je podzielić na: techniki manipulacyjne, techniki spowalniające działania innych algorytmów oraz techniki, które po prostu agresywnie wykorzystują przewagę, jaką daje technologia, do zawierania korzystnych transakcji.[15] Także najbardziej znane strategie

[13] C.J. Lenczewski Martins, *Zastosowanie drapieżnych strategii w handlu o wysokiej częstotliwości*, Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia, 2017/4, s. 210.
[14] Oehmke M., Brunnermeier M., *Predatory Short Selling*, NBER Working Papers 2013, Vol. 19514.
[15] *Ibidem*, s. 210

drapieżne opierają się na prędkości działania i są znane jako "quote stuffing", "smoking" lub "spoofing". Spośród tych strategii, *quote stuffing* jest prawdopodobnie najbardziej szkodliwą dla jakości rynku. Ogranicza ona dostęp wolniejszych traderów do rynków poprzez składanie dużej liczby zleceń, a następnie bardzo szybkie ich anulowanie. To z kolei prowadzi do zatłoczenia zleceń, co w najgorszym przypadku może powodować problemy techniczne i opóźnienia notowań o znaczną ilość czasu. Natomiast strategie *smokingu* i *spoofingu* polegają na manipulowaniu innymi uczestnikami rynku w taki sposób, aby brali udział w transakcjach w niekorzystnym momencie, np. tuż przed nadejściem istotnych wiadomości.[16] *Spoofing* jest metodą przeprowadzania handlu całkowicie zakazaną. Polega na składaniu zleceń o znaczących wartościach nominalnych tak, aby dać do zrozumienia, że cena danego instrumentu finansowego kieruje się w daną stronę. Nadaje on formalnie fałszywy obraz popytu bądź podaży.

Warto w tym miejscu zaznaczyć, że różnica między *quote stiffing oraz spoofing* polega na tym, że ta druga strategia jest kierowana do podmiotów nie będącymi podmiotami HFT. Ponadto *quote stiffing* ma na celu spowolnienie działania innych algorytmów w czasie, gdy *spoofing* wiąże się z manipulacją cenową, Oczywiście podane wyżej strategie to tylko przykłady, z którymi uczestnicy rynku mogą się spotkać.

Specyfikę działania HFT bardzo trafnie w swoim opracowaniu obrazuje Carlos Jorge Lenczewski Martins, który podaje, że o manipulacji będziemy mówić przykładowo, kiedy: „[...] instrument ZZZ jest pierwotnie kwotowany po 55,67 zł – 55,68 zł (Bid – Ask). Dzięki możliwościom technologicznym podmiot HFT wynajduje inny podmiot B, który ma zamiar złożyć zlecenie, podwyższając cenę do 55,68 zł – 55,70 zł. Zanim jednak jego zlecenie zostanie zrealizowane (przez podmiot B), podmiot HFT kupi wszelkie ilości instrumentu ZZZ, jakie są dostępne po 55,67 zł i niżej. Podmiot B nie wykona już żadnego zlecenia po 55,67 zł, ponieważ zostało już dokonane przez podmiot HFT, a dodatkowo cena wzrasta teraz, jak oczekiwano, do 55,68 zł – 55,70 zł. Z uwagi na fakt, że podmiot B może jedynie kupować po cenie 55,69 zł lub 55,70 zł, to w tym momencie podmiot HFT „odwraca" swoją pozycję, oferując teraz instrument ZZZ za 55,69 zł lub 55,70 zł. Jeśli podmiot jest dalej zainteresowany, będzie zmuszony zrealizować transakcję po oferowanej cenie. Podmiot HFT osiąga w ten sposób przychód w wysokości

[16] T.A. Vuorenmaa, *The Good, the Bad, and the Ugly of Automated High-Frequency Trading,* http://www.smallake.kr/wp-content/uploads/2014/11/The-Good-the-Bad-and-the-Ugly-of-Automated-High-Frequency-Trading.pdf (dostęp: 6.06.2022).

0,01 zł – 0,02 zł. Ta strategia może być szczególnie korzystna dla podmiotów HFT wówczas, kiedy mają do czynienia z algorytmami typu VWAP, opartymi na wielkości obrotu".

Ze względu na wysoką częstotliwość, często zidentyfikowanie użytej techniki rodzi wiele problemów. Dodatkowo ich konstrukcja może być często podobna. Jednakże co ciekawe, mimo że jedna technika może pociągać za sobą nielegalne zachowanie, o tyle druga, podobna do niej, może być już legalnie dozwolona.

Co ciekawe, stosowanie drapieżnych strategii nie jest niczym nowym. Najbardziej znanym przykładem drapieżnego handlu, choć nie ze świata HFT, są losy funduszu hedgingowego Long Term Capital Management (LTCM). W latach 90. LTCM zajmował się arbitrażem konwergencyjnym – strategią, w której pozycje *long-short* były przygotowane do zajęcia na długi okres (stąd nazwa "Long Term"). Jej słabym punktem było to, że pozycje LTCM były w dużym stopniu lewarowane i trudno było je utrzymać w tajemnicy. W 1998 r., w następstwie kryzysu zadłużeniowego w Rosji spowodowanego niespłaceniem długu nominowanego w rublach, pozycje LTCM w niektórych niepłynnych aktywach stały się dobrze znane w wielu dużych bankach inwestycyjnych na Wall Street, takich jak Goldman Sachs. Wiele z tych banków zaczęło następnie handlować przeciwko znanym pozycjom LTCM i w końcu doprowadziło LTCM na skraj bankructwa - co ciekawe, nieco później został on ponownie dokapitalizowany przez konsorcjum złożone z tych samych banków, które były (rzekomo) drapieżnikami. Tak więc drapieżne transakcje nie są niczym nowym na Wall Street[17].

6. SKŁADANIE OŚWIADCZEŃ WOLI

Jednym z najistotniejszych problemów, spowodowanych wykorzystywaniem HFT, jest kwestia składania oświadczeń woli.

W przypadku podejmowania czynności prawnych z innym podmiotem mamy zawsze do czynienia z drugim człowiekiem. Nawet jeśli, przykładowo, zawieramy umowę z osobą prawną, to nadal osoba ta działa przez organy, których członkami są przecież ludzie. W przypadku rozwiniętych technologii, takich jak roboty, sztuczna inteligencja i algorytmy - po drugiej stronie nie znajduje się żaden człowiek. Jego rola kończy się w momencie zaprogramowania, ewentualnie uru-

[17] Ibidem, s. 26.

chomienia, jednak żadna osoba fizyczna nie sprawuje bezustannej kontroli nad wyżej wymienionymi technologiami i nie podejmuje za nich decyzji.

Niniejsza sytuacja zachodzi również w przypadku transakcji zawieranych w ramach *high frequency trading*. Zlecenia składane są nie przez człowieka, ale przez algorytmy, które na podstawie obliczeń podejmują decyzje. Pojawia się więc pytanie - kto składa oświadczenia woli i na ile są one ważne?

Jedną z teorii jest przypisanie oświadczenia woli osobie, która władała komputerem (art. 60 i 61 § 2 KC)[18]. Jak zauważa *K. Ochocińska* we ,,Wpływie unijnej regulacji handlu algorytmicznego na polskie prawo giełdowe", oznacza to automatyzację obrotu prawnego, w którym zgoda, a nawet wiedza człowieka nie jest potrzebna do dokonania przez niego czynności prawnej.

Należy jednak zwrócić uwagę na fakt, że większość interpretacji przepisów KC dotyczących składania oświadczeń woli nie przewiduje uznania działań dokonywanych przez algorytmy jako prowadzących do zawierania umów: ,,Mamy tutaj osobę, a sztuczna inteligencja osobą nie jest, a więc nie ma zdolności do czynności prawnych (nawet ograniczonej) i przez to nie może składać oświadczeń woli skutecznych dla określonej czynności, np. zawarcia umowy sprzedaży czy o świadczenie usług"[19].

Zauważa się jednak konieczność uregulowania powyższej kwestii - do podjęcia takiego wyzwania zmierza prawodawstwo unijne[20].

7. OBOWIĄZKI FIRM INWESTYCYJNYCH I OSÓB PROWADZĄCYCH RYNEK REGULOWANY

W celu przeciwdziałania wspomnianym zagrożeniom na firmy inwestycyjne korzystające z rozwiązań HFT nałożono różne obowiązki, w tym obowiązek wdrażania systemów i mechanizmów kontroli ryzyka. Dodatkowo

[18] K. Ochocińska, *op. cit.*, s. 430.

[19] M. Nowakowski, *Czy sztuczna inteligencja będzie zawierała umowy, zgodnie z prawem?* https://alebank.pl/czy-sztuczna-inteligencja-bedzie-zawierala-umowy-zgodnie-z-prawem/?id=331389&catid=18911&cat2id=625&cat3id=25924&fbclid=IwAR2T3yEF6DF6K60oKolNe4yGE8N1b3Ev7_AW_WN4xo1LlQNG6UyoA7E0DYQ (dostęp: 6.06.2022).

[20] Wniosek rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (COM/2021/206 final).

dyrektywa MiFID II[21] przewiduje obowiązki informacyjne, polegające na powiadomieniu organu nadzoru i organu systemu obrotu o stosowaniu techniki handlu algorytmicznego, a także na przekazywaniu informacji związanych z wykorzystywaniem tejże techniki.

Obowiązkami objęte są także osoby prowadzące rynek regulowany, mianowicie do ich zadań należy posiadanie przez rynek regulowany systemów, procedur i mechanizmów w celu zapewnienia tego, że systemy handlu algorytmicznego nie doprowadzą lub nie przyczynią się do powstawania zakłóceń na rynku.

Profesor Chłopecki jednak słusznie zwraca uwagę na fakt, że w przypadku zawierania umów ze sztuczną inteligencją (a za jej słabą odmianę uważa HFT) ,,ludzki kontrahent ma prawo wiedzieć, że umowa jest zawierana za pośrednictwem SI", a co za tym idzie - powinien mieć możliwość odmowy zawarcia takiej umowy[22]. Ponieważ aktualnie ani unijne, ani krajowe regulacje nie przewidują nałożenia obowiązku ,,ujawnienia" umów zawieranych przez SI, należy uznać, że podmioty będące osobami fizycznymi, prawnymi lub niepełnymi osobami prawnymi (a więc w każdym przypadku działającymi za pośrednictwem człowieka) nie są objęte wystarczającą ochroną.

8. PODSUMOWANIE

Wykorzystywanie nowych technologii niesie za sobą wiele korzyści, ale jednocześnie obarczone jest pewnym ryzykiem. Nie inaczej jest w przypadku *high frequency trading*, który co prawda może przyczynić się do wzrostu tempa i wielkości obrotów, a także zwiększenia płynności rynku oraz obniżenia kosztów dokonywania transakcji[23], to jednak wywołuje liczne obawy uczestników rynku i nierozwiązane do tej pory dylematy prawne.

Nierzadko również ze względu na różnorodność technik HFT niełatwo jest określić, która z nich może być uznana za dozwoloną, a która za nielegalną. Rodzi to za tym szereg problemów, związanych zwłaszcza z kwestią składania oświadczeń woli. Niestety jest to temat rzeka, który wykracza swoim zakresem ponad ramy tego opracowania. Warte zauważenia jest jednak to, że ze względu na zwiększający się wpływ technologii na życie człowieka, biznes

[21] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE.

[22] A. Chłopecki, *Sztuczna inteligencja – szkice prawnicze i futurologiczne*. *Wyd. 2*, Warszawa 2021.

[23] K. Ochocińska, *op. cit.*, s. 430.

oraz rynek finansowy ustawodawstwo unijne powinno sprostać wymaganiom przed nim postawionym.

Pozostaje mieć nadzieję, że prawodawca sprosta wyzwaniu wprowadzenia adekwatnych regulacji, które zapewnią bezpieczeństwo obrotu, jednocześnie korespondując z zasadami prawa cywilnego (zwłaszcza w zakresie składania oświadczeń woli), nie doprowadzając jednocześnie do zablokowania *high frequency trading* i rozwoju technologicznego.

BIBLIOGRAFIA

BIS, *High-frequency trading in the foreign exchange market*, Basel 2011, www.bis.org/publ/mktc05.htm (dostęp: 6.06.2022).

Braun T., Fiegen J.A, Wagner D.C, Krause S.M., Guhr T., *Impact and recovery process of mini flash crashes: An empirical study*, PLoS ONE, 2018/13(5).

Buko J., Rozwałka M., *Wpływ rozwoju technologii teleinformatycznych na funkcjonowanie warszawskiej Giełdy Papierów Wartościowych, Ekonomiczne Problemy Usług*, 2016/123.

Chłopecki A., *Sztuczna inteligencja – szkice prawnicze i futurologiczne. Wyd. 2*, Warszawa 2021.

Lenczewski Martins C. J., *Zastosowanie drapieżnych strategii w handlu o wysokiej częstotliwości*, Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia, 2017/4.

Nowakowski M., *Czy sztuczna inteligencja będzie zawierała umowy, zgodnie z prawem?,* https://alebank.pl/czy-sztuczna-inteligencja-bedzie-zawierala-umowy-zgodnie-z-prawem/?id=331389&catid=18911&cat2id=625&cat3id=25924&fbclid=IwAR2T3yEF6DF6K60oKolNe4yGE8N1b3Ev7_AW_WN4xo1LlQNG6UyoA7E0DYQ (dostęp: 6.06.2022).

Ochocińska K., *Wpływ unijnej regulacji handlu algorytmicznego na polskie prawo giełdowe*, Monitor Prawniczy, 2018/8.

Oehmke M., Brunnermeier M., *Predatory Short Selling,* NBER Working Papers 2013/1951.

Vuorenmaa T.A. , *The Good, the Bad, and the Ugly of Automated High-Frequency Trading,* http://www.smallake.kr/wp-content/uploads/2014/11/The-Good-the-Bad-and-the-Ugly-of-Automated-High-Frequency-Trading.pdf (dostęp: 6.06.2022).

Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE.

Rozporządzenie delegowane Komisji (UE) 2017/565 uzupełniające Dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy (Dz.Urz.UE.L 2017 Nr 87, str. 1).

Wniosek rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (COM/2021/206 final).

https://businessinsider.com.pl/gospodarka/makroekonomia/hft-co-to-jest/v3w5bx1 (dostęp: 23.05.2022).

https://businessinsider.com.pl/gospodarka/makroekonomia/czym-jest-handel-algorytmiczny/0l8hy35 (dostęp: 22.05.2022).

https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206&from=PL (dostęp: 6.06.2022)

CHALLENGES AND LEGAL ISSUES RELATED TO HIGH-FREQUENCY TRADING

Abstract: High-frequency trading (hereinafter: "HFT") is a completely new phenomenon, a kind of premise of the technological progress of the 21st century. High-frequency trading is one form of algorithmic trading. In other words, it can be referred to as high-frequency trading, which mainly involves placing multiple orders in the shortest possible time (usually milli-seconds or even nanoseconds), while making small profits on each operation. HFT algorithms are mainly used to analyze price levels and positions during the session. Typically, trades are optimized during the session, without leaving the position open for another day. The system makes decisions much faster than any human could. The growing popularity of HFT is a result of increasing automation and the growing importance of new technologies in most market sectors, including the securities market. The role of man is limited - his task ends with programming the algorithm on which the system is based. Despite the many advantages, there are also risks associated with automated trading systems, such as the possibility of committing a crime of market manipulation using them and causing excessive volatility in prices. For this reason, many investors are skeptical about HFT systems, which are often blamed for causing crashes on the stock market. Additionally, as highlighted by K. Ochocińska, "computerization and automation lead to increasing interdependence between

stock exchanges on a global scale and faster transmission of crises[24]. The purpose of the following article is primarily to introduce the reader to the HFT phenomenon and to outline the most important doubts it raises, including those related to the possibility of making statements of intent by AI. The solutions that have been put in place to protect investors from market manipulation are also presented.

Key words:

[24] Ibidem.

CZĘŚĆ II.

WYMIAR SPRAWIEDLIWOŚCI I PRAWA CZŁOWIEKA

JULIA JĘDRYCZKO
UNIWERSYTET JAGIELLOŃSKI

PROGNOZA KRYMINOLOGICZNA SPRAWCY PRZESTĘPSTWA SPORZĄDZONA PRZEZ PROGRAM KOMPUTEROWY – PROBLEMATYKA STOSOWANIA ALGORYTMU COMPAS W AMERYKAŃSKIM WYMIARZE SPRAWIEDLIWOŚCI

Abstrakt: Artykuł przedstawia problematykę stosowania programu komputerowego podczas określania prognozy kryminologicznej sprawcy w amerykańskim systemie prawa karnego. Autorka opisuje sposób działania algorytmu matematycznego będącego podstawą owego programu wskazując na kontrowersje płynące z jego wykorzystywania. Przedmiotem opracowania jest również analiza wybranych procesów sądowych w Stanach Zjednoczonych podczas których użyto algorytmu COMPAS.

Słowa kluczowe: prognoza kryminologiczna, algorytm, COMPAS, środki probacyjne, recydywa, nowe technologie

1. WSTĘP

Dynamiczny rozwój nowych technologii w XXI wieku sprawił, że programy komputerowe są obecnie wykorzystywane w prawie każdej dziedzinie naszego życia. Nowoczesne narzędzia tworzone są przede wszystkim w celu zaoszczędzenia cennego czasu lub ułatwienia przeprowadzenia skomplikowanego procesu myślowego. Komputer co do zasady ma działać sprawniej i skuteczniej niż człowiek zmniejszając ryzyko popełnienia błędu w danym procesie. Zmiany związane z wprowadzaniem nowych technologii do życia

codziennego nie ominęły również systemów wymiaru sprawiedliwości na całym świecie. W sądownictwie na szeroką skalę wykorzystuje się obecnie programy komputerowe mające na celu między innymi planowanie wokandy, rejestrowanie przychodzących i wychodzących pism sądowych czy archiwizowanie akt sprawy.

Jednym z procesów, który do niedawna był zupełnie pozbawiony jakiegokolwiek udziału technologii jest proces określania prognozy kryminologicznej sprawcy. W Polsce, pozytywna prognoza kryminologiczna jest jedną z najważniejszych przesłanek orzeczenia środka probacyjnego w postaci warunkowego umorzenia postępowania, warunkowego zawieszenia wykonania kary lub warunkowego przedterminowego zwolnienia z zakładu karnego. Zastosowanie jednego z trzech środków probacyjnych polega na zwolnieniu sprawcy z dolegliwości jaką jest wykonywanie kary lub prowadzenie postępowania karnego na określony ustawowo okres próby, w trakcie którego na sprawcę nałożone są różnego rodzaju obowiązki. Nierzadko sąd poddaje również sprawcę dozorowi kuratora sądowego. Pozytywna prognoza kryminologiczna jest istotą szeroko pojętej probacji. Wskazuje ona na istnienie uzasadnionego przekonana, że sprawca nie popełni ponownie przestępstwa i jest przygotowany do życia w społeczeństwie, a więc tym samym jego przebywanie warunkach wolnościowych nie stanowi zagrożenia. W świetle polskich regulacji określając prognozę kryminologiczną sąd bierze pod uwagę między innymi postawę, właściwości i warunki osobiste sprawcy, a w przypadku niektórych środków probacyjnych także okoliczności popełnienia czynu, zachowanie po popełnieniu przestępstwa oraz dotychczasowy sposób życia sprawcy[1]. Szczegółowe elementy prognozy różnią się między sobą w zależności od specyfiki danego środka probacyjnego. W praktyce, sędzia analizuje poszczególne elementy prognozy kryminologicznej, wysłuchuje oskarżonego (lub osadzonego) i stwierdza czy istnieje owe uzasadnione przekonanie, że sprawca nie popełni ponownie przestępstwa i będzie przestrzegał porządku prawnego. Cały proces formułowania prognozy kryminologicznej jest więc *stricto* procesem myślowym sędziego, wynikającym z jego wiedzy i doświadczenia życiowego.

Wiedza, że w niektórych porządkach prawnych powyższego procesu dokonuje program komputerowy, skłoniła mnie do podjęcia szerszej analizy tej problematyki. Efektem mojej pracy jest niniejszy tekst, traktujący o funkcjonowaniu programu COMPAS, używanego do określania

1 A. Zoll [w:] *Kodeks karny. Część ogólna. Tom I. Część II. Komentarz do art. 53-116, wyd. V*, red. W. Wróbel, Warszawa 2016, art. 66, s. 279-280

prognozy kryminologicznej sprawcy m.in. w niektórych stanach Stanów Zjednoczonych. Niniejszy artykuł w sposób szczegółowy opisuje sposób działania algorytmu, na którym oparte jest funkcjonowanie programu COMPAS, z uwzględnieniem analizy zmiennych branych pod uwagę w całym procesie. Jako, iż działanie jakichkolwiek ingerencji w system prawa karnego najlepiej ocenia się poprzez skutki ich stosowania w praktyce, drugą część tekstu poświęciłam analizie orzecznictwa amerykańskiego, opisując najbardziej kontrowersyjne procesy sądowe, w których użyto programu COMPAS do określenia prognozy kryminologicznej oskarżonego. Ostatnia część artykułu opiera się na analizie śledztwa dziennikarzy ProPublica oraz ich raportu, w którym opisano główne wady działania algorytmu COMPAS, odnosząc je do konkretnych przypadków zastosowania programu. Biorąc pod uwagę fakt, iż postęp technologiczny związany z procesem globalizacji zwiększa tempo w każdej kolejnej dekadzie, analiza tytułowej problematyki poprzez zwrócenie uwagi na wady i zalety zastosowania programu komputerowego w określaniu prognozy kryminologicznej sprawcy ma ogromne znaczenie. Niewykluczone bowiem, że z czasem również polski ustawodawca zdecyduje się na wprowadzenie podobnych rozwiązań do polskiego systemu prawa karnego.

2. ALGORYTM COMPAS

W historii rozwoju nowych technologii przyszedł moment, w którym uznano, że analizy prognozy kryminologicznej sprawców przestępstw mógłby dokonywać komputer. W latach 90-tych XX wieku amerykańska firma Northpointe (obecnie Equivant) opracowała COMPAS (ang. *Correctional Offender Management Profiling for Alternative Sanctions*) – specjalny program ułatwiający analizę prognozy kryminologicznej sprawców. Narzędzie ma za zadanie zarządzać sprawami karnymi i wspomagać proces decyzyjny sędziów w zakresie oceny prawdopodobieństwa, że oskarżony stanie się recydywistą. Całość oparta jest na specjalnym algorytmie mającym na celu przypisać potencjalne ryzyko wystąpienia zjawiska recydywizmu w konkretnym przypadku. Northpointe stworzył trzy skale oceny ryzyka, które w założeniu mają być używane do różnych przestępstw w zależności od ich powagi:

- *Pretrial Release Risk Scale* bada możliwość niestawienia się danej osoby lub popełnienia nowych przestępstw podczas warunkowego zwolnienia. Oceniając ryzyko algorytm bierze pod uwagę między innymi zarzuty, historie aresztowań, stabilność mieszkaniową, status

zatrudnienia, więzi społeczne czy nadużywanie różnych substancji;

- *General Recidivism Scale* jest skalą ogólną przeznaczoną do oceny ryzyka popełnienia przestępstwa po warunkowym zwolnieniu. Głównymi zmiennymi są tutaj historia kryminalna sprawcy, udział w przestępczości narkotykowej czy przejawy przestępczości w okresie nieletniości;
- *Violent Recidivism Scale* służy do oceny prawdopodobieństwa popełnienia czynu brutalnego, z użyciem przemocy, po warunkowym zwolnieniu sprawcy. Skala obejmuje wskaźniki takie jak historia użycia przemocy, historia naruszeń przepisów prawa, problemy zawodowe, problemy edukacyjne, wiek w momencie przyjęcia do zakładu karnego oraz wiek pierwszego aresztowania.

Do każdej skali stworzono specjalny algorytm matematyczny służący określeniu poziomu prawdopodobieństwa wystąpienia zjawiska recydywy. Tytułem przykładu *Violent Recidivism Scale* oblicza owe prawdopodobieństwo w następujący sposób:

$$s = a\,(-w) + a_{first}\,(-w) + h_{violence}w + v_{edu}w + h_{nc}w$$

W powyższym wzorze s oznacza ocenę ryzyka recydywy, a obecny wiek, w mnożnik wagi, a_{first} wiek w momencie pierwszego aresztowania, $h_{violence}$ historię przemocy, v_{edu} poziom wykształcenia zawodowego, h_{nc} historię naruszeń przepisów prawa. Mnożnik wagi jest zmienną autorsko opracowaną przez Northpointe na podstawie badań własnych [2].

Podstawę danych potrzebnych do sporządzenia końcowej oceny prawdopodobieństwa wystąpienia zjawiska recydywy stanowi kwestionariusz składający się ze 137 pytań. Część pytań funkcjonariusze wypełniają indywidualnie na podstawie danych z państwowych rejestrów (podstawowe dane dotyczące osoby oskarżonego, a także te dotyczące jego historii kryminalnej). Jest też część pytań, na które odpowiada sam oskarżony. W puli pytań dla oskarżonego można znaleźć takie jak: „Czy któryś z Twoich rodziców odbywał kiedykolwiek karę pozbawienia wolności?", „Jak często wdawałeś się w bójki w okresie szkolnym?", „Ilu z Twoich przyjaciół nielegalnie przyjmuje narkotyki?", „Czy byłeś kiedykolwiek członkiem zorganizowanej grupy przestępczej?" [3].

[2] https://en.wikipedia.org/wiki/COMPAS_(software) (dostęp: 01.05.2022).
[3] https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE (dostęp: 01.05.2022).

COMPAS jest obecnie powszechnie używany w amerykańskich sądach, między innymi w stanie Nowy Jork, Wisconsin, California oraz na Florydzie. Podobnych systemów używa się także między innymi w Kanadzie, Holandii oraz Wielkiej Brytanii. Program traktowany jest jako narzędzie pomocnicze w sądownictwie. Oznacza to, że wynik badania w żaden sposób nie może narzucać sędziemu kształtu decyzji. Nie oznacza to jednak, że sędzia nie pozostaje pod choćby nieświadomym wpływem oceny dokonanej przez COMPAS, co może determinować sposób jego rozstrzygnięcia w sprawie. W związku z wyżej wymienionym ryzykiem COMPAS był wielokrotnie krytykowany. W opinii publicznej podnoszono między innymi, że ponieważ algorytm używany przez firmę stanowi przedmiot tajemnicy handlowej, nie może być weryfikowany przez społeczeństwo w zakresie poziomu jego bezstronności, co może stanowić naruszenie prawa do należytego procesu. Kolejnym zarzutem był fakt, iż algorytmy są ściśle zależne od danych, na których bazują. Jeśli więc dane są w jakikolwiek sposób stronnicze, wynik badania również będzie cechował się stronniczością[4].

3. COMPAS W AMERYKAŃSKIM ORZECZNICTWIE

Jedną z najgłośniejszych i najbardziej kontrowersyjnych spraw związanych z użyciem programu COMPAS jest sprawa *Loomis vs. Wisconsin*. Na początku 2013 roku Ericowi Loomisowi postawiono pięć zarzutów związanych z udziałem w samochodowej strzelaninie. Loomis zaprzeczył jakoby brał udział w samej strzelaninie, potwierdził jednak, iż później tego samego wieczoru prowadził samochód widziany na miejscu zdarzenia. Oskarżony przyznał się również do dwóch mniej surowych zarzutów tj. do próby ucieczki przed funkcjonariuszem ruchu drogowego oraz do prowadzenia pojazdu mechanicznego bez zgody właściciela. Przed wydaniem wyroku funkcjonariusz Departamentu Więziennictwa (*Department of Corrections*) przedstawił sądowi raport PSI [5], który zawierał ocenę ryzyka COMPAS. Na rozprawie sąd pierwszej instancji odniósł się do oceny COMPAS w swoim orzeczeniu i częściowo na jej podstwie skazał Erica Loomisa na sześć lat pozbawienia wolności

[4] K. Mamak, *Rewolucja cyfrowa a prognoza kryminologiczna* [w:] *Rewolucja cyfrowa a prawo karne*, LEX nr 369493164.

[5] PSI – ang. *Pre-Sentence Investigation*. Raporty wypełniane w Stanach Zjednoczonych przez kuratorów sądowych przed wydaniem wyroku, które dostarczają sądowi szczegółowych informacji na temat przestępców stawianych przed sądem w celu skazania. Raport zawiera między innymi informacje o historii kryminalnej, informacje biospołeczne, dane organów ścigania oraz ocenę ryzyka.

i pięć lat rozszerzonego nadzoru. Loomis odwołał się od wyroku skazującego argumentując, że poleganie przez sąd na ocenie ryzyka COMPAS naruszyło jego prawo do rzetelnego procesu. Ponieważ metodologia użyta do sporządzania raportów jest tajemnicą handlową oskarżony podnosił, iż naruszyło to również jego prawo do zindywidualizowanej kary oraz skazania na postawie rzetelnych informacji (odpowiednik polskiej zasady prawdy materialnej). Ponadto, Eric Loomis zarzucił sądowi, iż ten naruszył amerykańską Konstytucję opierając się na ocenie uzależniającej poziom ryzyka od płci sprawcy. Sąd pierwszej instancji odrzucił wniosek Erica Loomisa, jednak na dalszym etapie postępowania Sąd Apelacyjny Wisconsin zdecydował o skierowaniu apelacji do Sądu Najwyższego Wisconsin [6].

Sąd Najwyższy Wisconsin odrzucił apelację Erica Loomisa. W wyroku oddalono argumenty dotyczące naruszenia zasady należytego procesu oraz stwierdzono, że Loomis nie dostarczył wystarczających dowodów na to, iż sąd skazujący faktycznie uzależnił kształt wyroku od płci skazanego. Stwierdzono również, że COMPAS korzysta z publicznie dostępnych danych, a co za tym idzie oskarżony miał możliwość wyjaśnienia lub zaprzeczenia przed sądem informacjom, które posłużyły do sporządzenia raportu, a zatem istniała możliwość weryfikacji tych informacji. W kontekście indywidualizacji kary sędzia Bradley, członek składu orzekającego, podniósł, iż COMPAS dostarcza jedynie zbiorczych danych na temat ryzyka recydywy dla grup podobnych do sprawcy oraz że raport nie był jedyną podstawą do wydanie decyzji, a sądy mają możliwość niezgodzenia się z oceną programu w każdym z rozpatrywanych przypadków [7].

Mimo, iż argumenty oskarżonego nie zostały ostatecznie uznane co doprowadziło do odrzucenia apelacji, najważniejszym z punktu widzenia stosowania programu COMPAS wydaje się to, co sąd podniósł w dalszej części orzeczenia. Sędzia Bradley zaznaczył, że sędziowie muszą być bardzo ostrożni przy stosowaniu takich ocen ryzyka wystąpienia zjawiska recydywizmu. W uzasadnieniu określono sposób przedstawiania tych ocen sądom rozpatrującym sprawę przez kuratorów oraz zakres w jakim sędziowie mogą z tych

[6] Analiza systemu sądownictwa w Stanach Zjednoczonych i przepisów procesowych dotyczących apelacji są zagadnieniem zbyt obszernym aby poruszać je w niniejszym artykule. Kluczowym jest jedynie fakt, że system sądownictwa w Stanach Zjednoczonych nie jest scentralizowany – istnieją sądy federalne orzekające na podstawie prawa federalnego oraz odrębne stanowe systemy sądownictwa, zróżnicowane w zależności każdego stanu. Na czele sądownictwa stanowego stoi Stanowy Sąd Najwyższy. Omawiane zagadnienie prawne okazało się więc na tyle istotne iż trafiło ostatecznie pod rozstrzygnięcie Stanowego Sądu Najwyższego.

[7] https://harvardlawreview.org/2017/03/state-v-loomis/ (dostęp: 01.05.2022).

ocen korzystać. Sąd stwierdził również, że ocena ryzyka nie może być wykorzystywana do określenia surowości kary. Dodatkowo, sędziowie korzystający z raportów powinni wskazać w orzeczeniu inne czynniki, które zadecydowały o takim, a nie innym kształcie wyroku. Wskazano, że dokument jakim jest raport PSI z oceną ryzyka na podstawie COMPAS ma zawierać „pięć pisemnych ostrzeżeń" dla sędziów m.in. uwagi podkreślające, że wyniki COMPAS-u nie są w stanie zidentyfikować poziomu indywidualnego ryzyka, ponieważ opierają się na danych grupowych, oraz że dane opracowane zostały na podstawie próby krajowej, nie uwzględniającej danych z konkretnego stanu. Dodano również, że zalecenia dotyczące używania systemu COMPAS powinny być aktualizowane na bieżąco wedle najnowszej wiedzy. Tym samym, Sąd Najwyższy Wisconsin jasno przekazał potrzebę sceptycznego podejścia do dokładności narzędzia oceny ryzyka jakim jest COMPAS w procesie orzekania [8].

Orzeczenie w sprawie Loomis vs. Wisconsin nie zakończyło jednak sporu wokół kontrowersyjnego oprogramowania. 23 maja 2016 roku grupa amerykańskich dziennikarzy śledczych organizacji ProPublica opublikowała artykuł podsumowujący wyniki autorskich analiz nad rzetelnością algorytmu wykorzystywanego przez Northpointe. W tekście „Machine Bias" stwierdzono, iż sprawcy czarnoskórzy są prawie dwukrotnie bardziej narażeni na ocenę w przedziale wysokiego ryzyka przez program COMPAS niż pozostali sprawcy przestępstw, podczas gdy w rzeczywistości ostatecznie nie stają się recydywistami. Algorytmowi zarzucono również odwrotny błąd wśród osób białych, które znacznie częściej niż osoby czarnoskóre określane są jako sprawcy o niskim poziomie ryzyka, a zarazem znacznie częściej ponownie popełniają przestępstwa. Autorzy wskazali również, iż jedynie 20 % sprawców co do których przewidziano popełnienie w przyszłości przestępstwa z użyciem przemocy, rzeczywiście to przestępstwo popełniło [9].

Publikacja artykułu rozpoczęła w Stanach Zjednoczonych publiczną dyskusję medialną nad potencjalnym ryzykiem, iż algorytm narzędzia używanego w amerykańskim wymiarze sprawiedliwości jest silnie stronniczy, a dokładniej szerzy rasizm. Warto w tym miejscu zaznaczyć, iż fakt bycia osobą czarnoskórą nie jest w żaden sposób odnotowywany na kwestionariuszu pytań (tzn. nie ma wprost pytania o rasę sprawcy). Analiza dokonana przez ProPublica polegała więc na przekrojowych badaniach procesów karnych w kraju i wykazaniu, iż mimo iż algorytm „nie wie" jakiego koloru skóry jest sprawca, to liczby

[8] https://harvardlawreview.org/2017/03/state-v-loomis/ (dostęp: 01.05.2022).
[9] https://en.wikipedia.org/wiki/COMPAS_(software) (dostęp: 01.05.2022).

pokazują, że działa on z pokrzywdzeniem osób czarnoskórych. Wraz z publikacją artykułu ukazał się osobny tekst o tytule *„How we analized the Compas Recidivism Algorithm"* opisujący szczegóły powstawania analizy dziennikarzy tj. harmonogram pracy, metodologię badań, charakterystykę grupy badawczej czy przyjętą definicję recydywizmu [10].

Artykuł przytacza kilka przykładów spraw, w których stronniczość oprogramowania jest najbardziej widoczna i kontrowersyjna. Jednym z powołanych przykładów jest zestawienie spraw dwójki sprawców – 18-letniej czarnoskórej Brishy Borden oraz 41-letniego Vernona Pratera – mężczyzny o białym kolorze skóry. Brisha biegnąc w pośpiechu ze swoją przyjaciółką zauważa niezabezpieczony sprzęt przy ulicy - mały rower i dziecięcą hulajnogę. Zabierają je i jadą kawałek wzdłuż drogi. Po okrzykach matki dziecka, do którego należy skradziony sprzęt i która zauważyła całe zdarzenie, dziewczęta zostawiają rzeczy na poboczu i oddalają się z miejsca zdarzenia. Sytuację zauważa jednak sąsiad, który wzywa policje, a Brisha z przyjaciółką zostają aresztowane pod zarzutem kradzieży mienia o wartości 80 dolarów. Vernon Prater zostaje natomiast skazany za kradzież narzędzi o wartości 86 dolarów z pobliskiego sklepu Home Depot. Prater w momencie stawiania zarzutów jest już doświadczonym przestępcą – w przeszłości został skazany za napad z bronią w ręku oraz usiłowanie napadu z bronią i odbył karę 5 lat pozbawienia wolności. Brisha Borden również była karana w przeszłości, ale jedynie za kilka drobnych wykroczeń w czasie, gdy była nieletnia. Przed każdym z orzeczeń w sprawie powyższych sprawców program COMPAS badał prawdopodobieństwo popełnienia przez nich ponownie przestępstwa. W przypadku Brishy Borden program wskazał wysokie prawdopodobieństwo na poziomie 8, w przypadku Vernona Pratera program wskazał niskie ryzyko na poziomie 3. Po latach okazało się, że prognoza była zupełnie nietrafna. Brisha Borden nie popełniła ponownie przestępstwa, Vernon Prater wykonuje natomiast karę 8 lat pozbawienia wolności za włamanie do magazynu i kradzież elektroniki o wartości tysięcy dolarów [11].

Artykuł ukazuje również przykłady spraw, w których niezależnie od rzetelności algorytmu, zapoznanie się sędziego z raportem i oceną ryzyka COMPAS może zupełnie zmienić bieg procesu. Jedną z takich spraw był proces Paula Zilly'ego oskarżonego o kradzież kosiarki i kilku narzędzi. W trybie

[10] https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm (dostęp: 01.05.2022).
[11] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (dostęp: 01.05.2022).

podobnym do polskiego trybu konsensualnego prokurator zaproponował karę jednego roku pozbawienia wolności oraz dozór po zwolnieniu z zakładu karnego. Obrońca Zilly'ego przyjął warunki ugody. Sędzia James Babler zapoznał się z oceną ryzyka COMPAS sporządzoną dla Paula Zilly'ego, która stwierdzała wysokie prawdopodobieństwo popełnienia przestępstwa z użyciem przemocy oraz średnie ryzyko ogólnej recydywy. Sędzia stwierdził podczas procesu: „Kiedy patrzę na ocenę ryzyka, jest tak źle jak tylko może być", a następnie unieważnił ugodę uzgodnioną przez prokuraturę i obronę oraz skazał Paula Zilly'ego na 2 lata pozbawienia wolności i 3 lata dozoru [12].

Całe opracowanie dziennikarzy ProPublica jest bardzo obszerne, a przytoczenie wszystkich historii, liczb, statystyk nie jest możliwe na łamach niniejszego artykułu. Oprócz głównego zarzutu wobec algorytmu dotyczącego dyskryminacji oskarżonych ze względu na kolor skóry, tekst poddaje w wątpliwość fakt czy program wykorzystywany przez amerykański wymiar sprawiedliwości stanowi realne ułatwienie procesu dokonywania prognozy kryminologicznej przez sędziów, czy też w istocie wywołuje chaos i krzywdzi obywateli naruszając podstawowe zasady amerykańskiego procesu karnego. Podnosi się, że algorytm nie jest skuteczny, ponieważ stworzone przez niego przewidywania nie są ostatecznie zgodne z rzeczywistością. Badania dziennikarzy ProPublica wskazują na szereg spraw, w których ryzyko określone przez algorytm mija się z rzeczywistością. Z drugiej zaś strony, należy pamiętać, że prognoza kryminologiczna dokonywana indywidualnie przez sędziego, bez użycia jakiejkolwiek technologii również nie zawsze ma pokrycie z przyszłością oskarżonego. Ocena prognozy kryminologicznej nigdy nie dawała i nie będzie dawać stuprocentowej gwarancji, że sprawca nie popełni ponownie przestępstwa.

4. KONTROWERSJE WYNIKAJĄCE Z UŻYCIA ALGORYTMU COMPAS

Najbardziej kontrowersyjnym aspektem programu COMPAS pozostaje fakt, iż metodologia obliczeń stanowi tajemnice handlową i nie jest możliwe prześledzenie procesu, w którym uzyskano dla oskarżonego określony wynik. Z perspektywy oceny ryzyka dokonywanej przez sędziego również nie jest nam znany szczegółowy bieg jego procesu myślowego w czasie dokonywania

[12] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (dostęp: 01.05.2022).

oceny prognozy kryminologicznej W przypadku klasycznej oceny sprawcy przez sędziego zachodzi jednak pewna znacząca różnica.

Po pierwsze, sędzia uzasadnia swoją decyzję, w tym argumenty dotyczące pozytywnej lub negatywnej prognozy kryminologicznej w uzasadnieniu w wyroku. W ten sposób, zarówno oskarżony jak i obywatele mogą dokonać swoistej kontroli wyciągniętych przez sędziego wniosków. Znając rozumowanie sądu strony mają solidne podstawy, aby negować przytoczone fakty w postępowaniu apelacyjnym, mają więc materiał, na którym mogą się oprzeć sporządzając apelację, czego brakuje w przypadku sporządzenia prognozy kryminologicznej przez algorytm komputerowy. Co prawda w przypadku użycia COMPAS-u również wydawane jest orzeczenie wraz z uzasadnieniem, ale podważanie zasadności oceny ryzyka wydaje się znacznie utrudnione przy braku znajomości metodologii obliczeń programu.

Po drugie, program komputerowy, choćby najbardziej rozbudowany i nowoczesny nie konfrontuje się z oskarżonym na sali sądowej. Nie ulega wątpliwości fakt, iż chociaż nie jest to przesłanka formalna ujęta w Kodeksie karnym, prognoza kryminologiczna powstaje również w oparciu o to, co sędzia usłyszy od oskarżonego podczas bezpośredniego kontaktu z nim w budynku sądu. Wymagany obiektywizm sędziego i sformalizowanie wszystkich przesłanek nie zmieniają faktu, iż dokonanie oceny prognozy kryminologicznej przez sędziego jest w istocie procesem intuicyjnym i nacechowanym emocjami, co jest jego zarówno zaletą jak i wadą. Program komputerowy oparty na matematycznym algorytmie nie jest w stanie uchwycić wszystkich okoliczności popełnienia przestępstwa, w szczególności tych nacechowanych pewnymi emocjami.

W związku z powyższym, należy dojść do wniosku, że żaden program komputerowy nie jest w stanie zastąpić w prognozie kryminologicznej sprawcy tego ludzkiego pierwiastka jakim jest konfrontacja sędziego z oskarżonym. W związku z tym, wydaje się, że użycie raportu z oceną COMPAS jako narzędzia pomocniczego nie jest w stu procentach wykluczone, o ile sędzia zestawia uzyskane wyniki z indywidualnie wyciągniętymi wnioskami, a uzasadnienie wyroku przedstawia obok oceny COMPAS inne przesłanki determinujące decyzję sędziego. Wciąż jednak należy wziąć pod uwagę niebezpieczeństwo jakim jest nieświadoma siła sugestii jakiej może ulec sędzia po zapoznaniu się z oceną ryzyka.

Wdrażanie nowych technologii w obszarze wymiaru sprawiedliwości stawia nowe wyzwania przede wszystkim wobec pełnomocników stron postępowania. W przypadku użycia algorytmu COMPAS ich rola jest kluczowa.

Podczas klasycznego procesu obrona dba o przedstawienie klienta przed sądem[13] w jak najlepszym świetle opierają się na jego życiorysie oraz faktach zgromadzonych w aktach w sprawy. W przypadku użycia algorytmu i wysokiej w skali ocenie ryzyka sprawcy pojawia się w pewnym sensie nowy uczestnik postępowania, którego twierdzenia trzeba obalić. Jak zostało wspomniane wcześniej, w przypadku braku znajomości metodologii pracy programu komputerowego to zadanie wydaje się być utrudnione. Z drugiej zaś strony, w przypadku niskiej oceny ryzyka sprawcy argumentacja obrony diametralnie się zmienia i można zakładać, iż będzie ona polegała na utwierdzeniu sądu w przekonaniu, że system słusznie zakwalifikował ryzyko wobec oskarżonego.

5. ZAKOŃCZENIE

Temat użycia specjalnego oprogramowania do dokonywania oceny prognozy kryminologicznej sprawcy jest niezwykle istotny. Problem i kontrowersje dotyczące jego używania dotyczą obecnie głównie Stanów Zjednoczonych. Niewykluczone jest jednak, że postęp technologiczny na całym świecie doprowadzi do pomysłu wprowadzenia analogicznych algorytmów w Polsce. W mojej opinii należy zdecydowanie wstrzymać się z implementacją podobnych rozwiązań do polskiego systemu sprawiedliwości, dopóki liczne kontrowersje dotyczące stosowania algorytmu nie zostaną wyjaśnione. Bezrefleksyjne i niepoprzedzone odpowiednimi przygotowaniami wprowadzanie nowych technologii do polskiego wymiaru sprawiedliwości może okazać się tragiczne w skutkach. W przypadku implementacji algorytmu COMPAS może to skutkować naruszeniem prawa do rzetelnego procesu jego uczestników lub zasady prawdy materialnej.

BIBLIOGRAFIA

K. Mamak, *Rewolucja cyfrowa a prognoza kryminologiczna,* [w:] *Rewolucja cyfrowa a prawo karne*, LEX nr 369493164.

Wróbel W., Zoll A., *Kodeks karny. Część ogólna. Tom I. Część II. Komentarz do art. 53-116, wyd. V*, Warszawa 2016.

https://en.wikipedia.org/wiki/COMPAS_(software) (dostęp: 01.05.2022).

[13] W przypadku amerykańskiego systemu wymiaru sprawiedliwości również przed ławą przysięgłych.

https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE (dostęp: 01.05.2022).

https://harvardlawreview.org/2017/03/state-v-loomis/ (dostęp: 01.05.2022).

https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm (dostęp: 01.05.2022).

https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (dostęp: 01.05.2022).

OFFENDER'S CRIMINOLOGICAL PROGNOSIS MADE BY COMPUTER PROGRAM – ISSUES OF APPLYING COMPAS ALGORITHM IN AMERICAN ADMINISTRATION OF JUSTICE

Abstract: Article presents issues of using computer program while determining offender's criminological prognosis in American criminal law system. The author describes the operation of the mathematical algorithm that is the basis of this program, pointing to the controversy arising from its use. The subject of the study is also the analysis of selected lawsuits in the United States during which the COMPAS algorithm was used.

Keywords: criminological prognosis, algorithm, COMPAS, probation measures, recidivism, new technologies

PIOTR KONIECZNY
UNIWERSYTET WARSZAWSKI

STANDARD OCHRONY PRAW CZŁOWIEKA W PROJEKCIE AKTU W SPRAWIE SZTUCZNEJ INTELIGENCJI[1]

Abstrakt: Projekt Aktu w sprawie sztucznej inteligencji powstał między innymi w celu zapewnienia spójnego i wysokiego poziomu ochrony praw podstawowych w zgodzie z Kartą praw podstawowych Unii Europejskiej. W niniejszym artykule przedstawiono standard ochrony praw człowieka wyłaniający się z projektu Aktu oraz przeanalizowano zgłaszane do niego uwagi i poprawki ze strony organizacji pozarządowych, parlamentów narodowych oraz organów, instytucji i innych jednostek organizacyjnych Unii Europejskiej. Szczególną uwagę poświęcono zakazanym praktykom w zakresie sztucznej inteligencji oraz systemom sztucznej inteligencji wysokiego ryzyka. Omówiono systemową klasyfikację praw wynikających z projektu Aktu – w szczególności z punktu widzenia Karty praw podstawowych Unii Europejskiej. Wskazano również najistotniejsze postulaty odnoszące się do projektu Aktu oraz wskazano ryzyka i zagrożenia związane z przyjęciem Aktu w formie zaproponowanej przez Komisję Europejską.

Słowa kluczowe: sztuczna inteligencja, systemy sztucznej inteligencji wysokiego ryzyka, zakazane praktyki w zakresie sztucznej inteligencji, Akt w sprawie sztucznej inteligencji

1. WPROWADZENIE

Dynamiczny rozwój nowoczesnych technologii niesie ze sobą szereg wyzwań i zagrożeń dla europejskiego (choć nie jest to problem wyłącznie europejski) porządku prawnego. Technologie, które coraz dogłębniej ingerują w ludzkie życie, nieraz stoją w sprzeczności z wartościami, na których

[1] Tekst opisuje stan prawny na maj 2022 r.

zbudowana została Unia Europejska i jej prawodawstwo. W wartości te – takie jak poszanowanie godności osoby ludzkiej, zakaz dyskryminacji, wolność, demokrację, bezpieczeństwo osobiste, poszanowanie życia prywatnego czy ochronę danych osobowych – potencjalnie mogą ingerować rozwiązania zbudowane w oparciu o sztuczną inteligencję (dalej: AI).

Problemom tym, zanim jeszcze na szeroką skalę pojawią się w Europie, stara się przeciwdziałać Komisja Europejska, która za pomocą proponowanych przez siebie projektów rozporządzeń takich jak Akt o rynkach cyfrowych *(Digital Markets Act)*[2], Akt o usługach cyfrowych *(Digital Services Act)*[3] czy Akt w sprawie sztucznej inteligencji *(Artificial Intelligence Act)*[4], stara się budować ramy prawne dla cyfrowego świata. Ostatni z tych dokumentów, projekt Aktu w sprawie sztucznej inteligencji (dalej: Akt), powstał między innymi w celu zapewnienia spójnego i wysokiego poziomu ochrony interesów publicznych w dziedzinie zdrowia, bezpieczeństwa i praw podstawowych w zgodzie z Kartą praw podstawowych Unii Europejskiej[5]. Oznacza to, że Unia Europejska jest świadoma istnienia zagrożeń, które błyskawiczny rozwój AI może przynieść dla systemu ochrony praw człowieka.

Projekt Aktu został zaprezentowany w kwietniu 2021 roku i od tego czasu nieustannie toczą się nad nim prace i dyskusje. Swoje opinie i propozycje poprawek do projektu zgłosiło wiele organizacji pozarządowych (m.in. Amnesty International, Fundacja Panoptykon, Human Rights Watch), parlamentów narodowych (m.in. obie izby czeskiego parlamentu, polski Senat, włoska Izba Deputowanych) oraz organów, instytucji i innych jednostek organizacyjnych Unii Europejskiej (m.in. Europejska Rada Ochrony Danych, Komitet Ekonomiczno–Społeczny, Komitet Regionów, Rada Unii Europejskiej, wiele komisji Parlamentu Europejskiego). Oznacza to, że ostateczny tekst rozporządzenia z pewnością będzie odbiegał od tego zaproponowanego przez Komisję. Jako że znajdujemy się na dosyć wczesnym etapie procesu legislacyjnego, wciąż nie da się jednoznacznie stwierdzić, w którą stronę ostatecznie

[2] Komisja Europejska, *Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych)*, COM/2020/842 final, Bruksela, 2020

[3] Komisja Europejska, *Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE*, COM/2020/825 final, Bruksela, 2020

[4] Komisja Europejska, *Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre inne akty ustawodawcze Unii*, COM/2021/206 final, Bruksela, 2021, dalej jako: projekt Aktu.

[5] Projekt Aktu, motyw 13

będzie zmierzał europejski prawodawca – nie wiadomo, czy przepisy będą zaostrzane czy liberalizowane.

Niniejszy artykuł zostanie poświęcony analizie i ocenie projektu Aktu wyłącznie z punktu widzenia wyłaniającego się z niego standardu ochrony praw człowieka – w szczególności z perspektywy zakazanych praktyk w zakresie AI oraz systemów AI wysokiego ryzyka. Pozostałe kwestie oraz rozwiązania wynikające z projektu rozporządzenia wymagają odrębnego omówienia.

2. POJĘCIE SZTUCZNEJ INTELIGENCJI

Projekt rozporządzenia definiuje system AI jako „oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, 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". Załącznik I z kolei dookreśla te techniki i podejścia jako:

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) i systemy ekspertowe;
c) podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.

Co ważne, projekt Aktu przyznaje Komisji uprawnienie do modyfikowania wykazu technik i podejść określonych w załączniku I. Oznacza to, że Komisja jest świadoma, że sztywne definiowane tak wieloznacznego pojęcia jak AI nie sprawdzi się w praktyce. Co więcej, w myśl projektowanej regulacji AI to nie tylko współczesne osiągnięcia techniki (np. technologia uczenia maszynowego czy technologia rozpoznawania twarzy), ale również algorytmy oparte na regułach, które według większości klasycznych definicji nie zostałyby uznawane za system AI (np. algorytm wyznaczający wysokość świadczenia z ubezpieczenia społecznego lub algorytm szacujący prawdopodobieństwo znalezienia pracy w ciągu określonego przedziały czasowego)[6]. Oznacza to,

[6] Human Rights Watch, *Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net*, s. 4, https://www.hrw.org/sites/default/files/media_2021/11/202111hrw_eu_ai_regulation_qa_0.pdf (dostęp: 14.05.2022).

że Komisja interpretuje pojęcie AI bardzo szeroko i tym samym sprawia, że w zakres podmiotowy przyszłego rozporządzenia może być bardzo szeroki.

Takie zdefiniowanie systemu AI wywołało ożywione dyskusje przede wszystkim wśród unijnych organów i instytucji. Refleksje i wywodzące się z nich propozycje zmian są często zupełnie odmienne. Podczas gdy Komisja Rynku Wewnętrznego i Ochrony Konsumentów (IMCO) oraz Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE)[7], a także słoweńska Prezydencja w Radzie UE[8] w swoich rozważaniach rekomendują przede wszystkim drobne poprawki i zmiany redakcyjne, tak Komitet Ekonomiczno–Społeczny proponuje usunięcie załącznika I i zdefiniowanie systemu AI jako „oprogramowania, które może, w sposób zautomatyzowany – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje, wpływając na środowisko, z którym wchodzi w interakcję". Ponadto, w ocenie Komitetu, wśród naukowców zajmujących się AI panuje przekonanie, że szeregu spośród przykładów podanych w załączniku I nie można uznać za AI, a wiele innych ważnych technik AI pominięto[9].

Pojawiają się również opinie pośrednie, akcentujące potrzebę doprecyzowania definicji systemu AI, ale nienegujące założeń Komisji. I tak w opinii Komitetu Regionów należy zauważyć, że techniki i podejścia wymienione w załączniku I nie stanowią zamkniętego katalogu, a samo generowanie wyników przez system AI wychodzi „od postrzegania swojego otoczenia poprzez gromadzenie danych, interpretację zebranych ustrukturyzowanych lub nieustrukturyzowanych danych, zarządzanie wiedzą lub przetwarzanie informacji pochodzących z tych danych" [10]. Z kolei w opinii Komisji Transportu i Turystyki (TRAN) system AI powinien oznaczać system, który otrzymuje dane wejściowe pochodzące od maszyny lub człowieka, aby wywnioskować, jak osiągnąć dany zestaw celów określonych przez człowieka, wykorzystując

[7] Komisja IMCO i LIBE, *Draft report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, Bruksela, 2022.

[8] Rada Unii Europejskiej, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text*, Bruksela, 2021.

[9] Komitet Ekonomiczno-Społeczny, *Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii"*, Dz. Urz. UE C 517/61 z 22.12.2021 r., s. 2.

[10] Komitet Regionów, *Opinia Europejskiego Komitetu Regionów – Europejskie podejście do sztucznej inteligencji – akt w sprawie sztucznej inteligencji*, Dz. Urz. UE C 97/12 z 28.02.2022 r., s. 9.

uczenie się, rozumowanie lub modelowanie, wdrażany za pomocą technik i podejść wymienionych w załączniku I, oraz który generuje dane wyjściowe w postaci treści, przewidywań, zaleceń.

Podsumowując, unijne instytucje na ogół zgodnie przyznają, że zdefiniowanie systemu AI poprzez odniesienie do technik i podejść określonych w modyfikowalnym załączniku jest dobrym pomysłem, który sprawdzi się w praktyce. Często zwracają uwagę, że nieodłączną częścią systemu AI są dane, bez których działanie tego systemu byłoby niemożliwe (Komisja w ogóle nie poruszyła tej kwestii). Dodatkowo jako istotną wskazuje się także zdolność systemu AI do uczenia się i autonomicznego dostosowywania do nowych zadań.

3. SYSTEMY STOSUJĄCE TECHNIKI PODPROGOWE ORAZ SYSTEMY WYKORZYSTUJĄCE SŁABOŚCI OKREŚLONYCH GRUP OSÓB

Komisja zauważa, że oprócz wielu swoich korzystnych zastosowań, systemy AI mogą być również niewłaściwie wykorzystywane, a co za tym idzie mogą dostarczać narzędzi do praktyk manipulacji, wykorzystywania i kontroli społecznej. Zważywszy na fakt, że takie praktyki są szczególnie szkodliwe i sprzeczne z unijnymi wartościami poszanowania godności ludzkiej, wolności, równości, demokracji i praworządności oraz z prawami podstawowymi Unii (w tym z prawem do niedyskryminacji, ochrony danych i prywatności oraz z prawami dziecka), powinny zostać zakazane[11].

Aby osiągnąć ten cel, Komisja postuluje ustanowienie zakazu wprowadzania do obrotu, oddawania do użytku lub wykorzystywania zarówno systemów AI, które stosują techniki podprogowe będące poza świadomością danej osoby, jak i wykorzystują dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne w celu istotnego zniekształcenia zachowania danej osoby w sposób, które to systemy AI powodują lub mogą powodować u tej lub innej osoby szkodę fizyczną lub psychiczną. Komisja tym samym zauważa, że systemy AI stosujące techniki podprogowe wykorzystują mechanizmy, których osoby fizyczne nie są w stanie dostrzec, lub wykorzystują słabości dzieci i innych osób ze względu na ich wiek, niepełnosprawność fizyczną lub umysłową. Czynią to z zamiarem

[11] Projekt Aktu, motyw 15.

istotnego zniekształcenia zachowania danej osoby i w sposób, który powoduje lub może powodować szkodę dla tej lub innej osoby[12].

W obecnym kształcie regulacji, aby system AI został zakazany, musi on w istocie dążyć do wyrządzenia szkody osobie fizycznej. Komisja zakłada więc, że mogą istnieć systemy wykorzystujące techniki podprogowe lub wykorzystujące słabości określonych grup osób, które nie dążą do wyrządzenia szkody. Pojawia się pytanie, czy takie rozumowanie jest słuszne. Celem stosowania technik podprogowych jest wpłynięcie na ludzkie zachowania w sposób, którego ludzie nie są świadomi. Samo to podważa podstawy ludzkiej autonomii, a tym samym może uderzać w ludzką godność, wolność i prawa podstawowe. Podobnie rzecz się ma w odniesieniu do systemów wykorzystujących ludzkie słabości w celu zniekształcenia ich zachowania. Trudno wyobrazić sobie system, który – dla przykładu – manipulowałby odczuciami i potrzebami kilkuletnich dzieci, nie dążąc tym samym do wyrządzenia im szkody.

Dlatego też 123 organizacje pozarządowe zrzeszone w sieci European Digital Rights (EDRi) postulują usunięcie przesłanki wymagającej spowodowania lub możliwości spowodowania u osoby dotkniętej działaniem takiego systemu szkody fizycznej lub psychicznej[13]. Uważają one, że wykorzystywanie systemów AI stosujących techniki podprogowe powinno zostać całkowicie zabronione, ponieważ jakiekolwiek użycie takiego systemu prowadzi do naruszenia praw podstawowych. EDRi proponuje również znaczące rozszerzenie katalogu słabości, których nie mogą wykorzystywać systemy AI. Projekt Komisji przewiduje tylko 3 cechy – wiek, niepełnosprawność ruchową oraz zaburzenie psychiczne. EDRi chciałoby, aby zakaz ten został rozszerzony o wszelkie ludzkie słabości i wrażliwości – ze szczególnym uwzględnieniem wieku, płci i tożsamości płciowej, pochodzenia rasowego lub etnicznego, stanu zdrowia, orientacji seksualnej, cech płciowych, statusu społecznego, ekonomicznego, pracowniczego lub migracyjnego, a także niepełnosprawności[14]. Projekt Aktu w pierwotnej formie nie zabezpiecza w pełni osób fizycznych przed działaniem systemów AI stosujących techniki podprogowe lub wykorzystujących ludzkie słabości, ponieważ nie wprowadza całkowitego zakazu działania takich systemów, a jedynie ogranicza go do określonych kwestii, skutków czy ludzkich wrażliwości. Jeżeli postulowane poprawki nie zostaną

[12] Projekt Aktu, motyw 16.
[13] European Digital Rights, *An EU Artificial Intelligence Act for Fundamental Rights. A Civil Society Statement*, 2021, s. 2, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf (dostęp: 14.05.2022).
[14] *Ibidem*, s. 2.

uwzględnione, nie będą istniały prawne przeszkody dla działania systemu AI, który – dla przykładu – manipuluje zachowaniem danej osoby poprzez wykorzystanie wiedzy o jej nieuleczalnej chorobie nowotworowej.

Unijne instytucje komentują ten zakaz w różnorodny sposób. Część z nich nie zgłasza żadnych uwag do tego zakazu (np. Komisja IMCO i LIBE, Komisja ITRE), a inne ingerują w projekt jedynie w nieznacznym stopniu. Dla przykładu, słoweńska Prezydencja w Radzie Unii Europejskiej proponuje, aby przy kwestii istotnego zniekształcenia zachowania osoby fizycznej zwracać uwagę nie tylko na cel (jak chciałaby tego Komisja), ale również na skutek takiego działania. Jednocześnie Prezydencja proponuje zawężenie charakteru możliwości spowodowania szkody przez system AI jedynie do szkody racjonalnie prawdopodobnej (*reasonably likely*), a także zastąpienie słabości wynikającej z niepełnosprawności ruchowej lub zaburzenia psychicznego pojęciem społecznej lub ekonomicznej sytuacji danej osoby. Z uwagi na szerokie możliwości interpretacyjne tego pojęcia wydaje się, że rozwiązanie to może nie zabezpieczać należycie osób fizycznych przed działaniem systemów AI wykorzystujących ich słabości.

Podobnie omawiany zakaz ocenia Komitet Regionów, który proponuje doprecyzowanie katalogu potencjalnych szkód wynikających ze stosowania technik podprogowych przez system AI o działalność, która „narusza lub może naruszać prawa podstawowe innej osoby lub grupy osób, w tym ich fizyczne lub psychiczne zdrowie i bezpieczeństwo, powoduje lub może powodować szkody lub krzywdy dla konsumentów, takie jak straty pieniężne lub dyskryminacja ekonomiczna, lub podważa lub może podważać demokrację i praworządność”[15]. Dobrą propozycją jest tu bezpośrednie odwołanie się do naruszenia praw podstawowych, ale Komitet w żaden sposób nie odniósł się do innych problemów wskazywanych przez organizacje pozarządowe. Jako zaletę tej propozycji można potraktować również wskazanie, że techniki podprogowe nie mogą podważać zasad demokracji i praworządności. Jest to szczególnie istotne z perspektywy procesu wyborczego, gdzie przekaz podprogowy może mieć kluczowy wpływ na wynik wyborów.

Z kolei podejście zgodne z postulatami EDRi prezentuje Komisja Kultury i Edukacji (CULT). Proponuje ona zastąpienie zakazu dotyczącego technik podprogowych zakazem wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu AI, który stosuje techniki skutkujące lub mogące skutkować istotnym zniekształceniem zachowania tej osoby w sposób, który

[15] Komitet Regionów, *op. cit.*, s. 10.

powoduje lub może powodować wyrządzenie te osobie lub innej osobie szkody materialnej lub niematerialnej, w tym szkody fizycznej, psychologicznej lub ekonomicznej[16]. Wprawdzie Komisja CULT nie wspomina tutaj o zakazie stosowania przez systemy AI technik podprogowych, to zakaz w takiej formie wydaje się mieć o wiele szersze zastosowanie i odpowiadać uwagom strony społecznej. Również w odniesieniu do systemów wykorzystujących ludzkie słabości Komisja CULT postuluje zakaz wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu AI, który wykorzystuje dowolną słabość osoby fizycznej ze względu na jej znaną lub przewidywaną osobowość, sytuację społeczną lub ekonomiczną sytuację społeczną lub ekonomiczną, lub ze względu na wiek, zdolności fizyczne lub zdolności umysłowe. Oznaczałoby to, że zakazane byłoby wykorzystywanie jakiejkolwiek z ludzkich słabości, a cechy wskazane przez Komisję stałyby się tu jedynie elementem przykładowego wyliczenia.

4. SYSTEMY OCENY LUB KLASYFIKACJI WIARYGODNOŚCI OSÓB FIZYCZNYCH (*SOCIAL SCORINGU*)

Projekt Aktu przewiduje również zakaz wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów AI 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 z następujących skutków:

a) 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;
b) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi.

Komisja zauważa więc, że funkcjonowanie systemów punktowej oceny społecznej (*social scoringu*) może prowadzić do dyskryminacji i wykluczenia

[16] Komisja CULT, *Draft opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, Bruksela 2022, s. 22.

pewnych grup, a także może naruszać prawo do godności i niedyskryminacji oraz wartości, jakimi są równość i sprawiedliwość. Z uwagi na fakt, że ocena społeczna wystawiona przez takie systemy może prowadzić do krzywdzącego lub niekorzystnego traktowania, które jest nieproporcjonalne lub nieuzasadnione w stosunku do wagi ludzkich zachowań społecznych, takie systemy powinny zostać zakazane[17].

Postulowany zakaz nie jest jednak powszechny i bezwzględny, ponieważ dotyczy on jedynie systemów AI stosowanych przez organy publiczne lub podmioty działające w ich imieniu. Ponadto, zakaz punktowej oceny społecznej dotyczy jedynie oceny lub klasyfikacji osób fizycznych z punktu widzenia ich wiarygodności, a więc nie dotyczy jakiejkolwiek innej cechy lub postawy. Projekt Aktu stanowi również, że zakazana ocena lub klasyfikacja ma być „prowadzona przez określony czas", co jest pojęciem nieostrym i może budzić znaczne wątpliwości interpretacyjne przy stosowaniu zakazu.

W ocenie Human Rights Watch[18] oraz EDRi[19] powyższym zakazem powinny zostać objęte nie tylko podmioty publiczne, ale również prywatne. W przeciwnym razie nic nie stałoby na przeszkodzie w stosowaniu punktowej oceny społecznej m.in. w miejscu pracy lub w instytucjach finansowych. W ocenie Human Rights Watch, rozporządzenie powinno zabraniać stosowania wszelkiego rodzaju scoringów behawioralnych, które w nieuzasadniony sposób ograniczają lub mają negatywny wpływ na prawa człowieka, w tym prawo do zabezpieczenia społecznego, odpowiedniego standardu życia, prywatności i niedyskryminacji. Jako przykład wskazuje się zakaz działania systemu AI, który, na podstawie wcześniejszego zachowania danej osoby przewiduje, czy chce ona wyłudzić świadczenie z zabezpieczenia społecznego i na tej podstawie może odmówić jego przyznania[20]. Z kolei EDRi w swoim stanowisku zauważa, że pojęcia takie jak „ocena lub klasyfikacja wiarygodności" czy „*scoring* prowadzony przez określony czas" powinny zostać przemodelowane w celu lepszego zabezpieczenia praw jednostek. Nie pojawia się tutaj jednak postulat całkowitego zakazu działania takich systemów AI.

Podobnie jak wcześniej, unijne instytucje podchodzą do zakazu punktowej oceny społecznej w różnorodny sposób. Komisje IMCO i LIBE, Komisja ITRE czy Komisja Prawna (JURI) nie zgłosiły żadnych lub prawie

[17] Projekt Aktu, motyw 17.
[18] Human Rights Watch, *op. cit.*, s. 25.
[19] European Digital Rights, *op. cit.*, s. 2.
[20] Human Rights Watch, *op. cit.*, s. 25.

żadnych uwag do projektu. Jednakże, co do zasady, unijne instytucje zauważają potrzebę zmian w projekcie Aktu.

Słoweńska Prezydencja jest zgodna ze stanowiskiem EDRi i uważa, że zakaz stosowania określonych systemów scoringowych powinien dotyczyć wszystkich podmiotów (a nie tylko organów publicznych) oraz powinien zawierać zakaz oceny lub kwalifikacji osób fizycznych bez wskazywania, że chodzi o kryterium wiarygodności. Prezydencja nie przewiduje jednak zakazywania stosowania wszelkich praktyk w zakresie *social scoringu*, wobec czego nie ingeruje w regulacje dotyczący warunków, do jakich stosowanie takich systemów AI nie może prowadzić[21]. Podobny punkt widzenia przedstawia Komitet Ekonomiczno–Społeczny, według którego zakaz punktowej oceny obywateli powinien dotyczyć wszelkich podmiotów, a warunki uściślające stosowanie tego zakazu „powinny zostać doprecyzowane w taki sposób, aby jasno określić, co uznaje się za punktową ocenę społeczną i co można uznać za akceptowalną formę oceny w określonym celu, czyli kiedy informacje wykorzystane do oceny nie powinny być już uznawane za istotne lub racjonalnie związane z celem oceny"[22].

W inną stronę podążają postulaty wysuwane przez Komisję CULT oraz Komitet Regionów. Pierwsza z nich proponuje, aby zakazać wprowadzania do obrotu, oddawania do użytku uruchomienie lub wykorzystania systemów AI na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości[23]. Takie brzmienie zakazu byłoby całkowicie spójne z opinią Human Rights Watch, ponieważ propozycja Komisji CULT przewiduje całkowity zakaz stosowania tego rodzaju systemów nie tylko przez organy publiczne, ale również przez inne podmioty. Postuluje się także wykreślenie z treści przepisu fragmentu stanowiącego o prowadzeniu oceny lub klasyfikacji „przez określony czas". Komisja CULT w ogóle nie wspomina o systemach punktowej oceny społecznej, więc proponowany przez nią zakaz może być interpretowany bardzo szeroko.

Z kolei Komitet Regionów proponuje podkreślenie wagi i istotności wprowadzenia zakazu stosowania systemów punktowej oceny zachowań społecznych opartych na AI, ale nie postuluje żadnego z innych rozwiązań zaproponowanych przez Komisję CULT[24]. Oznacza to, że zakaz ten miał-

[21] Rada UE, *op. cit.*, s. 38.
[22] Komitet Ekonomiczno-Społeczny, *op. cit.*, s. 3.
[23] Komisja CULT, *op. cit.*, s. 23.
[24] Komitet Regionów, *op. cit.*, s. 11.

by dotyczyć jedynie organów publicznych (lub podmiotów działających w ich imieniu), a zagadnienia dotyczące wiarygodności stosowania *scoringu* przez określony czas nie powinny ulec modyfikacji. Komitet zauważa jedynie, że ocena lub klasyfikacja wiarygodności powinna dotyczyć nie tylko osób fizycznych, ale również grup osób.

5. SYSTEMY ZDALNEJ IDENTYFIKACJI BIOMETRYCZNEJ W CZASIE RZECZYWISTYM W PRZESTRZENI PUBLICZNEJ DO CELÓW EGZEKWOWANIA PRAWA

Ostatnią z praktyk, których Komisja chciałaby zakazać, jest wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa, chyba że wykorzystywanie takiego systemu mieściłoby się w ramach jednego z trzech przewidzianych wyjątków pod warunkiem, że takie wykorzystanie byłoby absolutnie konieczne do realizacji istotnego interesu publicznego, którego waga przeważałaby nad ryzykiem[25]. Do tych wyjątków należałyby:

a) ukierunkowane poszukiwanie konkretnych potencjalnych ofiar przestępstw;
b) zapobiegnięcie konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;
c) wykrywanie, lokalizowanie, identyfikowanie lub ściganie sprawcy przestępstwa lub podejrzanego o popełnienie jednego z 32 przestępstw wymienionych w decyzji ramowej Rady 2002/584/WSiSW pod warunkiem, że w danym państwie członkowskim przestępstwo to podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata.

Komisja zauważa, że tego rodzaju systemy AI szczególnie ingerują w ludzkie prawa i wolności, ponieważ mogą wpływać na życie prywatne dużej części społeczeństwa, wywoływać poczucie stałego nadzoru i pośrednio zniechęcać do korzystania z wolności zgromadzeń i innych praw podstawowych. Ponadto, bezpośredniość oddziaływania i ograniczone możliwości późniejszej

[25] Projekt Aktu, motyw 19.

kontroli lub korekty wykorzystania takich systemów niosą ze sobą zwiększone ryzyko dla praw i wolności osób, których dotyczą działania organów ścigania[26].

Dlatego, aby ograniczyć zakres wyjątkowego korzystania z tego rodzaju systemów AI, Komisja proponuje wprowadzenie szeregu zabezpieczeń, które mają ograniczyć ewentualne nadużycia. W przypadku potrzeby skorzystania z takiego systemu powinno się uwzględnić charakter sytuacji powodującej konieczność jego ewentualnego wykorzystania (w szczególności powagę, prawdopodobieństwo i skalę szkody wyrządzonej w przypadku niewykorzystania systemu) oraz konsekwencje jego wykorzystania dla praw i wolności wszystkich zainteresowanych osób (w szczególności wagę, prawdopodobieństwo i skalę tych konsekwencji). Ponadto, należy zachować niezbędne i proporcjonalne zabezpieczenia i warunki w odniesieniu do wykorzystywania systemu (w szczególności w odniesieniu do ograniczeń czasowych, geograficznych i osobowych). Dotyczy to zwłaszcza dowodów lub wskazówek dotyczących zagrożeń, ofiar lub sprawcy. Referencyjna baza danych osób powinna być odpowiednia dla każdego przypadku użycia systemu AI w każdej z trzech wyżej wymienionych sytuacji[27].

Uzupełnieniem tych obowiązków jest konieczność uprzedniego uzyskania zezwolenia na skorzystanie z takiego systemu AI udzielonego przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego, w którym ma nastąpić wykorzystanie. Pozwolenie to powinno zostać wydawane na uzasadniony wniosek zgodnie ze szczegółowymi przepisami prawa krajowego (treść i zakres tych przepisów pozostawia się do uregulowania państwom członkowskim). Wymóg uzyskania uprzedniego zezwolenia nie ma jednak charakteru bezwzględnego, ponieważ w należycie uzasadnionych nagłych przypadkach można rozpocząć wykorzystywanie systemu bez zezwolenia, a o jego udzielenie można wystąpić dopiero w trakcie lub po zakończeniu wykorzystywania. Wyjątek ten dotyczy sytuacji, w których potrzeba skorzystania z danego systemu jest na tyle duża, że uzyskanie zezwolenia przed rozpoczęciem korzystania jest faktycznie i obiektywnie niemożliwe. W takich sytuacjach nagłych wykorzystanie powinno być ograniczone do absolutnie niezbędnego minimum i powinno podlegać odpowiednim zabezpieczeniom i warunkom określonym w prawie krajowym i sprecyzowanym w kontekście każdego przypadku pilnego użycia przez sam organ ścigania. Ponadto organ ścigania powinien w takich sytuacjach dążyć do jak najszybszego uzyskania

[26] Projekt Aktu, motyw 19.
[27] Projekt Aktu, motyw 20.

zezwolenia, podając jednocześnie powody, dla których nie mógł wystąpić o nie wcześniej[28].

Należy również zauważyć, że możliwość korzystania z wyjątków dotyczących stosowania takich systemów AI zależy od ustanowienia właściwych przepisów przez państwa członkowskie. Oznacz to, że państwa mogą w ogóle nie przewidywać takiej możliwości lub przewidzieć ją jedynie w odniesieniu do niektórych celów określonych w projekcie Aktu[29].

W odniesieniu do proponowanego zakazu, EDRi postuluje jego rozszerzenie na wszystkie podmioty (a nie tylko organy ścigania w celu egzekwowania prawa) bez względu na to, czy zdalna identyfikacja następuje "w czasie rzeczywistym" czy "post factum". Zakaz ten powinien obejmować systemy AI, co do których można racjonalnie przewidzieć, że będą wykorzystywane w niedozwolony sposób. Organizacje zauważają, że wyjątki od konieczności stosowania takich systemów podważają wymogi zasady konieczności i proporcjonalności zawarte w Karcie praw podstawowych i z tego powodu powinny zostać usunięte[30].

Jak zauważa Komitet Ekonomiczno–Społeczny w swojej opinii, przyjęcie zakazu w proponowanej formie oznaczałoby, że identyfikacja danych biometrycznych po fakcie i z bliska jest dozwolona. W ten sposób zezwala się na rozpoznawanie danych biometrycznych nie dla celów identyfikacji danej osoby, lecz raczej dla oceny jej zachowania na podstawie jej cech biometrycznych (mikroekspresji, chodu, temperatury ciała, tętna itp.). Ograniczenie zakazu do „celów egzekwowania prawa" umożliwia stosowanie identyfikacji biometrycznej, a także wszelkich innych form rozpoznania biometrycznego, które nie mają na celu identyfikacji danej osoby, włączając w to wszystkie formy rozpoznawania emocji, w każdym innym celu, przez wszystkie inne podmioty, we wszystkich miejscach publicznych i prywatnych, w tym w miejscu pracy, w sklepach, na stadionach, w teatrach itp.[31]. Ponadto, rozpoznawanie emocji sklasyfikowano ogólnie jako niskie ryzyko, z wyjątkiem kilku dziedzin dotyczących użytkowników, w których uznano je za wysokie ryzyko. W praktyce jednak wszystkie te sposoby rozpoznawania przez systemy AI są niezwykle inwazyjne i stwarzają znaczne ryzyko naruszenia szeregu praw zawartych w Karcie praw podstawowych, takich jak prawo do godności człowieka,

[28] Projekt Aktu, motyw 21.
[29] Projekt Aktu, motyw 22.
[30] European Digital Rights, *op. cit.*, s. 4.
[31] Komitet Ekonomiczno-Społeczny, *op. cit.*, s. 4.

prawo człowieka do integralności (w tym integralności psychicznej) oraz prawo do życia prywatnego[32].

W związku z powyższym, Komitet Ekonomiczno–Społeczny poparł apel Europejskiego Inspektora Ochrony Danych i Europejskiej Rady Ochrony Danych[33], które wezwały do wprowadzenia zakazów:

a) stosowania systemów AI do zautomatyzowanej identyfikacji biometrycznej w przestrzeni publicznej i prywatnej, z wyjątkiem celów uwierzytelniania w szczególnych okolicznościach (np. zapewnienie dostępu do obiektów ważnych z punktu widzenia bezpieczeństwa);
b) wykorzystywania systemów AI do zautomatyzowanego rozpoznawania ludzkich sygnałów behawioralnych w przestrzeni publicznej i prywatnej,
c) stosowania systemów AI wykorzystujących dane biometryczne do podziału osób na grupy ze względu na pochodzenie etniczne, płeć, orientację polityczną lub seksualną lub z innych względów, które stanowią podstawę zakazu dyskryminacji na mocy Karty praw podstawowych,
d) wykorzystywania systemów AI do wykrywania emocji, zachowania, zamiarów lub charakterystycznych cech osób fizycznych, z wyjątkiem bardzo szczególnych przypadków, takich jak niektóre cele zdrowotne, w których rozpoznawanie emocji pacjenta jest istotne.

Jednakże nie wszystkie unijne instytucje postulują tak daleko idące zmiany. Tak jak to miało miejsce w przypadku wcześniejszych zakazów, Komisje IMCO i LIBE oraz Komisja ITRE nie zgłosiły żadnych uwag do projektu. Tak samo żadnych wątpliwości nie zgłosił Komitet Regionów. Komisja JURI postuluje zastąpienie zakazu „do celów egzekwowania prawa" zakazem stosowania tych systemów „przez organy ścigania lub w ich imieniu". Ponadto, Komisja JURI postuluje wykreślenie przesłanek absolutności i niezbędności przy stosowaniu wyjątków od tego zakazu[34]. Słoweńska Prezydencja, podobnie jak Komisja JURI, proponuje, aby zakaz dotyczył działania „przez organy

[32] Ibidem.
[33] Europejski Inspektor Ochrony Danych, Europejska Rada Ochrony Danych, *Apel o wprowadzenie zakazu stosowania AI do automatycznego rozpoznawania cech ludzkich w publicznie dostępnych przestrzeniach oraz do niektórych innych zastosowań sztucznej inteligencji, które mogą prowadzić do niesprawiedliwej dyskryminacji*, Bruksela, 2021, https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_pl (dostęp: 14.05.2022).
[34] Komisja JURI, *Draft opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, Bruksela, 2022, s. 37.

ścigania lub w ich imieniu". Ponadto, Prezydencja sugeruje objęcie regulacją wszystkich systemów identyfikacji biometrycznej w czasie rzeczywistym (a nie tylko tych działających zdalnie)[35].

Komisja Spraw Zagranicznych i Unii Europejskiej Senatu RP (KSZUE) wyraża wątpliwości co do możliwości wyjątkowego użycia systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa bez wcześniejszego zezwolenia wydanego przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego. W cenie KSZUE przypadki, w których może dojść do takiej sytuacji powinny zostać ograniczone i doprecyzowane, a sądowa kontrola takiego zezwolenia wzmocniona[36].

6. SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

Omówione powyżej systemy AI, których działanie w ocenie Komisji stanowi ryzyko tak duże, że powinny zostać zakazane, nie stanowią wyłącznego przedmiotu regulacji projektu Aktu. Poza systemami AI stwarzającymi niedopuszczalne ryzyko, Komisja przewiduje również funkcjonowanie systemów AI wysokiego ryzyka, systemów AI ograniczonego ryzyka, a także systemów AI charakteryzujących się niskim lub minimalnym ryzykiem. Podczas gdy tym dwóm ostatnim rodzajom systemów AI stawia się niewielkie wymagania (przede wszystkim z zakresu przejrzystości i obowiązków informacyjnych) lub nie stawia się ich wcale, tak proponowana regulacja odnosząca się do systemów AI wysokiego ryzyka jest bardzo szeroka[37].

Przy klasyfikowaniu danego systemu jako systemu AI wysokiego ryzyka zasadnicze znaczenie ma skala jego szkodliwego wpływu na prawa podstawowe chronione na mocy Karty praw podstawowych. Do praw tych należą: prawo do godności człowieka, poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, wolność wypowiedzi i informacji, wolność zgromadzania się i stowarzyszania się oraz niedyskryminacja, ochrona konsumentów, prawa pracownicze, prawa osób niepełnosprawnych, prawo

[35] Rada UE. *op. cit.*, s. 38.

[36] Senat RP, *Opinia Komisji Spraw Zagranicznych i Unii Europejskiej. Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej Inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*, Warszawa, 2021, s. 3.

[37] I. Małobęcka-Szwast, *Podejście oparte na ryzyku i nowe obowiązki w projekcie aktu w sprawie SI*, https://newtech.law/pl/podejscie-oparte-na-ryzyku-i-nowe-obowiazki-w-projekcie-aktu-w-sprawie-si/ (dostęp: 14.05.2022).

do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawo do obrony i domniemania niewinności, prawo do dobrej administracji[38].

Komisja proponuje, żeby systemy AI wysokiego ryzyka były określane na dwa sposoby. Pierwszym z nich byłoby zdefiniowanie takiego systemu poprzez odwołanie do unijnego prawodawstwa harmonizacyjnego, które zostało wymienione w załączniku II do projektu rozporządzenia. Zgodnie z tą klasyfikacją systemem AI wysokiego ryzyka byłby – przy jednoczesnym spełnieniu obu tych warunków:

a) system AI przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II lub sam będącym takim produktem;
b) produkt, którego związanym z bezpieczeństwem elementem jest system AI, lub sam system AI jako produkt podlegający ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku.

Drugą metodą definiowania systemów AI wysokiego ryzyka byłoby bezpośrednie wskazanie takich systemów poprzez wymienienie ich w załączniku III. Załącznik ten mógłby być uzupełniany przez Komisję, gdyby pojawił się nowy rodzaj systemu AI stwarzający ryzyko szkody dla zdrowia i bezpieczeństwa lub ryzyko niekorzystnego wpływu na prawa podstawowe.

Obecnie w załączniku tym wymienione są systemy AI działające w następujących obszarach:

a) Identyfikacja i kategoryzacja biometryczna osób fizycznych (w tym: zdalna identyfikacja biometryczna osób fizycznych „w czasie rzeczywistym" i „post factum"). Takie systemy cechują techniczne niedokładności, które mogą prowadzić do nieobiektywnych wyników i wywoływać dyskryminujące skutki – zwłaszcza w odniesieniu do wieku, pochodzenia etnicznego, płci lub niepełnosprawności[39].
b) Zarządzanie infrastrukturą krytyczną i jej eksploatacja (w tym: zarządzanie i obsługa ruchu drogowego oraz zaopatrzenia w wodę, gaz, ciepło i energię elektryczną). Awaria lub nieprawidłowe działanie takiego systemu może stanowić zagrożenie dla życia i zdrowia osób

[38] Projekt Aktu, motyw 28.
[39] Projekt Aktu, motyw 33.

na dużą skalę, a także prowadzić do znacznych zakłóceń w prowadzeniu działalności społecznej i gospodarczej[40].

c) Kształcenie i szkolenie zawodowe (w tym: decydowanie o dostępie do instytucji edukacyjnych i szkolenia zawodowego lub przydzielanie do tych instytucji; ocena uczniów oraz uczestników egzaminów powszechnych). Takie systemy mogą decydować o przebiegu kształcenia i kariery zawodowej danej osoby, czym wpływają na jej zdolność do zapewnienia sobie źródła utrzymania. Jeśli są one niewłaściwie zaprojektowane i stosowane, mogą naruszać prawo do nauki, prawo do niedyskryminacji, a także utrwalać historyczne wzorce dyskryminacji[41].

d) Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia (w tym: rekrutacja, selekcja podań o pracę, ocena kandydatów; decydowanie o awansie i rozwiązaniu stosunku pracy; przydzielanie zadań oraz monitorowanie i ocena wydajności i zachowania pracowników). Takie systemy mogą wpływać na przyszłe perspektywy zawodowe i źródła utrzymania osób fizycznych. Mogą utrwalać historyczne wzorce dyskryminacji, a także wpływać na prawo do ochrony danych i prywatności[42].

e) Dostęp do podstawowych usług prywatnych oraz usług i świadczeń publicznych, a także korzystanie z nich, w tym[43]:

   1) ocena kwalifikowalności osób fizycznych do świadczeń i usług publicznych oraz przyznawanie, ograniczanie, unieważnianie lub żądanie zwrotu takich świadczeń i usług (systemy te mogą one mieć znaczący wpływ na źródła utrzymania osób imogą naruszać ich prawa podstawowe, takie jak prawo do ochrony socjalnej, niedyskryminacji, godności człowieka lub skutecznego środka prawnego);

   2) ocena zdolności kredytowej osób fizycznych lub ustalenie ich punktowej oceny kredytowej (systemy te decydują dostępie do zasobów finansowych lub podstawowych usług, takich jak mieszkalnictwo, energia elektryczna i usługi telekomunikacyjne, a także mogą prowadzić do dyskryminacji i utrwalać historyczne wzorce dyskryminacji);

[40] Projekt Aktu, motyw 34.
[41] Projekt Aktu, motyw 35.
[42] Projekt Aktu, motyw 36.
[43] Projekt Aktu, motyw 37.

3) wysyłanie lub ustalanie priorytetów w wysyłaniu służb ratunkowych w sytuacjach kryzysowych (systemy te służą do podejmowania decyzji o krytycznym znaczeniu dla życia i zdrowia osób oraz ich mienia).

f) Ściganie przestępstw (w tym: ocena ryzyka popełnienia lub ponownego popełnienia przestępstwa; ocena ryzyka, na jakie narażone są potencjalne ofiary przestępstw; poligrafy i podobne narzędzia wykorzystywane w celu wykrywania stanu emocjonalnego osoby fizycznej; wykrywanie treści stworzonych z wykorzystaniem technologii *deepfake*; ocena wiarygodności dowodów; przewidywanie przestępstwom na podstawie profilowania, oceny cech osobowości i charakterystyki lub wcześniejszego zachowania przestępnego osób fizycznych lub grup; profilowanie osób fizycznych, o którym mowa w art. 3 pkt 4 dyrektywy (UE) 2016/680, w toku wykrywania i ścigania przestępstw lub prowadzenia dochodzeń w ich sprawie; analiza umożliwiająca przeszukiwanie złożonych, powiązanych i niepowiązanych dużych zbiorów danych w celu zidentyfikowania nieznanych wzorców lub odkrycia ukrytych zależności między danymi). Korzystanie z takich systemów może prowadzić do objęcia osoby fizycznej niejawnym nadzorem, do jej aresztowania lub pozbawienia wolności oraz do zaistnienia innych niekorzystnych skutków dla jej praw podstawowych. Jeśli system AI nie jest trenowany z wykorzystaniem danych wysokiej jakości, nie spełnia odpowiednich wymogów pod względem dokładności lub solidności lub nie został odpowiednio zaprojektowany i przetestowany, może on wskazywać osoby w sposób dyskryminacyjny lub w inny nieprawidłowy lub niesprawiedliwy sposób. Ponadto, korzystanie z istotnych procesowych praw podstawowych, takich jak prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, jak również prawo do obrony i domniemania niewinności, może być utrudnione – zwłaszcza gdy takie systemy AI nie są wystarczająco przejrzyste, wyjaśnialne i udokumentowane. Co ważne, za systemy AI wysokiego ryzyka o którym mowa powyżej, nie należy uznawać systemów AI specjalnie przeznaczonych do stosowania w postępowaniach administracyjnych prowadzonych przez organy podatkowe i celne[44].

g) Zarządzanie migracją, azylem i kontrolą graniczną (w tym: poligrafy i podobne narzędzia wykorzystywane w celu wykrywania stanu

[44] Projekt Aktu, motyw 38.

emocjonalnego osoby fizycznej; ocena ryzyka imigracji nieuregulowanej lub zagrożeń dla zdrowia; weryfikacja autentyczności dokumentów; wykrywanie dokumentów nieautentycznych; rozpatrywanie wniosków o udzielenie azylu, wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg). Systemy te mają wpływ na osoby, które często znajdują się w szczególnie trudnej sytuacji i które są zależne od rezultatów działań właściwych organów publicznych. Dokładność, niedyskryminujący charakter i przejrzystość systemów AI wykorzystywanych w tych kontekstach są szczególnie istotne w celu zapewnienia poszanowania praw podstawowych, w szczególności prawa do swobodnego przemieszczania się, niedyskryminacji, ochrony życia prywatnego i danych osobowych, ochrony międzynarodowej i dobrej administracji[45].

h) Sprawowanie wymiaru sprawiedliwości i procesy demokratyczne (w tym: pomoc organowi sądowemu w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego). Systemy te mogą wpływać na demokrację, praworządność, wolności osobiste, prawo do skutecznego środka odwoławczego oraz prawo do rzetelnego procesu sądowego. Co ważne, taka kwalifikacja nie powinna dotyczyć systemów AI przeznaczonych do czynności czysto pomocniczych, które nie mają wpływu na faktyczne sprawowanie wymiaru sprawiedliwości[46].

Uznanie systemu AI za system wysokiego ryzyka stworzy szereg obowiązków po stronie podmiotu, który taki system projektuje lub opracowuje. Systemy AI wysokiego ryzyka powinny podlegać wymogom dotyczącym jakości wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji użytkownikom, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Dodatkowe wymogi i obowiązki będą też stawiane przed dostawcami systemów AI wysokiego ryzyka – m.in. w zakresie certyfikacji, sporządzania dokumentacji technicznej czy rejestracji systemu. W ocenie Komisji wymagania te są konieczne, aby skutecznie ograniczyć zagrożenia dla zdrowia, bezpieczeństwa i praw podstawowych w przypadkach, gdy nie są racjonalnie dostępne inne, mniej ograniczające środki[47].

[45] Projekt Aktu, motyw 39.
[46] Projekt Aktu, motyw 40.
[47] Projekt Aktu, motyw 43.

Projekt Aktu nie wyczerpuje, ale też nie jest w stanie wyczerpać katalogu wszystkich istniejących lub mogących się pojawić nieakceptowalnych ryzyk w dziedzinie AI. Dlatego, aby reagować na pojawiające się zagrożenia dla praw człowieka, których w chwili obecnej nie jesteśmy w stanie przewidzieć, Human Rights Watch proponuje uwzględnienie w rozporządzeniu mechanizmu umożliwiającego rozszerzenie katalogu niedopuszczalnych ryzyk, a także wprowadzenie procesu przekształcania systemów AI wysokiego ryzyka w systemy o niedopuszczalnym ryzyku"[48].

Jak zauważa sieć EDRi, projekt Aktu nakłada obowiązki w zakresie systemów AI wysokiego ryzyka przede wszystkim na dostawców (podmioty opracowujące lub zlecające opracowanie takiego systemu), a nie na jego użytkowników (podmioty korzystające z takiego systemu). Podczas gdy część ryzyka stwarzanego przez systemy wymienione w załączniku III wynika ze sposobu, w jaki zostały one zaprojektowane, znaczące ryzyko wynika również z tego, jak są one wykorzystywane. Oznacza to, że dostawcy często nie będą w stanie kompleksowo ocenić potencjalnego wpływu systemów AI wysokiego ryzyka na przestrzeganie praw podstawowych, a prawdziwe ryzyko dla praw człowieka pojawi się ze strony użytkownika systemu AI, a nie jest dostawcy[49]. Przykładowo, system rozpoznawania twarzy pomagający sprawdzić, w jakich okularach będziemy dobrze wyglądać, powoduje nieporównywalnie mniejsze ryzyko niż ten sam system stosowany przez policję w trakcie demonstracji czy straż graniczną na lotnisku[50].

Dodatkowo, w ocenie Human Rights Watch, przed wdrożeniem lub zamówieniem systemu AI wysokiego ryzyka, powinno się wymagać od jego użytkowników przeprowadzania i opublikowania oceny skutków działania takiego systemu dla praw człowieka (*human rights impact assessment*). Analiza ta powinna określać, w jaki sposób system AI może chronić lub naruszać prawa człowieka, a także wskazywać sposoby zapobiegania lub łagodzenia takich naruszeń[51]. W zasadzie taki sam postulat przedstawia EDRi w swoim stanowisku[52].

Na potrzebę przeprowadzania oceny skutków działania systemu AI wysokiego ryzyka dla praw człowieka wskazuje również Komisja JURI. Ponadto wskazuje ona, że systemy wymienione w załączniku III powinny zostać

[48] Human Rights Watch, *op. cit.*, s. 25.
[49] Human Rights Watch, *op. cit.*, s. 26.
[50] Fundacja Panoptykon, *O co walczymy w unijnej regulacji AI? 5 postulatów*, https://panoptykon.org/regulacja-ai (dostęp: 14.05.2022).
[51] Human Rights Watch, *op. cit.*, s. 26.
[52] European Digital Rights, *op. cit.*, s. 3.

uznane za systemy AI wysokiego ryzyka dopiero, jeśli zajdzie prawdopodobieństwo wyrządzenia przez taki system znacznej szkody. W ocenie Komisji JURI, załącznik III nie stosuje zasady podejścia opartego na ryzyku (*risk–based approach*) oraz jest zbyt szeroki i niejasny, przez co kategoryzuje jako systemy AI wysokiego ryzyka wiele systemów, które nie stanowią prawie żadnego ryzyka dla praw podstawowych[53].

Komitet Ekonomiczno–Społeczny zauważa, że w projekcie Aktu powinny znaleźć się wymogi w zakresie etyki dotyczących godnej zaufania AI, takie jak: przewodnia rola człowieka; prywatności; różnorodności, niedyskryminacji i sprawiedliwości; wyjaśnialność; dobrostan środowiskowy i społeczny. Komitet uważa, że wiele zagrożeń związanych z AI dotyczy właśnie tych wartości, które znajdują odzwierciedlenie w prawach podstawowych[54].

Ponadto, wiele unijnych instytucji postuluje rozszerzenie załącznika III m.in. poprzez uwzględnienie w nim systemów AI: tworzących lub rozpowszechniających artykuły informacyjne generowane przez maszyny, a także tworzące zalecenia, rekomendacje, klasyfikacje lub ustalające priorytety określonych treści audiowizualnych w interfejsie online audiowizualnej usługi medialnej[55]; przeznaczonych do użytku przez dzieci w sposób, który ma znaczący wpływ na ich rozwój osobisty, w tym poprzez spersonalizowaną edukację lub ich rozwój poznawczy lub emocjonalny[56]; przeznaczonych do wykorzystania przez partie polityczne, kandydatów politycznych, organy publiczne lub w ich imieniu w celu wpływania na osoby fizyczne podczas głosowania w wyborach lokalnych, krajowych lub do Parlamentu Europejskiego;[57] przeznaczonych do przetwarzania lub liczenia kart do głosowania w wyborach lokalnych, krajowych lub do Parlamentu Europejskiego[58].

7. BRAKI W PROJEKCIE ROZPORZĄDZENIA

Do projektu Aktu zgłoszono wiele uwag i poprawek wykraczających ponad to, co zostało już omówione. EDRi w swoim stanowisku wskazuje, że projekt Aktu nie przyznaje żadnych praw ani roszczeń odszkodowawczych osobom, na które oddziałują systemy AI, a także nie przewiduje żadnego mechanizmu, za pomocą którego jednostki lub organizacje społeczne mogłyby

[53] Komisja JURI, *op. cit.*, s. 40-41.
[54] Komitet Ekonomiczno-Społeczny, *op. cit.*, s. 4.
[55] Komisja CULT, *op. cit.*, s. 32-33.
[56] Komisja IMCO i LIBE, *op. cit.*, s. 150.
[57] Komisja IMCO i LIBE, *op. cit.*, s. 152.
[58] *Ibidem.*

uczestniczyć w procesie badania systemów AI wysokiego ryzyka. Aby wpłynąć na możliwość naprawienia szkody wyrządzonej działaniem takich systemów proponuje się włączenie do Aktu dwóch praw stanowiących podstawę dla dalszych środków sądowych. Są to: prawo do niepodlegania systemom AI, które stanowią niedopuszczalne ryzyko lub nie są zgodne z Aktem, a także prawo do otrzymania jasnego i zrozumiałego wyjaśnienia, w sposób dostępny dla osób niepełnosprawnych, decyzji podjętych przy pomocy systemów w zakresie objętym Aktem[59].

Jako uzupełnienie tego stanowiska postuluje się zagwarantowanie prawa do skutecznego środka odwoławczego dla osób, których prawa zostały naruszone wskutek działania systemu AI. Proponuje się także stworzenie mechanizmu umożliwiającego organizacjom pozarządowym składanie skarg w przypadku naruszenia przepisów Aktu lub w przypadku systemów AI, które naruszają prawa podstawowe lub interes publiczny[60].

Ze stanowiskiem EDRi zgadza się Komitet Ekonomiczno–Społeczny, według którego w projekcie Aktu brakuje mechanizmów umożliwiających wnoszenie skarg i dochodzenia roszczeń przez organizacje społeczne i obywateli, którzy ponieśli szkody w wyniku stosowania jakiegokolwiek systemu lub praktyki w zakresie AI[61].

Komisje IMCO i LIBE wskazują potrzebę uzupełnienia zakazu stosowania systemów AI do celów egzekwowania prawa. Komisje chciałyby zakazać wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów AI służących do dokonywania indywidualnej oceny osób fizycznych w celu oceny ryzyka popełnienia lub ponownego popełnienia przestępstwa przez osobę fizyczną lub w celu przewidywania wystąpienia lub ponownego wystąpienia rzeczywistego lub potencjalnego przestępstwa w oparciu o profilowanie osoby fizycznej lub ocenę jej cech i właściwości lub przeszłych zachowań przestępczych osób fizycznych lub grup osób fizycznych. Jako że praktyki predykcyjne naruszają godność człowieka i zasadę domniemania niewinności, a także stwarzają szczególne ryzyko dyskryminacji, powinny zostać zakazane[62].

Ponadto, Komisja Spraw Zagranicznych i Unii Europejskiej Senatu RP sugeruje, aby w toku dalszych prac nad projektem Aktu zwrócić szczególną uwagę na odniesienia do ochrony środowiska naturalnego. Ze względu na szerokie zastosowanie systemów AI w przemyśle wymagana byłaby ich

[59] European Digital Rights, *op. cit.*, s. 3.
[60] *Ibidem*, s. 4-5.
[61] Komitet Ekonomiczno-Społeczny, *op. cit.*, s. 2.
[62] Komisja IMCO i LIBE, *op. cit.*, s. 54.

uprzednia weryfikacja pod kątem oddziaływania na środowisko naturalne[63]. Z kolei Izba Poselska Parlamentu Republiki Czeskiej wskazuje, że projekt Aktu nie uwzględnia obszaru „masowej inwigilacji przez przedsiębiorstwa", w którym prywatne firmy mogą przechowywać ilość danych o osobach fizycznych, które w skrajnych przypadkach pozwolą im na stworzenie własnej „korporacyjnej oceny kredytowej"[64].

8. KLASYFIKACJA I PODSUMOWANIE PRAW WYNIKAJĄCYCH Z PROJEKTU ROZPORZĄDZENIA

Projekt Aktu w wersji przedstawionej przez Komisję raczej nie przewiduje rewolucji, jeśli chodzi o postrzeganie całokształtu systemu ochrony praw człowieka w Unii Europejskiej. Projekt rozporządzenia nie próbuje definiować praw, które można by uznać za „nowe", a jedynie reguluje i dostosowuje prawa wynikające z Karty praw podstawowych do środowiska, w którym działają systemy AI. Taki sam sposób rozumowania przedstawiają inne unijne instytucje, które w swoich opiniach i postulatach nie przewidują rozszerzania obowiązującego w Unii katalogu praw podstawowych.

Odmienny punkt widzenia prezentują organizacje pozarządowe skupione w sieci EDRi. W ich ocenie w projekcie rozporządzenia Komisja w ogóle nie przewiduje uprawnień dla ludzi czy organizacji działających w ich imieniu[65]. EDRi stoi na stanowisku, że w Akcie powinny zostać wprost zagwarantowane dwa uprawnienia dla osób poddanych działaniu systemów AI: prawo do niepodlegania systemom, które wiążą się z nieakceptowalnym ryzykiem albo nie spełniają wymogów prawnych, a także prawo do wyjaśnienia decyzji podjętych z udziałem systemów AI wysokiego ryzyka[66]. Komisja z kolei stara się osiągnąć podobny efekt poprzez stworzenie szerokiego systemu obowiązków, nakazów i zakazów nakładanych przede wszystkim na dostawców systemów AI. Zgodnie z zamysłem Komisji, stosowanie tych systemów w zgodzie z Aktem ma sprawić, że osiągnięte zostaną wszystkie postulaty dotyczące ochrony praw podstawowych – w tym również te zgłaszane przez organizacje pozarządowe.

Komisja w projekcie Aktu nie tworzy nowego katalogu praw człowieka, ale odwołuje się do potrzeby ochrony wielu konkretnych wartości

[63] Senat RP, *op. cit.*, s. 3.
[64] Izba Poselska Parlamentu Republiki Czeskiej, *Rezolucja nr 471*, Praga, 2021, s. 19.
[65] Fundacja Panoptykon, *op. cit.*
[66] *Ibidem.*

przewidzianych w Karcie praw podstawowych. Należą do nich m.in.: prawo do godności człowieka, poszanowanie życia prywatnego, ochrona danych osobowych, niedyskryminacja, równość kobiet i mężczyzn, wolność wypowiedzi, wolność zgromadzania się, prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawa do obrony i domniemanie niewinności, prawo do należytych i sprawiedliwych warunków pracy, prawo do rokowań i działań zbiorowych, prawa dziecka, integracja osób niepełnosprawnych oraz prawo do wysokiego poziomu ochrony środowiska i poprawa jego jakości.

Potrzebę ochrony części z nich Komisja akcentuje wielokrotnie i zdecydowanie – np. jako potencjalnie uderzające w godność człowieka, poszanowanie życia prywatnego i zasadę niedyskryminacji niejednokrotnie wskazuje się systemy o niedopuszczalnym ryzyku. Inne wartości – jak np. domniemanie niewinności czy prawo do należytych i sprawiedliwych warunków pracy – wskazywane są jako konieczne do ochrony przede wszystkim przed szkodliwymi skutkami działania niektórych systemów AI wysokiego ryzyka. Jeszcze inne – jak np. prawo do wysokiego poziomu ochrony środowiska i poprawy jego jakości – wskazuje się wyłącznie jako postulowany cel, który dostawcy systemów AI mogliby uwzględnić przy projektowaniu takich systemów. Są też jednak wartości, które Komisja wskazuje w uzasadnieniu do projektu Aktu jako istotne, ale nie wskazuje jednocześnie żadnego, nawet potencjalnego działania systemu AI, które mogłoby stanowić dla nich zagrożenie – tu należy wyróżnić np. prawo do ochrony środowiska naturalnego.

9. OCENA SYSTEMU OCHRONY PRAW CZŁOWIEKA WYNIKAJĄCEGO Z PROJEKTU ROZPORZĄDZENIA

Projektowana regulacja, mimo że nie jest idealna i wymaga zmian, jest potrzebna i konieczne jest jej dalsze procedowanie. Należy zgodzić się ze stwierdzeniem Komisji, że mimo wielu niezaprzeczalnych korzyści społeczno–ekonomicznych we wszystkich gałęziach przemysłu i obszarach działalności społecznej, AI może być również źródłem ryzyka i szkody dla interesu publicznego i przywilejów chronionych prawem Unii[67]. Jednakże, aby skutecznie ograniczyć te ryzyka, projekt Aktu wymaga modyfikacji, które sprawią, że ostateczna wersja rozporządzenia będzie bardziej odpowiednia i adekwatna do realizacji celów, które zostały przed nią postawione.

[67] Projekt Aktu, motywy 3-4.

W chwili obecnej w projekcie Aktu znajduje się wiele potencjalnych luk, które mogą sprawić, że prawa podstawowe nie będą chronione w należyty sposób. Do wielu z istniejących zagrożeń Komisja podchodzi zbyt liberalnie – często zauważa istniejące ryzyko, ale zakaz lub ograniczenie korzystania z określonych systemów AI uzależnia dopiero od spełnienia szeregu wymagań.

Biorąc pod uwagę powyższą analizę, aby zagwarantować skuteczność projektu Aktu z perspektywy systemów AI o niedopuszczalnym ryzyku, konieczne będzie wprowadzenie do rozporządzenia kilku kluczowych modyfikacji.

Przede wszystkim powinno się usunąć przesłankę wymagającą spowodowania lub możliwości spowodowania szkody u osoby dotkniętej działaniem systemu AI stosującego techniki podprogowe. W przeciwnym razie uznamy, że stosowanie technik podprogowych manipulujących ludzkim zachowaniem może być dobre i pożądane, a przecież ich stosowanie wprost godzi w autonomię woli jednostki, co z kolei uderza w podstawowe prawa człowieka.

Kolejną istotną kwestią wymagającą interwencji jest potrzeba rozszerzenia zakazu korzystania z systemów AI wykorzystujących ludzkie słabości o wszelkie możliwe słabości i wrażliwości. Nie może być bowiem tak, że zniekształcanie ludzkiego zachowania z uwagi na niepełnosprawność danej osoby uważamy za moralnie naganne i godzące w jej prawa podstawowe, ale to samo zachowanie oparte o czyjąś chorobę nowotworową nie budzi już naszych zastrzeżeń.

Istotną kwestią jest również potrzeba rozszerzenia zakazu stosowania systemów social scoringu na podmioty prywatne oraz usunięcie z zakazu przesłanki klasyfikacji „wiarygodności". Zakazane powinny zostać wszelkie systemy klasyfikacji osób fizycznych, które prowadzą do krzywdzącego lub niekorzystnego traktowania tych osób, a nie jedynie systemy AI klasyfikujące te osoby pod względem wiarygodności. System AI klasyfikujący osoby fizyczne ze względu na ich kolor skóry, płeć czy wiek może być bowiem równie krzywdzący co system AI dokonujący klasyfikacji pod względem wiarygodności. Ponadto stosowanie takich systemów AI przez podmioty prywatne (np. w galeriach handlowych, podczas wydarzeń kulturalnych czy podczas korzystania z różnego rodzaju usług) będzie tak samo szkodliwe jak ich stosowanie przez organy publiczne.

Warto również zadbać o wprowadzenie mechanizmu pozwalającego przekształcić istniejący już system AI wysokiego ryzyka w system o niedopuszczalnym ryzyku. Aktualnie nie jesteśmy w stanie przewidzieć wszystkich ryzyk, które w przyszłości będą się wiązały z funkcjonowaniem systemami AI.

Dlatego, aby projekt Aktu nie uległ szybkiej dezaktualizacji, konieczne jest wprowadzenie takiej zmiany.

Natomiast kwestią niezwykle istotną z punktu widzenia systemów AI wysokiego ryzyka jest potrzeba nałożenia na określone podmioty obowiązku przeprowadzania oceny skutków działania systemu AI dla praw człowieka oraz zagwarantowanie osobom, których prawa zostały naruszone działaniem systemu AI, prawa do wniesienia skutecznego środka odwoławczego. Podobne rozwiązania funkcjonują już w europejskim systemie prawnym, gdzie dla przykładu art. 35 ogólnego rozporządzenia o ochronie danych (RODO) przewiduje obowiązek dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Z kolei art. 77 RODO umożliwia każdemu wniesienie skargi do organu nadzorczego, jeżeli dana osoba sądzi, że przetwarzanie jej danych osobowych narusza prawo. Nic więc nie stoi na przeszkodzie, żeby podobne przepisy wprowadzić do projektu Aktu, co z pewnością pomogłoby umocnić projektowany system ochrony praw człowieka.

Należy także zadbać, aby wymogi stawiane dostawcom systemów AI wysokiego ryzyka były adresowane również do użytkowników takich systemów AI, a decyzje podejmowane przy pomocy systemów AI powinny być jasne i możliwe do wyjaśniania. Może się bowiem zdarzyć, że użytkownicy będą korzystać z systemu AI w sposób, który nie został przewidziany przez jego dostawcę, a sposób ten będzie naruszał prawa lub wolności człowieka. Jednocześnie ważne jest, żeby systemy AI nie generowały wyników, które będą zrozumiałe co najwyżej tylko dla nich samych, natomiast ludzie, którzy zostali dotknięci negatywną dla nich decyzją wydaną przez system AI, będą pozbawieni prawa do uzyskania uzasadnienia takiej decyzji.

Ponadto należy zaktualizować wykaz systemów, które będą uznawane za systemy AI wysokiego ryzyka. W szczególności dotyczy to systemów AI wpływających na funkcjonowanie systemu demokratycznego oraz procedury wyborczej – zarówno w okresie trwającej kampanii wyborczej, jak i późniejszego liczenia głosów. Jak pokazał przykład sprawy Cambridge Analytica, działanie systemu AI analizującego dane kilkudziesięciu milionów wyborców może mieć znaczący wpływ na wynik ogólnokrajowych wyborów[68]. Tak samo ogromne znaczenie dla demokracji i praw wyborczych może mieć system AI odpowiadający za liczenie głosów. Dlatego kluczowe jest, aby tego typy systemy AI również były uznawane za systemy AI wysokiego ryzyka.

[68] B. Schippers, *Artificial Intelligence and Democratic Politics*, POLITICAL INSIGHT, 2020.

Bez wprowadzenia tych zmian system ochrony praw człowieka stworzony w oparciu o projekt Aktu pozostanie niekompletny i nie w pełni skuteczny. Lista systemów AI o niedopuszczalnym ryzyku nie będzie zawierała w sobie wszystkich najistotniejszych i możliwych do zidentyfikowania ryzyk, przez co projektowana regulacja nie będzie chroniła wszystkich wartości, do ochrony których została stworzona. Równocześnie systemy AI wysokiego ryzyka wciąż będą generowały wiele ryzyk i zagrożeń dla standardu ochrony praw człowieka, ale projekt Aktu nie zapewni nam narzędzi, które pozwolą je zneutralizować.

BIBLIOGRAFIA

Schippers B., *Artificial Intelligence and Democratic Politics*, POLITICAL INSIGHT, 2020.

European Digital Rights, *An EU Artificial Intelligence Act for Fundamental Rights. A Civil Society Statement*, 2021, https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf (dostęp: 14.05.2022)

Europejski Inspektor Ochrony Danych, Europejska Rada Ochrony Danych, *Apel o wprowadzenie zakazu stosowania AI do automatycznego rozpoznawania cech ludzkich w publicznie dostępnych przestrzeniach oraz do niektórych innych zastosowań sztucznej inteligencji, które mogą prowadzić do niesprawiedliwej dyskryminacji,* Bruksela, 2021, https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_pl (dostęp: 14.05.2022)

Fundacja Panoptykon, *O co walczymy w unijnej regulacji AI? 5 postulatów*, https://panoptykon.org/regulacja-ai (dostęp: 14.05.2022)

Human Rights Watch, Q*&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net*, https://www.hrw.org/sites/default/files/media_2021/11/202111hrw_eu_ai_regulation_qa_0.pdf (dostęp: 14.05.2022)

Małobęcka-Szwast I., *Podejście oparte na ryzyku i nowe obowiązki w projekcie aktu w sprawie SI*, https://newtech.law/pl/podejscie-oparte-na-ryzyku-i-nowe-obowiazki-w-projekcie-aktu-w-sprawie-si/ (dostęp: 14.05.2022)

Izba Poselska Parlamentu Republiki Czeskiej, *Rezolucja nr 471*, Praga, 2021.

Komisja CULT, *Draft opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, Bruksela 2022.

Komisja Europejska, *Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych)*, COM/2020/842 final, Bruksela 2020.

Komisja Europejska, *Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE*, COM/2020/825 final, Bruksela 2020.

Komisja Europejska, *Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre inne akty ustawodawcze Unii*, COM/2021/206 final, Bruksela 2021.

Komisja IMCO i LIBE, *Draft report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, Bruksela 2022.

Komisja JURI, *Draft opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*, Bruksela 2022.

Komitet Ekonomiczno-Społeczny, *Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii"*, Dz. Urz. UE C 517/61 z 22.12.2021 r.

Komitet Regionów, *Opinia Europejskiego Komitetu Regionów – Europejskie podejście do sztucznej inteligencji – akt w sprawie sztucznej inteligencji*, Dz. Urz. UE C 97/12 z 28.02.2022 r.

Rada Unii Europejskiej, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text*, Bruksela 2021.

Senat RP, Opinia *Komisji Spraw Zagranicznych i Unii Europejskiej. Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej Inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*, Warszawa 2021.

KAJA HECKERT
UNIWERSYTET ADAMA MICKIEWICZA W POZNANIU

KRYPTOWALUTY - MOŻLIWOŚCI I ZAGROŻENIA W ICH UŻYTKOWANIU. PERSPEKTYWA PRAWNOKARNA

Abstrakt: Głównym celem artykułu jest poddanie pod rozwagę złożonego problemu, mianowicie czy obowiązujące w Polsce prawo karne obejmuje swoim zakresem przestępstwa kryptowalutowe i czy tym samym zapewnia ochronę użytkownikom walut kryptograficznych. Przedstawione zostaną główne problemy definicyjne oraz status kryptowalut w odniesieniu do pojęć normatywnych. Kolejnym zagadnieniem poruszonym w artykule będą możliwości i zagrożenia związane z użytkowaniem walut kryptograficznych. Jak pokazuje praktyka, kryptowaluty są nie tylko przedmiotem przestępstwa, mogą bowiem stanowić również narzędzie do jego popełnienia. Zbadane zostaną zagadnienia dotyczące: spekulacji i piramid finansowych, nieautoryzowanego wydobywania kryptowalut oraz darknetu. Powyższe nastąpi w oparciu o badania przeprowadzone przez czołowe instytucje zajmujące się cyberprzestępczością.

Słowa kluczowe: kryptowaluty, bitcoin, blockchain, prawo karne

1. WSTĘP

W ostatnich latach jesteśmy świadkami tego, jak z pozoru surrealistyczna koncepcja stała się kamieniem węgielnym dla rewolucji w rozumieniu pieniądza, ponieważ pytanie o kryptowaluty to w zasadzie wątpliwość dotycząca redefinicji systemów płatniczych, jakie znamy dotychczas. Po 12 latach od dokonania pierwszej transakcji z użyciem bitcoinów kryptowaluty zyskały popularność i na stałe zagościły w publicznej debacie. Mimo znacznego upływu czasu, w doktrynie polskiej i zagranicznej wciąż brakuje jednolitych stanowisk

dotyczących kryptowalut. Tymczasem, wzrost popularności walut kryptograficznych sprawia, że stają się one przedmiotem spraw sądowych oraz czynności wykonawczych.

Można zatem zadać pytanie, czy kryptowaluty jako zjawisko niespotykane wcześniej w polskim porządku prawnym wymagają dodatkowej regulacji? Z uwagi na charakter przedmiotowego tekstu pytanie to zostanie przeanalizowane z perspektywy prawa karnego. W tym miejscu warto rozważyć dwa scenariusze. Pierwszy z nich to sytuacja, w której aktualne przepisy nie wymagają dostosowania do omawianej problematyki, ponieważ ich konstrukcja pozwala na odpowiednie stosowanie. W ten sposób waluty kryptograficzne można by zaimplementować do istniejącego porządku prawnego bez konieczności wprowadzania znaczących zmian. Druga wersja, mniej optymistyczna, wiązałaby się z koniecznością przekształcenia obowiązujących już przepisów bądź uchwalenia nowych. Z punktu widzenia ustawodawcy poszerzanie katalogu przestępstw zawartych w kodeksie karnym jest zachowaniem niepożądanym, mogącym nosić znamiona nadmiernej kazuistyki. Co więcej, zmiana przepisów wiązałaby się z koniecznością przeprowadzenia rzetelnej oceny skutków owej regulacji oraz prawdopodobnie długim i żmudnym procesem legislacyjnym. Tymczasem, rozwój technologii postępuje, a rosnąca liczba użytkowników kryptowalut uzasadnia wpisanie ich w katalog dóbr chronionych prawem karnym.

Zanim przejdziemy do omówienia zagadnień natury karnistycznej pokrótce opisane zostaną kwestie dotyczące samej technologii. Nie sposób bowiem dokonać analizy tematu ze styku prawa i nowych technologii bez wcześniejszego uporządkowania podstawowych pojęć, które składają się na zakres omawianej materii.

2. TECHNOLOGIA

By zobrazować funkcjonowanie technologii blockchain autorzy często porównują łańcuch bloków do cyfrowej księgi rachunkowej, w której rejestrowane są rozmaite transakcje. Dzięki wzajemnym powiązaniom blockchain tworzy ciągły łańcuch informacji podzielonych w bloki, które można porównać do kolejnych rozdziałów ów księgi, a dokonanych „transakcji" nie można zmienić ani cofnąć[1]. Przedstawiona struktura jest zaś niczym innym, jak rozproszoną bazą danych, która może przechowywać nieskończenie wiele

[1] https://bitcoin.org/bitcoin.pdf (dostęp:18.05.2022).

informacji.

Mimo, że początki technologii sięgają 1979 roku i struktury o nazwie drzewo skrótów, prawdziwy wzrost popularności blockchain zyskał dopiero w 2008 roku za sprawą tzw. The White Paper autorstwa osoby lub grupy osób działających pod pseudonimem Satoshi Nakamoto. Wykorzystywany w architekturze Bitocina opiera się na sieci nazywanej z języka angielskiego *peer-to-peer (P2P)*, czyli sieci, w której nie występują centralne serwery, a wymiana danych następuje bezpośrednio między użytkownikami.[2] Łańcuch bloków bitcoina rozpoczyna wpis stanowiący o tym, że właściciel konkretnego adresu publicznego wygenerował pierwszych 50 bitcoinów, jest to tak zwany *genesis block*. Kolejne bloki poza zapisem dotyczącym nowych bitcoinów zawierają również informacje dotyczące wcześniej powstałych bitcoinów. Bloki bitcoina mają ograniczoną pojemność wynoszącą 1 MB[3].

Aktualnie istnieje ponad 6 tysięcy różnych rodzajów kryptowalut, które różnią się szeregiem cech[4]. Wyróżnić można kryptowaluty wymienialne bezpośrednio na tradycyjne waluty fiducjarne, kryptowaluty odporne na inflację, takie jak bitcoin oraz takie, których algorytm dopuszcza inflację. Waluty kryptograficzne różnią się między sobą także stopniem anonimowości użytkowników. Mimo licznej konkurencji najpopularniejszą z kryptowalut pozostaje bitcoin, jego udział w rynku wynosi ok 43%[5]. Ze względu na powyższe przedmiotowe opracowanie dotyczyć będzie przede wszystkim bitcoina.

Celem twórcy (lub twórców) bitcoina było stworzenie międzynarodowego środka płatniczego, dzięki któremu pieniądze mogłyby przepływać bezpośrednio do portfeli użytkowników bez tzw. zaufanej trzeciej strony (np. banku). Jest to możliwe z uwagi na wartości przyświecające społeczności bitcoinowej *„Społeczność danej kryptowaluty sprawuje nad nią nadzór, przy czym zasady rządzące systemem zapisane są w kodzie komputerowym, który staje się „prawem" (code is law)"*[6]. Transakcje są dokonywane przez użytkowników z wykorzystaniem dwóch rodzajów kluczy. Wyróżniamy klucz prywatny, znany tylko właścicielowi i klucz publiczny, który można udostępniać innym użytkownikom. W sytuacji, gdy użytkownik A chce przesłać określoną liczbę bitcoinów użytkownikowi B nadawca tworzy wiadomość zawierającą klucz publiczny, a następnie „podpisuje" wiadomość swoim kluczem prywatnym.

---

[2] J. Konieczny, R. Prabucki, R. Wielki, *Kryptowaluty. Perspektywa kryminologiczna i kryminalistyczna,* Warszawa 2018, s. 8-26.
[3] https://bitcoin.org.pl/technologia-blockchain/ (dostęp: 18.05.2022).
[4] https://coinlib.io/coins (dostęp: 18.05.2022).
[5] https://coinmarketcap.com/pl/currencies/bitcoin/ (dostęp: 18.05.2022).
[6] https://bitcoin.org.pl/zalety-i-wady-walut-cyfrowych/ (dostęp: 18.05.2022).

Klucz prywatny nie może być udostępniany innym użytkownikom. Natomiast, dzięki kluczowi publicznemu każdy używający bitcoinowego oprogramowania może sprawdzić, czy transakcja została podpisana odpowiednim kluczem prywatnym oraz czy środki, które zostały przekazane są aktualnie powiązane z adresem odbiorcy. Prawidłowe funkcjonowanie sieci jest zapewniane przez użytkowników zwanych górnikami (ang. *miners*), którzy są nagradzani za weryfikowanie transakcji dokonywanych przez pozostałych użytkowników sieci, zatwierdzone transakcje są przechowywane w publicznym rejestrze (łańcuchu bloków). Dzięki takiej konstrukcji można prześledzić historię przepływu każdego bitcoina[7]. W posiadanie bitcoinów można wejść również nie będąc górnikiem, wystarczy skorzystać z usług kantoru, bitomatu lub giełdy kryptowalutowej. Przechowywanie większej ilości kryptowalut na giełdach nie jest jednak wskazane, dlatego warto wyeksportować zakupione środki do tzw. portfela. Portfele te służą do przechowywania aktywów cyfrowych chronionych kluczem prywatnym. Występują portfele on-line i off-line, którym może być chociażby pendrive czy kartka papieru z wydrukowanym adresem i kluczem prywatnym.

Przedstawione powyżej podstawowe zasady zasad funkcjonowania walut kryptograficznych takie, jak anonimowość czy pominięcie organu kontrolnego (np. banku) tworzą z punktu widzenia prawa karnego wiele potencjalnych zagrożeń. Do wymienionych aspektów sprzyjających rozwojowi przestępczości należy dodać niską świadomość społeczeństwa dotyczącą kryptowalut i trudności jakie niesie za sobą od strony technicznej wykrywanie tego typu przestępstw. Pojawiają się na również tezy, że to czarny rynek jest motorem napędowym istnienia krytpowalut[8]. Na podstawie badań przeprowadzonych przez Chainanalysis w 2021 r. przestępczość związana z kryptowalutami rekordowy poziom 14 mld USD, co stanowi wzrost z 7,8 mld USD w 2020 r.[9]

3. KRYPTOWALUTY W ODNIESIENIU DO POJĘĆ NORMATYWNYCH

W styczniu 2009 roku powstała sieć Bitcoin. Pierwszy, realny kurs bitcoina ustalono na podstawie kosztu wydobycia. Było to dokładnie 5 października 2009 roku i za jednego dolara amerykańskiego (1 USD) można było wówczas kupić 1309 BTC. Dziś role się odwróciły i mimo licznych fluktuacji, to

[7] J. Konieczny, R. Prabucki, R. Wielki, *op. cit.,* s. 10-57.
[8] https://comparic.pl/bitcoin-pozostaje-glownie-w-rekach-przestepcow/ (dostęp:18.05.2022).
[9] K. Grauer, W. Kueshner, H. Updegrave, *The 2022 Crypto Crime Report,* Chainalysis, s. 3.

bitcoin jest zdecydowanie droższy od dolara amerykańskiego. Kryptowaluty na coraz szerszą skalę wchodzą do mainstreamu. W Stanach Zjednoczonych firma Milo uruchomiła pierwsze kredyty hipoteczne zabezpieczone aktywami cyfrowymi[10], Burmistrz Nowego Jorku Eric Adams powiedział, że zaakceptuje swoje pierwsze trzy wypłaty w kryptowalucie[11].

Rosnąca popularność walut kryptograficznych nie uszła uwadze ustawodawcy. Z ekonomicznego punktu widzenia najistotniejsze okazało się uregulowanie nowego zagadnienia w kontekście prawa podatkowego, stąd też linia orzecznicza dotycząca problematyki opodatkowania jest stosunkowo szeroka. Ze względu na praktyczne zastosowanie walut kryptograficznych, które w praktyce służą jako środek do inwestycji i dokonywania płatności, w doktrynie podjęto rozważania dotyczące cywilnoprawnej natury problemu. Niewiele jest jednak publikacji dotyczących zagadnienia kryptowalut w kontekście prawa karnego. Tymczasem, jak wynika z dostępnej literatury, doniesień medialnych oraz komunikatów prasowych organów ścigania i instytucji finansowych problem istnieje. Płatności dokonywane przy pomocy kryptowalut zapewniają uczestnikom transakcji większą anonimowość niż w przypadku klasycznych przelewów bankowych. Dzięki wykorzystaniu technik szyfrujących trudniej również ustalić pochodzenie pieniędzy. Co więcej, kryptowaluty mogą służyć jako środek płatniczy w tzw. darknecie, a więc na przykład do finansowania terroryzmu, zakupu nielegalnych substancji, pornografii dziecięcej i innych. Kryptowaluty mają również określoną wartość odzwierciedloną w pieniądzu, oznacza to, że stają się celem złodziei i oszustów.

Wraz z tzw. V Dyrektywą AML[12] oraz polską Ustawą z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu pojawiła się definicja legalna obejmująca swoim zakresem waluty wirtualne. Na marginesie jedynie należy zaznaczyć, że w doktrynie istnieje spór dotyczący rozróżnienia pojęć waluty kryptograficzne, waluty wirtualne oraz waluty cyfrowe[13]. Zgodnie jednak z definicją wskazaną w art. 2 ust. 2 pkt 26 z ww. ustawy, *waluta wirtualna jest to cyfrowe odwzorowanie wartości, które nie jest:*

[10] https://bitcoin.pl/bitcoin-hipoteka (dostęp: 18.05.2022).

[11] https://www.rp.pl/polityka/art19078251-burmistrz-elekt-nowego-jorku-wezmie-pierwsze-wyplaty-w-bitcoinach (dostęp: 18.05.2022).

[12] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z 30.5.2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

[13] J. Czarnecki, *Nie tylko bitcoin, czyli rodzaje wirtualnych walut,* Wardyński i Wspólnicy, Warszawa 2014, s. 11.

a) *prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,*
b) *międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,*
c) *pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,*
d) *instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,*
e) *wekslem lub czekiem*

oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego;

Przytoczona definicja pozostawia szerokie pole do interpretacji, co z jednej strony może stanowić zaletę, z drugiej zaś, bez jasno skonstruowanej definicji, trudno jest wskazać istotę interesującej nas instytucji. Z drugiej strony, dokładne zdefiniowanie prowadziłoby do sytuacji, w której dana definicja szybko by się dezaktualizowała, w głównej mierze przez wzgląd na nieustanny rozwój technologii.

Urząd Komisji Nadzoru Finansowego opublikował stanowisko w sprawie wydawania i obrotu kryptoaktywami, w którym wskazano, że kryptowaluty lub waluty wirtualne są tokenami płatniczymi[14]. Zdefiniowano je jako rodzaj kryptoaktywów służących jako środek wymiany za dobra lub usługi i jako takie mogące pełnić rolę odpowiadającą środkom płatniczym. Nie stanowią jednak zalegalizowanego środka płatniczego– nie są emitowane przez bank centralny lub inny organ publiczny, nie posiadają gwarantowanej przepisami prawa zdolności do umarzania zobowiązań pieniężnyc, a „płatność" nimi może być dokonana jedynie wtedy, gdy wierzyciel wyrazi wolę przyjęcia takiej „płatności" i zwolnienia dłużnika z zobowiązania pieniężnego.

Próbując odnaleźć miejsce dla kryptowalut w polskim porządku prawnym proponuję przyjąć stanowisko przyjęte przez Naczelny Sąd Administracyjny, który w wyroku z dnia 6 marca 2018 r., sygn. II FSK 488/16,

[14] https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_70296.pdf (dostęp: 18.05.2022).

wskazał, że: „(...) 2. w praktyce stosunków cywilno-prawnych bitcoin stanowi rodzaj mienia w rozumieniu art. 44 ustawy Kodeks cywilny – dalej k.c."[15] Mienie w przywołanym przez NSA art. 44 k.c. definiowane jest jako własność i inne prawa majątkowe. Stanowisko to zostało potwierdzone w oficjalnym komunikacie Ministerstwa Finansów, w którym możemy przeczytać, że „Mając na uwadze, że w powszechnym obrocie kryptowaluty są wymieniane na tzw. giełdach kryptowalut na waluty fiducjarne będące prawnymi środkami płatniczymi, należy je zakwalifikować jako prawa majątkowe o charakterze zbywalnym."[16] Stanowisko doktryny nie jest jednak jednolite i pojawiają się głosy proponujące inną kwalifikację walut kryptograficznych. Przyjmując jednak kwalifikację kryptowalut jako prawa majątkowego możemy przejść do ich relacji z porządkiem prawnym, a ta jest dość skomplikowana.

4. RODZAJE ZAGROŻEŃ

Kryptowaluty budzą wiele kontrowersji, nie tylko wśród prawników, lecz również w środowisku czołowych przedstawicieli świata finansów oraz nowych technologii. Wielokrotnie nazywano je bańką, oszustwem czy piramidą finansową[17]. Trudno się dziwić tego typu poglądom, szczególnie mając na uwadze zmienność kursów kryptowalut, które są, bardziej niż waluty fiducjarne, podatne chociażby na doniesienia medialne[18]. Giełdy kryptowalutowe bywają przejmowane przez hakerów lub niespodziewanie zamykane[19]. W 2014 roku zamknięta została największa w tamtym czasie giełda kryptowalutowa świata, straty oszacowano według ówczesnego kursu btc na około 473 mln dolarów[20]. Tego typu sytuacje nie są domeną wyłącznie giełd zagranicznych, w październiku 2016 roku z sieci zniknęła polska giełda Bitcurex pochłaniając bitcoiny o wartości około 100 mln złotych.

[15] Wyrok Naczelnego Sądu Administracyjnego z 6.03.2018 r., II FSK 488/16.
[16] http://orka2.sejm.gov.pl/INT9.nsf/klucz/ATTBRHJ27/%24FILE/i08208-o1.pdf (dostęp 18.05.2022)..
[17] https://www.cnbc.com/2019/05/04/warren-buffett-says-bitcoin-is-a-gambling-device-with-a-lot-of-frauds-connected-with-it.html (dostęp: 18.05.2022)..
[18] https://businessinsider.com.pl/gielda/kryptowaluty/elon-musk-a-kurs-bitcoina-wpis-miliardera-o-tesli-i-kryptowalucie/0ttyy3g (dostęp: 18.05.2022)..
[19] Zob. Grzybkowski M., Bentyn Sz., *Kryptowaluty. Dlaczego jeden bitcoin wart będzie milion dolarów?,* Poznań 2018, s. 90 – 94.
[20] https://www.fxmag.pl/edukacja/kryptowaluty/mt-gox-historia-najwiekszego-upadku-w-dziejach-rynku-kryptowalut (dostęp: 18.05.2022)..

5. SPEKULACJE I PIRAMIDY FINANSOWE

Mimo, że część ekonomistów uważa kryptowaluty za piramidę finansową, to poddając analizie schemat działania np. bitcoina zauważyć należy, że nie spełnia on cech charakterystycznych dla piramid finansowych[21]. Art. 7 pkt 14 Ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (t.j. Dz. U. z 2017 r. poz. 2070) wskazuje, że w ramach tzw. piramid konsument wykonuje świadczenie w zamian za możliwość otrzymania korzyści materialnych, które są uzależnione przede wszystkim od wprowadzenia innych konsumentów do systemu, a nie od sprzedaży lub konsumpcji produktów.

Piramida opiera się na działaniach organizatorów dążących do pozyskiwaniu środków finansowych od inwestorów jednocześnie gwarantując nieprzeciętnie wysokie zyski. Istotnym elementem struktury piramid finansowych jest to, że zyski uzależnione są od werbowania nowych osób i dokonywanych przez nich wpłat. Tymczasem, w przypadku kryptowalut nie występuje organizator, tym samym wyeliminowany zostaje aspekt psychologiczny, mianowicie nakłanianie do inwestowania umotywowane szybką i wysoką stopą zwrotu poczynionych nakładów. Zakup kryptowalut przypomina mechanizm giełdowy na zasadzie kupuj-sprzedaj, nie ma tu mowy o pozyskiwaniu nowych użytkowników i czerpaniu z tego korzyści, a w szczególności nie zachodzi sytuacja, w której zyski byłyby zależne od wpłat dokonanych przez zwerbowanych użytkowników.

Fakt, że kryptowaluty nie są same w sobie piramidą finansową nie oznacza jednak, że nie mogą być wykorzystywane do takich działań przez giełdy, pośredników oraz twórców tzw. kopalni kryptowalut. 27 marca 2019 roku Prezes Urzędu Ochrony Konkurencji i Konsumentów wydał specjalne oświadczenie, w którym ostrzega przed inwestowaniem w licencje oferowane przez jedną z Singapurskich spółek. Jak podano w oświadczeniu, zachodzi uzasadnione podejrzenie, że spółka stosuje praktyki naruszające zbiorowe interesy konsumentów, mogące spowodować straty finansowe dla licznej grupy konsumentów[22]. Narodowy Bank Polski i Komisja Nadzoru Finansowego również ostrzegały przed zakupem tzw. walut wirtualnych, motywując swoje

[21] https://tokeneo.com/pl/schiff-bitcoin-btc-to-piramida-finansowa/ (dostęp: 18.05.2022).
[22] Komunikat Prezesa Urzędu Ochrony Konkurencji i Konsumentów z 27.03.2019r., RGD.610-10/18/MLM.

stanowisko wysokim ryzykiem oszustwa oraz tym, że część form inwestowania w kryptowaluty może mieć charakter piramidy finansowej[23].

6. ATAKI DOKONYWANE W CELU POZYSKANIA KRYPTOWALUT I ICH KWALIFIKACJA

Jak wynika z badań w 2021 roku użytkownicy kryptowalut w wyniku szeroko rozumianego *scamu* stracili ponad 7,7 miliarda dolarów[24]. Analizując poszczególne incydenty można zauważyć, że sprawcy w celu uzyskania dostępu do środków ofiar używają głównie metod socjotechnicznych w tym phishingu, wirusów i innych ataków[25]. Atak phishingowy ma miejsce, gdy atakujący podszywa się pod zaufany podmiot i nakłania ofiarę do kliknięcia w fałszywy link, otwarcia załącznika lub wiadomości tekstowej, a następnie pozyskuje od ofiary np. dane logowania do konta bankowego.

Czy powyższe czyny mogłyby zostać zakwalifikowane w świetle polskiego prawa karnego jako oszustwa? Scharakteryzowane w art. 286 k.k. przestępstwo oszustwa ze względu na szerokie sformułowanie strony podmiotowej wydaje się znajdować zastosowanie dla przestępstw kryptowalutowych. Przedmiotem ochrony powyższego przepisu jest mienie, natomiast czynność sprawcza objawia się poprzez doprowadzenie innej osoby do niekorzystnego rozporządzenia nim. Nie mamy tutaj zatem do czynienia z kategorią rzeczy ruchomych czy też koniecznością dokonania zaboru, wyjęcia spod władztwa, co ja już zauważono mogłoby dyskwalifikować przestępstwa kryptowalutowe. Kwalifikacja z art. 286 § 1 k.k. jest również stosowana przez organy ścigania. Za przykład może posłużyć chociażby sprawa giełdy kryptowalutowej BitMarket. 9 lipca 2019 roku jedna z najstarszych w Polsce giełd oferujących wymianę walut kryptograficznych opublikowała na swojej stronie oświadczenie o zakończeniu działalności. Tym samym użytkownicy giełdy zostali pozbawieni dostępu do swoich środków, które były ulokowane na giełdzie. W sprawie zostało wszczęte śledztwo o przestępstwo z art. 286§1 k.k. w zw. z art. 294 § 1 k.k. w zw. z art. 12 k.k.

Kolejnym czynem zasługującym na szerszą analizę jest przestępstwo oszustwa komputerowego. Przedmiotem ochrony jest w tym przypadku szeroko pojęte mienie, a czynność sprawcza polega na ingerowanie w zapis danych

[23] Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie „walut" wirtualnych, NBP i KNF, Warszawa, 2017 r.
[24] K. Grauer, W. Kueshner, H. Updegrave, *op. cit.,* s. 79.
[25] https://binance.zendesk.com/hc/en-us/articles/360028031711 (dostęp: 18.05.2022).

informatycznych. Mając na uwadze przedstawioną do tej pory charakterystykę obrotu kryptowalutami nietrudno wyobrazić sobie sytuację, w której przestępca – haker, przełamuje zabezpieczenia portfela kryptowalutowego bądź giełdy i wyprowadza ulokowane tam środki. W 2015 roku Komenda Powiatowa Policji w Olkuszu poinformowała o zatrzymaniu 28-latka, który dzięki ingerencji w zapisy danych wyprowadził z giełdy waluty kryptograficzne o wartości ponad 85 tys. złotych. Mężczyźnie przedstawiono zarzuty o czyn oszustwa komputerowego tj. art. 287 § 1 k.k. Przestępstwa oszustwa komputerowego powiązanego z walutami kryptograficznymi dotyczy również wyrok Sądu Okręgowego w Poznaniu z dnia 29 marca 2017 roku o sygnaturze akt XVII Ka 146/17. Jak wynika z uzasadnienia wyroku sądu drugiej instancji oskarżony, z zawodu programista, wykorzystał błędy w zabezpieczeniach giełdy kryptowalutowej, której nazwa została zanonimizowana jako B. (...) pl. Przy użyciu tzw. płatności testowych oskarżony wyprowadził z serwisu kryptowaluty o wartości ok. 85 tys. złotych, za co został oskarżony o czyn z art. 287 § 1 k.k.tj. oszustwo komputerowe. W uzasadnieniu podano, że oskarżony „działając w celu osiągniecia korzyści majątkowej (jaką było uzyskanie bitcoinów bez uprzedniego zasilenia konta na ich zakup środkami pieniężnymi), nie będąc upoważniony do wykonywania płatności testowych, realizując 66 takich płatności wpłynął na automatyczne przetwarzanie danych Portalu B. (...) powodując szkodę w mieniu właściciela portalu w wysokości 85.137 zł." Oskarżony został uznany przez sąd pierwszej instancji za winnego i został skazany na karę 1 roku pozbawienia wolności, warunkowo zawieszoną na okres 3 lat oraz grzywnę i środek kompensacyjny pod postacią obowiązku naprawienia szkody. Wyrok sądu rejonowego został w całości zaskarżony przez obrońcę oskarżonego, jednak sąd drugiej instancji przychylił się do apelacji jedynie w zakresie uchylenia środka kompensacyjnego.

Giełdy oraz kantory zajmujące się wymianą kryptowalut są częstym celem ataków hakerskich. W 2018 roku z giełdy Coincheck skradziono kryptowalutę NEM o wartości 400 mln dolarów[26]. Kolejny analizowany incydent dotyczy włamania do bitomatu we wrześniu 2018 roku, w wyniku którego skradziono kwotę 200 tysięcy dolarów. Doszło do tego, ponieważ twórcy bankomatu operującego bitcoinami nie wzięli pod uwagę podstaw funkcjonowania bitcoinowego blockchain, otóż transakcje dokonywane przy użyciu bitcoinów nie są zapisywane w bloku w momencie wykonania, w pierwszej kolejności trafiają do kolejki, ponieważ każdy blok ma ograniczoną pojemność.

[26] J. Konieczny, R. Prabucki., R. Wielki, *op. cit.*, s. 78-79.

Nowe bloki są tworzone w regularnych odstępach czas, w pierwszej kolejności zapisywane są transakcje dokonywane przez osoby, które uiściły wyższą opłatę na rzecz twórcy bloku. Bankomat BTC został zaprojektowany w taki sposób, że wydawał gotówkę przed zaakceptowanie transakcji umożliwiając tym samym podwójne wydatki. W doniesieniach medialnych opisujących przypadki zbliżone do powyższych można odnaleźć wiele nagłówków zawierających słowo kradzież np. „Atak na giełdę Bisq: skradziono kryptowaluty warte przeszło 250.000 dolarów", „Nastolatek podejrzany o kradzież 50.000.000 dolarów w kryptowalutach", „21-latek skazany na 10 lat więzienia za kradzież kryptowalut". Jest to uzasadnione, ponieważ kryptowaluty mogą funkcjonować w świadomości ich użytkowników jako forma pieniądza. Myśląc o kryptowalutach jako składniku mienia reprezentującym konkretną wartość oczywiste jest, że ich utrata ma realne skutki. Intuicyjnie zatem sytuacja, w której ktoś zostaje bezprawnie pozbawiony kryptowalut może być postrzegana jako kradzież, tak jak miałoby to miejsce w przypadku tradycyjnego pieniądza czy rzeczy.

Tymczasem należy zadać pytanie, czy na gruncie aktualnych przepisów kodeksu karnego kryptowaluty można ukraść? Zgodnie z przepisem art. 278 § 1 k.k. przedmiotem czynności wykonawczej jest cudza rzecz ruchoma. Kodeks karny posiłkuje się w tym względzie definicją cywilistyczną zawartej w przepisie art. 45 k.c., zgodnie z którą rzeczami są tylko przedmioty materialne. Definicja ta została sprecyzowana przez doktrynę prawa cywilnego, otóż przesłankami uznania za rzecz są materialny charakter oraz wyodrębnienie z przyrody. Kryptowaluty, jak wskazuje definicja są cyfrowym odwzorowaniem wartości, co przekreśla możliwość zakwalifikowania ich jako rzeczy, a tym samym nie zostają spełnione przesłanki konieczne do zakwalifikowania czynu jako przestępstwo z art. 278 § 1 k.k.

Nie podlega wątpliwości, że prawo karne jest częścią systemu prawnego, który powinien być spójny i nie zawierać wewnętrznych sprzeczności, jednak prawo karne jest samodzielną gałęzią prawa, a co za tym idzie definicje zapożyczane z innych dziedzin powinny odpowiadać potrzebom prawa karnego. Powyższe znajduje potwierdzenie w tekstach doktryny „To nawiązanie do terminologii zaczerpniętej z prawa cywilnego nakazuje w procesie interpretacji znamion kradzieży w tym zakresie odwoływać się do brzmienia i wykładni tego pojęcia w prawie cywilnym. Nie oznacza to jednak, że sposób wyznaczania zakresu znaczeniowego pojęcia rzeczy ruchomej w cywilistyce determinuje zakres znaczeniowy tego terminu w prawie karnym. O konieczności dokonania odpowiednich modyfikacji znaczeniowych pojęcia rzeczy ruchomej w prawie karnym w porównaniu ze znaczeniem nadawanym temu terminowi

w prawie cywilnym przesądza nie tylko wyjątkowo wąskie rozumienie "rzeczy ruchomej" w cywilistyce, lecz także wprowadzenie do tzw. słowniczka wyrażeń ustawowych definicji tego pojęcia." W ten sposób definicja rzeczy została rozszerzona poprzez katalog zawarty w przepisie art. 115 § 9 k.k. Rzeczami ruchomymi na gruncie prawa karnego są również polski albo obcy pieniądz lub inny środek płatniczy zapisany na rachunku oraz dokument uprawniający do otrzymania sumy pieniężnej albo zawierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach, albo stwierdzenie uczestnictwa w spółce. Aktualnie w Polsce kryptowaluty nie są uznawane za pieniądze, środki płatnicze, waluty obce ani papiery wartościowe, oznacza to zatem, że kryptowaluty wymykają się spod jurysdykcji przepisu art. 278 § 1 k.k.

Czy zatem „kradzież" kryptowalut można zakwalifikować na podstawie art. 278 § 2 k.k. dotyczącego kradzieży programu komputerowego? Sąd Apelacyjny w Katowicach w wyroku z dnia 29 listopada 2017 roku (sygn. akt II AKa 379/17) opisał przesłanki popełnienia przestępstwa uzyskania programu komputerowego bez zgody uprawnionej osoby. Na marginesie jedynie należy zaznaczyć, że sformułowanie „kradzież programu komputerowego" jest swoistym skrótem myślowym. Sąd Apelacyjny w Katowicach orzekł, że by zakwalifikować czyn jako przestępstwo z art. 278 § 2 k.k. wcale nie musi dojść do zaboru nośnika zapisu programu. Znamiona przestępstwa wypełnia sama wymiana plików między urządzeniami, nieautoryzowane kopiowanie programu, czy też niezgodne z prawem wejście w posiadanie cudzego programu. Zdanie to podziela część doktryny. Takie rozwiązanie stanowiłoby znaczące uproszczenie dla organów ścigania, gdyż rozwiązałoby problem z kwalifikacją „kradzieży" walut kryptograficznych.

7. DARKNET

Mając na uwadze raporty stworzone przez takie instytucje, jak Europol, CERT Polska czy Ministerstwo Spraw Wewnętrznych i Administracji można dostrzec, że przestępczość kryptowalutowa wpisuje się we wzrostowy trend dotyczący tzw. cyberprzestępczości[27]. Nie bez znaczenia dla wzrostu cyberprzestępczości pozostaje łatwy dostęp do przeglądarek sieci typu TOR, dzięki

[27] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (dostęp: 18.05.2022); Krajobraz bezpieczeństwa polskiego Internetu , Raport roczny z działalności CERT Polska 2018, CERT Polska, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (dostęp: 18.05.2022); Raport o stanie bezpieczeństwa w Polsce 2 2015 roku, https://archiwumbip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html (dostęp: 18.05.2022).

którym nawet niewprawiony użytkownik może dotrzeć do zasobów tzw. Głębokiego Internetu *(ang. Deep Web),* czyli stron niewidocznych dla wyszukiwarek takich jak Google, które z jednej strony spełniają szlachetną funkcję zapewnienia prywatności użytkownikom, a z drugiej są polem rozwoju *darknetu.*

Analiza ofert publikowanych w 17 największych *darkmarketów* wykazała, że prawie połowę wszystkich ofert stanowią narkotyki i inne środki psychoaktywne. Drugą pod względem liczebności kategorią są bazy danych, książki elektroniczne i poradniki, które mimo, że same w sobie mogą nie być nielegalne, to w darknecie sprzedawane są z pominięciem licencji i praw autorskich. Nieco ponad 15 % stanowią oferty dotyczące tzw. „pirackich" oprogramowani, programów służących do popełniania przestępstw itp. Kolejno, ex aequo z wynikiem około 3% udziału w rynku uplasowały się fałszywe i kradzione dokumenty oraz usługi np. usługi hackerskie. 2,4% ofert stanowią falsyfikaty dóbr, a około 0,7 oferty dotyczące broni[28]. Na podstawie wielu doniesień medialnych oraz danych gromadzonych przez takie serwisy, jak www.havocscope.com można domyślać się, że powyższej klasyfikacji wymykają się transakcje związane z handlem ludźmi, organami czy zabójstwami na zlecenie.

Często przytaczanym przykładem ukazującym skalę funkcjonowania darkmarketów jest głośna sprawa działającego w latach 2011-2013 *Silk Road.* Główna działalność portalu skupiała się na międzynarodowym, anonimowym handlu nielegalnymi produktami, głównie narkotykami i złośliwym oprogramowaniem. Anonimowość użytkownikom zapewniało umiejscowienie portalu w tzw. Deep Web oraz używanie bitcoinów jako oficjalnej jednostki rozliczeniowej. Transakcje między użytkownikami przebiegały następująco, w pierwszej kolejności kupujący wysyłał bitcoiny na rynek online, gdzie były one przechowywane, dopóki zamówienie nie zostało dostarczone odbiorcy, gdy to następowało bitcoiny były przekazywane sprzedającemu, od każdej transakcji pobierana była prowizja. Silk Road został zamknięty w październiku 2013 roku, a jego twórca Ross Ulbricht został aresztowany, a finalnie skazany na karę dożywotniego pozbawienia wolności. Według danych zgromadzonych przez organy ścigania Stanów Zjednoczonych w latach 2011–2013 tysiące użytkowników skorzystało z Silk Road, aby sprzedać narkotyki o wartości około 183 mln dolarów[29].

[28] *Ibidem.*
[29] Wyrok z 31.05.2017 r., United States v. Ulbricht, No. 15-1815 (2d Cir. 2017).

8. NIEAUTORYZOWANE WYDOBYWANIE KRYPTOWALUT

Cryptojacking, czyli złośliwe wydobywanie kryptowalut. Wykorzystuje ono przepustowość i moc obliczeniową użytkowników Internetu do wydobywania kryptowalut. Jest to możliwe dzięki umieszczeniu na stronach internetowych skryptu, który poprzez przeglądarkę użytkownika pozwala witrynie wykorzystać moc obliczeniową odwiedzających do wydobywania kryptowalut w trakcie korzystania ze strony. Wydobywanie kryptowalut przy użyciu mocy obliczeniowej osób odwiedzających strony internetowe, nie zawsze jest nielegalne. Niektóre witryny wykorzystują ową metodę w celach zarobkowych jednak kluczowa jest uprzednia zgoda użytkownika.

Nielegalne wydobywanie kryptowalut może polegać także na wykorzystywaniu służbowego sprzętu, czy też być związane z kradzieżą energii. Według doniesień Reuters władze Iranu skonfiskowały około 1.000 sztuk koparek kryptowalutowych, które ulokowane zostały w opuszczonych fabrykach. Władze Iranu szacują, że nielegalne kopalnie kryptowalut stanowią około 7% krajowego zużycia energii[30]. W Internecie można znaleźć wiele artykułów dotyczących wydobywania kryptowalut przy użyciu służbowego sprzętu. W marcu 2019 roku burmistrz Polkowic złożył do miejscowej prokuratury zawiadomienie o możliwości popełnienia przestępstwa. Jak wynika z komunikatu rzecznika Prokuratury Okręgowej w Legnicy czterem pracownikom urzędu gminy w Polkowicach zostały przedstawione zarzuty kradzieży energii elektrycznej. Pracownicy urzędu podłączyli tzw. koparkę do sieci elektrycznej Urzędu, czym spowodowali szkodę w wysokości minimum 7.500 zł[31]. Podobne przypadki miały miejsce również w Stanach Zjednoczonych i Czechach[32]. Jednak najbardziej spektakularny pod względem wielkości wyrządzonej szkody incydent miał miejsce w 2018 roku w Rosji, szacuje się, że sprawcy ukradli energię elektryczną wartą 60 mln rubli, co wówczas stanowiło równowartość około 1mln dolarów[33].

[30] https://www.reuters.com/article/us-crypto-iran/iran-seizes-1000-bitcoin-mining-machines-using-subsidized-power-idUSKCN1TS2VL (dostęp: 18.05.2022).
[31] https://www.dziendobrypolkowice.pl/2019/07/09/urzednicy-z-zarzutami-kradziezy-pradu/ (dostęp: 18.05.2022).
[32] https://www.fxmag.pl/artykul/bitcoin-cytrusy-i-pracownicy-amerykanskich-departamentow (dostęp: 18.05.2022).
[33] https://bitcoinpl.org/wielka-kopalnia-kryptowalut-odkryta-w-opuszczonej-fabryce-w-rosji/ (dostęp: 18.05.2022).

9. PROBLEMATYKA AML

Dyrektywa AML rozszerzyła katalog objętych nią podmiotów o prowadzące działalność gospodarczą w zakresie wymiany walut wirtualnych, a więc objęte nią zostały wszystkie giełdy i kantory obsługujące transfery kryptowalut. Działania mające przeciwdziałać praniu pieniędzy i finansowaniu terroryzmu opierają się na stosowaniu przez zobowiązane podmioty procedur KYC, czyli poznaj swojego klienta oraz prowadzeniu analiz transakcji mających na celu wyłapanie tych podejrzanych. Głównym zadaniem KYC jest zminimalizowanie działalności tzw. „słupów", dlatego niezbędnymi elementami tych działań są pozyskiwanie, sprawdzanie i przechowywanie danych osobowych klientów, a także sprawdzanie historii klientów i monitorowanie zmian.

Pranie pieniędzy można zdefiniować jako przetwarzanie dochodów pochodzących z działalności przestępczej w celu ukrycia ich nielegalnego pochodzenia. Strategię prania pieniędzy dzieli się tradycyjnie na cztery podstawowe kroki: fazę wstępną, umieszczenie, nakładanie warstw i integrację. W styczniu 2020 roku firma Chainalysis specjalizująca się w analizie zjawisk związanych z blockchainem opublikowała raport dotyczący przestępstw kryptowalutowych. Autorzy raportu na wstępie zauważają, że kryptowaluty działające na publicznie dostępnym blockchainie, takiej jak np. bitcoin są dobrym źródłem dla badania przepływów środków. Przyczynia się to do łatwiejszego zidentyfikowania krajów oraz giełd, do których wysyłane są nielegalnie pozyskane fundusze. Jak wynika z raportu w 2019 roku namierzono transakcje o przestępczym charakterze, których wartość wyniosła około 2,8 mld dolarów. Co istotne ponad 50% tych transakcji przepływało przez popularne giełdy Binance i Hubi, które mają obowiązek stosować procedury KYC. Oznacza to, że wdrożone procedury nie odnoszą oczekiwanych skutków.

Czy tego typu zachowania można kwalifikować jako typ czynu zabronionego scharakteryzowany w art. 299 § 1 k.k.? Sugerując się wyłącznie użytkową nazwą tj. pranie brudnych pieniędzy należałoby na to pytanie odpowiedzieć negatywnie, ponieważ jak ustalono w poprzednich rozdziałam kryptowaluty nie są w rozumieniu polskiego prawa pieniędzmi. Jednak treść przepisu art. 299 § 1 k.k. wskazuje, że dotyczy on nie tylko pieniędzy, lecz również środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych, a także innego mienia ruchomego lub nieruchomości pochodzących z korzyści związanych z popełnieniem czynu zabronionego. Co za tym idzie należy stwierdzić, że przepisy dotyczące prania pieniędzy znajdują zastosowanie w przypadku kryptowalut

Kolejnym zagadnieniem jest finansowanie terroryzmu. Problem ten istnieje i jest poważny, ponieważ organizacje terrorystyczne szybko dostrzegły korzyści płynące z dobrodziejstwa nowych technologii. W 2014 roku światło dzienne ujrzał manifest Al.-Kaidy, w którym podkreślono zalety użycia bitcoinów w walce z niewiernymi. Użycie kryptowalut przez islamskich terrorystów zostało opisane w briefie programowym Instytutu Kościuszki, autor zwraca uwagę na profesjonalny charakter zbiórek organizowanych przez terrorystów, załączanie instrukcji dokonania płatności oraz dbałość o socjotechnikę. Z drugiej strony autor porusza problematykę państw, takich jak Iran czy Koreańska Republika Ludowo-Demokratyczna, które wykorzystują kryptowaluty do finansowania swoich reżimów.

We wspomnianym już raporcie firmy Chainalysis podkreślono, że prowadzone przez organizacje terrorystyczne kampanie wchodzą na coraz bardziej zaawansowany pod kątem technologicznym poziom. Dla zobrazowania różnic autorzy raportu dokonali zestawienia dwóch tego typu kampanii, z których jedna miała miejsce w latach 2016-2018, a druga rozpoczęła się w 2019 roku. Pierwsza kampania dotyczyła ITMC Media Center odpowiedzialnego za media Shury czyli rady mudżahedinów. Zorganizowana przez ITMC zbiórka crowdfundingowa z wykorzystaniem kryptowalut została nazwana „Wyposaż Nas", a zebrane dzięki niej środki miały zostać przeznaczone na zakup broni, o czym darczyńcy byli otwarcie informowani. Organizatorzy zbiórki dla wzmocnienia oddziaływania na potencjalnych darczyńców używali fragmentów Koranu, uzasadniając darowiznę jako obowiązek religijny. Zbiórka była promowana na powszechnie dostępnych platformach takich jak YouTube i Twitter, w jej trakcie udostępniano adres bitcoinowego portfela, na który miały zostać przekazywane kryptowaluty. Jak wynika z analizy Chainalysis połowa przekazanych środków pochodziła z ze wspominanych już mikserów kryptowalut. Druga omawiana kampania dotyczyła wojskowego oddziału Hamasu i charakteryzuje się znacznie wyższym poziomem zaawansowania. W przeciwieństwie do akcji ITMC, gdzie wszystkie środki były przekierowywane na jeden adres bitcoinowy, w tym przypadku dla każdego darczyńcy został wygenerowany nowy adres, co znacznie utrudnia prześledzenie dokonywanych przelewów oraz oszacowanie ich skali.

Powyższa problematyka ma charakter międzynarodowy i wymaga nieustannej współpracy państw. Mimo wprowadzania kolejnych nowelizacji chociażby dyrektywy AML prawo nie jest w stanie nadążyć za postępem technologicznych i nigdy nie będzie. Przypomina to nieco sytuację występującą na rynku tzw. dopalaczy. Wraz z wprowadzaniem kolejnych ograniczeń

przez ustawodawcę i wycofywaniem z użycia jednych substancji w ich miejsce wprowadzano kolejne, coraz bardziej modyfikowane i szkodliwe.

10. WNIOSKI

Technologia blockachain okazała się nie tylko technologiczną rewolucją, lecz także dużym wyzwaniem z punktu widzenia prawa. Kryptowaluty przestały być wyłącznie obiektem zainteresowania niszowych grup inwestorów i stały się przedmiotem dyskusji szerszych środowisk. W stosunku do części zagadnień powiązanych z kryptowalutami udało się wypracować wspólne stanowisko doktryny, chociaż należy zaznaczyć, że wciąż istnieją kwestie budzące spory, a problemy zaczynają się na tak podstawowym poziomie.

Po przeanalizowania statusu kryptowalut w polskim prawie karnym odnoszę wrażenie, że brakuje nie tyle regulacji, lecz wiarygodnych źródeł czerpania wiedzy na temat relacji kryptowalut i prawa. Najlepszym i najbardziej aktualnym źródłem wiedzy okazują się blogi, fora internetowe oraz zagraniczna literatura. Ministerstwo Cyfryzacji w ramach programu „Od papierowej do cyfrowej Polski" stworzyło „Strumień Blockchain/DLT i Waluty Cyfrowe"[34], który kompleksowo opracował szereg zagadnień następnie je publikując, jednak w owych publikacjach znajdujemy następujący zapis „Opinie wyrażone w niniejszym opracowaniu są stanowiskiem Strumienia „Blockchain i Kryptowaluty". Dokument nie odzwierciedla poglądów Ministerstwa Cyfryzacji czy rządu Rzeczpospolitej Polskiej." Należy zatem zadać pytanie jakie są poglądy Ministerstwa Cyfryzacji i rządu Rzeczpospolitej Polskiej oraz czy w związku z tym, że Strumień zakończył swoją działalność ktokolwiek monitoruje sytuację prawną kryptowalut w Polsce.

Co do zasady zgadzam się ze stanowiskiem wyrażonym przez Strumień w publikacji pt. „Stanowisko Strumienia w sprawie kierunków ewentualnych prac legislacyjnych oraz działań regulacyjnych instytucji publicznych. Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych, zgodnie z którym na chwilę obecną nie ma konieczności wprowadzania nowelizacji obowiązujących przepisów kodeksu karnego. Jednocześnie opinia ta stanowi twierdzącą odpowiedź na kluczowe pytanie mojej pracy, a mianowicie, czy aktualne przepisy polskiego prawa karnego obejmują swoim zasięgiem przestępstwa kryptowalutowe.Jednak, tak jak wskazano w przywołanej publikacji, uważam, że należy na bieżąco

[34] https://www.gov.pl/web/cyfryzacja/od-papierowej-do-cyfrowej-polski (dostęp: 18.05.2022).

monitorować rozwój technologii oraz wszelkie pojawiające się stany faktyczne, by móc szybko zareagować na ewentualną potrzebę dostosowania do nich prawa karnego. Brak odpowiednich regulacji może bowiem prowadzić do tak skrajnych sytuacji, jaka miała miejsce 30 czerwca 2020 roku w Rosji, kiedy to sąd uznał, że z racji braku statusu prawnego kryptowaluty nie mogą być własnością, a co za tym idzie nie mogą być skradzione.

Odrębną, jednak równie istotną kwestią jest poruszana przez Strumień konieczność szkolenia sędziów, prokuratorów, a także funkcjonariuszy organów ścigania. Z racji braku konkretnych regulacji, to na wymiarze sprawiedliwości oraz organach ścigania spoczywa obowiązek umiejętnego kwalifikowania omawianych czynów. Samo wykrywanie przestępstw związanych z cyberprzestrzenią jest niezwykle trudne i wymaga wykwalifikowanego zespołu oraz odpowiednich narzędzi.

Przedstawione zagrożenia, również te o charakterze międzynarodowym pokazują, że tematyki kryptowalut nie należy ignorować, gdyż jest to aspekt istotny nie tylko dla jednostkowych obywateli, ale również z punktu widzenia gospodarki i bezpieczeństwa państwa. Mimo, że kryptowaluty powstały w myśl szlachetnej idei zapewnienia użytkownikom pełnej wolności i prywatności, to niekontrolowane mogą przeistoczyć się w zaawansowaną technologicznie broń, która wymknęła się spod kontroli, a której siłę rażenia trudno sobie wyobrazić. Nie należy zatem zapominać, że przestępstwa kryptowalutowe, mimo że dzieją się w cyberprzestrzeni mają swoje skutki świecie rzeczywistym. Jest to problem dotyczący szerszego zagadnienia, a mianowicie cyberprzestępczości.

BIBLIOGRAFIA

Literatura:

Ammous S., *Standard Bitcoina. Zdecentralizowana alternatywa dla bankowości centralnej.* Wrocław 2020

Butkiewicz E., *Czy Bitcoin poddaje się skutecznej regulacji prawnej?*, Raport wirtualne waluty, Warszawa 2014, s. 11-14.

Czarnecki J., *Nie tylko bitcoin, czyli rodzaje wirtualnych walut*, Raport waluty wirtualne, Warszawa 2014, s. 9-11

Dąbrowska J., *Charakter prawny bitcoin*, Człowiek w cyberprzestrzeni, Warszawa 2017, s. 54-76.

Foley S., Jonathan K. R., Putnins T. J., *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?*, The Review of Financial Studies 2019, s. 1798–1853

Grauer K., Keushner W., Updegrave H., *The 2022 Crypto Crime Report.* Chainalysis 2022.

Grzybkowski M., Bentyn Sz., *Kryptowaluty. Dlaczego jeden bitcoin wart będzie milion dolarów?,* Poznań 2018, s. 90 – 94.

Konieczny J., Prabucki R. i Wielki R., *Kryptowaluty. Perspektywa kryminologiczna i kryminalistyczna,* Warszawa 2018.

Królikowski M., *Prawo karne - część szczególna.* Warszawa 2011.

Królikowski M. i Zawłocki R., *Część szczególna. Tom II. Komentarz do artykułów 222–316,* Kodeks karny, Warszawa 2017.

Pasternak Ł., *Kryptowaluta i pieniądz wirtualny jako przedmiot przestępstwa z art. 310 § 1 k.k.,* Prokuratura i prawo 2017, nr 4, s. 77-94.

Susskind R., *Online courts and the future of justice.* Oxford 2021.

Szewczyk J., *O cywilnoprawnych aspektach bitcoina,* Monitor Prawniczy 2018.

Zacharzewski K., *Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego*, Monitor Prawniczy, Warszawa 2015, s. 187-195.

Zacharzewski K. i Piech K., *Stanowisko Strumienia w sprawie kierunków ewentualnych prac legislacyjnych oraz działań regulacyjnych instytucji publicznych. Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych,* Warszawa 2017.

Źródła internetowe:

https://bitcoin.org/bitcoin.pdf (dostęp:18.05.2022)

https://bitcoin.org.pl/technologia-blockchain/ (dostęp: 18.05.2022).

https://coinlib.io/coins (dostęp: 18.05.2022).

https://coinmarketcap.com/pl/currencies/bitcoin/ (dostęp: 18.05.2022).

https://bitcoin.org.pl/zalety-i-wady-walut-cyfrowych/ (dostęp: 18.05.2022).

https://comparic.pl/bitcoin-pozostaje-glownie-w-rekach-przestepcow/ (dostęp:18.05.2022).

https://bitcoin.pl/bitcoin-hipoteka (dostęp: 18.05.2022).

https://www.rp.pl/polityka/art19078251-burmistrz-elekt-nowego-jorku-wezmie-pierwsze-wyplaty-w-bitcoinach (dostęp: 18.05.2022).

https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_70296.pdf (dostęp: 18.05.2022).

http://orka2.sejm.gov.pl/INT9.nsf/klucz/ATTBRHJ27/%24FILE/i08208-o1.pdf (dostęp 18.05.2022).

https://www.cnbc.com/2019/05/04/warren-buffett-says-bitcoin-is-a-gambling-device-with-a-lot-of-frauds-connected-with-it.html (dostęp: 18.05.2022).

https://businessinsider.com.pl/gielda/kryptowaluty/elon-musk-a-kurs-bitcoina-wpis-miliardera-o-tesli-i-kryptowalucie/0ttyy3g (dostęp: 18.05.2022).

https://www.fxmag.pl/edukacja/kryptowaluty/mt-gox-historia-najwiekszego-upadku-w-dziejach-rynku-kryptowalut (dostęp: 18.05.2022).

https://tokeneo.com/pl/schiff-bitcoin-btc-to-piramida-finansowa/ (dostęp: 18.05.2022).

https://binance.zendesk.com/hc/en-us/articles/360028031711 (dostęp: 18.05.2022).

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (dostęp: 18.05.2022).

https://www.reuters.com/article/us-crypto-iran/iran-seizes-1000-bitcoin-mining-machines-using-subsidized-power-idUSKCN1TS2VL (dostęp: 18.05.2022).

https://www.dziendobrypolkowice.pl/2019/07/09/urzednicy-z-zarzutami-kradziezy-pradu/ (dostęp: 18.05.2022).

https://www.fxmag.pl/artykul/bitcoin-cytrusy-i-pracownicy-amerykanskich-departamentow (dostęp: 18.05.2022).

https://bitcoinpl.org/wielka-kopalnia-kryptowalut-odkryta-w-opuszczonej-fabryce-w-rosji/(dostęp: 18.05.2022).

https://www.gov.pl/web/cyfryzacja/od-papierowej-do-cyfrowej-polski (dostęp: 18.05.2022).

Pozostałe źródła:

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z 30.5.2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu

oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

Wyrok Naczelnego Sądu Administracyjnego z 6.03.2018 r., II FSK 488/16.

Wyrok z 31.05.2017 r., United States v. Ulbricht, No. 15-1815 (2d Cir. 2017).

Komunikat Prezesa Urzędu Ochrony Konkurencji i Konsumentów z 27.03.2019r., RGD.610-10/18/MLM.

Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego w sprawie „walut" wirtualnych, NBP i KNF, Warszawa 2017.

Krajobraz bezpieczeństwa polskiego Internetu, Raport roczny z działalności CERT Polska 2018, CERT Polska, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (dostęp: 18.05.2022).

Raport o stanie bezpieczeństwa w Polsce 2 2015 roku, https://archiwumbip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html (dostęp: 18.05.2022).

CRYPTOCURRENCIES - OPPORTUNITIES AND THREATS IN THEIR USE, A CRIMINAL LAW PERSPECTIVE

Abstract: The main objective of the article is to discuss a complex problem, namely whether the criminal law in Poland covers with its scope cryptocurrency offences and thus whether it provides protection to users of cryptocurrencies. The main definitional problems and the status of cryptocurrencies in relation to normative concepts will be presented. Another issue addressed in the article will be the opportunities and risks associated with the use of cryptocurrencies. As practice shows, cryptocurrencies are not only an object of crime, because they can also be a tool for committing it. The following issues will be examined: speculation and financial pyramids, unauthorized mining of cryptocurrencies and the darknet. The above will be based on research conducted by leading institutions dealing with cybercrime.

Keywords: cryptocurrencies, bitcoin, blockchain, criminal law

MICHALINA MARCIA
UNIWERSYTET WARSZAWSKI

WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI W PROCESIE KARNYM W KONTEKŚCIE PRAWA DO OBRONY

Abstrakt: Systemy sztucznej inteligencji (SI) ulegają stopniowemu rozpowszechnieniu, stając się przedmiotem uwagi zarówno przedstawicieli prawa prywatnego, jak i publicznego, a także organizacji takich jak Unia Europejska. Uważa się, że systemy sztucznej inteligencji mogą znacząco zmodyfikować kształt procesu karnego i przynieść wiele korzyści jego uczestnikom. Mogą usprawnić wiele z podejmowanych czynności procesowych, poprawić ich efektywność, skrócić ich czas trwania, a także zredukować koszt ich przeprowadzenia. Co więcej, mogą też przyczynić się do ograniczenia arbitralności podejmowanych decyzji, zminimalizować dyskrecjonalność działań organów, a także wyeliminować stronniczość związaną z czynnikiem ludzkim w postępowaniu. Tym samym mogą również stanowić istotny wkład w ujednolicenie praktyki stosowania prawa. Wykorzystanie systemów SI jednocześnie budzi równie wiele kontrowersji w zakresie ochrony praw człowieka i praw procesowych uczestników postępowań, w tym prawa do obrony. Celem opracowania jest ustalenie, w jaki sposób zastosowanie sztucznej inteligencji może wpływać na poszanowanie standardu prawa do obrony w postępowaniu karnym. W celu odpowiedzi na postawione pytanie badawcze analiza przedstawia podstawowe kwestie związane z pojęciem sztucznej inteligencji, sposobem jej opisu, główne problemy odnoszące się do jej wykorzystania oraz możliwości i przykłady jej zastosowania w procesie karnym. Przedstawia również podstawowe założenia projektu Rozporządzenia unijnego w sprawie sztucznej inteligencji. Następnie opracowanie prezentuje elementy niezbędne do zagwarantowania efektywnego prawa do obrony oraz wskazuje uprawnienia szczególnie narażone na naruszenie przez użycie systemów SI, opierając się przede wszystkim na treści Europejskiej Konwencji Praw Człowieka i orzecznictwie strasburskim. Wreszcie w części podsumowującej podejmuje próbę sformułowania wniosków odnoszących się do celu badań w oparciu o przeprowadzoną analizę, a także podstawowych postulatów *de lege ferenda*, w szczególności w zakresie odpowiedniego uwzględnienia obowiązków informacyjnych oraz udziału biegłych w postępowaniu.

Słowa kluczowe: Sztuczna inteligencja, SI, black box problem, prawo do obrony, ETPCz

1. WPROWADZENIE

Postępujący rozwój technologiczny, który można zaobserwować coraz częściej w sferze tworzenia oraz stosowania prawa, zdecydowanie nie pozostaje bez wpływu także na proces karny[1]. Wpływ ten pojawia się zarówno na etapie gromadzenia dowodów, biorąc pod uwagę m. in. szeroko pojęte środki inwigilacyjne oraz technologie bazujące na badaniach nieświadomych reakcji organizmu, ale również na etapie sądowym, w tym przy przeprowadzaniu zdalnych rozpraw[2]. W ostatnim czasie przedmiotem zainteresowania doktryny, ale także ponadnarodowych i międzynarodowych organizacji, takich jak Unia Europejska, czy Rada Europy stało się jednak kolejne zagadnienie, a mianowicie problem wykorzystania sztucznej inteligencji w postępowaniach, m. in. w postępowaniu karnym.

Sztuczna inteligencja (SI) ulega stopniowemu rozpowszechnieniu i staje się przedmiotem uwagi zarówno przedstawicieli prawa prywatnego, jak i publicznego. Uważa się, że systemy sztucznej inteligencji mogą znacząco zmodyfikować kształt procesu karnego i przynieść wiele korzyści jego uczestnikom. Wskazuje się m. in., że mogą usprawnić wiele z podejmowanych czynności procesowych, mogą poprawić ich efektywność, skrócić czas ich trwania, a także zredukować część kosztów postępowania[3]. Co więcej, mogą też przyczynić się do ograniczenia arbitralności podejmowanych decyzji, ograniczyć dyskrecjonalność działań organów, a także wyeliminować stronniczość związaną z czynnikiem ludzkim w postępowaniu. Tym samym mogą również stanowić istotny wkład w ujednolicenie praktyki stosowania prawa.

Wykorzystanie systemów SI może niewątpliwie przynieść wiele korzyści dla procesu karnego, ale jednocześnie budzi równie wiele kontrowersji w zakresie ochrony praw człowieka i praw procesowych uczestników postępowań. Jednym z problemów związanych z wykorzystaniem sztucznej inteligencji w procesie karnym jest jej wpływ na efektywne wykonywanie prawa

[1] M. Caianiello, *Criminal Process faced with the Challenges of Scientific and Technological Development*, European Journal of Crime, Criminal Law and Criminal Justice 2019, vol. 27. https://doi.org/10.1163/15718174-02704001, M. Simonato*, Defence rights and the use of information technology in criminal procedure*, *Revue internationale de droit pénal*, vol. 85, no. 1-2, 2014

[2] K. Kremens, W. Jasiński, *Editorial of dossier "Admissibility of Evidence in Criminal Process. Between the Establishment of the Truth, Human Rights and the Efficiency of Proceedings",* Revista Brasileira de Direito Processual Penal 2021, vol. 7, n. 1, s. 30-32, https://doi.org/10.22197/rbdpp.v7i1.537 (dostęp: 05.06.2022).

[3] H.B., Dixon, *Artificial Intelligence: Benefits and Unknown Risk*, https://www.americanbar.org/groups/judicial/publications/judges_journal/2021/winter/artificial-intelligence-benefits-and-unknown-risks/ (dostęp: 05.06.2022).

do obrony. Kluczowym elementem efektywnego i skutecznego prawa do obrony jest prawo do aktywnego udziału w postępowaniu, które może być realizowane m. in. przez składanie wniosków dowodowych, środków zaskarżenia, czy też uczestnictwo w czynnościach dowodowych[4]. Co więcej, nieodłącznym elementem rzeczywiście skutecznego, aktywnego udziału jest prawo do notyfikacji oraz informacji o czynnościach podejmowanych względem podejrzanego lub oskarżonego[5]. Wykorzystanie nowych technologii, w szczególności tak skomplikowanych jak sztuczna inteligencja, nasuwa jednak pytanie, w jakim stopniu wskazane prawo do informacji rzeczywiście może być realizowane. Rozważenia wymaga, czy jeśli odtworzenie działania mechanizmów sztucznej inteligencji wymaga szczególnej wiedzy specjalistycznej, niedostępnej co do zasady zarówno dla przeciętnego obywatela, jak i profesjonalnych pełnomocników, czy też nawet w świetle dostępnych środków jest niemożliwe, to w związku z tym podejrzany rzeczywiście może w sposób efektywny podważać legalność oraz proporcjonalność przeprowadzonych względem niego czynności, powoływać je m. in. w środkach zaskarżenia i czy w rzeczywistości może efektywnie wykonywać przysługujące mu prawo do obrony.

Celem opracowania jest wskazanie, w jaki sposób zastosowanie sztucznej inteligencji może wpływać na poszanowanie standardu prawa do obrony w postępowaniu karnym. Główną hipotezą badawczą jest, że na obecnym etapie regulacji wykorzystanie sztucznej inteligencji w postępowaniu karnym przynosi więcej zagrożeń niż korzyści standardom prawa do obrony. W celu odpowiedzi na postawione pytanie badawcze przedstawione zostaną podstawowe kwestie związane z pojęciem sztucznej inteligencji, główne problemy odnoszące się do jej ogólnego wykorzystania oraz możliwości jej zastosowania w procesie karnym. Następnie wyszczególnione zostaną elementy niezbędne do zagwarantowania efektywnego prawa do obrony oraz wskazane zostaną uprawnienia szczególnie narażone na naruszenie. Pozwoli to na przedstawienie wniosków w części podsumowującej przeprowadzoną analizę.

Przedmiot opracowania stanowi przede wszystkim europejski standard prawa do obrony. Zakres ten został wybrany ze względu na aktualność problematyki na poziomie unijnym w związku z projektem Rozporządzenia Parlamentu Europejskiego i Rady, ustanawiającego zharmonizowane przepisy

[4] P. Wiliński, *Proces karny w świetle Konstytucji*, Warszawa 2011, s. 175-177.
[5] A. Lach, *Rzetelne postępowanie dowodowe w sprawach karnych w świetle orzecznictwa strasburskiego,* Warszawa 2018, s. 112-115.

dotyczące sztucznej inteligencji[6] oraz potrzebie wypracowania wspólnych standardów unijnych w tym względzie. W związku z tym, że Wyjaśnienia do Karty Praw Podstawowych[7] w zakresie jej art. 47 i 48, tj. odnoszącym się do prawa do obrony, wprost odsyłają do postanowień Europejskiej Konwencji Praw Człowieka[8], natomiast postanowienia Traktatu o Unii Europejskiej[9] podnoszą postanowienia Konwencji do rangi ogólnych zasad prawa UE, w celu odtworzenia standardu prawa do obrony wykorzystane zostaną przede wszystkim postanowienia EKPC oraz orzecznictwo ETPCz.

Połączenie wymienionych elementów umożliwi uzyskanie ostatecznej odpowiedzi na przedstawione pytanie badawcze oraz ustalenie, w jaki sposób wykorzystanie sztucznej inteligencji w postępowaniu karnym może wpływać na efektywne wykonywanie prawa do obrony. Wydaje się, że spełnienie opisanego celu badawczego może pozytywnie wpłynąć na przyszłą praktykę ustawodawczą wprowadzającą systemy SI do procesu, na zapewnienie poszanowanie prawa do obrony, a także proporcjonalności projektowanych regulacji. Wykorzystanie sztucznej inteligencji w procesie karnym jest zagadnieniem dopiero wkraczającym w sferę legislacji państw europejskich, natomiast poszczególne kwestie problematyczne dla wielu systemów z dużym prawdopodobieństwem okażą się tożsame. Wypracowanie natomiast odpowiednich standardów z pewnością może przyczynić się do usprawnienia współpracy w sprawach karnych, wzajemnej uznawalności orzeczeń oraz dopuszczalności dowodów pomiędzy państwami.

2. SZTUCZNA INTELIGENCJA

2.2. Pojęcie sztucznej inteligencji

Zdefiniowanie sztucznej inteligencji jest jednym z bardziej problematycznych zagadnień w obrębie prawa nowych technologii[10]. Wśród przedsta-

[6] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii [COM(2021) 206 final], dalej jako „Rozporządzenie w sprawie sztucznej inteligencji" lub „Rozporządzenie".

[7] Wyjaśnienia dotyczące Karty Praw Podstawowych, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32007X1214(01)&from=EN, (dostęp: 17.06.2019).

[8] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz. U. z 1993, nr 61, poz. 284, dalej jako „EKPCz" lub „Konwencja".

[9] Traktat o Unii Europejskiej, Dz. Urz. UE C 326.

[10] Zob. J.D. Bruyne, C. Vanleenhove, *Artificial Intelligence and the Law*, Intersentia 2021, s. 1-23.

wicieli doktryny brak konsensusu co do tego, czy przyjęcie jednej, sztywnej definicji sztucznej inteligencji jest zabiegiem koniecznym i korzystnym w świetle nieustannie zmieniających się środków i technik oraz pojawiających się nowych, możliwych do wykorzystania rozwiązań. Niektórzy z autorów wskazują, ze przyjęcie takiej definicji może okazać się bezcelowe i ograniczające[11]. Niemniej jednak, ustalenie pewnych istotnych cech pozwalających przypisać systemowi miano sztucznej inteligencji, odróżniając je m. in. od zwykłych systemów opartych na algorytmach, wydaje się kluczowe. Wyróżnienie tych elementów będzie miało wpływ na zidentyfikowanie zagrożeń dla praw procesowych stron w postępowaniu, jak i na wypracowanie pewnych wymogów i standardów w celu zapobieżenia tym zagrożeniom.

Zaawansowane prace w zakresie prób ustalenia definicji sztucznej inteligencji, a także próby usystematyzowania dotychczasowych osiągnięć w tym względzie, zostały przeprowadzone przez Wspólne Centrum Badawcze (JRC) Komisji Europejskiej, w ramach którego wypracowano tzw. użytkową definicję SI[12]. JRC wskazało, że celem badań było stworzenie spójnej systematyki i klasyfikacji słów kluczowych, które określałyby istotę i przekrojowe sfery sztucznej inteligencji. Tymi elementami miałyby być uwzględnienie złożoności otaczającego świata, przetwarzanie informacji, podejmowanie decyzji i wreszcie osiąganie określonych celów[13].

Swoją własną definicję „systemu sztucznej inteligencji" wprowadza również propozycja rozporządzenia UE w sprawie sztucznej inteligencji. Zgodnie z przyjętą definicją system ten oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku do projektu, 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"[14]. W ramach tych technik Rozporządzenie 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) i systemy ekspertowe; c) podejścia

[11] McDaniel J., Pease K., *Predictive Policing and Artificial Intelligence*, Routledge 2021, Frankish, K., Ramsey, W. M., *The Cambridge Handbook of Artificial Intelligence*, Cambridge 2014.
[12] Misuraca, G. and Van Noordt, C., *AI Watch - Artificial Intelligence in public services*, Publications Office of the European Union, Luxembourg, 2020, doi:10.2760/039619.
[13] *Ibidem.*
[14] Artykuł 3 pkt 1 Rozporządzenia.

statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji[15]. W uzasadnieniu projektu wskazano, że definicję sformułowano w taki sposób, żeby była jak najbardziej neutralna pod względem technologicznym i nie ulegała dezaktualizacji. Wykaz technik ma podlegać ciągłemu dostosowywaniu przez Komisję do zmieniających się realiów otaczającego świata i osiągnięć technologicznych.

Pojęcie uczenia maszynowego *(machine learning)*, zawarte w treści projektu, bardzo mocno łączy się z głównymi cechami sztucznej inteligencji i niejako naprowadza na jeden z elementów odróżniających systemy SI od tych opartych na algorytmach. "Uczący się" program powinien na podstawie wprowadzonych do systemu danych wejściowych (*input*) oraz w powiązaniu z oczekiwanym rezultatem i wynikiem (*output*) samodzielnie modyfikować i kształtować zasady przetwarzania tych danych, a więc uczyć się poprzez swoje doświadczenie[16]. *Deep learning* oraz *reinforcement learning*[17] stanowią natomiast odmiany uczenia maszynowego, które za pomocą wykorzystania sieci neuronowych, są w stanie operować większą ilością zróżnicowanych danych i tym samym doskonalić techniki ich przetwarzania[18]. Do pojęcia uczenia maszynowego odsyłają także mniej oficjalne, informacyjne źródła UE, które podejmują się definicji SI, podkreślając zdolność systemów do automatycznego poprawiania swojego działania[19].

Z uczeniem maszynowym, zwłaszcza z uczeniem głębokim, wiąże się jednak jeden z głównych problemów wykorzystania sztucznej inteligencji w postępowaniu, a mianowicie *black box problem*. Problem ten wiąże się z ograniczonymi możliwościami wyjaśnienia mechanizmów działania SI, a w szczególności podejmowania określonego rodzaju decyzji przez systemy sztucznej inteligencji. W związku z tym, że systemy, zwłaszcza w przypadku wykorzystania zaawansowanych sieci neuronowych, posiadają wiele ukrytych warstw, na poziomie których dochodzi do przetwarzania danych, odtworzenie mechanizmu wypracowania określonego rezultatu przez system SI będzie

[15] Załącznik I do Rozporządzenia Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii [COM(2021) 206 final].

[16] M. Kubit, *Rozwój sztucznej inteligencji w świetle prawa Unii Europejskiej – dylematy i wyzwania*, Warszawa 2021, s. 39-40.

[17] W. Ertel, *Introduction to Artificial Intelligence, Springer* 2018, s. 289-311.

[18] R. Vargas, A. Mosavi, R. Ruiz, *Deep Learning: A review*, Advances in Intelligent Systems and Computing 2017, 5(2).

[19] Parlament Europejski, *Sztuczna inteligencja. Co to jest i jakie ma zastosowania?* https://www.europarl.europa.eu/news/pl/headlines/society/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania (dostęp: 05.06.2022).

znacząco utrudniony albo wręcz niemożliwy. Im częściej będą zatem wykorzystywane systemy sztucznej inteligencji w procesie i im dalej będzie sięgać ich zastosowanie, tym większa będzie powstawać obawa o ewentualną arbitralność decyzji oraz o ogólną rzetelność postępowania[20].

Tym samym pojawiła się potrzeba stworzenia tzw. wyjaśnialnej SI, czyli *explainable AI* (xAI). xAI, w przeciwieństwie do SI, której system ma przedstawić jedynie określony rezultat, ma w założeniu również wyjaśnić swoje działanie w sposób zrozumiały dla człowieka[21]. Koncepcja xAI niewątpliwie jest również zakorzeniona w uwarunkowaniach rynkowych, oczekiwaniach społecznych i możliwości dostarczenia produktu, który budziłby zaufanie użytkownika[22]. Niewątpliwie może również jednak mieć ogromne znaczenie w zakresie wykorzystania SI przez organy państwowe i jednoczesnego zapewnienia poszanowania praw człowieka.

W nawiązaniu do pojęcia wyjaśnianej sztucznej inteligencji podkreślono również znaczenie nie tyle samej definicji systemu SI, ale opisu jego działania. Jedna z klasyfikacji takich opisów została zaproponowana przez A. Deeks[23]. Zgodnie z nią można wyróżnić tzw. podejście dekompozycyjne (*decompositional approach),* które ma na celu wyjaśnienie lub odtworzenie „rozumowania" systemu SI i podejście egzogenne (*exogenous approach*), które nie obejmuje wyjaśnienia wewnętrznego działania systemów. Drugi z wymienionych sposobów opisu SI koncentruje się natomiast na dostarczeniu ogólnych informacji o przyjętym modelu systemowym, jego założeniach i celach, na sposobie wpływu na inne podmioty, wobec których był wykorzystywany, elementach porównawczych i w tym zakresie bazuje na czynnikach zewnętrznych, wykraczający poza sposób działania wewnętrznego mechanizmu. Wybór opisu systemu SI może mieć zatem znaczący wpływ na zapewnienie odpowiednich standardów rzetelnego procesu, w tym prawa do obrony oraz dostarczenia informacji niezbędnych dla skutecznej realizacji tego prawa.

---

[20] S. Wachter, B. Mittelstadt, C. Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, Harv. J.L. & Tech. 2018 (31).

[21] D., Gunning, M. Stefik, J. Choi, T. Miller, S. Stumpf, G.-Z. Yang, *XAI-Explainable artificial intelligence*, Science Robotics 2019, 4 (37). doi:10.1126/scirobotics.aay7120.

[22] F. Alizadeh, *I Don't Know, Is AI Also Used in Airbags?: An Empirical Study of Folk Concepts and People's Expectations of Current and Future Artificial Intelligence*, I- com 2021, 20(1), s. 2-17, doi:10.1515/icom-2021-0009.

[23] A. Deeks, *The Judicial Demand for Explainable Artificial Intelligence*, Colum. L. Rev. 2019 (51), s. 1835 i n.

2.3. Wykorzystanie sztucznej inteligencji w procesie karnym

Sztuczna inteligencja, oprócz wykorzystania jej w sferze prywatnej, usprawnienia życia codziennego i stosunkach umownych, może znaleźć także zastosowanie w domenie prawa publicznego, w tym w procesie karnym. Sposób jej wykorzystania w postępowaniu będzie natomiast różnił się w zależności od etapu procesu.

Systemy SI w szczególności w postępowaniu przedsądowym będą mogły być wykorzystywane do szeroko pojętych działań w zakresie prewencji generalnej i indywidualnej oraz stanowić element środków czynności operacyjnych wykorzystywanych przez policję[24]. Dane powstałe w wyniku działania sztucznej inteligencji będą mogły ostatecznie stanowić również materiał dowodowy podlegający gromadzeniu przez organy ścigania[25].

Jeżeli chodzi o kwestie wiązane przede wszystkim z etapem sądowym postępowania, to największe kontrowersje wzbudza oczywiście możliwość podejmowania decyzji za pomocą systemów sztucznej inteligencji[26]. Dużo bardziej prawdopodobne niż samodzielne wyrokowanie przez sędziego – robota są jednak systemy wspierające podejmowanie określonego rodzaju rozstrzygnięć, sygnalizowanie możliwych przeoczeń, braków lub asystowanie poprzez proponowanie i wyliczenie np. elementów wymiaru kary w oparciu o dane wprowadzone przez sędziego[27]. Duże nadzieje w zakresie usprawnienia przebiegu procesu karnego i ułatwienia przeprowadzenia niektórych z jego czynności wiązane są także z systemami rozpoznawania mowy oraz z tłumaczeniem materiału dowodowego przy wykorzystaniu SI[28].

---

[24] See e.g. S. Hänold, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, [w:] *Robotics, AI and the Future of Law*, red. M. Corrales, M. Fenwick, N. Forgó, Springer 2018, p. 123-153.

[25] S. Gless, *AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials*, GJIL 2020 (51).

[26] Nie oznacza to jednak oczywiście wykluczenia możliwości asystowania systemów SI przy podejmowaniu decyzji procesowych na wcześniejszych etapach przez organy postępowania, m. in. prokuratora, przy np. rozstrzygnięciach w zakresie środków zapobiegawczych, czy też decyzji w zakresie kierowania oskarżenia do sądu Zob. m. in. T. H. Tran, *China created an AI "Prosecutor" that can charge people with crimes*, https://futurism.com/the-byte/china-ai-prosecutor-crimes (dostęp: 05.06.2022).

[27] Završnik, A. *Criminal justice, artificial intelligence systems, and human rights*. ERA Forum 2020, 20, s. 567–583.

[28] Pojawiają się B. Oyetunde, *Introducing Salme, Estonian courts' speech recognition assistant, https://investinestonia.com/introducing-salme-estonian-courts-speech-recognition-assistant/*, FRA – European Union Agency for Fundamental Rights, *Artificial Intelligence, Big Data and Fundamental Rights Country Research Estonia,* 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-ai-project-estonia-country-research_en.pdf, (dostęp: 05.06.2022)

Część z opisanych powyżej rozwiązań została już wprowadzona w praktyce. Wdrożone zostały m. in. systemy służące przewidywaniu typu przestępstw, ich daty, czasu i miejsca ich popełnienia. Przykładami w tym zakresie mogą być Risk Terrain Modeling[29], PredPol[30], włoskie X-Law[31], KeyCrime[32], niemieckie Precobs wykorzystywane też w Szwajrcarii[33], czy też brytyjskie HART[34]. Systemy te mogą być wykorzystywane w prewencji generalnej, ale mogą też służyć wykrywaniu sprawców popełnionych wcześniej czynów zabronionych[35]. W przypadku działań śledczych i reakcji czasu rzeczywistego, czyli w oknie czasowym pomiędzy podjęciem decyzji o popełnieniu przestępstwa a jego dokonaniem mogą też wpływać na ostateczne wdrożenie w życie zamiaru przez sprawcę[36]. Do użytku wprowadzono również systemy prewencji indywidualnej, związane m. in. z zapobieganiem recydywy (COMPAS)[37]. Pojawiają się również systemy wspomagające pracę organów ścigania, jak np. systemy rozpoznawania twarzy, analizy DNA, wykrywania wystrzałów, do których wykorzystuje się właśnie sztuczną inteligencję[38].

Jak jednak pokazała praktyka, wykorzystanie tych systemów łączy się z dużymi ryzykami w zakresie poprawności danych, jak i uprzedzeń systemowych (*system bias)*. Uprzedzenia te mogą być związane ze zniekształceniami wprowadzanych danych, mogą wynikać ze stronniczości wprowadzających, ale też mogą kształtować się w sposób zupełnie niezawiniony. Wraz z zarysowaniem się problemów praktycznych wzrosło niewątpliwie zapotrzebowanie

[29] https://www.riskterrainmodeling.com/ (dostęp: 05.06.2022).
[30] https://www.predpol.com/ (dostęp: 05.06.2022).
[31] https://www.xlaw.it/presentazione/index_eng.asp (dostęp: 05.06.2022).
[32] https://keycrime.com/ (dostęp: 05.06.2022).
[33] https://www.stadt-zuerich.ch/portal/de/index/politik_u_recht/stadtrat/weitere-politikfelder/smartcity/english/projects/precobs.html, https://land-der-ideen.de/en/project/precobs-software-for-predicting-crimes-355 (dostęp: 05.06.2022).
[34] M.Oswald, J. Grace, S. Urwin, G. C. Barnes, *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality*, Information & Communications Technology Law 2018, 27(2), 223-250, DOI: 10.1080/13600834.2018.1458455.
[35] S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings A Framework for A European Legal Discussion*, Springer 2020, s. 39-40.
[36] M. A. Utset*, Predictive policing and criminal law*, [w:] *Predictive Policing and Artificial Intelligence*, J. McDaniel, K. Pease (red), Routledge 2021, s. 163-183.
[37] D. Kehl, P. Guo, S. Kessler, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative*, Berkman Klein Center for Internet & Society, Harvard Law School 2017, https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf
[38] N. Wickramarathna and E. Edirisuriya, *Artificial Intelligence in the Criminal Justice System: A Literature Review and a Survey*, s. 4-5, https://www.researchgate.net/publication/358635259_Artificial_Intelligence_in_the_Criminal_Justice_System_A_Literature_Review_and_a_Survey_N_A_Wickramarathna_1_and_EATA_Edirisuriya/link/620c9b36afa8884cabe7a7c6/download (dostęp: 05.06.2022).

na poprawienie precyzyjności i przejrzystości stosowanych systemów SI. Możliwość wyjaśnienia działania mechanizmu oraz przetwarzania przez niego wprowadzonych danych stała się jednym z głównych wyzwań wprowadzania nowych technologii do procesu[39].

Możliwość stosowania sztucznej inteligencji w procesie karnym przewiduje również projekt Rozporządzenia. W związku z tym, że wizja postępowań, w których systemy SI rzeczywiście mogą odgrywać znaczącą rolę staje się coraz bardziej realna i nie stanowi już jedynie teoretycznych rozważań, ustalenie pewnych wspólnych standardów stało się kluczowe również na poziomie unijnym. Należy jednak zauważyć, że Rozporządzenie nie poświęca szczegółowo miejsca zagadnieniom związanym z właśnie z systemami wykorzystywanymi do celów ścigania i zapobiegania przestępstwom. Akt ten klasyfikuje ww. mechanizmy jako systemy wysokiego ryzyka. W preambule do rozporządzenia (pkt 38) prawodawca unijny wskazuje na możliwość zainicjowania niejawnych czynności operacyjnych, tymczasowego aresztowania lub pozbawienia wolności oraz innych daleko idących skutków dla stron postępowania. Zwraca również uwagę na podstawowe problemy w zakresie praw podstawowych, które mogą wiązać się z zastosowaniem systemów SI przez organy ścigania. Podkreśla znaczący brak równowagi sił, utrudniony dostęp do skutecznego środka prawnego i dostęp do bezstronnego sądu, jak również ograniczenia prawa do obrony i domniemania niewinności w związku z tym, że systemy nie są w wystarczającym stopniu przejrzyste, wyjaśnialne i udokumentowane. W przypadku zastosowania słabej jakości danych, braku dokładności lub rzetelności systemu, a także braków w zakresie odpowiednich testów przed wprowadzeniem do obrotu lub oddaniem do użytku w inny sposób systemy te ponadto mogą okazać się błędne lub dyskryminujące.

Powstaje jednak pytanie, czy prawodawca unijny w wystarczający sposób kształtuje standardy w szczególności w zakresie przejrzystości i wyjaśnialności systemów, tym samym zapobiegając ewentualnym naruszeniom praw podstawowych. Wydaje się, że główny nacisk w treści Rozporządzenia został położony na rzetelność danych, odpowiednio szerokie grupy badawcze, analizy ryzyk oraz ochronę danych osobowych[40]. Wątpliwości może natomiast budzić, czy jest to wystarczające do zapewnienia spełnienia standardu rzetelnego procesu, w tym poszanowania prawa do obrony.

[39] Zob. m. in. A. Deeks, *The Judicial…*, s. 1830.
[40] Zob. m. in. art. 9, 10, 15-17 Rozporządzenia.

2. PRAWO DO OBRONY

Ujęcie prawa do obrony będzie podlegać pewnym modyfikacjom w zależności od przyjętego wzorca i systemu prawnego. Niezależnie jednak od wyboru system, podstawowym standardem jest, że prawo to powinno być efektywne i rzeczywiste[41]. W ramach prawa do obrony można wyróżnić szereg uprawnień, które składają się na kształt jego ostatecznego standardu, można także dokonywać różnego rodzaju klasyfikacji, m. in. z podziałem na aspekt czynny, bierny, materialny, czy też formalny[42].

Dla zapewnienia spójnego toku analizy i uporządkowania pojęć, przydatna może natomiast okazać się systematyka przyjęta w Europejskiej Konwencji Praw Człowieka. W związku z punktem widzenia przyjętym i przedstawionym we wprowadzeniu do opracowania, za główny przedmiot badań posłuży w tym wypadku treść Konwencji oraz odnoszące się do niej orzecznictwo ETPCz. Zgodnie z art. 6 ust. 3 EKPCz w ramach prawa do obrony każdy oskarżony o popełnienie czynu zagrożonego karą ma co najmniej prawo do:

a) niezwłocznego otrzymania szczegółowej informacji w języku dla niego zrozumiałym o istocie i przyczynie skierowanego przeciwko niemu oskarżenia (prawo do informacji)
b) posiadania odpowiedniego czasu i możliwości do przygotowania obrony (prawo dostępu do materiałów postępowania)
c) bronienia się osobiście lub przez ustanowionego przez siebie obrońcę, a jeśli nie ma wystarczających środków na pokrycie kosztów obrony - do bezpłatnego korzystania z pomocy obrońcy wyznaczonego z urzędu, gdy wymaga tego dobro wymiaru sprawiedliwości (prawo do pomocy osobistej i przez adwokata)
d) przesłuchania lub spowodowania przesłuchania świadków oskarżenia oraz żądania obecności i przesłuchania świadków obrony na takich samych warunkach jak świadków oskarżenia
e) korzystania z bezpłatnej pomocy tłumacza, jeżeli nie rozumie lub nie mówi językiem używanym w sądzie (prawo do tłumaczenia)[43].

[41] Zob. M. in. J. D. Jackson *Responses to Salduz: Procedural Tradition, Change and the Need for Effective Defence,* The Modern Law Review 2016, 79(6).
[42] P. Wiliński, *Zasada prawa do obrony w polskim procesie karnym*, Kraków 2006, A. Lach, *Rzetelne…* s. 51 – 181, P. Wiliński, *Proces…* s. 174-179.
[43] Szerzej na ten temat zob. D. Harris, M. O'Boyle, E. Bates, *Law of the European Convention on Human Rights*, Oxford 2018.

Uprawnienia te zostały w pewien sposób przełożone także na grunt prawa unijnego poprzez szereg dyrektyw wydanych w ramach Programu Sztokholmskiego[44].

Należy również zaznaczyć, że Konwencja przyjmuje szeroki zakres podmiotowy prawa do obrony, w przeciwieństwie do zakresu określonego w polskim k.p.k.[45] Dla objęcia ochroną konwencyjną nie jest konieczne wydanie żadnego formalnego aktu, czy decyzji procesowej, ale wystarczy podjęcie pierwszej czynności nakierowanej na ściganie konkretnej osoby, żeby tę ochronę uruchomić[46]. W przypadku systemów SI wykorzystywanych przez organy ścigania wraz z użyciem ww. narzędzi często będzie w istocie dochodzić do nakierowania toku postępowania przeciwko określonemu podmiotowi. Cechy systemów wykorzystywanych jeszcze przed konkretyzacją strony biernej postępowania mogą się również okazać istotne na późniejszych etapach procesu, kiedy osoba potencjalnego sprawcy zostanie zindywidualizowana.

Jednym z kluczowych elementów zapewnienia efektywnego i realnego prawa do obrony jest prawo do informacji. Obejmuje ono informację nie tylko o skierowanym przeciwko niemu oskarżeniu, o jego przyczynach i istocie, ale ETPCz rozszerza prawo do informacji również na inne elementy, takie jak np. informacje o przysługujących stronie prawach procesowych[47].

Co szczególnie istotne, informacja powinna zostać przedstawiona oskarżonemu lub podejrzanemu w taki sposób i w takiej formie, żeby mógł

[44] Program sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli Dz.Urz. UE C 115.

[45] Na ten temat zob. więcej W. Jasiński, *Dostęp osoby oskarżonej o popełnienie czynu zagrożonego karą do adwokata na wstępnym etapie ścigania karnego – standard strasburski*, Europejski Przegląd Sądowy 2019/1, S. Steinborn, *Dostęp do obrońcy na wczesnym etapie postępowania karnego. Uwagi de lege lata i de lege ferenda*, Europejski Przegląd Sądowy 2019/1, S. Steinborn, M. Wąsek-Wiaderek*, Moment uzyskania statusu biernej strony postępowania karnego z perspektywy konstytucyjnej i międzynarodowej*, [w:] M. Rogacka-Rzewnicka, H. Gajewska-Kraczkowska, B. Bieńkowska (red.), *Wokół gwarancji współczesnego procesu karnego. Księga jubileuszowa Profesora Piotra Kruszyńskiego*, Warszawa 2015, S. Steinborn, *Status osoby podejrzanej w procesie karnym z perspektywy Konstytucji RP (uwagi de lege lata i de lege ferenda)* [w:] *Państwo prawa i prawo karne. Księga jubileuszowa Profesora Andrzeja Zolla,* red. P. Kardas, T. Sroka, W. Wróbel, Warszawa 2012.

[46] Wyroki ETPCz z dnia 12 lutego 2013 r. w sprawie 26524/04 *Dimitar Krastev przeciwko Bułgarii*, z dnia 20 października 1997 r. w sprawie *Serves przeciwko Francji,* nr skargi 20225/92, z dnia 15 listopada 2005 r. w sprawie *Lammi przeciwko Finlandii*, nr skargi 53835/00, z dnia 19 lutego 1991 r. w sprawie *Frau przeciwko Włochom,* nr skargi 12147/86, z dnia 31 października 2013 r. w sprawie *Bandaletov przeciwko Ukrainie,* nr skargi 23180/06, HUODOC.

[47] K. Kowalik-Bańczyk, *Prawo do obrony w unijnych postępowaniach antymonopolowych. W kierunku unifikacji standardów proceduralnych w Unii Europejskiej*, Warszawa 2012, s.334.

on ją bez przeszkód zrozumieć[48]. Musi być również przedstawiona odpowiednio wcześnie, żeby zapewnić rzeczywistą możliwość wykonywania prawo do obrony, co związane jest z treścią art. 6 ust. 3 lit. b Konwencji[49]. Informacja powinna być prosta, zrozumiała, ujęta w jasnym i przystępnym języku[50]. Elementy te zostały również przeniesione na grunt postanowień Dyrektywy 2012/13/UE[51].

W związku z taką treścią prawa do informacji powstaje pytanie, czy przedstawiony standard informacyjny może rzeczywiście zostać zapewniony w przypadku użycia sztucznej inteligencji w postępowaniu karnym. Przede wszystkim biorąc pod uwagę kontekst *black box problem* i ukrytych warstw uczenia maszynowego, jeśli system SI zostanie wykorzystany jako podstawa oskarżenia, czy też przedstawienia zarzutów albo jakiejkolwiek decyzji związanej z nakierowaniem postępowania karnego przeciwko określonej osobie, efektywne prawo do informacji może zostać poddane w wątpliwość.

Co więcej, efektywność przedstawienia informacji odpowiednio wcześnie w celu możliwości przygotowania się do obrony może również zostać zakwestionowana w przypadku zastosowania sztucznej inteligencji w postępowaniu. Ogólne użycie środków opartych na nowych technologiach może przyczyniać się do przeniesienia centrum procesu na etap przedsądowy, sprawiając, że staje się on dłuższy i coraz bardziej skomplikowany[52]. Może to stanowić problem w szczególności w systemach, gdzie ramy prawne lub praktyka stosowania prawa jest restrykcyjna w odniesieniu do udostępniania podejrzanemu informacji na etapie przedsądowym[53].

---

[48] Wyrok ETPCz z 25 lipca 2000 r. w sprawie *Mattoccia przeciwko Włochom*, skarga nr 23969/94, wyrok ETPC z 26 września 2006 r. w sprawie *Miraux przeciwko Francji*, skarga nr 73529/01, HUDOC.

[49] Wyrok ETPCz z 25 marca 1999 r. w sprawie *Pelissier i Sassi przeciwko Francji*, skarga nr 25444/94, HUDOC.

[50] Wyrok ETPCz z 11 grudnia 2008 r. w sprawie *Panovits przeciwko Cyprowi*, skarga nr 4268/04, HUDOC.

[51] Dyrektywa Parlamentu Europejskiego i Rady 2013/48/UE z dnia 22 października 2013 r. w sprawie prawa dostępu do adwokata w postępowaniu karnym i w postępowaniu dotyczącym europejskiego nakazu aresztowania oraz w sprawie prawa do poinformowania osoby trzeciej o pozbawieniu wolności i prawa do porozumiewania się z osobami trzecimi i organami konsularnymi w czasie pozbawienia wolności, Dz. Urz. UE L 294.

[52] R. Stoykova, *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, Computer Law & Security Review 2021. https://doi.org/10.1016/j.clsr.2021.105575.

[53] Zob. P. Wiliński, *Odmowa dostępu do akt sprawy w postępowaniu przygotowawczym*, Prokuratura i Prawo 2006, nr 11, 7 K. Wróblewski, A. M. Tęcza-Paciorek, *Dostęp podejrzanego do akt postępowania w przedmiocie tymczasowego aresztowania po nowelizacji kodeksu postępowania karnego*, Prawo i Prokuratura 2016 (3), M. Wąsek-Wiaderek, *Dostęp do akt sprawy oskarżonego tymczasowo aresztowanego i jego obrońcy w postępowaniu przygotowawczym - standard europejski a prawo polski,* Palestra 2003, 48(3-4), s. 55-71.

Wszystkie te wątpliwości, w szczególności związane z etapem postępowania przygotowawczego mogą również być odnoszone do spełnienia standardów art. 6 ust. 3 lit. b Konwencji, w zakresie dostępu do materiałów postępowania[54]. Oskarżenie powinno przedstawić cały istotny dla sprawy materiał dowodowy, zarówno w zakresie dowodów za i przeciw skierowaniu aktu oskarżenia do sądu. Standard ten ma w założeniu sprzyjać również poszanowaniu zasady równości broni w postępowaniu[55]. Ten element szczególnie podkreślany jest w przypadku zatrzymania i tymczasowego aresztowania, gdzie ogólny standard informacyjny powinien być szczególnie wysoki[56]. Jak wskazuje chociażby treść uzasadnienia projektu Rozporządzenia w sprawie sztucznej inteligencji, również do tych celów mogą być wykorzystywane systemy SI. Może to nastąpić zarówno w zakresie asystowania przy podejmowaniu decyzji, jak i w zakresie środków podejmowanych przez organy ścigania, które będą prowadzić do rozstrzygnięcia tej treści.

Jeśli natomiast podejrzany lub oskarżony otrzyma wprawdzie dostęp do zgromadzonego materiału dowodowego w sprawie, ale nie będzie mógł z niego uzyskać żadnej konkretnej, istotnej informacji, prawo do zapewnienia odpowiednich środków dla możliwości przygotowania obrony również będzie musiało zostać poddane w wątpliwość.

Znaczące wątpliwości pojawiają się również w związku z prawem ujętym w artykule 6 ust. 3 lit. c Konwencji, tj. prawa do obrony osobistej lub prawa do adwokata. Jednym z kluczowych elementów podkreślanych przez ETPCz w kontekście tego prawa jest to, że musi być ono efektywne i rzeczywiste[57]. Oskarżony musi posiadać możliwości podejmowania rzeczywistych środków, inicjowania czynności, składania wniosków dowodowych, brania udziału w postępowaniu dowodowym, a także składania odpowiednich środków zaskarżenia oraz inicjowania kontroli sądowej[58]. Niezbędnym elementem aktywnego udziału jest ponadto prawo do notyfikacji i informacji o podejmowanych względem oskarżonego lub podejrzanego czynności procesowych. Jeśli jest on reprezentowany w postępowaniu przez adwokata, powinien mieć

[54] Wyrok ETPCz z 9 października 2008 r. w sprawie *Moiseyev przeciwko Rosji*, skarga nr 62936/00, HUDOC.
[55] Wyrok ETPCz z 13 lutego 2001 r. w sprawie *Garcia Alva przeciwko Niemcom*, skarga nr 23541/94, HUDOC.
[56] Wyrok ETPCz z 30 marca 1989 r. w sprawie *Lamy przeciwko Belgii*, skarga nr 10444/83, HUDOC.
[57] Wyrok ETPCz z 13 maja 1980 r. w sprawie *Artico przeciwko Włochom*, nr skargi 6694/74, HUODOC.
[58] M. A. Nowicki, *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, Warszawa 2017, s. 609-617.

on możliwość kontroli przebiegu procesu, poddawania kontroli określonych środków i decyzji procesowych. Co więcej, adwokat powinien również mieć możliwość obecności przy przeprowadzanych poszczególnych czynnościach oraz aktywnego uczestnictwa w ich przebiegu[59].

Wszystkie te elementy zwykle odnoszone są do tradycyjnego modelu postępowania i materiału dowodowego, do tego, czy oskarżony lub jego adwokat jest obecny na sali sądowej, czy też np. przy konfrontacji świadków, czy może swobodnie brać udział w postępowaniu. W przypadku natomiast znacznej digitalizacji procesu, braku przejrzystości jego przebiegu w związku z wykorzystaniem niektórych z systemów, ostateczny rezultat w sferze uprawnień procesowych oskarżonego lub podejrzanego może być taki sam, jak gdyby nie brali oni w ogóle udziału w postępowaniu. Jeśli nie można uzyskać wiedzy na temat wykorzystywanych systemów, jeśli ich mechanizm działania nie może być odtworzony, czy adwokat może skutecznie poddać określony środek lub decyzję kontroli sądowej i czy może skutecznie czuwać nad prawidłowością przebiegu postępowania? Jeśli poznanie sposobu podejmowania decyzji przez system SI wymaga wiedzy specjalistycznej niedostępnej dla przeciętnego obywatela albo nawet jest niemożliwe, czy oskarżony lub podejrzany skutecznie może podważać czynności procesowe? Jest to szczególnie istotne w świetle możliwości podjęcia ostatecznej decyzji o skazaniu na podstawie wyników tych czynności. Wreszcie należy wskazać, że sam sędzia, który ma ostatecznie podejmować rozstrzygnięcie w większości wypadków nie będzie dysponować wystarczająco szeroką wiedzą techniczną. Czy zatem może on skutecznie ocenić ewentualne nieprawidłowości, potencjalne uprzedzenia systemu SI, nieproporcjonalność środka i w tym zakresie odnieść się do złożonego środka zaskarżenia?

Nowe problemy w zakresie w szczególności prawa dostępu do adwokata mogą również pojawić się wraz z dalszym rozwojem systemów SI i ich szerszego wykorzystywania. Niewątpliwą korzyścią, która może płynąć z rozwoju systemów SI jest możliwość ich zastosowania do m. in. kształtowania strategii obrończych[60]. Istnieje natomiast ryzyko, że systemy te, zwłaszcza w początkowej fazie, mogą nie być dostępne dla większości uczestników procesu,

[59] Wyrok ETPCz z 13 maja 1980 r. w sprawie *Artico przeciwko Włochom*, nr skargi 6694/74; Wyrok ETPC z 23 listopada 1993 r. w sprawie *Poitrimol przeciwko Francji*, skarga nr 14032/88; Wyrok ETPC z 11 grudnia 2008 r. w sprawie *Panovits przeciwko Cyprowi*, skarga nr 4268/04; Wyrok ETPC z 18 listopada 2014 r. w sprawie *Aras przeciwko Turcji*, skarga nr 15065/07; Wyrok ETPC z 26 lipca 2011 r. w sprawie *Huseyn i inni przeciwko Azerbejdżanowi*, skargi nr 35485/05, 45553/05, 35680/05 i 36085/05, HUDOC.

[60] S. Quattrocolo, *Artificial…* s. 108-122.

m. in. choćby ze względu na ich koszt. Przewaga technologiczna części podmiotów nie jest niczym nowym i do pewnego stopnia musi być tolerowalna jako element rzeczywistości rynkowej. Natomiast w przypadku daleko idącej digitalizacji procesu oraz jego ewentualnej znacznej modyfikacji przy użyciu systemów SI, konieczne będzie zagwarantowanie, aby oskarżony dysponował choćby w podstawowym zakresie narzędziami niezbędnymi do zapewnienia efektywnej obrony. W przeciwnym wypadku może dojść również do naruszenia zasady równości broni w postępowaniu.

Ponadto powstaje też pytanie, czy systemy wykorzystywane do celów obrończych powinny być poddawane jakiejkolwiek kontroli, która mogłaby ocenić ich jakość. Obecne orzecznictwo szeroko odnosi się do sytuacji, kiedy adwokat nie wykonuje swoich obowiązków w odpowiedni sposób, nie uczestniczy aktywnie w postępowaniu. ETPCz postrzega te wypadki jako przejaw braku efektywnej obrony. Jeśli natomiast system, na którym miałaby opierać się obrona oskarżonego byłby niesprawny, nieprawidłowy i obarczony błędami, ostateczny efekt w istocie mógłby być bardzo zbliżony. Rozważenia wymaga zatem nie tylko, kto byłby ewentualnie odpowiedzialny za tego rodzaju nieprawidłowości, ale także jaki byłby ich skutek procesowy, tj. czy w jakimkolwiek względzie mogłoby to konstruować podstawę odwoławczą.

W kontekście efektywnego wykonywania działań obrończych należy także zwrócić uwagę na problem automatycznego uznawania wiarygodności materiału dowodowego w przypadku systemów SI. Możliwość kwestionowania wartości dowodowej zgromadzonych materiałów stanowi podstawowe prawo tradycyjnie pojmowanej obrony. Część autorów wskazuje również na silny związek tego elementu z uprawnieniem wynikającym z art. 6 ust. 3 lit. d Konwencji[61]. Osobowe źródła dowodowe, dokumenty przedstawiane przez strony postępowania z natury rzeczy wiążą się z pewną dozą wątpliwości, która ostatecznie podlega weryfikacji przy swobodnej ocenie dowodów.

W przypadku dowodów opartych na nowych technologiach pojawia się jednak problem automatycznego przyznawania im niekwestionowanej wiarygodności dowodowej, czasem nawet niepodważalności[62]. Wydaje się jednak, że zwłaszcza na tym etapie rozwoju technologicznego i wprowadzania SI do systemów prawnych państw, możliwość kwestionowania materiału zebranego za pomocą sztucznej inteligencji stanowi kwestię kluczową, która zapewni efektywność prawa do obrony.

[61] *Ibidem,* s. 82.
[62] S. Gless, *AI in the…*, s. 207-218.

Wreszcie, w związku ze znaczącymi oczekiwaniami w zakresie usprawnienia przebiegu procesu karnego za pomocą mechanizmów rozpoznawania mowy i systemów przekładów językowych, pojawia się również kwestia prawa do tłumaczenia w procesie, zawartego w art. 6 ust. 3 lit. e Konwencji. Istnieje niewątpliwie wiele korzyści związanych z wykorzystaniem systemów SI przy tłumaczeniu zarówno zeznań i wyjaśnień, przebiegu rozprawy, jak i treści dowodów. Systemy te mogą przyczynić się do przyspieszenia przeprowadzanych czynności, ograniczenia kosztów, a także ostatecznego zwiększenia dostępności i przyswajalności materiałów procesu. Tym samym mogą ostatecznie ułatwić osiągnięcie ogólnego standardu wynikającego z art. 6 Konwencji, w szczególności biorąc pod uwagę, że tłumaczenie powinno być zapewnione w rozsądnym czasie[63]. O spełnieniu tego standardu możemy jednak mówić jedynie, jeśli dojdzie do spełnienia wymogów stawianym tłumaczeniu przez wykładnię ETPCz.

Zgodnie z orzecznictwem Trybunału tłumaczenie powinno być przede wszystkim odpowiedniej jakości[64]. Właściwe organy (w postępowaniu sądowym sąd, w przygotowawczym prokurator) powinny czuwać nad jego jakością[65], także poprzez kontrolę następczą tłumaczenia[66]. Oskarżony powinien zatem mieć możliwość kwestionowania jakości tłumaczenia[67]. W przypadku użycia do celów przekładu systemów SI, elementy te również muszą być wdrożone do systemów prawnych państw. Należy jednak zauważyć, że do tego celu również powinna zostać zachowana jak największa klarowność wykorzystywanych systemów oraz względna możliwość odtworzenia ich mechanizmów działania.

3. PODSUMOWANIE

Systemy sztucznej inteligencji, jak pokazuje praktyka, z powodzeniem mogą być wykorzystywane w postępowaniu karnym. Zastosowanie tych systemów obejmuje zarówno etap postępowania przygotowawczego, jak i sądowego. Mogą być używane do celów prewencji generalnej, indywidualnej,

[63] Zob. m. in. Dyrektywa Parlamentu Europejskiego i Rady 2010/64/UE z dnia 20 października 2010 r. w sprawie prawa do tłumaczenia ustnego i tłumaczenia pisemnego w postępowaniu karnym (Dz. Urz. UE L nr 280 z 26 października 2010 r.

[64] Wyrok ETPCz z 19 grudnia 1989 r. w sprawie *Kamasinski przeciwko Austrii*, skarga nr 9783/82, HUDOC.

[65] Wyrok ETPCz z 24 stycznia 2019 r. w sprawie *Knox przeciwko Włochom*, skarga nr 76577/13, HUDOC.

[66] Wyrok ETPCz z 18 października 2006 r. w sprawie *Hermi przeciwko Włochom*, skarga nr 18114/02, HUDOC.

[67] Wyrok ETPCz z 19 grudnia 1989 r. w sprawie *Kamasinski przeciwko Austrii*, skarga nr 9783/82, HUDOC.

do wykrywania sprawców czynów zabronionych, podejmowania różnego rodzaju decyzji procesowych, a także usprawnienia przebiegu rozprawy.

Jednocześnie jednak ich wykorzystanie budzi poważne wątpliwości nie tylko z punktu widzenia poszanowania prawa do prywatności, najczęściej podnoszonego w kontekście wykorzystania nowych technologii w postępowaniu karnym[68], ale także rzetelności postępowania i prawa do obrony. Głównym problemem niewątpliwie pozostają daleko idące braki w zakresie wyjaśnialności systemów SI, zwłaszcza w kontekście zastosowania *deep learningu.* Szczególnie narażone na naruszenie pozostaje w tym wypadku skuteczne prawo do informacji w postępowaniu. Jak pokazuje natomiast przedstawiona analiza, kluczowym elementem w zakresie wątpliwości co do poszanowania prawa do obrony przy użyciu sztucznej inteligencji w procesie jest efektywność i realność tego prawa. Trudno do końca przewidzieć, na jaką skalę i przy jakiej liczbie czynności sztuczna inteligencja będzie wykorzystywana w postępowaniu karnym. Jeżeli natomiast systemy SI miałyby być wykorzystywane na szeroką skalę i stanowić główną podstawę wydawania rozstrzygnięć, to nawet gdyby poszczególne elementy prawa do obrony byłyby formalnie zapewnione – informacja o zarzutach zostałaby przedstawiona, materiały postępowania udostępnione, obrońca wyznaczony itd., powstaje pytanie o rzeczywistą efektywność tych praw. Jeśli nie będą one niosły za sobą żadnych wymiernych korzyści dla oskarżonego i jeśli zostanie on na etapie wniesienia oskarżenia do sądu przytłoczony niezrozumiałym, obszernym materiałem dowodowmy, to istota poszczególnych uprawnień przysługującemu oskarżonemu w ramach prawa do obrony może zostać naruszona. Co więcej, decyzja wydana w wyniku postępowania, w którym informacje o rzeczywiście istotnych elementach materiału dowodowego i ich charakterze są znacząco ograniczone, może stronom, w szczególności oskarżonemu, wydawać się arbitralna. Tym samym doszłoby w rzeczywistości do zaprzeczenia jednemu z głównych celów wykorzystania algorytmów i SI w postępowaniu.

Niewątpliwie wzmocniony powinien zostać nacisk na obowiązki informacyjne w postępowaniu, a prawo do rzetelnej informacji wraz z rozwojem nowych technologii powinno ulegać odpowiedniemu dostosowaniu. Kluczowa wydaje się również w zapewnieniu skutecznych praw procesowych i możliwości przeprowadzenia skutecznej kontroli podejmowanych czynności, rola biegłego. W przypadku spraw, gdzie znacząca większość

[68] B. Loftus, *Normalizing covert surveillance: the subterranean world of policing*, The British Journal of Sociology, p. 2070-2091, https://doi.org/10.1111/1468-4446.12651

materiału dowodowego miałaby się opierać na systemach technologicznych m. in. z użyciem SI, trudno sobie wyobrazić brak obecności specjalisty w tym zakresie w postępowaniu. Być może powinna też zostać zwiększona możliwość i upowszechniona praktyka powoływania prywatnych opinii w tym zakresie, która mogłaby pełnić dodatkową funkcję ochronną. W przypadku systemów, które niechętnie odnoszą się do dowodów prywatnych, ewentualne czerpanie korzyści przez obronę z nowych rozwiązań technologicznych może zostać znacząco ograniczone, tym samym znacząco ograniczając możliwość zapewnienia przeciwwagi dla zaplecza technicznego organów ścigania i równości broni w postępowaniu.

Projekt rozporządzenia unijnego w sprawie sztucznej inteligencji, chociaż wprowadza szereg wymogów systemowych dla narzędzi SI, nie wydaje się niwelować wszystkich tych problemów i rozwiewać wszystkich wątpliwości. Rozporządzenie, w związku ze stawianym dużym naciskiem na zapewnienie odpowiedniej jakości wprowadzanych danych, wprowadzeniem wymogów w odniesieniu do analizy ryzyk i bezpieczeństwa danych wydaje się przede wszystkim umożliwiać eliminowanie części zagrożeń związanych ze stronniczością systemu, wgranymi błędami oprogramowania oraz z naruszeniem ochrony danych osobowych. Problemów proceduralnych nie sposób jednak rozwiązać jednym uniwersalnym aktem, dlatego być może, wzorem dyrektyw Programu sztokholmskiego, niezbędne okaże się wdrożenie osobnego aktu, który regulowałby zapewnienie właściwego standardu praw procesowych w postępowaniu karnym przy użyciu systemów SI.

Rozporządzenie jednak wskazuje na niekwestionowaną potrzebę stworzenia pewnych wspólnych wymogów i standardów w zakresie wykorzystania sztucznej inteligencji. Opracowanie takich wymogów może okazać się również nie bez znaczenia w kontekście europejskiej współpracy w sprawach karnych, wzajemnego uznawania orzeczeń oraz współpracy organów ścigania UE. Znaczące różnice systemowe w zakresie choćby standardów dowodowych mogą utrudnić efektywną reakcję karną na czyn zabroniony. Wątpliwości związane z podejmowaniem decyzji sądowych w oparciu o systemy SI oraz brak możliwości poddania ich skutecznej kontroli, może sprawić, że nie będą one uznawane w innych państwach członkowskich UE. Tym samym określenie minimum gwarancyjnego może okazać się szczególnie istotne i korzystne nie tylko dla regulacji krajowych, ale także na poziomie europejskim.

BIBLIOGRAFIA

Alizadeh F., *I Don't Know, Is AI Also Used in Airbags?: An Empirical Study of Folk Concepts and People's Expectations of Current and Future Artificial Intelligence*, I- com 2021, 20(1), s. 2-17, doi:10.1515/icom-2021-0009.

Bruyne J. D., Vanleenhove C., *Artificial Intelligence and the Law*, Intersentia 2021.

Caianiello, M., *Criminal Process faced with the Challenges of Scientific and Technological Development*, European Journal of Crime, Criminal Law and Criminal Justice 2019 (27), https://doi.org/10.1163/15718174-02704001.

Committee on Civil Liberties, Justice and Home Affairs, *Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (2020/2016(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html.

Deeks, A., *The Judicial Demand for Explainable Artificial Intelligence,* Colum. L. Rev. 2019 (51).

Dixon, H. B., *Artificial Intelligence: Benefits and Unknown Risk*, https://www.americanbar.org/groups/judicial/publications/judges_journal/2021/winter/artificial-intelligence-benefits-and-unknown-risks/.

Ertel, W., *Introduction to Artificial Intelligence*, Springer 2018.

FRA – European Union Agency for Fundamental Rights, *Artificial Intelligence, Big Data and Fundamental Rights Country Research Estonia,* 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-ai-project-estonia-country-research_en.pdf.

Frankish, K., Ramsey, W. M., *The Cambridge Handbook of Artificial Intelligence*, Cambridge 2014.

Gless, S., *AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials*, GJIL 2020 (51).

Gunning D., Stefik M, Choi J., Miller T., Stumpf S., Yang G.Z., *XAI-Explainable artificial intelligence*. Science Robotics 2019, 4 (37). doi:10.1126/scirobotics.aay7120.

Harris D., O'Boyle M., Bates E., *Law of the European Convention on Human Rights*, Oxford 2018.

Hänold, S., *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, [w:] *Robotics, AI and the Future of Law*, Corrales M., Fenwick M., Forgó N. (red.) Springer 2018.

Jackson J. D., *Responses to Salduz: Procedural Tradition, Change and the Need for Effective Defence,* „The Modern Law Review" 2016, 79(6).

Jasiński W., *Dostęp osoby oskarżonej o popełnienie czynu zagrożonego karą do adwokata na wstępnym etapie ścigania karnego – standard strasburski*, Europejski Przegląd Sądowy 2019/1.

Kehl, D., Guo, P., Kessler, S., *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative*, Berkman Klein Center for Internet & Society, Harvard Law School, 2017, https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf.

Kowalik-Bańczyk K., *Prawo do obrony w unijnych postępowaniach antymonopolowych. W kierunku unifikacji standardów proceduralnych w Unii Europejskiej*, Warszawa 2012.

Kremens K., Jasiński W., *Editorial of dossier "Admissibility of Evidence in Criminal Process. Between the Establishment of the Truth, Human Rights and the Efficiency of Proceedings"*, Revista Brasileira de Direito Processual Penal 2021, vol. 7, n. 1, s. 30-32, https://doi.org/10.22197/rbdpp.v7i1.537.

Kubit M., *Rozwój sztucznej inteligencji w świetle prawa Unii Europejskiej – dylematy i wyzwania*, Warszawa 2021.

Lach A., *Rzetelne postępowanie dowodowe w sprawach karnych w świetle orzecznictwa strasburskiego,* Warszawa 2018.

Loftus B., *Normalizing covert surveillance: the subterranean world of policing,* The British Journal of Sociology, https://doi.org/10.1111/1468-4446.12651.

McDaniel J., Pease K., *Predictive Policing and Artificial Intelligence*, Routledge 2021.

Misuraca, G. and Van Noordt, C., *AI Watch - Artificial Intelligence in public services*, Publications Office of the European Union, Luxembourg, 2020, doi:10.2760/039619.

Nowicki M. A., *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, Warszawa 2017.

Oswald M., Grace J., Urwin S., Barnes G.C., *Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality*, Information & Communications Technology Law 2018, 27(2), 223-250, DOI: 10.1080/13600834.2018.1458455.

Oyetunde, B., *Introducing Salme, Estonian courts' speech recognition assistant,* https://investinestonia.com/introducing-salme-estonian-courts-speech-recognition-assistant/

Parlament Europejski, *Sztuczna inteligencja. Co to jest i jakie ma zastosowania?* https://www.europarl.europa.eu/news/pl/headlines/society/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania.

Simonato, M.*, Defence rights and the use of information technology in criminal procedure*, *Revue internationale de droit pénal*, 2014, 85(1-2).

Steinborn S., *Dostęp do obrońcy na wczesnym etapie postępowania karnego. Uwagi de lege lata i de lege ferenda*, Europejski Przegląd Sądowy 2019/1.

Steinborn S., Wąsek-Wiaderek M.*, Moment uzyskania statusu biernej strony postępowania karnego z perspektywy konstytucyjnej i międzynarodowej*, [w:] M. Rogacka-Rzewnicka, H. Gajewska-Kraczkowska, B. Bieńkowska (red.), *Wokół gwarancji współczesnego procesu karnego. Księga jubileuszowa Profesora Piotra Kruszyńskiego*, Warszawa 2015.

Steinborn S., *Status osoby podejrzanej w procesie karnym z perspektywy Konstytucji RP (uwagi de lege lata i de lege ferenda)* (w:) *Państwo prawa i prawo karne. Księga jubileuszowa Profesora Andrzeja Zolla,* red. P. Kardas, T. Sroka, W. Wróbel, Warszawa 2012.

Stoykova, R., *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, Computer Law & Security Review, 2021 (42).

Tran T. H., *China created an AI "Prosecutor" that can charge people with crimes*, https://futurism.com/the-byte/china-ai-prosecutor-crimes.

Quattrocolo S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings A Framework for A European Legal Discussion*, Springer 2020.

Utset M. A., *Predictive policing and criminal law*, [w:] *Predictive Policing and Artificial Intelligence*, J. McDaniel, K. Pease (red), Routledge 2021.

Vargas R., Mosavi A., Ruiz R., *Deep Learning: A review*, Advances in Intelligent Systems and Computing 2017, 5(2),

Wachter, S., Mittelstadt, B., Russell, C., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, Harv. J.L. & Tech. 2018 (31).

Wąsek-Wiaderek M., *Dostęp do akt sprawy oskarżonego tymczasowo aresztowanego i jego obrońcy w postępowaniu przygotowawczym - standard europejski a prawo polski,* Palestra 2003, 48(3-4).

Wickramarathna N., Edirisuriya E., *Artificial Intelligence in the Criminal Justice System: A Literature Review and a Survey*, s. 4-5, https://www.researchgate.net/publication/358635259_Artificial_Intelligence_in_the_Criminal_Justice_System_A_Literature_Review_and_a_Survey_N_A_Wickramarathna_1_and_EATA_Edirisuriya/link/620c9b36afa8884cabe7a7c6/download.

Wiliński P., *Odmowa dostępu do akt sprawy w postępowaniu przygotowawczym*, Prokuratura i Prawo 2006, nr 11 (7).

Wiliński P., *Proces karny w świetle Konstytucji*, Warszawa 2011.

Wiliński P., *Zasada prawa do obrony w polskim procesie karnym*, Kraków 2006.

Wróblewski K., Tęcza-Paciorek A. M., *Dostęp podejrzanego do akt postępowania w przedmiocie tymczasowego aresztowania po nowelizacji kodeksu postępowania karnego*, Prawo i Prokuratura 2016 (3).

Wyjaśnienia dotyczące Karty Praw Podstawowych, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32007X1214(01)&from=EN, (dostęp: 17.06.2019).

Završnik, A. *Criminal justice, artificial intelligence systems, and human rights.* ERA Forum 2020 (20).

Orzecznictwo:

Wyrok ETPCz z 13 maja 1980 r. w sprawie *Artico przeciwko Włochom*, skarga nr 6694/74, HUODOC.

Wyrok ETPCz z 30 marca 1989 r. w sprawie *Lamy przeciwko Belgii*, skarga nr 10444/83, HUODOC.

Wyrok ETPCz z 19 grudnia 1989 r. w sprawie *Kamasinski przeciwko Austrii*, skarga nr 9783/82, HUODOC.

Wyrok ETPCz z 19 lutego 1991 r. w sprawie *Frau przeciwko Włochom,* skarga nr 12147/86, HUODOC.

Wyrok ETPCz z 23 listopada 1993 r. w sprawie *Poitrimol przeciwko Francji*, skarga nr 14032/88, HUODOC.

Wyrok ETPCz z 20 października 1997 r. w sprawie *Serves przeciwko Francji,* skarga nr 20225/92, HUODOC.

Wyrok ETPCz z 25 marca 1999 r. w sprawie *Pelissier i Sassi przeciwko Francji*, skarga nr 25444/94, HUODOC.

Wyrok ETPC z 25 lipca 2000 r. w sprawie *Mattoccia przeciwko Włochom*, skarga nr 23969/94 HUODOC.

Wyrok ETPCz z 13 lutego 2001 r. w sprawie *Garcia Alva przeciwko Niemcom*, skarga nr 23541/94, HUODOC.

Wyrok ETPCz z 15 listopada 2005 r. w sprawie *Lammi przeciwko Finlandii*, skarga nr 53835/00 HUODOC.

wyrok ETPCz z 26 września 2006 r. w sprawie *Miraux przeciwko Francji*, skarga nr 73529/01, HUODOC.

Wyrok ETPC z 18 października 2006 r. w sprawie *Hermi przeciwko Włochom*, skarga nr 18114/02, HUDOC.

Wyrok ETPCz z 9 października 2008 r. w sprawie *Moiseyev przeciwko Rosji*, skarga nr 62936/00, HUODOC.

Wyrok ETPCz z 11 grudnia 2008 r. w sprawie *Panovits przeciwko Cyprowi*, skarga nr 4268/04.

Wyrok ETPCz z 26 lipca 2011 r. w sprawie *Huseyn i inni przeciwko Azerbejdżanowi*, skargi nr 35485/05, 45553/05, 35680/05 i 36085/05, HUDOC.

Wyrok ETPCz z dnia 12 lutego 2013 r. w sprawie *Dimitar Krastev przeciwko Bułgarii*, skarga nr 26524/04, HUODOC.

Wyrok ETPCz z 31 października 2013 r. w sprawie *Bandaletov przeciwko Ukrainie,* skarga nr 23180/06, HUODOC.

Wyrok ETPCz z 18 listopada 2014 r. w sprawie *Aras przeciwko Turcji*, skarga nr 15065/07 HUODOC.

Wyrok ETPCz z 24 stycznia 2019 r. w sprawie *Knox przeciwko Włochom*, skarga nr 76577/13, HUDOC.

Źródła internetowe:

https://www.riskterrainmodeling.com/ (dostęp: 05.06.2022).

https://www.predpol.com/(dostęp: 05.06.2022).

https://www.xlaw.it/presentazione/index_eng.asp (dostęp: 05.06.2022).

https://keycrime.com/ (dostęp: 05.06.2022).

https://www.stadt-zuerich.ch/portal/de/index/politik_u_recht/stadtrat/weitere-politikfelder/smartcity/english/projects/precobs.html (dostęp: 05.06.2022).

https://land-der-ideen.de/en/project/precobs-software-for-predicting-crimes-355 (dostęp: 05.06.2022).

THE USE OF ARTIFICIAL INTELLIGENCE IN THE CRIMINAL PROCEDURE IN THE CONTEXT OF THE RIGHT TO DEFENCE

Abstract: Artificial intelligence (AI) undergoes gradual dissemination and becomes more and more topical both in the private and in the public law as well as organisations such as European Union. AI systems are considered to modify criminal process in a significant way and bring many benefits to their users. They are believed to facilitate many activities taken during the course of proceedings, make them more effective, efficient and quicker. They could also limit some of the costs. Finally, they can contribute to limiting the arbitrary decisions of the competent bodies and eliminate the bias connected with human factor in the proceedings. As a result, they can contribute to unification of the practice of applying the law. The use of AI systems can be also controversial in terms of the protection of human and procedural rights, including the right to defence. The objective of the study is to determine how the use of artificial intelligence may affect the standard of the right to defence in criminal proceedings. In order to answer the main research question, the analysis presents basic issues related to the concept of artificial intelligence, the ways of its description, main problems relating to its application, as well as the possibilities and examples of its use in a criminal trial. It also presents the basic aims of the draft EU Act on Artificial Intelligence. In the next part, the study introduces the elements necessary to guarantee an effective right to defence and indicates the rights that are particularly vulnerable to infringement by the use of AI systems, based primarily on the content of the European Convention on Human Rights and the ECtHR case law. Finally, in the summary, the paper attempts to formulate general conclusions referring to the objective of the research on the basis of the conducted analysis. It also aims to provide for the basic *de lege ferenda* proposals, in particular with regard to appropriate consideration of informational obligations and the role of experts in the proceedings.

Keywords: Artificial intelligence, AI, black box problem, right of defence, ECtHR

JULIA SIDYK
UNIWERSYTET JAGIELLOŃSKI

PRAWO DO SPRAWIEDLIWEGO SĄDU A AUTOMATYZACJA WYMIARU SPRAWIEDLIWOŚCI – PERSPEKTYWA W ŚWIETLE REGULACJI EUROPEJSKICH

Abstrakt: Dynamiczny rozwój sztucznej inteligencji wzbudził potrzebę stworzenia legislacyjnych regulacji na potrzeby przyszłego prawa. Akt w sprawie sztucznej inteligencji UE jest odpowiedzią na tę potrzebę, a proces regulacji tak kompleksowego i nieprzewidywalnego zagadnienia wymaga rozpatrzenia zagadnienia pod wieloma aspektami, w tym w wymiarze sprawiedliwości i powiązanych procesach decyzyjnych. Niniejszy rozdział analizuje poszczególne elementy powszechnie rozumianego prawa do sprawiedliwego sądu, równocześnie odnosząc je do planowanych w Akcie regulacji i rozwiązań. Omówione są również już badane formy szeroko rozumianej automatyzacji wymiaru sprawiedliwości, w odniesieniu do całego pojęcia LegalTech, a także sztucznej inteligencji. Wskazano ponadto słabości Aktu wobec realizacji prawa do sprawiedliwego sądu.

Słowa kluczowe: prawo do sprawiedliwego sądu, akt w sprawie sztucznej inteligencji, LegalTech, sztuczna inteligencja, automatyzacja

1. WPROWADZENIE

Dynamiczność i wiążąca się z nią nieprzewidywalność rozwoju technologicznego sprawia, iż karkołomnym wyzwaniem jest stworzenie legislacji, która skutecznie uregulowałaby przyszłe potrzeby prawa. Pomimo faktu, że pierwsze wzmianki o sztucznej inteligencji (SI) pojawiły się już w latach 50. XX wieku, dopiero teraz podjęto próbę uchwalenia aktu skutecznie regulującego

ten obszar. Projekt aktu w sprawie sztucznej inteligencji (AIA) (procedura 2021/0106/COD) opublikowany przez Komisję Europejską w kwietniu zeszłego roku[1] jest pierwszą tego typu regulacją. Stanowi on równocześnie zilustrowanie sentencji *hominum causa omne ius constitutum sit*, bowiem można zaryzykować stwierdzenie, iż to sytuacje takie jak skandal związany z Cambridge Analytica i wyborami prezydenckimi w Stanach Zjednoczonych w 2016[2] stały się jedną z jego przyczyn. W obecnych regulacjach europejskich pojawia się jedynie wzmianka na ten temat. Dotyczy ona automatyzacji sprawowania wymiaru sprawiedliwości w kontekście ochrony danych osobowych w Rozporządzeniu o Ochronie Danych Osobowych, a dokładniej w art. 22[3]. Podejmowanie decyzji mających prawne skutki lub istotne znaczenie wyłącznie na podstawie algorytmów nie jest obecnie zabronione, ale osoba, której dane dotyczą, ma prawo nie podlegać decyzji podjęte w taki sposób, w celu ochrony wymiaru sprawiedliwości. Tego zapisu zdecydowanie nie można uznać jako wystarczającą regulację odpowiadającą na teraźniejsze potrzeby, a co dopiero te przyszłe.

AIA jest oczywiście odpowiedzią na rozwój technologiczny, ale też na malejącą wydajność sądów. W Polsce, na jednego sędziego powinno przypadać około dwóch pracowników sądu, a w rzeczywistości w tym podziale uwzględnia się również np. osoby zajmujące się pracami remontowymi[4]. Należy zauważyć pewną dwoistość zagadnienia: z jednej strony, sztuczna inteligencja może stanowić odpowiedź na naruszenie prawa do sprawiedliwego sądu, natomiast z drugiej, stosowanie SI w procesach jurysdykcyjnych może naruszać te prawa z powodu SI. Według AIA to właśnie wymiar sprawiedliwości i procesy demokratyczne, wśród kilku innych systemów, są wyróżnione w kategorii wysokiego ryzyka - AIA opiera się na analizie ryzyka. Co jednak należy zauważyć, projekt regulacji nadal zawiera luki, tym bardziej, mając na uwadze płynność i pilność procesu na tym etapie, konieczna jest dalsza analiza. Warto nadmienić, iż przed sfinalizowaniem projektu rozporządzenia

[1] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.

[2] P. N. Howard et al., *Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration,* Journal of Information Technology & Politics 15:2, s 81-92.

[3] 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).

[4] https://www.prawo.pl/prawnicy-sady/brak-pracownikow-sadowych-uderza-w-pracesadow,507593.html (dostęp: 22.05.2022).

AIA, powstały m.in.: Komisja na rzecz Efektywności Wymiaru Sprawiedliwości, Coordinated Plan on Artificial Intelligence 2021, Communication on Fostering an European Approach to Artificial Intelligence, i wiele innych podmiotów.

Zagadnienie będące przedmiotem niniejszych rozważań warto równocześnie umiejscowić w perspektywie całego trójdzielnego, według podziału O. Goodenough[5], LegalTech. W 1.0 zawierają się podstawowe, rozpowszechnione już technologie i oprogramowanie, które mają charakter jedynie wspierający[6]. Zaliczają się do nich m.in prawnicze bazy danych, jak Lex czy Legalis, jak i również systemy komunikacji z sądami, czy też narzędzia do przeprowadzania wideokonferencji i rozpraw online[7]. Choć brak jest w nich zaawansowanej analizy, są niewątpliwie przydatne, a szczególne uznanie zyskały, z oczywistych przyczyn, w czasie pandemii COVID–19.

LegalTech 2.0 odnosi się do technologii, które są bardziej zaawansowane, ale wciąż nie są autonomiczne, choć mogą częściowo zastępować ludzi. Służą np. do automatycznego sporządzania umów, kontraktów, pozwów, etc., ale też tokenizacji czy ustalania faktów[8]. Narzędzia te zyskują na popularności, bowiem cechuje je niskie ryzyko związane z ich użytkowaniem. Można zaliczyć do nich np. *CreateiQ* od Linklaters – jest to platforma służąca do automatyzacji kontraktów i przeprowadzania negocjacji[9]. Jak można przeczytać, Linklaters zapewnia o efektywności i szybkości systemu, który określają jako szyfrowany i bezpieczny. W taki sposób umożliwiają nie tylko zawieranie kontraktów, ale też ich negocjację, czy zarządzanie nimi.

W końcu – LegalTech 3.0. Ta kategoria, będąca niejako najwyższą, a zarazem tą, na której skupi się niniejsza analiza, opiera się na rozwiązaniach, gdzie celem nie jest samo w sobie zastąpienie człowieka, a możliwość podjęcia autonomicznej decyzji[10]. Kluczowe jest tutaj nie odtwarzanie wcześniej zaprogramowanych zdarzeń, a podejmowanie decyzji na podstawie samodzielnie pozyskiwanych danych, bądź też różnych form samokształcenia[11]. Zawiera się

[5] https://www.huffpost.com/entry/legal-technology-30_b_6603658 (dostęp: 22.05.2022).
[6] D. Szostek, *The Concept of Legal Technology (LegalTech) and Legal Engineering,* [w:] *LegalTech. Information technology tools in the administration of justice,* red. D. Szostek, M. Załucki, Baden-Baden, 2021, s. 20.
[7] *ibidem.*
[8] *ibidem,* s. 21.
[9] https://www.linklaters.com/en/about-us/nakhoda (dostęp: 22.05.2022).
[10] D. Szostek, *The Concept of…* et al., s. 22.
[11] D. Szostek, *Pojęcie Legal Technology (LegalTech),* [w:] *LegalTech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym*, red. D. Szostek, 2021.

w niej zarówno technologie uwzględniające udział człowieka w decyzji, czyli „słabą" SI, ale też te funkcjonujące samodzielnie opierające się na „silnej" SI. To ta druga realizuje wizję o cyfrowym umyśle[12], rozpowszechnione w kulturze popularnej. Stanowi to równocześnie przeszkodę w szerszej implementacji SI, bowiem błędnie domniemywa się, że celem rozwoju SI jest stworzenie odpowiednika ludzkiego umysłu, która to perspektywa znajduje swoje początki już w 1950 roku, w tzw. teście Turinga[13]. Chociaż obecnie wciąż nie istnieje w pełni działająca „silna" SI, to bez wątpienia należy wziąć ją pod uwagę w legislacji. Z kolei "słaba" SI jest tą najbardziej rozpowszechnioną, działającą obecnie.

To właśnie w kategorii 3.0 można odnaleźć innowacyjne przykłady użycia SI w prawie.

1.1 Przykłady LegalTech 3.0

1.1.1 Europejski Trybunał Praw Człowieka

W 2016 roku podjęto próbę zastosowania algorytmu dla oceny spraw w toku przed Europejskim Trybunałem Praw Człowieka. Opracowano binarną klasyfikację, gdzie danymi wejściowymi była zawartość tekstowa pochodząca z danych sprawy, zaś wyjściowymi – binarna ocena, czy doszło do naruszenia praw człowieka, czy też nie[14]. Sprawy dotyczyły art. 3 (zakaz tortur), 6 (*nomen omen*, prawo do rzetelnego procesu sądowego) oraz 8 (prawo do poszanowania życia prywatnego i rodzinnego) EKPCz. Co również istotne, średnia trafność przewidywanego wyniku wyniosła 79%, co sklasyfikowano jako wysoką dokładność[15]. W tej analizie użyto zarówno *Natural Language Processing* (przetwarzanie języka naturalnego – NLP), jak i *Machine Learning* (uczenia maszynowego – ML). Choć ten eksperyment można nazwać sukcesem, nie oznacza to bynajmniej, że jest to metoda na tyle skuteczna, by mogła regularnie wejść w życie. Przykładowo, zauważono, że średnio

[12] M. Rojszczak, *Prawne aspekty systemów sztucznej inteligencji – zarys problemu,* [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe,* red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa, 2019.
[13] *Ibidem.*
[14] N. Aletras et al., Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing Perspective, PeerJ Computer Science, 2:e93.
[15] M. Załucki, *The road to modern judiciary* [w:] *Internet and New Technologies Law,* Baden-Baden, 2021, s. 165.

najważniejszą częścią przy najskuteczniejszych przewidywaniach były informacje o stanie faktycznym[16].

Podobną próbę przeprowadzono w 2019 roku, również przy użyciu NLP[17]. Ta druga próba zbadała dziewięć artykułów EKPCz, oprócz trzech wymienionych uprzednio, zawierała też art. 2 (prawo do życia), 5 (prawo do wolności i bezpieczeństwa osobistego), 10 (wolność wyrażania opinii), 11 (wolność zgromadzania się i stowarzyszania się), 13 (prawo do skutecznego środka odwoławczego), oraz 14 (zakaz dyskryminacji). W tym badaniu średnia skuteczność wynosiła 75%. Zbadano także klasyfikację w przypadku przewidywania wyniku przyszłych spraw bazując na wynikach poprzednich, gdzie dokładność miała zakres od 58 do 68%[18]. Ponadto, w porównaniu do badania z 2016 roku, przeanalizowano więcej spraw przypadających na dany artykuł, jak i również pominięto jedną z sekcji aktów spraw (tę dotyczącą argumentów Trybunału) czemu przypisuje się mniejsze ryzyko stronniczości[19]. Równocześnie osiągnięto dokładność na poziomie 65% oceniając rezultaty wyłącznie na podstawie nazwisk sędziów przypisanych do sprawy[20]. Rodzi to pytania natury filozoficznej, a mianowicie, czy obecność czynnika ludzkiego, choć będąca nieodłącznym elementem osądzania, właściwie już od czasów prawa pretorskiego, jest wskazana, oraz czy znajdzie swoje miejsce w prawie przyszłości, co pozostaje do samorefleksji.

1.1.2 Próby utworzenia autonomicznych systemów – przykład Estonii i Holandii

W Estonii, która ujrzała stworzenie tzw. cyfrowego społeczeństwa w ciągu ostatnich dwudziestu lat[21], z powodzeniem wprowadza się rozwiązania z użyciem nowych technologii. Jednym z nich jest system „e-File", który został wprowadzony w 2005 roku[22], a dzięki któremu znacznie przyspieszono postępowania sądowe. Funkcjonują tam zarazem inne technologiczne narzędzia w sferze życia publicznego, umożliwiające na przykład odnowienie prawa

[16] N. Aletras et al, *op. cit.*
[17] M. Medvedeva et al., *Using machine learning to predict decisions of the European Court of Human Rights*, Artificial Intelligence and Law, 2020/28, s. 237-266.
[18] *Ibidem.*
[19] *Ibidem.*
[20] *Ibidem.*
[21] T. Kerikmäe, E. Pärn - Lee, *Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race.* AI & SOCIETY, 36, 2021.
[22] https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ (dostęp: 22.05. 2022).

jazdy, rejestrację zakupu pojazdu, wysyłanie zeznania podatkowego, czy nawet głosowanie w ogólnokrajowych wyborach[23]. Już około 2019 roku można było usłyszeć o pilotażowym programie, w którym planowano wykształcić autonomicznego sędziego, który miałby rozpoznawać drobne roszczenia, w których przedmiot postępowania nie przewyższa 7000 EUR[24]. Nie przewidywano udziału "tradycyjnego" sędziego w takich procesach. Brak jest jednak najnowszych danych o postępach tych działań, oprócz nielicznych wzmianek o potencjale przedsięwzięcia.

Analogiczna sytuacja ma miejsce w Holandii[25], gdzie podjęto próby opracowania "robosędziego" mającego mieć właściwość w sprawach, gdzie rozpoznaje się odwołania co do wysokości mandatu drogowego. Podobnie, brak jest aktualnych informacji o postępie projektu.

Być może, brak nowych kroków w tym obszarze można przypisać powstaniu AIA, która, nadal nie przyjmując końcowej formy, może skutecznie zniechęcać do podejmowania starań, dopóki nie będzie jasne co, i w jakim stopniu, jest dozwolone.

1.1.3 Przykład Polski

Choć poziom cyfryzacji życia publicznego w Polsce niewątpliwie nie jest tak daleko posunięty, jak ma to miejsce w przypadku Estonii, podejmowane są próby użycia nowych technologii w procesach decyzyjnych, funkcjonują bowiem cztery elektroniczne sądy polubowne, nazwane również e-arbitrażami[26]. Jak można przeczytać na stronie internetowej jednego z nich, «„Ultima Ratio", Pierwszy Elektroniczny Sąd Polubowny przy Stowarzyszeniu Noratiuszy Rzeczypospolitej Polskiej w Warszawie, to elektroniczny sąd arbitrażowy zajmujący się rozpoznawaniem sporów gospodarczych w obrocie krajowym i międzynarodowym, w którym całość postępowania prowadzona jest elektronicznie, sprawy kończą się ostatecznym wyrokiem w ciągu około 3 tygodni i są prowadzone bez fizycznego udziału stron»[27]. Jest to wyjątkowo uproszczona, z perspektywy zainteresowanego, procedura, gdzie strony umieszczają argumentu w formularzu, a później system automatycznie przygotowuje pismo, co można zrobić o dowolnej porze dnia, a rozmowy prowadzi się przez

[23] *Ibidem.*
[24] Z. Franciska et al. *The AI is now in session. The impact of digitalisation on courts.*
[25] M. Załucki, op. cit, s. 168.
[26] https://www.infor.pl/prawo/nowosci-prawne/4673991,Esady-arbitrazowe-polubowne-w-Polsce.html (dostęp: 22.05.2022).
[27] https://ultimaratio.pl/o-sadzie (dostęp: 22.05.2022).

specjalny czat. Taki sąd należałoby jednak zakwalifikować do LegalTech 2.0, ponieważ do sprawy przypisany jest mediator lub arbiter, a automatyzacja ograniczona jest do kwestii materiałów dowodowych. Niewątpliwie natomiast zaobserwowany sukces takiej formy rozstrzygania sporów zwiastuje zwiększone starania wprowadzenia takich rozwiązań na większą skalę w Polsce.

Wśród tych przykładów, jedynie Holandia i Estonia dążą do pełnej automatyzacji, a choć to właśnie kwestii dopuszczenia "silnej" wersji SI dotyczy główny dyskurs i na tym skupia się niniejsza analiza, należy też mieć na uwadze bardziej powszechne zastosowanie SI, a nie jedynie te *hard cases* stanowiące argumenty w niejednej debacie, choć, oczywiście, one również wymagają uwagi. Trzeba bowiem pamiętać, iż przecież mało która sprawa jest niepowtarzalna, mało która wiąże ze sobą precedens i mało która wymaga odwołania się do wartości jak choćby w *Riggs v. Palmer*. Mając za sobą fakty natury zarówno formalnej i materialnej, można przejść do właściwej analizy. Należy postawić pytanie: czy pełna automatyzacja wymiaru sprawiedliwości za pomocą sztucznej inteligencji spełnia prawo do sprawiedliwego sądu?

2. ANALIZA

2.1 Akt w sprawie sztucznej inteligencji

Warto zacząć od samej AIA, stanowiącej fundamenty niniejszych rozważań.

Artykuł 3 pkt. 1, w którym zawarto definicje, przedstawia „system sztucznej inteligencji" jako „oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, 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"[28], zaś wspomniany Załącznik I, wymienia trzy techniki i podejścia, t.j.: „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) i systemy ekspertowe; c)podejścia

[28] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.

statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji"[29]. Nie trudno zauważyć, że te definicje są wyjątkowo szerokie. Z jednej strony, mając na uwadze nieprzewidywalność rozwoju technologii w tym obszarze, jest to do pewnego stopnia uzasadnione działanie, mające na celu stworzenie katalogu otwartego, ograniczające konieczność uchwalania znacznej ilości nowelizacji, czy też redukujące nadmierność regulacji. Z drugiej jednak strony, tak nieostre pojęcia będą wymagały wypracowania linii orzeczniczej, która zaś, do pewnego stopnia, sama może być zautomatyzowana, potencjalnie prowadząc do paradoksu paragrafu 22. Ponadto, brak odrębnego organu kontrolnego, jak i wdrożenie jednego aktu obejmującego równocześnie wiele różniących się od siebie obszarów, a także oparcie regulacji na ocenie algorytmu już po jego sfinalizowaniu, stwarzają bardzo dużo możliwości na potencjalne nadużycia.

Podjęto jednak adekwatne próby wykształtowania „bezpieczników", mających na celu ograniczenie nadużyć. Jednym z najważniejszych jest zapobieganie tzw. *blackbox efffect*, czyli efektowi czarnej skrzynki, w AIA nazywanego *opacity*. Jest to taki rodzaj programu, w którym człowiek wprowadza dane, a następnie, nie widząc procesu ich analizy, otrzymuje rezultat. Jest to szczególne zagrożenie, na które Rada Europejska zwróciła uwagę już dnia 21 października 2020[30]. W [sekcji] 3.5 (Prawa podstawowe) sam wniosek wskazuje, że efekt czarnej skrzynki może mieć negatywny wpływ na szereg praw zawartych w Karcie praw podstawowych UE[31]. Jedną z form zapobiegania temu zjawisku jest czteropoziomowa kwalifikacja systemów SI, bazująca na analizie poziomu potencjalnego ryzyka danego systemu, wiążąca się z różnymi procedurami ich wdrażania i mechanizmami kontroli. Są to mianowicie: niedopuszczalne ryzyko, wysokie ryzyko, ograniczone ryzyko, minimalne ryzyko. Przykładowo, w przypadku systemów ograniczonego ryzyka, jakim są, m.in. chatboty, obowiązki w zakresie przejrzystości są minimalne[32]. Egzekwowanie prawa (rozumiane jako m.in prowadzenie postępowania przygotowawczego, zapobieganie przestępczości, wykrywanie i ściganie czynów zabronionych, egzekwowanie sankcji karnych) oraz sprawowanie wymiaru sprawiedliwości i procesy demokratyczne, zaliczone są do kategorii systemów

[29] *ibidem*.
[30] https://www.consilium.europa.eu/media/46496/st11481-en20.pdf (dostęp: 22.05.2022).
[31] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.
[32] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_pl (dostęp: 22.05.2022).

wysokiego ryzyka. Szczególnie podkreśla się konieczność takiej kwalifikacji systemów, które pomagają w interpretacji faktów i stosowaniu przepisów do stanu faktycznego[33], a więc te omówione uprzednio jako zawierające się w LegalTech 3.0. Tytuł III rozdział 1 wskazuje na konieczność kontroli *ex ante*, takich systemów, przykładowo za pomocą *sandboxes*, czyli piaskownic regulacyjnych, które mają być rozwiązanie pozwalającym na testowanie danego systemu SI w kontrolowanych warunkach.

Risk-based assessment, czyli podejście oparte na analizie ryzyka, sprawdza się już w przypadku RODO[34]. Jak również wspomniano w uzasadnieniu wniosku AIA, po konsultacjach wniosku „[u]znano, że zastosowanie ram opartych na analizie ryzyka jest lepszym rozwiązaniem niż ogólne uregulowanie wszystkich systemów sztucznej inteligencji. (..) Ryzyko należy również kalkulować, biorąc pod uwagę wpływ na prawa i bezpieczeństwo"[35].

Co jednak należy zauważyć, AIA dopuszcza możliwość wprowadzenia do obrotu lub oddania do użytku systemów sztucznej inteligencji, których nie poddano ocenie zgodności, jeżeli nastąpiłyby „nadzwyczajne względy dotyczące bezpieczeństwa publicznego lub ochrony zdrowia i życia osób fizycznych oraz ochrony własności przemysłowej"[36], co może niejako stanowić furtkę do nadużyć, ze względu na nieostrość pojęcia „nadzwyczajnych względów". Szczególnie mając na uwadze zakwalifikowanie identyfikacji biometrycznej do kategorii niedopuszczalnego ryzyka, czego powodów można dopatrywać się w polityce Chin, gdzie digitalizacja społeczeństwa wzmacnia potencjał państwa do kontrolowania 1,4 miliarda mieszkańców[37], szczególnie łącząc tożsamość osób z podejmowanymi przez nich działaniami. Takie działanie zostało określone jako „cyfrowe totalitarne państwo"[38]. Pozostawienie tak szerokiej luki nie wydaje się być odpowiednim rozwiązaniem, uwzględniając tendencję do autokratyzacji państw na świecie, które to zjawisko nazywa się

[33] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.
[34] https://www.enisa.europa.eu/risk-level-tool/risk (dostęp: 22.05.2022).
[35] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.
[36] *ibidem.*
[37] X. Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State,* Journal of Democracy, 30/1, 2019, s 64.
[38] https://www.economist.com/essay/2018/09/13/the-economist-at-175 (dsotęp: 22.05.2022).

trzecią falą autokratyzacji[39]. Tym bardziej istotna jest zgodność implementacji systemów SI z prawami człowieka, w tym prawem do sprawiedliwego sądu.

AIA już w uzasadnieniu odnosi się do praw podstawowych – "Niniejszy wniosek opiera się na unijnych wartościach i prawach podstawowych"[40]. Dalej, [sekcja] 3.5 uzasadnienia odnosi się kolejno do praw zawartych w Karcie Praw Podstawowych UE, a dokładniej: art. 1, czyli prawa do godności człowieka; art. 7 i 8, czyli poszanowania życia prywatnego i ochrony danych osobowych; art. 21, czyli niedyskryminacji; art. 23, czyli równości kobiet i mężczyzn; art. 11, czyli zapobieganiu ograniczania prawa do wolności wypowiedzi; art. 12, czyli wolności zgromadzania się; art. 47 i 48, czyli zapewnienia ochrony prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawa do obrony i domniemania niewinności; ogólnej zasady dobrej administracji[41]. Dla kompletności rozważań warto również zawrzeć art. 6 oraz 13 EKPCz, które kolejno wskazują na: prawo do sprawiedliwego i publicznego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd; a także prawo do skutecznego środka odwoławczego. Można tu również nadmienić art. 45 Konstytucji RP, dla odniesienia do polskiego porządku prawnego. Zatem, zostaną wyróżnione następujące części podlegające analizie: sprawiedliwosc procesu, jawność (publiczność) procesu, rozsądność terminu rozpatrzenia sprawy, niezawisłość i bezstronność sądu, prawo do obrony, prawo do skutecznego środka odwoławczego.

2.2. Sprawiedliwość procesu

Przyjmując ulpianowską definicję sprawiedliwości, głoszoną przez paremię *iustitia est constans et perpetua voluntas ius suum cuique tribuendi*, postrzeganą przez pryzmat koncepcji Rawlsa, można wywnioskować, że jako sprawiedliwość należy rozumieć właściwe wyważenie konkurujących roszczeń[42]. Według takiego spojrzenia na sprawiedliwość, algorytm nie może operować na uniwersalistycznej zasadzie *one size fits all*, bowiem nie byłby równościowy. Wracając do przykładu ETPCz, stworzenie systemu analizującego, czy miało miejsce naruszenie praw człowieka, czy nie, wymagało znacznych

[39] A. Lührmann, *A third wave of autocratization is here: what is new about it?*, Democratization, 2019, 26:7, s. 1096. 2019.
[40] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.
[41] *ibidem*.
[42] M. Łuszczyk, *Zasada sprawiedliwości w paradygmacie rozwoju trwałego a koncepcja Johna Rawlsa*, Optimum. Studia Ekonomiczne, 4(88), 2017, s. 27.

uproszczeń – przynajmniej na obecnym etapie konieczne jest stworzenie pewnego modelu, będącego bezpośrednio uzależnionego od ekspertyzy czy nawet systemu wartości osoby go tworzącej, w którym nie ma miejsca na uwzględnienie wielu czynników kontekstualnych. Algorytm, jako seria działań lub kalkulacji „słabej" SI, operuje na już istniejących uproszczeniach. W przypadku SI „silnej", konieczny byłby wertykalny podział czynników według pewnej hierarchii, która, ponownie, zależna byłaby w głównej mierze od systemu wartości twórcy, na podstawie którego zostałby wykształcony autonomiczny system. Wymagałaby tym samym uproszczenia i niejako gradacji, a więc, w świetle obecnego rozwoju, pełna automatyzacja wymiaru sprawiedliwości nie jest możliwa ze względu na niemożliwość uwzględnienia licznych wyjątkowych przypadków. Dopuszczalne byłoby jednak do pewnego stopnia zautomatyzowanie spraw rutynowych, gdzie dodatkowe okoliczności sprawy byłyby albo ściśle skodyfikowane, albo wyrok nie byłby od nich zależny. Przejdźmy jednak do nieco bardziej ścisłych zasad, zawartych we wcześniej przytoczonych aktach prawnych, wyrażających poszczególne elementy sprawiedliwego sądu.

2.2.1 Jawność (publiczność) procesu

Bez wątpienia, nawet w obecnej, „tradycyjnej" postaci procesu pojawiają się trudności z jawnością i publiczną dostępnością procesu, o czym świadczą m.in. programy monitoringu przestrzegania zasady jawności przez sądy, prowadzone przez Fundację Court Watch. Szczególnie problematyczna okazała się jawność procesu w trakcie pandemii, gdzie zakaz wstępu dla publiczności obowiązywał w 36% z 392 objętych badaniem sądów[43]. Odpowiedzią na ten problem stały się postępowania prowadzone za pośrednictwem technologii umożliwiających łączenie się na odległość, które mogą być nie tylko bardziej kosztowo efektywne, ale także bezpieczniejsze i wygodniejsze[44]. Należy jednak zauważyć trudności związane z wykluczeniem technologicznym, które mogą być jedynie bardziej uwydatnione w sytuacji automatyzacji procesu. Jeżeli już teraz problematyczne jest zrozumienie kompleksowości procesu przez osoby nie zajmujące się prawem, nie sposób przypuścić, że dodatkowa konieczność zrozumienia działania algorytmów jakkolwiek rozwiąże problem. O ile od strony programisty możliwe jest szczegółowa analiza danego algorytmu,

[43] https://prawo.gazetaprawna.pl/artykuly/1491865,court-watch-polska-koronawirus-sadu-raport.html (dostęp: 22.05.2022).

[44] P. Lewandowski, *Sądy dostępne przez Internet. Szanse i zagrożenia,* Fundacja Court Watch Polska, 2020, s. 34.

nie można tego uznać za przejaw jawności. Postulowane jest zatem skonstruowanie prawa podmiotowego, wyjaśniającego działania algorytmu[45].

Ponadto, pojawia się również problem efektu czarnej skrzynki. O ile, jak wspomniano, AIA stara się im zapobiegać, to dla osoby, która nie w pełni rozumie działanie nawet relatywnie przejrzystego mechanizmu, rezultat pozostaje ten sam. Koalicja The Public Voice już w październiku 2018 ogłosiła dwanaście zasad, które powinny być przestrzegane w związku z funkcjonowaniem elementów SI w społeczeństwie[46], wśród których zawarta jest właśnie przejrzystość. W odniesieniu do wymiaru sprawiedliwości, to właśnie przejrzystość algorytmu oraz dążenie do eliminacji wykluczenia technologicznego, czy to z powodu wieku, niepełnosprawności, miejsca zamieszkania lub statusu majątkowego, są kluczowe, aby można było mówić o jawności procesu prowadzonego w sposób zautomatyzowany.

2.2.2 Rozsądność terminu rozpatrzenia sprawy

Rozsądność terminu rozpatrzenia sprawy jest bez wątpienia znaczącym problemem. Konsekwencje jej braku są szerokie, bowiem dotyczą nie tylko braku poczucia sprawiedliwości, ale też mogą prowadzić do niewymiernego środka prawnego, przykładowo na skutek dewaluacji czy pomniejszenia wartości rynkowej nieruchomości[47]. O problemie świadczy także wprowadzenie, jako rezultat orzecznictwa ETPCz (Kudła przeciwko Polsce[48]), mechanizmu skargi dotyczącej długości trwania procesu[49].

W przypadku terminu rozpatrzenia sprawy, automatyzacja procesu ma niewątpliwie dużą przewagę. Sama prędkość podejmowania decyzji jest uzależnione jedynie od zdolności obliczeniowych danego komputera czy serwera. Jak ma to miejsce np. w przypadku Elektronicznego Sądu Polubownego (1.1.3), czas trwania całego procesu szacuje się na trzy tygodnie, przy czym nadal zawiera on udział człowieka (mediatora lub arbitra). Właściwie, długość trwania procesu zdaje się być uzależniona od czasu poświęconego na odpowiednie wprowadzenie danych do gotowego algorytmu, przyjmując, że istnieje już system odpowiedni do rozpoznania danej sprawy, bez konieczności

[45] M. Araszkiewicz, *Sztuczna Inteligencja i prawo do wyjaśnienia,*Trzeci Sektor, 44 (4/2018).
[46] Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.
[47] M. Załucki, op. cit. s. 162.
[48] Kudła przeciwko Polsce - wyrok ETPC z dnia 26 października 2000 r., skarga nr 30210/96.
[49] M. Załucki, op. cit. 163.

modyfikacji czy aktualizacji sposobu jego działania. Czas przeznaczony na rozpatrzenie sprawy może ulec wydłużeniu w przypadku nowelizacji danego aktu prawnego o czas jego wprowadzenia do systemu, o ile ten proces nie zostałby również zautomatyzowany. Zatem, automatyzacja wymiaru sprawiedliwości, nawet na poziomie „słabej" SI, redukuje czas trwania procesu, szczególnie na etapie postępowania przygotowawczego, bezsprzecznie realizując prawo do rozpatrzenia sprawy w rozsądnym terminie, korzystniej niż "tradycyjny" sąd.

2.2.3 Niezawisłość i bezstronność sądu

Ten aspekt budzi najwięcej obaw, bowiem jest wielopoziomowy, a równocześnie jest tym, który powszechnie kojarzy się z pojęciem prawa do sprawiedliwego sądu. Spełnienie tego warunku uzależnione jest od przyjętej metody uczenia „silnej" SI, a konkretniej, źródła danych wejściowych. Jeżeli przyjęta metoda opierałaby się na znajdowaniu wzorów w już istniejących wyrokach, za pośrednictwem NLP, to powielałaby błędy poznawcze i heurystyki już istniejące w orzecznictwie. Ponadto, szczególnie istotne jest dla tej kwestii zjawisko *algorithmic bias* (stronniczość algorytmów). Może wynikać z obecności uprzedzeń nie tylko w już istniejących danych, ale też z wartości i cech twórcy danego algorytmu. Źródłem *algorithmic bias* może być również zwyczajnie złe skonstruowanie algorytmu, gdzie używane byłyby nieodpowiednie lub nierelewatne dane[50]. Skutkiem tego zjawiska może być np. inna wysokość kary za podobne przewinienie dla kobiet i mężczyzn, nawet, jeżeli błąd zawarty w algorytmie nie jest intencjonalny[51]. Podobny problem może zaistnieć na tle pochodzenia, wyznania, czy innych elementów tożsamości.

Ponadto, przeprowadzono badanie, które sprawdzało wpływ przerwy celem zjedzenia posiłku, na wyrok. Wszystkie sprawy (n=1112) dotyczyły zwolnienia warunkowego[52], a zatem decyzja była binarna (zgoda lub jej brak). Wykazano, że gdy decyzje podejmowane były bez przerwy, sędziowie mieli tendencję do pozostawania przy *status quo*, będącej odmową, zaś po przerwie mieli większą skłonność do przyznawania zwolnienia[53]. Tego typu

[50] M. Kuśmierczyk, *Algorithmic Bias in the Light of the GDPR and the proposed AI Act.* red. M. Olejnik, W. Morawska, Wrocław, 2022, s. 2.
[51] C. Criado Perez, *Invisible women*, Londyn, 2020, s.108.
[52] J. C. Bublitz, *What is wrong with hungry judges? A case study of legal implications of cognitive science.* Tom 14, red. A. Watermann et al., Haga, 2018, s. 13.
[53] S. Danziger et al., *Extraneous factors in judicial decisions*, Proceedings of the National Academy of Sciences, 2011, 108/17, s. 6892.

zjawiska wskazują na wady wymiaru sprawiedliwości, które są możliwe do wyeliminowania drogą automatyzacji.

Z drugiej strony, automatyzacja może pozwolić na wyeliminowanie zjawiska np. *framing effect*, czyli efektu sformułowania, zwanego też ramowaniem. Polega na położeniu nacisku na wybraną informację, w wyniku czego uwaga skupiona jest na wskazanym aspekcie problemu[54] i odnosi się do teorii ryzyka, szczególnie w wyborze między dwoma opcjami. Nawet, jeżeli oczekiwana wartość jest taka sama w dwóch podanych przypadkach, decyzja uzależniona jest od sposobu, w jaki problem został przedstawiony. Ma on też miejsce w wydawaniu wyroku, gdzie sędzia może podświadomie inaczej interpretować wiadomości zależnie od sposobu, w jaki zostały przedstawione, nawet będąc w pełni kompetentnym.

Automatyzacja wymiaru sprawiedliwości wymaga zrewidowania podejścia do obecności czynnika ludzkiego w sądownictwie. Element ten, choć dotychczas postrzegany jako nieodłączny, nie jest wskazany w każdym przypadku.

2.2.4 Prawo do obrony

Znaczna większość opisanych rozwiązań wykorzystujących SI w wymiarze sprawiedliwości opiera się na mechanizmie, w którym najpierw przygotowuje się dane wejściowe, następnie są one przetwarzane, po czym otrzymuje się dane wyjściowe. W takim modelu, obrona możliwa jest jedynie na pierwszym etapie i musiałaby wymagać interwencji ludzkiej, przykładowo przygotowując argumenty przeciwko drugiej stronie, przed wprowadzeniem ich do systemu. W takim rozwiązaniu niemożliwe wydaje się zapewnienie prawa do obrony ze strony SI, nawet gdyby hipotetycznie była wykształcona na poziomie, by być do tego zdolna, bowiem na poziomie podmiotowym miałaby miejsce do pewnego stopnia kolizja z zasadą *nemo iudex in causa sua*, co wiąże się z bezstronnością sędziego. Nie może być obrońcą podmiot, który równocześnie odpowiada za werdykt. Aby zachować prawo do obrony, procedura, według której funkcjonowałby system, musiałaby opierać się nie tylko na wprowadzeniu samych faktów, ale też kontrargumentów. Mając na uwadze powyższe, zachowanie prawa do obrony w automatycznych procesach wymiaru sprawiedliwości zależne jest w głównej mierze od aspektów proceduralnych, a przy odpowiednich ich ukształtowaniu, jest możliwe.

[54] P. Zielonka, *Framing, czyli efekt sformułowania*, Decyzje 2017 (27), s. 41-68.

2.2.5 Prawo do skutecznego środka odwoławczego

Zagadnienie prawa do skutecznego środka odwoławczego w odniesieniu do zautomatyzowanego procesu można rozpoznać na dwóch płaszczyznach: możliwości wniesienia odwołania oraz potrzebie jego wniesienia.

W pierwszej kwestii zależy to od podjętych ustaleń. Można zarówno przewidzieć ponowne rozpoznanie z użyciem innego argumentu bądź z inaczej przedstawionymi danymi, jak i powrót do „tradycyjnej" formy w drugiej instancji. Brak jest ograniczeń w tej formie wynikających z automatyzacji, o ile nie przyjmie się za cel absolutnej automatyzacji.

W drugiej kwestii należy odnieść się do zaufania ludzi do wyników pochodzących z komputera. Ilustratywnie, nikt nie podważa poprawności obliczenia kalkulatora, choć mało kto wie, jaki mechanizm przeprowadza kalkulacje. Ludzie są bardziej skłonni zaufać komputerowi[55]. Komputer, robot, czy inne narzędzie automatyzacji, oczywiście nie ma cech ludzkich, a zatem wywołuje to mechanizm, gdzie dana osoba nie obawia się negatywnej oceny, eliminuje się zatem negatywne skutki zjawisk funkcjonujących w społeczeństwie. To zjawisko może być korzystne przy składaniu zeznań. Tak duże zaufanie dla technologii zmniejszyłoby prawdopodobieństwo złożenia apelacji, czego nie sposób jednak uznać za przejaw sprawiedliwości sądu, ponieważ nie nie dotyczyłoby zaufania do sprawiedliwości procesu, a pewności poprawności kalkulacji.

3. WNIOSKI

W samej AIA największymi zagrożeniami są brak w pełni opracowanego mechanizmu testowania systemów SI oraz dopuszczenie oddania do użytku systemów SI, które nie zostały poddane ocenie. Choć ma mieć to miejsce w uzasadnionych przypadkach, może stanowić potencjalne zagrożenie dla praworządności. Podjęte próby automatyzacji procesów decyzyjnych są wciąż pilotażowe, a ich różniące się skutecznością rezultaty nie zwiastują, by autonomiczne rozwiązania będące elementem LegalTech 3.0 na poziomie „silnej" SI weszły w życie powszechnie w najbliższym czasie.

W najogólniejszym znaczeniu, automatyzacja, by była sprawiedliwa, musi zawierać element indywidualizacji pozwalającej na odpowiednie przygotowanie systemu do podjęcia decyzji. Problematyka efektu czarnej skrzynki

[55] https://www.bbc.com/worklife/article/20160412-truth-be-told-were-more-honest-with-robots (dostęp 22.05.2022).

wymaga dokładniejszych ustaleń, zarówno w samej AIA, jak i w odniesieniu samego dogmatycznego elementu jawności procesu. W obecnej formie, proponowane formy automatyzacji wymiaru sprawiedliwości nie spełniają w stopniu satysfakcjonującym tego elementu. Ponadto, pojawiają się obawy dotyczące braku inkluzywności procesu i wiążącego się z tym ryzyka dyskryminacji. W odniesieniu do rozsądności terminu rozpatrzenia sprawy, zautomatyzowane rozwiązania są nieporównywalnie bardziej efektywne w porównaniu do obecnego stanu. Co do niezawisłości i bezstronności, automatyzacja redukuje interferencję heurystyk i błędów poznawczych, ale w niektórych metodach samouczenia się SI, możliwe są ograniczenia wynikające z aspektów lingwistycznych NLP. W przypadku prawa do obrony, przy odpowiednio ukształtowanych aspektach proceduralnych, jego realizacja jest możliwa. Mając na uwadze prawo do skutecznego środka odwoławczego, pozostawione jest szerokie pole do interpretacji tego zagadnienia, umożliwiając różnorakie jego ukształtowanie. Istnieją jednakże zagrożenia, wynikające z dużego zaufania ludzi do komputerów, co znajduje swoje źródło w psychologii.

Automatyzacja wymiaru sprawiedliwości, nawet w formie możliwie jak najbardziej autonomicznej, może stanowić odpowiedź na problemy współczesnego sądownictwa, t.j. długi czas trwania procesu, wysokie koszty postępowania, czy trudności w dostępności. Aby jednak spełniła prawidłowo swoją funkcję, konieczne jest spełnienie wszystkich elementów prawa do sprawiedliwego sądu, co wymaga innego spojrzenia na formę przedmiotową odbywania się decyzji związanych z wymiarem sprawiedliwości. Tym samym AIA, choć odpowiada na liczne obawy związane z SI, będzie wymagać silnego systemu kontroli i aktualizacji, aby wprowadzane do obiegu systemy nie tylko ułatwiły procesy decyzyjne, ale również pozostawały zgodne z prawami człowieka.

BIBLIOGRAFIA

Piśmiennictwo

Aletras, N. et al., Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing Perspective, PeerJ Computer Science, 2:e93.

Araszkiewicz, M., *Sztuczna Inteligencja i prawo do wyjaśnienia,* Trzeci Sektor, 44 (4/2018).

Bublitz, J. C., *What is wrong with hungry judges? A case study of legal implications of cognitive science.* Tom 14, red. A. Watermann et al., Haga, 2018, s. 13.

Criado Perez, C., *Invisible women*, Londyn, 2020, s. 108.

Danziger, S. et al., *Extraneous factors in judicial decisions*, Proceedings of the National Academy of Sciences, 2011, 108/17, s. 6892.

Franciska, Z. et al., *The AI is now in session. The impact of digitalisation on courts.*

Howard, P. N., et al., *Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration,* Journal of Information Technology & Politics 15:2, s 81-92.

Kerikmäe, T., E. Pärn - Lee, *Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race.* AI & SOCIETY, 36, 2021.

Kuśmierczyk, M., *Algorithmic Bias in the Light of the GDPR and the proposed AI Act.* red. M. Olejnik, W. Morawska, Wrocław, 2022, s. 2.

Lewandowski, P., *Sądy dostępne przez Internet. Szanse i zagrożenia,* Fundacja Court Watch Polska 2020, s. 34.

Lührmann, A., *A third wave of autocratization is here: what is new about it?*, Democratization, 2019, 26:7, s. 1096. 2019.

Łuszczyk, M., *Zasada sprawiedliwości w paradygmacie rozwoju trwałego a koncepcja Johna Rawlsa*, Optimum. Studia Ekonomiczne, 4(88), 2017, s. 27.

Medvedeva, M., et al., *Using machine learning to predict decisions of the European Court of Human Rights*, Artificial Intelligence and Law, 2020/28, s. 237-266.

Qiang, X., *The Road to Digital Unfreedom: President Xi's Surveillance State,* Journal of Democracy, 30/1, 2019, s 64.

Rojszczak, M., *Prawne aspekty systemów sztucznej inteligencji – zarys problemu,* [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe,* red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa, 2019.

Szostek, D., *Pojęcie Legal Technology (LegalTech)* [w:] *LegalTech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym*, red. D. Szostek, 2021.

Szostek, D., *The Concept of Legal Technology (LegalTech) and Legal Engineering,* [w:] *LegalTech.*

technology tools in the administration of justice. red. D. Szostek, M. Załucki, Baden-Baden, 2021, s. 20.

Załucki, M., *The road to modern judiciary* [w:] *Internet and New Technologies Law,* Baden-Baden, 2021, s. 165.

Zielonka, P., *Framing, czyli efekt sformułowania*, Decyzje 2017 (27), s. 41-68.

Akty prawne

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).

Wniosek - Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii z dnia 21 kwietnia 2021 r., COM/2021/206 final.

Orzecznictwo

Kudła przeciwko Polsce - wyrok ETPC z dnia 26 października 2000 r., skarga nr 30210/96.

Źródła internetowe:

https://www.bbc.com/worklife/article/20160412-truth-be-told-were-more-honest--with-robots(dostęp 22.05.2022).

https://www.consilium.europa.eu/media/46496/st11481-en20.pdf (dostęp: 22. 05.2022).

https://www.economist.com/essay/2018/09/13/the-economist-at-175 (dsotęp: 22. 05.2022).

https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ (dostęp: 22.05.2022).

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_pl (dostęp: 22.05.2022).

https://www.enisa.europa.eu/risk-level-tool/risk (dostęp: 22.05.2022).

https://www.huffpost.com/entry/legal-technology-30_b_6603658 (dostęp: 22. 05.2022).

https://www.infor.pl/prawo/nowosci-prawne/4673991,Esady-arbitrazowe-polubowne-w-Polsce.html (dostęp: 22.05.2022).

https://prawo.gazetaprawna.pl/artykuly/1491865,court-watch-polska-koronawirus-sadu-raport.html(dostęp: 22.05.2022).

https://www.prawo.pl/prawnicy-sady/brak-pracownikow-sadowych-uderza-w-prace-sadow,507593.html (dostęp: 22.05.2022).

https://ultimaratio.pl/o-sadzie (dostęp: 22.05.2022).

THE RIGHT TO A FAIR TRIAL AND AUTOMATING JUSTICE – PERSPECTIVE IN THE LIGHT OF EU REGULATIONS

Abstract: The dynamic development of artificial intelligence brought about the need for creating legislative regulations for the purpose of future law. The Artificial Intelligence Act is a response to this need, and the process of regulating such a complex and unpredictable issue requires a multidimensional analysis, including one in terms of justice systems and other decision-making processes. This chapter analyses the elements of the commonly understood right to fair trial, simultaneously juxtaposing them with regulations and solutions planned in the Act. Existing forms of broadly understood justice automation are also considered, in regard to LegalTech as a whole, as well as in regard to artificial intelligence. Moreover, weaknesses of the Act in regard to the right to fair trial are outlined.

Keywords: right to a fair trial, Artificial Intelligence Act, LegalTech, artificial intelligence, automation

CZĘŚĆ III.
INTERNET

ADAM RYBCZYŃSKI
UNIWERSYTET GDAŃSKI

WYBRANE PROBLEMY PRAWNE ZWIĄZANE Z FUNKCJONOWANIEM METAWERSÓW

Abstrakt: Obecnie metawersa są coraz bardziej rozpowszechnionym środowiskiem, mającym według entuzjastów tego typu technologii zastąpić istniejące sieci społecznościowe oraz umożliwić każdemu zainteresowanemu funkcjonowanie w zupełnie nowym świecie wirtualnym. Metawersa są rozwinięciem i twórczym przetworzeniem światów tworzonych na potrzeby gier MMORPG, a pionierem na tym polu jest gra *Second Life,* posiadająca rozbudowany system tworzenia dóbr wirtualnych, oraz ich obrotu. W 2021 roku Mark Zuckerberg ogłosił zmianę nazwy swojej spółki na *Meta Platforms Inc.* i zapowiedział dalszą rozbudowę swojego metawersum zwanego jako *Horizon Worlds,* promując je nie tylko jako rozwinięcie już istniejących sieci społecznościowych, ale również miejsce służące do wykonywania pracy. W niniejszej pracy autor skupił się na czterech obszarach, w których funkcjonowanie metawersów może rodzić problemy prawne. W tym celu dokonał podsumowania obecnego reżimu prawnego dotyczącego wskazanych obszarów, a w drugiej części rozdziału wskazał na potencjalne obszary wymagające uregulowania oraz przedstawił swoje propozycje. Te obszary to: Ochrona praw autorskich w metawersach i funkcjonowanie NFT, ochrona nowych typów danych osobowych w metawersach, oświadczenia woli w metawersach, oraz czyny zabronione w metawersach. Tak jak wskazał wcześniej, w każdym z tych obszarów ustawodawca nie wdrożył regulacji prawnych pozwalających na uzyskanie stanu pewności prawnych i każdy z nich wymaga odmiennego podejścia.

Słowa kluczowe: Metawersum, ochrona praw autorskich, oświadczenia woli, czyny zabronione, światy wirtualne, ochrona danych osobowych.

1. WSTĘP

1.1. Założenia pracy

Termin „metawersum[1]" nie jest terminem, który posiada swoją definicję legalną, a definicje słownikowe różnią się w znaczącym stopniu między sobą, co świadczy m.in. o dużej liczbie możliwych interpretacji tego terminu, jak i o tym, że nie jest to zjawisko, które odcisnęło swój ślad w świecie rzeczywistym. Pomimo tego jednak, najwięksi gracze rynkowi w branży mediów społecznościowych na czele z Markiem Zuckerbergiem zauważyli potencjał w nich drzemiący i postanowili zainwestować w tę technologię. Już sam brak definicji legalnej, świadczy o tym, że ustawodawca nie zajął żadnego stanowiska, wobec tego zjawiska, a to oznacza, że w stosunku do metawersów zastosowanie mogą mieć wyłącznie istniejące przepisy prawne, które należałoby w odpowiedni sposób zinterpretować, celem m.in. zapewnienia należytej ochrony podmiotom korzystającym z metawersów bądź należytego egzekwowania oświadczeń woli w nich zawartych. W niniejszej pracy autor podjął się próby przybliżenia terminu „metawersum", wskazując zarówno na etymologię słowa, jak i ukazania wcześniejszych zjawisk i technologii, z których metawersa czerpią zasady działania, i które chcą je twórczo rozwijać. Ponadto autor podjął się wskazania czterech obszarów, w których metawersa nie są zdaniem autora należycie uregulowane pod względem prawnym. W każdym z tych obszarów a są to: własność intelektualna, dane osobowe, oświadczenia woli oraz czyny zabronione autor opisał obecnie funkcjonujący reżim prawny na terytorium RP, z uwzględnieniem regulacji unijnych, a następnie wskazał, w których miejscach w wymienionych obszarach konieczne może okazać się uregulowanie prawne. Jako metodę badawczą autor przyjął, jak wskazano wcześniej analizę obecnego porządku prawnego, oraz wewnętrznych regulaminów funkcjonujących w metawersach, a w szczególności dokonał wykładni celowościowej, celem określenia faktycznych skutków regulacji pochodzących z tych źródeł prawa.

1.2. Definicja metawersum

Mark Zuckerberg 28 października 2021 roku, podczas dorocznego wydarzenia „Connect[2]", postanowił opowiedzieć o przyszłości mediów

[1] W stosunku do tego słowa nie ma jeszcze ujednoliconych zasad pisowni w języku polskim.
[2] https://vrpolska.eu/facebook-connect-2021-podsumowanie-konferencji/ (dostęp 27.11.2022).

społecznościowych. Ogłosił podczas niej, po pierwsze zmianę nazwy spółki na Meta Platforms, Inc. a następnie przedstawił plan rozwoju, który ma polegać na stworzeniu metawersum o nazwie *Horizon Worlds*. Według słów założyciela spółki metawersum to kolejny krok w rozwoju nie tylko sieci społecznościowych, ale zgoła całego Internetu[3]. Metawersum zostało przedstawione jako miejsce, w którym możliwe będzie wszystko to co w dotychczasowych sieciach społecznościowych, a nawet więcej. Kluczową funkcjonalnością ma być tutaj możliwość działania w świecie wirtualnym z użyciem tzw. awatarów, czyli wirtualnych obrazów użytkowników. Rynek zareagował dosyć zachowawczo czego skutkiem był brak większych zmian w wycenie spółki na parkiecie giełdowym po ogłoszeniu tej informacji[4]. Te wszystkie informacje podane wcześniej są fragmentaryczne i nie pozwalają na stworzenie funkcjonalnej definicji metawersum, a tym bardziej definicji legalnej, co może okazać się kluczowe w przyszłym ustawodawstwie mającym na celu uregulowanie tej gałęzi rynku. Pewnych wskazówek co do możliwego zdefiniowania metawersów może dostarczyć lektura stron internetowych powiązanych z *Horizon Worlds*, i na jednej z nich, która należy do spółki Meta pojawia się informacja, że metawersum to „zestaw wirtualnych przestrzeni w których można tworzyć i które można odkrywać z innymi ludźmi niebędącymi w tym samym miejscu przestrzeni rzeczywistej[5]". Z kolei słownik oksfordzki podaje następującą definicję „termin potoczny używany do opisania wirtualnej reprezentacji rzeczywistości za pomocą oprogramowania rzeczywistości wirtualnej[6]". Obydwie te definicje nie podają informacji czy owe światy wirtualne mają za zadanie odwzorować świat rzeczywisty czy mogą się od niego różnić. W niniejszej pracy autor przyjął tę drugą wersję, opierając się na już istniejących metawersach, w których możliwe jest tworzenie konstrukcji oraz wybranie awataru, nie posiadającego odpowiednika w fizycznej rzeczywistości (dla przykładu w jednym z najpopularniejszych metawersów „VR Chat" możliwe jest stworzenie awatara od zera, przy czym użytkownicy nie są ograniczeni do ciał ludzkich).

[3] https://www.facebook.com/Meta/videos/577658430179350/ (dostęp 27.11.2022).
[4] https://finance.yahoo.com/quote/META/ (dostęp 27.11.2022).
[5] W oryginale "The "metaverse" is a set of virtual spaces where you can create and explore with other people who aren't in the same physical space as you.", https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/ (dostęp 04.05.2022).
[6] W oryginale "A slang term used to describe a virtual representation of reality implemented by means of virtual reality software." https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100153307 (dostęp, 04.05.2022).

1.3. Historia metawersów

Źródła dosyć zgodnie podają, że termin „metawersum" pierwszy raz został użyty w powieści science-fiction z 1992 roku „Snow Crash", autorstwa Neal'a Stephensona[7], i już wtedy idea stojąca za tym zjawiskiem była bardzo podobna do tej, do której dąży m.in. Mark Zuckerberg. Przyjmując jednak definicję z poprzedniego punktu, należy uznać, że nie jest on pionierem tego typu rozwiązań, ponieważ występowały one wcześniej w grach określanych jako MMORPG (Massively Multiplayer Online Role-Playing Game). Pozwalały i pozwalają, ponieważ istnieją nadal na tworzenie wirtualnych awatarów, wpisujących się w ramy świata stworzonego przez programistów, które służą do realizacji określonych zadań (m.in. wspólne eksplorowanie świata, tworzenie wirtualnych przedmiotów, walka ze sobą bądź przeciwnikami generowanymi komputerowo[8]). Za jedną z pierwszych gier MMORPG uznaje się produkcję studia *Beyond Software* wydaną przez *Strategic Simulation* a funkcjonującą w ekosystemie sieci *America Online,* grę *Neverwinter Nights*[9] wydaną w 1991 roku, czyli rok przed pierwszym użyciem słowa metawersum. Cel takich gier różni się jednak od tego który przyświeca obecnym konstruktorom technologii metawersów. Przede wszystkim gry te nastawione są na zysk związany z jej dystrybucją (głównie sprzedane kopie, ale również abonamenty pozwalające w daną grę zagrać, bądź sprzedaż wirtualnych przedmiotów w grze za prawdziwą gotówkę), natomiast metawersa współcześnie nie wysuwają na pierwszy plan kwestii opłat. Po drugie w grach typu MMORPG pozycję dominującą ma twórca świata wirtualnego tj. spółka, która daną grę stworzyła, natomiast we współczesnych metawersach obserwuje się trend polegający na oddaniu w ręce użytkownika większej kontroli nie tylko nad awatarem, ale i nad światem, w którym on funkcjonuje. Należy więc uznać, że gry typu MMORPG za pierwszy krok do stworzenia metawersum. Z postępem technologii niektórzy twórcy gier zaczęli stawiać sobie za cel stworzenie świata bardziej przypominającego fizyczną rzeczywistość, w której użytkownicy mieliby więcej swobody w kreowaniu awatarów i relacji pomiędzy nimi. Z takiej

[7] Por. informacje z https://www.washingtonpost.com/technology/2021/08/30/what-is-the-metaverse/; https://medium.com/swlh/the-technology-of-the-metaverse-its-not-just-vr-78fb3c603fe9 (dostęp 04.05.2022).

[8] https://www.masterclass.com/articles/what-does-mmorpg-stand-for (w tym miejscu warto wskazać, iż według tego artykułu pierwszą grą MMORPG jest *Ultima Online,* jednak w istocie jak wskazano poniżej wcześniej wydane zostało m.in. *Neverwinter Nights* (dostęp 27.11.2022).

[9] W. S. Bainbridge, *Berkshire Encyclopedia of Human-Computer Interaction. Vol. 2*. Berkshire Publishing Group 2004, p. 474.

właśnie idei w 2003 narodził się produkt o nazwie *Second Life*[10], będący obecnie (pomijając współczesne próby) najpełniejszą realizacją idei metawersum. W świecie tym użytkownicy (zwani też mieszkańcami), tworzą swoje wirtualne awatary, które funkcjonują w siatce serwerów (czyli systemie połączonych światów wirtualnych), i ich jedynym celem jest funkcjonowanie w nim. Mogą oni również nabywać wirtualną ziemię celem zagospodarowania według swojego uznania (jest to jednak obwarowane koniecznością wydania realnej gotówki) oraz zarabiać realne pieniądze tworząc przedmioty dedykowane tej grze[11]. To w czym *Second Life* jest podobne do wcześniej wspomnianych gier jest model biznesowy. Konta użytkowników podzielone są na dwie kategorie – podstawowe i premium (za te drugie należy uiszczać abonament wysokości kilkunastu dolarów miesięcznie), które daje możliwość pełnego uczestnictwa w świecie pod względem ekonomicznym (wspomniane wcześniej nabywanie wirtualnych terenów). Co warto zaznaczyć *Second Life* jest fenomenem na skalę światową do tego stopnia, że niektóre państwa zdecydowały się otworzyć swoje wirtualne ambasady (pierwszym krajem, który to zrobił były Malediwy w 2007 roku[12]). Podsumowując *Second Life* pozwala w ograniczonym stopniu ze względu na technologię użytą do produkcji funkcjonować w świecie wirtualnym w bardzo podobny sposób jakiego chcieliby współcześni twórcy metawersów.

1.4. Obecny wzrost popularności metawersów

Współcześnie za wzrost medialnej popularności metawersów odpowiada właśnie Mark Zuckerberg, ponieważ kieruje pierwszym tak dużym podmiotem rynkowym, który postawił sobie za cel stworzenie w pełni funkcjonalnego metawersum. Wspomniany wcześniej *Second Life,* pomimo imponującego dorobku, ma pewne ograniczenia, które nie pozwalają w pełni wykorzystać nowych technologii na których ma bazować *Horizon Worlds* (tak obecnie nazywa się metawersum twórcy Facebooka), takich jak NFT, bądź technologie VR (w tym miejscu warto nadmienić, że spółka Meta posiada również jednego

[10] https://wiki.secondlife.com/wiki/History_of_Second_Life (dostęp 27.11.2022).
[11] Jest to możliwe za pomocą strony internetowej udostępnionej przez twórców gry. https://marketplace.secondlife.com/, oraz systemu LindeX będącego miejscem wymiany gotówki z gry na prawdziwe pieniądze
[12] https://www.diplomacy.edu/event/diplomacy-goes-virtual-inauguration-diplomacy-island-and-virtual-embassy-second-life/ (dostęp, 04.05.2022 r.)

z liderów produkcji urządzeń do doświadczania wirtualnej rzeczywistości[13]). Ponadto jak wcześniej wspomniano niebagatelny wpływ na zainteresowanie inwestorów oraz przeciętnych obywateli (w samym 2021 roku na produkcję sprzętu do doświadczania wirtualnych rzeczywistości wydane zostało 10 miliardów dolarów[14], a to nie koniec inwestycji zarówno w warstwę *software,* czyli produkcje programów, jak i *hardware,* czyli ulepszanie sprzętu).

1.5. Problemy prawne stojące przed metawersami

Ze względu na zaawansowanie technologiczne metawersów obecne regulacje prawne nie posiadają odpowiednich narzędzi, żeby w sposób skuteczny regulować działalność tego typu podmiotów, poczynając od braku definicji legalnej metawersum, poprzez rozwiązania prawne dotyczące własności intelektualnej oraz tego co jest czynem zabronionym w takim środowisku, aż do interpretowania oświadczeń woli które mogą być podejmowane w takich światach. Niniejsza praca ma na celu zanalizowanie wybranych aspektów funkcjonowania takich środowisk oraz podjęcie próby rozwiązania niektórych problemów, mogących się pojawić. Na potrzeby tej pracy wspomniane wyżej aspekty zostaną przeanalizowane na przykładzie dokumentów typu *End User License Agreement (EULA)* oraz *Terms of Service* metawersum *Horizon Worlds* będącego powiązanym do Regulaminu Meta[15], oraz porównane z istniejącym stanem prawnym. W zakresie rozwiązań dotyczących własności intelektualnej oraz oświadczeń woli w skład porównania wejdą również analogiczne dokumenty związane ze światem gry *Second Life* i innymi tego typu programami. Warto również w tym miejscu zaznaczyć, że te licencje stanowią podstawę funkcjonowania światów wirtualnych i mogą w bardzo różny sposób kreować pozycję użytkownika końcowego, a brak jest możliwości ich negocjowania ze względu na ich adhezyjny charakter[16].

[13] Spółka *Oculus* została założona w 2012 roku, zaś w 2014 ówcześnie Facebook Inc. zakupił ją za 2 miliardy dolarów. Obecnie spółka nazywa się *Reality Labs.*

[14] https://www.nytimes.com/2022/02/02/technology/meta-facebook-earnings-metaverse.html (dostęp 04.05.2022).

[15] https://www.facebook.com/legal/terms (dostęp 06.05.2022)

[16] J. Zimmer-Czekaj, *Prawa własności intelektualnej w wirtualnych światach*, ZNUJ. PPWI 2009, nr 3, s. 97.

2. WŁASNOŚĆ INTELEKTUALNA W METAWERSACH

2.1. Obecne regulacje prawne dotyczące własności intelektualnej

Aby właściwie przeanalizować możliwości stojące przed twórcami treści podlegającej ochronie w metawersach, należy po pierwsze poznać stan prawny dotyczący praw związanych z własnością intelektualną w Polsce. Aktem prawnym który reguluje ten zakres funkcjonowania rynku jest ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[17]. Główną jego intencją jest ochrona autorów utworów rozumianych w artykule pierwszym wspomnianej ustawy jako każdy przejaw działalności twórczej o indywidualnym charakterze ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia. Warto również wspomnieć, że zgodnie z artykułem 5 ww. ustawy będzie miała ona zastosowanie, do utworów które mają łącznik z RP czy to w postaci polskiego obywatelstwa autora dzieła, miejsca powstania na terytorium RP, bądź języka publikacji. Prawa autorskie podzielone są w myśl ustawy na dwie kategorie – osobiste których katalog znajduje się w artykule 16 ustawy i jest on otwarty (ustawa ogranicza się do wymienienia poszczególnych przypadków, takich jak prawo do autorstwa utworu, oznaczania go swoimi danymi jego nienaruszalności rozumianej jako władzy nad jego treścią oraz praw związanych z udostępnianiem utworu i nadzorem nad jego korzystaniem). Druga grupa praw z kolei odnosi się do komercyjnego wykorzystania utworów (artykuł 17 ustawy określa, że autor ma wyłączne prawo do korzystania z utworu oraz możliwego udostępniania go za wynagrodzeniem bądź bez wynagrodzenia (ww. przypadki mogą być ograniczone jedyne przez ustawę, czego przykładem jest występujące w artykule 29 prawo cytatu[18])). Na marginesie warto dodać, że według polskiego prawa twórcą może być wyłącznie człowiek, co może stanowić problem w przypadku utworów tworzonych z wykorzystaniem narzędzi opartych na sztucznej inteligencji[19]. Kluczowym zagadnieniem jest określenie, kiedy dana

[17] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2021 r. poz. 1062 z późn. zm.).

[18] A. Niewęgłowski, [w:] *Prawo autorskie. Komentarz*, Warszawa 2021, art. 17.

[19] Systemy oparte na uczeniu maszynowym oraz sztucznej inteligencji, pomimo swoich niedoskonałości już teraz potrafią m.in. tworzyć według opisu obrazy https://openai.com/dall-e-2/ (dostęp, 21.05.2022 r.), bądź przy wsparciu profesjonalnych muzyków tworzyć muzykę. W tym ostatnim obszarze odbywają się konkursy, w których systemy oparte o AI mają za zadanie wygenerować utwór muzyczny w stylu Eurowizji, https://www.inside.unsw.edu.au/campus-life/you-little-beauty-australian-team-wins-ai-eurovision-style-song-contest (dostęp 21.05.2022), jednak przeprowadzenie rozważań na ten temat przekracza zakres niniejszej pracy.

aktywność użytkownika w świecie wirtualnym posiada cechy oryginalnej twórczości, a kiedy jest jedynie odtwórczą rekombinacją elementów. Problem ten musi być rozpatrywany w każdym z przypadków osobno, ze względu na bardzo różny stopień swobody użytkowników w zakresie tworzenia wirtualnych przedmiotów (dla przykładu w popularnej grze MMORPG *World of Warcraft* możliwe jest tworzenie postaci wyłącznie z predefiniowanych przez producenta gry elementów co ma przełożenie nie tylko w wyglądzie postaci, którą użytkownik operuje, ale również tworzenia wirtualnych przedmiotów[20]). W tym przypadku element twórczości co do zasady nie występuje, jednak C. Ondrejka w swoim artykule twierdzi, że to stwierdzenie jest prawdą, tylko wtedy, kiedy liczba elementów bazowych jest stosunkowo mała – jeżeli ich liczba jest bardzo duża może pojawić się element twórczości w postaci unikalnego ich połączenia[21]. C. Ondrejka proponuje tutaj wprowadzenie koncepcji własności atomistycznej, używając tutaj analogii do klocków Lego z których można tworzyć unikalne konstrukcje, zawierające w sobie działalność twórczą[22]. Podsumowując w polskim prawie nie istnieją przeszkody, aby uznawać, że wirtualne przedmioty stworzone przez użytkowników nie miałyby korzystać z ochrony na podstawie ustawy o prawach autorskich, jednak zagadnienie jest bardziej skomplikowane ze względu na dokumenty wewnętrzne każdego z metawersów z osobna.

2.2. Własność intelektualna w poszczególnych metawersach

Tak jak wspomniano wcześniej kluczowymi dokumentami warunkującym zasady uczestnictwa w metawersum bądź grze typu MMORPG są *EULA* oraz *TOS*. Na ich gruncie użytkownicy korzystają z dobrodziejstw tzw. „magicznego kręgu", czyli po prostu miejsca gry. Pozwalają one bez przeszkód dopuszczać się zachowań które w świecie realnym mogłyby zostać ukarane a w kontekście działalności artystycznej, tworzyć przedmioty nie mające odpowiedników w świecie rzeczywistym[23]. Każde metawersum oraz gra posiadają swoje własne postanowienia dotyczące własności przedmiotów wytworzonych w grze, i tak umowa licencyjna spółki Blizzard-Activision (będąca właścicielem

[20] https://worldofwarcraft.com/en-us/start (dostęp 27.11.2022).
[21] C. Ondrejka, *Escaping the Gilded Cage: User Created Content and Building the Metaverse,* "New York Law School Law Review" 2004/1, s. 92.
[22] Tamże.
[23] J. Zimmer-Czekaj, *op. cit.*, s. 92 (termin „magiczny krąg" nie odnosi się wyłącznie do rzeczywistości wirtualnych, a może obejmować również określone przestrzenie w rzeczywistości fizycznej, tymczasowo wyjęte spod jurysdykcji prawnej takie jak areny do uprawiania sportów).

wspomnianego *World of Warcraft*) przewiduje przekazywanie praw do treści stworzonych przez użytkownika na jej rzecz[24], podobnie jak w przypadku gry *EVE Online* użytkownik udziela nieodpłatnej i wyłącznej licencji CCP Games będącej twórcą gry[25]). Z kolei w przypadku gry *Second Life* spełniającej więcej kryteriów metawersum i umożliwiającej użytkownikom tworzenie obiektów nie tylko z gotowych elementów dostarczanych przez *Linden Labs,* ale również z importowanych z zewnątrz, brak podobnych zapisów. Zamiast tego twórcy gry pozwalają użytkownikom nie tylko na zachowanie własności stworzonych przedmiotów, ale również na swobodny nimi obrót w kontrolowanym środowisku[26]. Ponadto producenci współpracują bardzo mocno z użytkownikami oraz markami w przypadkach naruszenia własności intelektualnej (m.in. podrabianie markowych produktów[27]). W przypadku przywołanego na początku i będącego punktem odniesienia dla pozostałych usług tego typu *Horizon Worlds* użytkownik udziela licencji na wykorzystywanie wszelkich przejawów jego twórczości skutkujących powstaniem własności intelektualnej spółce *Meta* włącznie z prawem innych użytkowników do ich modyfikacji[28]. Podsumowując oznacza to zmniejszenie swobody użytkowników do dysponowania przejawami swojej twórczości w stosunku do wcześniej przywołanego *Second Life.* Odpowiadając na problemy związane z identyfikacją autora poszczególnych utworów oraz umożliwienia im zarabiania na swoich dziełach spółka produkująca i dystrybuująca *Horizon Worlds* zdecydowała się z kolei na zaimplementowanie w swoim oprogramowaniu technologii NFT (non-fungible tokens)[29].

[24] https://www.blizzard.com/pl-pl/legal/08b946df-660a-40e4-a072-1fbde65173b1/umowa-licencyjna-uzytkownika-koncowego-blizzard-emea (dostęp, 06.05.2022).

[25] https://community.eveonline.com/support/policies/eve-eula-en/ (*EVE Online* jest przykładem gry z bardzo silną i złożoną ekonomią, i miejscem, w którym ww. zakres „magicznego kręgu" jest bardzo duży (Por. J. Zimmer-Czekaj, *Prawa…*, ZNUJ. PPWI 2009, nr 3, s. 95. na której opisany jest przykład oszustw dokonanych przez jednego z użytkowników oraz reakcji wymiaru sprawiedliwości oraz twórców gry na zaistniałe wydarzenie) (dostęp, 06.05.2022).

[26] https://marketplace.secondlife.com/ (dostęp 06.05.2022).

[27] https://marketplace.secondlife.com/listing_guidelines oraz https://www.lindenlab.com/legal/intellectual-property-infringement-notification-policy (dostęp 06.05.2022).

[28] https://store.facebook.com/pl/pl/legal/quest/horizon-terms-of-service/?utm_source=https%3A%2F%2Fl.facebook.com%2F&utm_medium=organicsearch (dostęp 06.05.2022).

[29] https://cryptoslate.com/social-media-giant-meta-eyes-47-5-cut-on-every-nft-sale-in-horizon-worlds/ (w tym miejscu warto również zaznaczyć, iż wedle brzmienia tego artykułu Meta będzie pobierać prawie połowę ceny sprzedaży pojedynczego NFT) (dostęp 27.11.2022).

2.3. Sposób funkcjonowania NFT

NFT to specjalny typ tokenów opartych o technologię blockchain, która powstała w 2017 roku[30], jednak to od roku 2021 notuje się ich gwałtowny wzrost popularności, objawiający się m.in. sprzedażą kolażu znanego artysty Mike'a Winkelmanna na aukcji za 69 milionów dolarów[31]. Tokeny NFT oparte są o technologię blockchain i aby w pełni zrozumieć w jaki sposób funkcjonują, należy wskazać właśnie podstawy działania blockchain (łańcucha bloków). Technologia blockchain powstała w 2008 roku i pierwotnie służyła do obsługi kryptowalut takich jak najbardziej popularny Bitcoin. Łańcuch bloków jest rozproszonym systemem opartym na zasadzie interakcji poszczególnych użytkowników między sobą w systemie *peer-to-peer*[32]. Blockchain rozumiany jako technologia ma za zadanie uporządkować dane wymieniane przez użytkowników właśnie w sieci rozproszonej, czyli takiej która posiada nieznaną ilość użytkowników, których wiarygodność jest nieznana[33]. Robi to za pomocą zapisywania w rejestrze danych związanych z transakcjami[34], opatrzonych cyfrowymi podpisami tzw. hashami, pozwalającymi zachować unikatowość każdej transakcji oraz zabezpieczyć użytkowników przed próbami kradzieży własności zapisanych w takich blokach[35]. Łańcuch bloków może służyć jako narzędzie do potwierdzania własności, i to właśnie ta cecha okazała się kluczowa w użyciu jako narzędzie do przeprowadzania i gromadzenia aktywów w postaci kryptowalut[36]. Tokeny stworzone w standardzie ERC-20 używane w transakcjach na rynku kryptowalut są zamienne na takiej samej zasadzie jak pieniądze[37] (nie jest ważne to którą monetą dokonywana jest płatność pod warunkiem, że będzie miała wartość odpowiadającą cenie przedmiotu), natomiast tokeny stworzone zgodnie ze standardem ERC-721 w przeciwieństwie do poprzednich nie są możliwe do podzielenia oraz nie są wymienialne. Podsumowując tokeny NFT to w istocie tokeny oparte o standard ERC-721 których obrót i własność rejestrowana są za pomocą

[30] N. Urbach, "*NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application"* Fraunhofer Research Center, Finance and Information Management, Fortieth International Conference on Information Systems, Munich 2019, s.1
[31] https://www.latimes.com/business/technology/story/2021-03-11/nft-explainer-crypto-trading-collectible (dostęp, 06.05.2022).
[32] D. Drescher *Blockchain. Podstawy technologii łańcucha bloków w 25 krokach,* wyd. Helion, 2019 rok, s. 31.
[33] Tamże, s. 37.
[34] Tamże, s. 49.
[35] Tamże, s. 78.
[36] Tamże, s. 202.
[37] N. Urbach, *op. cit*, s.3.

technologii blockchain. Ten sposób ich przechowywania jest dodatkową gwarancją bezpieczeństwa dla użytkowników końcowych.

2.4. Wykorzystanie NFT w Horizon Worlds

Cechy, które posiadają ww. tokeny w połączeniu ze sposobem ich przechowywania pozwoliły na rozwiązanie problemu istniejącego w świecie informatyki, wynikającego z własności systemów cyfrowych, brzmiącego następująco: w jaki sposób można osiągnąć sytuację, w której jest możliwe rozpoznanie oryginalnego posiadacza dzieła/autora pliku, jeżeli jego kopia jest pod względem budowy identyczna? NFT służą tutaj jako dowody na przypisanie dzieła do konkretnego autora, co obecnie wykorzystywane jest w świecie sztuki. Niejednokrotnie również posiadanie NFT należącego do określonej kolekcji uprawnia właściciela do określonych benefitów, żeby wspomnieć obecnie jedną z najbardziej popularnych kolekcji *Bored Ape Yacht Club,* którego twórcy udostępniają w tym momencie wirtualną i wspólną przestrzeń do tworzenia graffiti[38]. W przypadku *Horizon Worlds,* twórcy wybrali podobne rozwiązanie i pozwolili użytkownikom na tworzenie wirtualnych galerii sztuki, w których mogą być wystawione dzieła z przypisanym do nich NFT. Pewnych wskazówek co do kierunku rozwoju *Horizon Worlds* może dostarczyć również obserwacja jednego z bardziej znanych metawersów, powstałego w 2015 roku *Decentraland*[39]. W tym metawersum twórcy oddali użytkownikom bardzo dużo swobody, włącznie z możliwością kupowania wirtualnych nieruchomości oraz ustanawiania na nich podatków. Dodatkowo w warunkach użytkowania wyraźnie wskazali, że wszelka twórczość użytkowników, włącznie z utworami posiadającymi NFT, należy tylko i wyłącznie do nich[40]. O ile *Horizon Worlds,* tak jak wspomniano wcześniej nie pozwala na *posiadanie* swoich dzieł (użytkownik udziela licencji), tak umożliwia ich *monetyzację,* czyli czerpanie dochodu ze sprzedaży. Pod względem praw autorskich

[38] https://boredapeyachtclub.com/#/home (dostęp, 09.05.2022).
[39] https://decentraland.org/ (dostęp 27.11.2022).
[40] https://decentraland.org/terms/ (dostęp, 09.05.2022).

w punkcie 3.1 regulamin *Horizon Worlds* wyraźnie wskazuje, że użytkownik zrzeka się do egzekwowania wszelkich praw związanych z byciem autorem[41].

2.5. Podsumowanie

Wobec braku właściwych regulacji dotyczących obrotu NFT, rozliczania dochodów z obrotu NFT, a przede wszystkim regulacji praw autorskich dotyczących przedmiotów stworzonych w metawersach, za konieczność należy uznać uregulowanie tych kwestii zarówno w polskim, jak i międzynarodowym porządku prawnym. Należy przede wszystkim stworzyć definicje pozwalające określić czym w istocie jest NFT w rozumieniu polskiego prawa, umożliwić rozliczenie podatkowe dochodów osiągniętych z obrotu NFT, tak jak to uregulowano w zakresie kryptowalut (pomimo tego że NFT to w istocie inny rodzaj tokenów mających z kryptowalutami wspólne źródło, to właśnie ich niewymienialność oraz powiązanie z prawami autorskimi stanowią wyzwanie), a także wdrożyć regulacje na poziomie międzynarodowym, które pozwolą m.in. uniknąć niepewności związanych z rozliczaniem dochodów które osiąga polski użytkownik, dokonujący transakcji na terenie metawersum, które jest zarządzane przez spółkę z USA.

3. DANE OSOBOWE W METAWERSACH I ICH OCHRONA

3.1. Obecny reżim prawny ochrony danych osobowych w Polsce

Prawo dotyczące danych osobowych jest pochodną prawa do prywatności, będącego uznawanym za jedno z podstawowych praw człowieka. Ze względu na obecność Polski w Unii Europejskiej oraz organizacjach międzynarodowych, ochronę danych osobowych będzie regulować nie tylko prawodawstwo krajowe, ale również szereg dokumentów międzynarodowych. Jednym z podstawowych jest Międzynarodowy Pakt Praw

[41] https://store.facebook.com/pl/legal/quest/horizon-terms-of-service/ (…) W możliwie największym zakresie dozwolonym przez prawo użytkownik zrzeka się i zobowiązuje się nie egzekwować żadnych praw znanych pod nazwą „praw osobistych", „praw twórcy", „autorskich praw osobistych" lub innych tego typu praw do takich treści. (dostęp, 10.05.2022); Dodatkowy problem związany z monetyzacją, którego dokładne rozważenie przekracza ramy niniejszego tekstu jest związany z odpowiednim zakwalifikowaniem dochodów pochodzących ze sprzedaży NFT dla celów podatkowych. Obecnie nie istnieje jednolita podstawa prawna, która regulowałaby tę kwestię, podejmowane są jednak próby polegające na zakwalifikowaniu ww. dochodów jako przychodów z praw autorskich, a następnie opodatkowanie tak jak kryptowalut, zgodnie ze stanowiskiem Ministerstwa Finansów https://www.podatki.gov.pl/pit/rozliczenie-ze-sprzedazy-kryptowalut/#podstawa-opodatkowania (dostęp, 21.05.2022).

Obywatelskich i Politycznych, który w artykule 17 stanowi, że każdy ma prawo do ochrony prywatności, oraz możliwość prawnego przeciwdziałania jej naruszeniu[42]. Aktem prawnym o regionalnym zasięgu terytorialnym i odnoszącym się już bezpośrednio do ochrony danych osobowych jest Konwencja Rady Europy z 28 stycznia 1981 roku, ratyfikowana przez Polskę w 2002 roku[43]. W niej też można zaobserwować pierwszą próbę ujęcia w aktach prawa międzynarodowego czym są dane osobowe. Zostały one zdefiniowane w artykule 2, w punkcie a) jako „Każda informacja dotycząca osoby fizycznej o określonej tożsamości lub dająca się zidentyfikować". Przechodząc do regulacji na poziomie unijnym, kluczowe będzie rozporządzenie o danych osobowych (dalej RODO)[44] mające kluczowe znaczenie i obowiązujące na terenie całej wspólnoty. Jest ono o tyle ważne, że definicja danych osobowych zawarta w rozporządzeniu jest stosowana również przez ustawodawcę w Polsce. Ochrona danych osobowych i prywatności w krajowym porządku prawnym oparta jest na stosowaniu artykułów 47, 49 oraz 51 Konstytucji RP[45], oraz na ustawie o ochronie danych osobowych[46]. Ustawa ta jednak służy implementacji i dostosowaniu polskiego prawa do regulacji unijnych, a w szczególności właśnie RODO. Podsumowując, w Polsce najważniejszym i najbardziej kompleksowo regulującym aktem prawnym dotyczącym ochrony danych osobowych jest RODO uzupełnione przez ustawę o ochronie danych osobowych i rozporządzenia wykonawcze do ww. ustawy[47].

3.2. Ochrona danych osobowych w metawersach

Aby należycie rozpatrzyć sposób ochrony oraz określić czy dana informacja jest daną osobową należy rozpocząć od przywołania definicji

[42] Międzynarodowy Pakt PRAW OBYWATELSKICH I POLITYCZNYCH otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167).
[43] Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 z późn. zm.).
[44] 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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).
[45] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.).
[46] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).
[47] I tak np. rozporządzeniem wykonawczym będzie Rozporządzenie Rady Ministrów z dnia 20 marca 2019 r. w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych (Dz.U. 2019 poz. 697).

legalnej. Za dane osobowe uznaje się według RODO wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[48]. Według doktryny, aby daną informację zakwalifikować jako daną osobową należy spełnić kumulatywnie następujące przesłanki: musi to być informacja[49], musi ona dotyczyć, czyli „być o", osobie fizycznej, co oznacza, że np. w stosunku do zmarłych nie istnieją informacje mogące być zakwalifikowane jako dane osobowe, a ostatnią przesłanką musi być możliwość zidentyfikowania osoby fizycznej której dotyczy informacja[50]. Podczas użytkowania metawersów, użytkownicy zmuszeni są do podania informacji stanowiących dane osobowe, takich jak wiek, imię, nazwisko czy płeć, tak jak przy sieciach społecznościowych i są one chronione na podstawie RODO oraz wewnętrznych regulaminów[51]. Niektóre metawersa pozwalają jednak na aktywniejsze uczestnictwo w Internecie, poprzez wykorzystanie technologii związanych z VR, takich jak okulary wirtualnej rzeczywistości. Za ich pomocą możliwe jest przekazywanie informacji i nastroju, za pomocą nowych sposobów takich jak mimika twarzy czy gesty[52]. W tym momencie powstaje problem prawny czy takie informacje podlegają ochronie, ponieważ nie należą bezpośrednio do osoby fizycznej,

[48] RODO, art. 4, p. 1).

[49] Termin ten może mieć różne znaczenia, natomiast w kontekście ochrony danych osobowych oznacza to skatalogowane i sformalizowane fakty, które mogą zostać przetworzone, zinterpretowane bądź rozpowszechnione dalej, por. P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679 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) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* wyd. II, Warszawa 2022, art. 4. (dostęp, 09.05.2022).

[50] D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018, art. 4. (dostęp 09.05.2022).

[51] https://store.facebook.com/pl/legal/quest/horizon-terms-of-service/ (1.1.d. regulaminu: „Użytkownik musi podać dokładne i aktualne informacje (w tym dane rejestracyjne), do których mogą się zaliczać dane osobowe. Użytkownik nie może podszywać się pod inną osobę", w punkcie 1.3 regulowany jest zakres udostępniania danych podmiotom trzecim, w tym konkretnym przypadku reklamodawcom, i według zapewnień regulaminu dane te są przed udostępnieniem zanonimizowane w odpowiedni sposób.) (dostęp 27.11.2022).

[52] Obecnie możliwe jest to w ograniczonym zakresie w *Horizon Worlds* bądź wspomnianej wcześniej *VR Chat*, który jest pod tym względem najprawdopodobniej najdoskonalszym narzędziem do odwzorowania gestów i mimiki postaci, przy czym nie muszą być one nawet ludźmi.

ale awatara, którego jednak użytkownik kontroluje. Jednym z niewielu miejsc w którym ustawodawca pochyla się nad tą kwestią, chociaż też nie bezpośrednio, jest motyw 30 RODO, w którym wspomina się o przypisaniu do osób fizycznych identyfikatorów internetowych które w połączeniu ze swoistym zachowaniem użytkownika w platformie pozwalają na jego identyfikacje[53]. Można przypuszczać, że właśnie te nowe typy danych takie jak mimika twarzy, gesty bądź tembr głosu mogą podlegać ochronie na tej podstawie – obecnie jednak w orzecznictwie unijnym nie pojawiła się sprawa, która dotyczyłaby naruszenia tej nowej kategorii danych osobowych.

Warto w tym miejscu wspomnieć, że RODO, pomimo że jest dosyć kompleksową regulacją, nie zawsze będzie miało zastosowanie do użytkowników metawersów. Zgodnie z artykułem 3, ustępem 3, RODO nie będzie miało zastosowania, jeżeli podmiot będący właścicielem metawersum nie będzie miał jednostki organizacyjnej na terenie, gdzie prawo międzynarodowe publiczne wskaże zastosowania prawa członkowskiego Unii. Wtedy kluczowe obok zapisów państwa właściwego stają się przepisy regulaminów poszczególnych produktów, i tak w *Horizon Worlds* w punkcie 4.3 regulaminu wspominane jest, że administrator nagrywa „na żywo" zachowanie użytkownika, celem przeciwdziałania łamaniu prawa oraz regulaminu usługi[54]. Jest to jeden z najbardziej rygorystycznych regulaminów istniejących w metawersach i akurat w przypadku *Horizon Worlds,* możliwa będzie ochrona danych osobowych na podstawie RODO, jednak tak jak wspomniano użytkownicy mogą mieć problem w przypadku platform mających siedzibę na terenach państw, które nie posiadają tak zaawansowanych mechanizmów ochrony danych osobowych.

3.3. Podsumowanie

Jak wskazano w rozdziale, kwestia danych osobowych w metawersach rodzi wiele problemów, i jest mocno nieuregulowana. Jedną z dróg która może rozwiązać ten problem jest globalizacja prawa ochrony danych osobowych, poprzez podpisanie nowych konwencji międzynarodowych poświęconych temu zagadnieniu. Pozwoli to na uniknięcie sytuacji, w której użytkownicy

[53] Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób, RODO motyw 30.

[54] https://store.facebook.com/pl/legal/quest/horizon-terms-of-service/ (dostęp, 10.05.2022).

funkcjonujący w metawersach posiadaliby słabszą bądź silniejszą ochronę, w zależności od miejsca, w którym podmiot administrujący metawersum posiada swoją siedzibę. Ponadto warto również rozważyć wprowadzenie uregulowań odnoszących się w sposób *stricto* do metawersów, odrębnych od uregulowań dotyczących prawa właściwego, tak aby nie była możliwa sytuacja w której wykorzystując luki prawne, spółka administrująca metawersami przetwarzała i udostępniała dane osobowe w sposób sprzeczny z brzmieniem RODO, wykazując że owe dane osobowe są przypisane do *awatara* nie zaś rzeczywistej osoby w związku z czym nie podlegają tak rygorystycznej ochronie.

4. OŚWIADCZENIA WOLI[55] I ICH FORMY W METAWERSACH

4.1. Obecny reżim prawny dotyczący form oświadczeń woli

Następna klasa problemów prawnych które mogą występować w metawersach jest związana z oświadczeniami woli które są istotnymi elementami czynności prawnych. Obecnie w polskim systemie prawa oświadczenia woli mogą zostać podzielone według skutków ich niedochowania (na formę pod rygorem nieważności, dla celów dowodowych oraz dla wywołania szczególnych skutków prawnych[56]) oraz według sposobu ich składania. Według drugiego sposobu można wyróżnić następujące formy oświadczeń woli: dokumentową, pisemną, elektroniczną oraz pisemną kwalifikowaną która dzieli się na formę pisemną z urzędowym poświadczeniem daty, urzędowym poświadczeniem podpisu oraz formę aktu notarialnego. Istnieją również formy składania oświadczeń woli które nie widnieją w kodeksie cywilnym, takie jakie mają zastosowanie m.in. przy zawarciu małżeństwa, jednak nie będą one przedmiotem rozważań w niniejszej pracy.

Forma dokumentowa jest najpopularniejszą oraz najprostszą formą składania oświadczeń woli. Została ona uregulowana w artykule 77^2 Kodeksu Cywilnego[57] (dalej KC), i polega ona na złożeniu oświadczenia woli na

[55] W niniejszym rozdziale autor posługuje się zwrotem „Forma oświadczenia woli" zamiast „Forma czynności prawnych", za doktryną, por. (…)„W doktrynie stwierdzono przy tym, że lepiej posługiwać się ściślejszym zwrotem „forma oświadczenia woli" niż mniej precyzyjną nazwą ustawową „forma czynności prawnych", ponieważ w rzeczywistości tylko istotny element każdej czynności prawnej, jakim jest oświadczenie woli, może być ujęty w określonej formie, na co zresztą wyraźnie wskazał sam prawodawca w art. 78 i 79, odnosząc formę do „treści oświadczenia woli". W *M. Maciejewska-Szałas [w:] Kodeks cywilny. Komentarz,* red. M. Balwicka-Szczyrba, A. Sylwestrzak, Warszawa 2022, art. 73.

[56] Tamże.

[57] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2020 r. poz. 1740 z późn. zm.).

dokumencie, którym zgodnie z artykułem 77^3 KC, jest każdy nośnik informacji pozwalający zapoznać się z treścią dokumentu, w sposób który pozwala zidentyfikować osobę która składa oświadczenie. Wspomniana definicja jest szeroka i pozwala ona na zakwalifikowanie jako dokumentu zarówno materiałów wideo z oznaczoną osobą, jak i nagrań audio z umieszczonym oświadczeniem woli. W kontekście metawersów natomiast należy rozważyć sytuację, w której oświadczenie woli składa awatar określonej osoby fizycznej. Według autora tekstu oświadczenie woli wyrażone w ten sposób można zakwalifikować jako złożone w formie dokumentowej, ponieważ dane przypisane do awataru takie jak wiek, imię, nazwisko, oraz wspomniane wcześniej identyfikatory o naturze internetowej takie jak adres IP, pozwalają ustalić kto składa oświadczenie woli. Forma dokumentowa w przypadku niedochowania opatrzona jest rygorem dowodowym (ad probationem)[58].

Forma elektroniczna oznacza każde oświadczenie woli które zostało złożone w formie elektronicznej oraz opatrzone kwalifikowanym podpisem elektronicznym[59]. Podpis elektroniczny musi spełniać szereg przesłanek, żeby zostać uznany za kwalifikowany, a jego obszar jego zastosowania związany jest z ograniczeniami technicznymi twórców podpisów. Obecnie najpopularniejszą formą składania podpisów elektronicznych jest opatrywanie dokumentów w formacie .pdf takim podpisem[60]. Forma elektroniczna cieszy się taką samą ochroną prawną jak forma pisemna, ale pod warunkiem opatrzenia jej owym podpisem. W kontekście metawersów nie jest obecnie możliwe złożenie oświadczenia woli w formie elektronicznej (żaden system nie wspiera „wewnątrz" takiej funkcjonalności). Forma elektroniczna opatrzona jest podobnie jak forma dokumentowa rygorem dowodowym.

Forma pisemna zgodnie z artykułem 78 KC polega na złożeniu podpisu pod treścią dokumentu, na którym utrwalono oświadczenie woli, a do zawarcia umowy, wystarczy wymiana dokumentów, z których każdy opatrzony jest podpisem jednej ze stron. Obecnie nie istnieje definicja legalna podpisu, jednak doktryna i orzecznictwo przez szereg lat wypracowały definicję, według której podpis to znak graficzny, wykonany własnoręcznie przez składającego oświadczenie woli, za pomocą pisma, obejmujący imię i nazwisko

[58] Podawane rygory występują w sytuacjach, w których ustawodawca nie przewidział szczególnego rygoru (i tak na przykład, ustanowienie pełnomocnictwa ogólnego zgodnie z artykułem 99 KC wymaga jest formy pisemnej, jednak ustawodawca przewidział rygor nieważności w przypadku niedochowania formy w miejsce stosowanego przy formie pisemnej rygoru dowodowego)

[59] Kodeks Cywilny, art. 78^1.

[60] https://esign.pl/blog/jak-wyglada-podpis-elektroniczny/ (dostęp 27.11.2022).

składającego, zawierający indywidualne cechy charakteru pisma[61]. Obecnie uznaje się również, że złożenie podpisu na ekranie dotykowym, który pozwala na wygenerowanie pliku obejmującego treść dokumentu oraz unikalne cechy charakteru pisma, za akceptowalne w obrocie prawnym[62]. Forma pisemna w swojej najbardziej typowej postaci obarczona jest rygorem dowodowym.

Forma pisemna posiada również formy kwalifikowane, w przypadku których rygor niedochowania obejmuje nieważność całej czynności prawnej. Takimi formami są – forma pisemna z datą pewną, forma pisemna z podpisem notarialnie poświadczonym oraz akt notarialny. W przypadku formy pisemnej z datą pewną, potwierdzenie daty można uzyskać w dwojaki sposób – pierwszym z nich będzie urzędowe poświadczenie daty przez notariusza. Drugą drogą jest potwierdzenie daty w związku z wystąpieniem określonych zdarzeń przewidzianych w ustawie[63]. Kolejną formą kwalifikowaną jest forma pisemna z urzędowym poświadczeniem podpisu. W tym przypadku podpis poświadcza notariusz[64]. Ostatnią formą kwalifikowaną jest forma aktu notarialnego. Akt notarialny to dokument sporządzany przez notariusza, aplikanta notarialnego bądź zastępcę notarialnego, którego konstrukcja, oraz sposób sporządzenia określony jest w prawie o notariacie, a w szczególności w artykułach od 91 do 95[65]. Ustawodawca określił ten sposób jako konieczny przy dokonywaniu m.in. zbycia nieruchomości czy umowy zobowiązującej do zbycia spadku (odpowiednio artykuł 158 oraz 1052 KC).

Poszczególne kwalifikowane formy pisemne ułożone są w taki sposób, że jedna forma zawiera się w drugiej, i tak dokument z podpisem notarialnie poświadczonym jest również dokumentem z datą pewną, którą stwierdza notariusz przy poświadczaniu podpisu, a akt notarialny jest również dokumentem woli z podpisem notarialnie poświadczonym. Podsumowując struktura oświadczeń woli w polskim porządku prawnym oparta jest przede wszystkim o podpis składany czy to fizycznie na papierze czy to na dokumentach

[61] M. Maciejewska-Szałas, [w:] *Kodeks cywilny*…, red. M. Balwicka-Szczyrba, A. Sylwestrzak, Warszawa 2022, art. 78.

[62] P. Nazaruk, [w:] *Kodeks cywilny. Komentarz*, red. J. Ciszewski, Warszawa 2019, art. 78.

[63] Do takich zdarzeń zgodnie z artykułem 81 §2 oraz §3 KC należy zaliczyć – stwierdzenie dokonania czynności przez dokumenty urzędowe, umieszczenia na dokumencie wzmianki przez organ państwowy, organ jednostki samorządu terytorialnego lub notariusza, opatrzenia dokumentu kwalifikowanym podpisem elektronicznym ze znacznikiem czasu (nie wszystkie podpisy elektroniczne oferują tę funkcjonalność), bądź śmierci osoby składającej podpis.

[64] Nie zawsze wymagana jest poświadczenie akurat przez notariusza, ponieważ istnieją przypadki, w których to sąd może potwierdzić podpis, tak jak w artykule 1018 KC, stanowiącym o złożeniu oświadczenia o przyjęciu bądź odrzuceniu spadku. Takie wypadki są jednak wyjątkowo rzadkie.

[65] Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie (t.j. Dz. U. z 2020 r. poz. 1192 z późn. zm.).

elektronicznych. Formom pisemnym, szczególnie w ich kwalifikowanej postaci jest przypisywana największa doniosłość prawna, ze względu na rodzaj czynności prawnych do których są wymagane.

4.2. Potencjalne problemy związane z obecnym porządkiem prawnym dotyczącym oświadczeń woli

We wstępie wspomniano o ambicjach właściciela spółki Meta, który chciałby, aby jego metawersum *Horizon Worlds,* stało się nie tylko nową siecią społecznościową, doskonalszą od wcześniejszych, ale również miejscem, w którym możliwe będzie podejmowanie pracy, a co za tym idzie dokonywanie obrotu profesjonalnego. Wzbudza to nie tylko nadzieje wśród potencjalnych podmiotów zainteresowanych chociażby przeniesieniem swoich biur w przestrzeń wirtualną (zwłaszcza że od 2020 roku obserwuje się coraz większe zainteresowanie pracą zdalną zarówno ze strony pracodawców jak i pracowników[66], na co wpływ miała pandemia COVID-19), ale również obawy co do kształtu m.in. zawierania umów w świecie wirtualnym, miejsca i sposobu funkcjonowania kancelarii prawnych, oraz tego jak i czy urzędy mogą działać w świecie wirtualnym.

Tak jak wspomniano wcześniej obecnie w metawersach zastosowanie ma praktycznie wyłącznie forma dokumentowa, co związane jest z niemożnością wykorzystania formy elektronicznej (metawersa nie obsługują kwalifikowanych podpisów elektronicznych, a producenci systemów kwalifikowanych podpisów elektronicznych nie wprowadzili możliwości podpisywania dokumentów stworzonych w metawersach*)*, co oznacza że w przypadku zawarcia przykładowo umowy kupna przedmiotu dla awatara, możliwa jest jedynie ograniczona możliwość ochrony prawnej użytkowników, mogących paść ofiarą nadużyć. Z prawnego punktu widzenia transakcja nabycia wirtualnej czapki za ułamek dolara chroniona jest w ten sam sposób co kupno parceli z nieruchomością wartą miliony dolarów. Powoduje to niespójność, ze względu na różne potraktowanie transakcji mających ten sam przedmiot obrotu, w zależności od miejsca, w którym jest ona dokonywana. Użytkownicy którym zależy na jak największej ochronie transakcji, ze względu na trudności związane z wyegzekwowaniem swoich środków w przypadku oszustów postanowili stworzyć system który miałby ich ochronić przed tego typu problemami,

[66] https://knowledge.clickmeeting.com/uploads/2021/04/praca_zdalna_kwiecien_2021.pdf (dostęp: 11.05.2022).

i obecnie coraz więcej transakcji dokonywanych jest w formule tzw. *smart contractu*.

Smart contract jest programem bądź protokołem dokonującym zautomatyzowanego przekazania własności po spełnieniu określonych warunków, a za jego najwcześniejszy przykład uznaje się automaty z jedzeniem. Obecnie są one bardziej zaawansowane i opierają się na zapisie treści transakcji w blockchainie Etherum[67]. Według zwolenników tej metody, umieszczenie umowy w publicznie dostępnym miejscu, a jednocześnie odporność na zmiany osiągnięta dzięki decentralizacji i zastosowaniu algorytmów rozwiązujących problem bizantyjskich generałów[68] pozwala na bezpieczne zawieranie transakcji, które nie wymagają udziału pośredników, włącznie z notariuszami. Przeciwnicy tej metody wskazują z kolei na niemożność ukrycia treści umowy przed innymi uczestnikami rynku, czego niejednokrotnie oczekują uczestnicy rynku oraz brak ochrony w przypadku funkcjonowania kodu posiadającego niewykryte luki bezpieczeństwa. Obecnie *smart contracty* nie są uwzględnione w polskim porządku prawnym, jednak według autora należy się spodziewać w przyszłości ich oficjalnego uwzględnienia w obrocie prawnym[69].

Specyfika zawierania *smart contractów* stawia pytanie, o adekwatność funkcjonowania notariuszy w systemie prawnym. Zwolennicy ograniczenia ich roli argumentują to w następujący sposób: skoro treść umowy jest oparta o wydarzenia ustalone przez samych uczestników transakcji, jej konstrukcja wymaga więcej wiedzy na temat programowania (ustawienie odpowiednich warunków wywołania określonych zdarzeń), a zdecentralizowane algorytmy dają prawdopodobieństwo sięgające pewności że treść umowy nie zostanie sfałszowana, i zostanie ona wyegzekwowana to uczestnictwo pośrednika

[67] https://www.ibm.com/topics/smart-contracts (dostęp 27.11.2022 r.)

[68] Problem bizantyjskich generałów został sformułowany w 1990 roku i przedstawia się następująco: Grupa armii bizantyjskich otacza miasto nieprzyjaciela. Rozkład sił jest taki, że jeśli wszystkie armie zaatakują razem, to będą w stanie zdobyć miasto. Innym sposobem uniknięcia porażki jest odwrót wszystkich armii. Generałowie poszczególnych armii mają zaufanych posłańców, którzy z powodzeniem dostarczą każdy komunikat od jednego generała do innego. Jednak niektórzy generałowie mogą być zdrajcami usiłującymi doprowadzić do porażki armii bizantyjskich. Należy opracować algorytm, który umożliwi wszystkim wiernym generałom uzgodnienie pewnego planu działania. Ostateczna decyzja powinna być z grubsza taka, jaka zostałaby podjęta w drodze głosowania większościowego nad decyzjami poszczególnych generałów. W przypadku nierozstrzygnięcia głosowania końcową decyzją ma być odwrót. *(Mordechai Ben-Ari: Podstawy programowania współbieżnego i rozproszonego.* Warszawa: Wydawnictwa Naukowo-Techniczne, 2009, s. 238.) Algorytmy rozwiązujące ten problem przewidują albo wzmocnienie głosu jednego z generałów, albo wymianę dużej liczby komunikatów informujących czego dany generał dowiedział się od innych.

[69] Tak jak w 2017 roku zrównano status prawny *smart contractów* z klasycznymi umowami na terenie Białorusi https://www.fxmag.pl/artykul/dolina-krzemowa-na-bialorusi-raj-dla-kryptowalut (dostęp 11.05.2022).

w postaci notariusza jest niepotrzebne, a wręcz może stwarzać problemy i ryzyko oszustw (jedną z idei stojącą za stworzeniem *smart contractów* było wyeliminowanie pośredników, którzy w Internecie mają większą możliwość popełniania oszustw). Przeciwnicy z kolei wskazują na niejednolitość ochrony transakcji o podobnej wartości pieniężnej w zależności od tego czy dokonywana jest w świecie wirtualnym czy rzeczywistym. Ponadto wyrażają wątpliwość dotyczącą ochrony transakcji i uważają, że niezależny czynnik ludzki, cieszący się zaufaniem publicznym jest niezbędny, aby wyeliminować potencjalne ryzyko fałszerstwa. Autor tekstu skłania się ku stanowisku kompromisowemu – nie neguje on argumentów natury technologicznej przywoływanych przez zwolenników wyeliminowania funkcji notariusza. Przyznaje on rację jednak osobom, które uważają, że czynnik ludzki powinien się pojawić, jednak postuluje daleko idące zmiany w sposobie funkcjonowania notariuszy w świecie wirtualnym, polegające na ograniczeniu formalizmu. Proponuje on przykładowo, możliwość nagrania momentu zawarcia *smart contractu,* a następnie przechowywania jej w bazie danych. Takie nagranie służyłoby jako poręczenie faktu, i usunęło formalizm związany z podpisaniem aktu notarialnego przez Internet.

Kolejnym zagadnieniem mogącym sprawiać problemy jest funkcjonowanie urzędów i innych organów administracji publicznej w metawersach. Znane są przypadki otwierania wirtualnych przedstawicielstw, tak jak ambasada Szwecji w *Second Life*[70]. Należy jednak ocenić to działanie bardziej jako symbol i informacje o tym, że rząd szwedzki ma świadomość istnienia metawersów, ponieważ w ramach swojej działalności nie przeprowadza procesów zwykle związanych z działalnością ambasady, a jedynie informuje o tym w jaki sposób można skontaktować się ze swoim odpowiednikiem w życiu rzeczywistym, oraz dostarcza informacje o charakterze kulturalnym swojego kraju[71]. Obecnie sytuacja się nie zmieniła i wszelkie takie przedstawicielstwa mają charakter informacyjno-kulturalny, nie są natomiast miejscem, w którym obywatele mogliby załatwić swoje sprawy. Należy spodziewać się, że w przypadku wzrostu popularności metawersów, coraz większa część obywateli będzie spędzać coraz więcej czasu w środowiskach wirtualnych a brak dostępności urzędów może stanowić dla nich problem. Autor postuluje w następującej sytuacji dwa działania, które mogłyby urzeczywistnić ideę załatwiania spraw w świecie wirtualnym. Po pierwsze zmianę regulacji prawnych

[70] https://www.reuters.com/article/us-sweden-secondlife-idUSL3034889320070530 (dostęp: 12.05.2022).
[71] Tamże.

w zakresie postępowania administracyjnego, która dopuszczałaby tę formę kontaktu, w sposób analogiczny do załatwiania spraw przez Internet, a następnie stworzenie architektury technicznej która pozwalałaby na używanie podpisów elektronicznych do podpisywania dokumentów przesyłanych przez awatary osób fizycznych w metawersach.

Funkcjonowanie przedsiębiorstw i kancelarii prawnych w opinii autora mogłoby działać podobnie. Zaimplementowanie podpisów elektronicznych dopuściłoby możliwość zawierania umów w formie elektronicznej, gdyż nawet według obecnego prawa taka forma zrównana jest z formą pisemną, a w określonych wypadkach nawet z formą pisemną z datą pewną. W przypadku transakcji, które wymagałyby notarialnego potwierdzenia podpisu bądź sporządzenia aktu notarialnego, autor postuluje zmiany w zakresie prawa o notariacie podobne do tych o których wspomniał w miejscu omawiania *smart contractów.* Poprawiłoby to zarówno pewność obrotu prawnego w przypadku transakcji dobrami wirtualnymi o znacznej wartości (na przykład wirtualnych parcel), zlikwidowało niejednolitość ochrony prawnej ze względu na środowisko zawierania umowy oraz zlikwidowało swoistą szarą strefę, która może zniechęcać inwestorów do wkroczenia w ten nowy, obiecujący sektor rynku.

Podsumowując oświadczenia woli w metawersach są w polskim (i nie tylko) porządku prawnym nieuregulowane. Ustawodawca nie podjął próby uporządkowania tej strefy, co obecnie wzbudza niepewność podmiotów zainteresowanych działaniem w zgodzie z prawem, a jednocześnie chcących funkcjonować na tym nowym rynku, również pod względem obrotu profesjonalnego (z innymi przedsiębiorcami). Postulowane przez autora działania są jedną z propozycji i nie obejmują całościowej próby regulacji prawnej funkcjonowania oświadczeń woli w tym środowisku, ponieważ przekraczałoby to ramy publikacji[72].

[72] Jednym z problemów który również może wymagać uregulowania, jest kwestia prawa właściwego, w przypadku, gdy awatar z kraju A dokona czynności prawnej w środowisku państwa B (przy okazji pojawia się problem następującej treści – czy państwo powinno móc posiadać terytorium w metawersach, a jeżeli tak to na jakich zasadach), zarządzanym przez spółkę z kraju C, z innym podmiotem w kraju D.

5. CZYNY ZABRONIONE W METAWERSACH

5.1. Obecny reżim prawny dotyczący czynów zabronionych w Polsce

W Polsce prawo karne oparte jest o ustawę z 1997 roku – Kodeks Karny[73], ale nie jest to wyłączne źródło przepisów mających charakter represyjny w systemie prawa, ponieważ odnaleźć można w innych ustawach, nawet tak odległych jak prawo atomowe, bądź też wspomniane we wstępie prawo autorskie. Ustawodawca w artykule 1, § 1 kodeksu karnego, nie podał definicji legalnej czynu zabronionego – ograniczył się do opisania, że dany czyn musi zostać uznany za zabroniony przez ustawę, a aby ponieść odpowiedzialność karną, musi on być uznany za zabroniony w trakcie jego trwania. W doktrynie przyjmuje się, że aby dany czyn zabroniony został uznany za przestępstwo, musi spełnić łącznie następujące warunki: musi to być czyn realizujący znamiona określone w ustawie karnej, musi naruszać normę, czyli być bezprawnym, musi być społecznie szkodliwy, bardziej niż w stopniu znikomym, musi być zawiniony, oraz musi być zagrożony karą w ustawie[74]. Pierwszą przesłanką jest przesłanka czynu tj. zewnętrznego zachowania człowieka które jest wyrazem jego woli (nie znajduje się pod tzw. *vis absoluta,* czyli sytuacją fizycznego przymusu bądź stanu wyłączającego świadome podejmowanie decyzji)[75]. Druga przesłanka jest związana z zasadą praworządności i oznacza, że nie można sankcjonować czynów w akcie prawnym niebędącym ustawą (np. rozporządzeniem). Kolejna przesłanka oznacza, że czyn wyraźnie musi być wyrażony w ustawie, i nie jest dopuszczona wykładnia rozszerzająca w celu określenia czy dany czyn spełnia przesłanki przestępstwa[76]. Społeczna szkodliwość odnosi się w tym przypadku do zjawiska, w którym zachowanie działa demoralizująco na społeczeństwo. Według doktryny zawinienie odnosi się do sytuacji, w której sprawcę ocenia się na podstawie szeregu czynników zewnętrznych m.in. jego wiek, czy znajdował się w stanie wyższej konieczności, czy popełnił usprawiedliwiony błąd. Ostatnia przesłanka dotyczy z kolei ustawodawcy oraz organu stosującego prawo i kieruje wobec nich postulat umieszczenia w ustawie konkretnych sankcji, które mogą być zastosowane wobec sprawcy

[73] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2021 r. poz. 2345 z późn. zm.).
[74] Por. J. Giezek, [w:] D. Gruszecka, K. Lipiński, G. Łabuda, J. Giezek*, Kodeks karny. Część ogólna. Komentarz,* Warszawa 2021, art. 1 oraz M. Mozgawa, M. Budyn-Kulik, P. Kozłowska-Kalisz, M. Kulik [w:] M. Mozgawa, M. Budyn-Kulik, P. Kozłowska-Kalisz, M. Kulik*, Kodeks karny. Komentarz aktualizowany,* LEX/el. 2022, art. 1.
[75] Tamże.
[76] Tamże.

przestępstwa, oraz możliwość wymierzenia przez sąd tylko tych sankcji, które wcześniej umieścił tam ustawodawca[77].

5.2. Problemy związane z definicją czynu zabronionego w metawersum

W kontekście funkcjonowania metawersów istotne jest to, że nie został wprowadzony podział na środowisko popełnienia przestępstwa – równie dobrze może on funkcjonować w świecie wirtualnym co i rzeczywistym, co oznacza, że istnieje możliwość po pierwsze popełnienia przestępstwa w metawersum, a po drugie ścigania go w zgodzie z porządkiem prawnym (pod warunkiem spełnienia przesłanek wymienionych w poprzednim akapicie). W polskim porządku prawnym, najwięcej do tej pory przestępstw było ściganych w związku z kradzieżą przedmiotów wirtualnych w grach MMORPG[78]. Druga kategoria przestępstw najczęściej występująca w światach wirtualnych to przestępstwa związane ze sferą seksualną, takie jak publikowanie treści pornograficznych z udziałem małoletnich czy to w formie animacji, czy zgoła odgrywania ról osób małoletnich dokonujących czynności seksualnych[79]. Podkreślić należy, że w tych przypadkach na wskutek braku regulacji prawnych, większa odpowiedzialność spoczywa na twórcach metawersów, którzy mogą szybciej i bardziej skutecznie zareagować na tego rodzaju zachowania[80]. Twórcy metawersów umieszczają również odpowiednie zapisy w swoich regulaminach, zabraniające m.in. umieszczania treści o charakterze pornograficznym w swoich usługach, jednak wspomnieć należy, że maksymalną karą na tej podstawie może być jedynie wyrzucenie z metawersum i nałożenie zakazu uczestnictwa w nim w przyszłości (który obecnie można dosyć łatwo obejść, korzystając m.in. z rozwiązań ukrywających znaczniki internetowe takie jak IP czy państwo, z którego następuje połączenie).

Podsumowując system prawny w Polsce w ocenie autora nie posiada rozwiązań, które w wystarczającym stopniu chroniłyby ofiary przestępstw

[77] J. Giezek [w:] D. Gruszecka, K. Lipiński, G. Łabuda, J. Giezek, *Kodeks karny…,* Warszawa 2021, art. 1.

[78] J. Kulesza, *Prawo karne w wirtualnych światach,* PiP 2014, nr 5, s. 46-47, i w przykładach wymienionych w artykule najczęściej wymierzano karę pozbawienia wolności z warunkowym jej zawieszeniem.

[79] Tamże, s. 53, ww. zachowania istniały w *Second Life,* czyli w grze będącej najbliżej współczesnych metawersów pod względem możliwości, co umożliwia spojrzenie na to jakie zachowania mogą występować w przyszłości i być bliższe rzeczywistości co związane jest bezpośrednio z techniką w jakiej metawersa są tworzone

[80] https://www.euronews.com/next/2022/02/06/preventing-another-gang-rape-is-facebook-s-new-tool-enough-to-stop-sexual-assault-in-the-m (w tym przypadku twórca metawersum sam dodał narzędzie po otrzymaniu zgłoszenia o napastowaniu seksualnym w swoim świecie).

w metawersach. Najczęściej i najbardziej skutecznie ścigane są przestępstwa o charakterze majątkowym takie jak kradzieże przedmiotów wirtualnych, w czym pomaga fakt, że niejednokrotnie uzyskiwane są za prawdziwą gotówkę. Nie istnieją jednak dokładne przepisy dotyczące ingerencji w sferę seksualną użytkowników metawersów, i to w tym zakresie regulacje prawne mogą okazać się potrzebne.

6. ZAKOŃCZENIE

Obecnie metawersa stanowią technologię, z którą wiele podmiotów, zarówno z sektora prywatnego, jak i publicznego wiąże nadzieję, i mogą być postrzegane zarówno jako naturalne rozwinięcie istniejących już sieci społecznościowych, jak i zupełnie nowe miejsca podejmowania działalności nie tylko biznesowej, ale również społecznej. Coraz szersza obecność metawersów w społeczeństwie obecnie wydaje się nieunikniona, a co za tym idzie coraz więcej będzie występować sytuacji, które nie są należycie uregulowane w systemie prawnym. Szczególnie wiele uwagi zdaniem autora należy poświęcić uregulowaniu sytuacji prawnej oświadczeń woli oraz umożliwić podmiotom działającym w metawersach podejmowanie działalności gospodarczej w warunkach stabilności i pewności prawa. Istnienie metawersów, a co za tym idzie nowych sposobów ekspresji zarówno artystycznej, jak i dotyczącej funkcjonowania awatarów (wykorzystywanie technologii VR), już teraz stwarza sytuacje, które wymagają od ustawodawców pilnego działania, tak jak w przypadku danych osobowych, których nowe typy są zdaniem autora niewystarczająco mocno uregulowane. Podobne wnioski można wyciągnąć w stosunku do egzekwowania oraz funkcjonowania praw autorskich wykorzystujących NFT – ustawodawca polski ogranicza się do kopiowania rozwiązań stosowanych przy obrocie kryptowalut, ponieważ nie był w stanie wypracować unikalnych zastosowań, które odpowiadałyby na potrzeby podmiotów zajmujących się w sposób profesjonalny tworzeniem przedmiotów w wirtualnych światach. Polski ustawodawca nie uważa metawersów za sferę, która wymagałaby dodatkowych regulacji, w obszarze oświadczeń woli, co zmniejsza ilość podmiotów chcących w większym stopniu przenieść swoją działalność do świata wirtualnego. Odnosząc się do przestępstw popełnianych w metawersach, należy wskazać, iż najwięcej uwagi wymiar sprawiedliwości poświęcał jak dotąd przypadkom kradzieży przedmiotów wirtualnych, wykazując bierność w zakresie regulacji dotyczących przestępstw związanych z seksualnością, podczas gdy podobne

regulacje istnieją i są wykorzystywane w państwach ościennych takich jak Niemcy.

BIBLIOGRAFIA

Akty prawne:

Międzynarodowy Pakt PRAW OBYWATELSKICH I POLITYCZNYCH otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167).

Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 z późn. zm.).

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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2020 r. poz. 1740 z późn. zm.).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2021 r. poz. 2345 z późn. zm.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie (t.j. Dz. U. z 2020 r. poz. 1192 z późn. zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2021 r. poz. 1062 z późn. zm.).

Publikacje naukowe i artykuły:

Bainbridge W.S., *Berkshire Encyclopedia of Human-Computer Interaction*, Vol. 2. Berkshire Publishing Group, 2004.

Kodeks cywilny. Komentarz, red. J. Ciszewski, Warszawa 2019.

Drescher D. *Blockchain. Podstawy technologoii łańcucha bloków w 25 krokach*, Helion, 2019.

Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 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)*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022.

Gruszecka D., Lipiński K., Łabuda G., Giezek J., *Kodeks karny. Część ogólna. Komentarz*, Warszawa 2021.

Kulesza J., *Prawo karne w wirtualnych światach*, PiP 2014, nr 5.

Lubasz D., Chomiczewski W., Czerniawski M., i in. [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018.

Maciejewska-Szałas M. [w:] *Kodeks cywilny. Komentarz*, red. M. Balwicka-Szczyrba, A. Sylwestrzak, Warszawa 2022.

Mordechai B. *Podstawy programowania współbieżnego i rozproszonego,* Warszawa 2009.

Mozgawa M., Budyn-Kulik M., Kozłowska-Kalisz P., Kulik M., *Kodeks karny. Komentarz aktualizowany*, LEX/el. 2022.

Niewęgłowski A. [w:] *Prawo autorskie. Komentarz*, Warszawa 2021.

Ondrejka C., *Escaping the Gilded Cage: User Created Content and Building the Metaverse*, "New York Law School Law Review" 2004/1.

Urbach N., "*NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application"* Fraunhofer Research Center, Finance and Information Management, Fortieth International Conference on Information Systems, Munich 2019

Zimmer-Czekaj J., *Prawa własności intelektualnej w wirtualnych światach*, ZNUJ. PPWI 2009, nr 3.

Strony internetowe:

https://vrpolska.eu/facebook-connect-2021-podsumowanie-konferencji/

https://www.facebook.com/Meta/videos/577658430179350/

https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/

https://finance.yahoo.com/quote/META/

https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100153307

https://www.washingtonpost.com/technology/2021/08/30/what-is-the-metaverse/

https://medium.com/swlh/the-technology-of-the-metaverse-its-not-just-vr-78fb-3c603fe9

https://www.masterclass.com/articles/what-does-mmorpg-stand-for

https://wiki.secondlife.com/wiki/History_of_Second_Life

https://marketplace.secondlife.com/

https://www.diplomacy.edu/event/diplomacy-goes-virtual-inauguration-diplomacy--island-and-virtual-embassy-second-life/

https://www.nytimes.com/2022/02/02/technology/meta-facebook-earnings-metaverse.html

https://openai.com/dall-e-2/

https://www.inside.unsw.edu.au/campus-life/you-little-beauty-australian-team-wins-ai-eurovision-style-song-contest

https://worldofwarcraft.com/en-us/start

https://www.blizzard.com/pl-pl/legal/08b946df-660a-40e4-a072-1fbde65173b1/umowa-licencyjna-uzytkownika-koncowego-blizzard-emea

https://community.eveonline.com/support/policies/eve-eula-en/

https://marketplace.secondlife.com/listing_guidelines

https://www.lindenlab.com/legal/intellectual-property-infringement-notification--policy

https://store.facebook.com/pl/pl/legal/quest/horizon-terms-of-service/?utm_source=https%3A%2F%2Fl.facebook.com%2F&utm_medium=organicsearch

https://cryptoslate.com/social-media-giant-meta-eyes-47-5-cut-on-every-nft-sale-in--horizon-worlds/

https://www.latimes.com/business/technology/story/2021-03-11/nft-explainer-crypto-trading-collectible

https://boredapeyachtclub.com/#/home

https://cryptoslate.com/social-media-giant-meta-eyes-47-5-cut-on-every-nft-sale-in--horizon-worlds/

https://decentraland.org/terms/

https://store.facebook.com/pl/legal/quest/horizon-terms-of-service/

https://esign.pl/blog/jak-wyglada-podpis-elektroniczny/

https://www.podatki.gov.pl/pit/rozliczenie-ze-sprzedazy-kryptowalut/#podstawa-opodatkowania

https://store.facebook.com/pl/legal/quest/horizon-terms-of-service/

https://knowledge.clickmeeting.com/uploads/2021/04/praca_zdalna_kwiecien_2021.pdf

https://www.ibm.com/topics/smart-contracts

https://www.fxmag.pl/artykul/dolina-krzemowa-na-bialorusi-raj-dla-kryptowalut

https://www.reuters.com/article/us-sweden-secondlife-idUSL3034889320070530

https://www.euronews.com/next/2022/02/06/preventing-another-gang-rape-is-facebook-s-new-tool-enough-to-stop-sexual-assault-in-the-m

SELECTED LEGAL ISSUES OF METAVERSES

Abstract: In our times metaverses are increasingly popular worlds, and according to enthusiasts, they are designed to replace existing social networks, and allow to everyone interested work and live in this whole new virtual environment. Metaverses are extension of worlds, created for MMORPG games. Second Life is now probably the most advanced world, focused not in playing virtual game, but on creating and monetization of virtual goods. In 2021 Mark Zuckerberg has announced that his company name will switch to Meta Platforms Inc. and will focus on further development of his metaverse called Horizon Worlds. In announcement he described that Horizon World will be not only extension of social network but also the perfect platform for working. In this paper author has looked at four areas in which there is a lack of law regulation. To accomplish this, he firstly described and summarized current law situation, and in second part of chapter, pointed sample issues which need to be regulated and presented his proposals. These areas are protecting author rights, and how NFT are working, protection of new type of personal data in metaverses, declarations of will in metaverses and prohibited acts in metaverses. As he pointed out earlier in every area legislator has not introduced acts of law, which could answer these problems, and every area needs a different approach.

Key words: Metaverse, copyright protection, declarations of intent, prohibited acts, virtual worlds, personal data protection.

EMILIA JANKIEWICZ
UNIWERSYTET WARSZAWSKI

DEMOKRACJA W ŚWIECIE NOWYCH TECHNOLOGII - POLITYCZNA ROLA MEDIÓW SPOŁECZNOŚCIOWYCH A PRAWO

Streszczenie: Artykuł przedstawia wpływ nowych technologii, a zwłaszcza mediów społecznościowych, na funkcjonowanie demokratycznego państwa, ze szczególnym uwzględnieniem kształtowania za ich pomocą opinii publicznej oraz prowadzenia polityki. Artykuł zawiera opis zagrożeń jakie stwarzają nowe technologie w kontekście prawidłowego działania demokracji i szanowania demokratycznych wartości. Autorka przedstawia wady i zalety politycznego wykorzystywania mediów społecznościowych oraz postulaty zmian prawa, by w mediach społecznościowych szanowane były wartości, takie jak wolność słowa czy pluralizm polityczny.

Słowa kluczowe: demokracja, nowe technologie, media społecznościowe, polityka, algorytmy

1. WPROWADZENIE

Nowe technologie zdominowały współczesny świat i wkroczyły do niemal każdej dziedziny życia człowieka. Aktualnie trudno sobie wyobrazić funkcjonowanie bez licznych urządzeń, aplikacji i platform, które wspierają codzienność. Szczególną rolę w tym nowoczesnym świecie pełni Internet wraz z portalami społecznościowymi, takimi jak Facebook czy Twitter. Przy pomocy portali i stron internetowych społeczeństwo komunikuje się ze sobą bez przeszkód geograficznych, robi zakupy korzystając ze sklepów w sieci, prowadzi internetowe konta bankowe, czy też korzysta z dostępnych tam rozrywkowych treści. Trudno opisać wszystkie aspekty i dziedziny życia

człowieka na jakie wpływ ma dostęp do wirtualnej rzeczywistości. Z racji tak szerokiego i silnego oddziaływania nowych technologii na każdą dziedzinę życia społeczeństwa, nie budzi szczególnego zdziwienia fakt, że wpływają one również na sposób działania organów państwowych, komunikację na linii obywatel – państwo czy na sposób prowadzenia polityki. W związku z coraz powszechniejszym wykorzystywaniem wirtualnych form aktywności i narzędzi przez obywateli oraz instytucje państwowe, pojawiają się pojęcia odnoszące się do tego zjawiska, na przykład pojęcie społeczeństwa informacyjnego[1], w którym szczególnie ceniony jest dostęp do informacji oraz pojęcie e-demokracji. Jeśli chodzi o elektroniczną demokrację (e-demokrację), to należy ją rozumieć jako: „każdy system polityczny, w którym używa się komputerów i sieci komputerowych do realizacji podstawowych funkcji demokratycznych, takich jak informowanie i komunikacja, artykulacja interesów oraz proces decyzyjny"[2]. Wydaje się, że zmiany, które dokonują się w życiu publicznym poprzez zastosowanie nowych technologii, nie są obojętne dla stanu demokracji. Zależności między rozwojem nowych technologii a funkcjonowaniem demokracji oraz możliwe skutki tej relacji, były i nadal stanowią przedmiot rozważań badaczy. Dla przykład Anthony Wilhelm wyróżnił trzy podejścia do zjawiska rozwoju nowoczesnych mediów we współczesnych demokracjach[3]. Pierwsze z wyróżnionych przez niego podejść – neofuturyzm, to podejście optymistyczne, zwracające uwagę na to, że rozwój Internetu sprzyja zmniejszaniu się dystansu między obywatelami a politykami oraz może zwiększać partycypację społeczną i rzeczywiste wykorzystywanie form demokracji bezpośredniej. Drugie podejście, które zaprezentował – dystopia, to stanowisko krytyczne, wskazujące na problem istnienia grup pozbawionych dostępu do sieci lub nieumiejących sprawnie korzystać z narzędzi informatycznych, co może wobec takich grup powodować negatywne następstwa informatyzacji, jakimi będzie cyfrowe wykluczenie oraz przeciążenie informacyjne. Ostatnia z wyróżnionych postaw – technorealizm, pozwala dostrzegać zarówno plusy, jak i minusy rozwoju działalności w wirtualnej przestrzeni. Wydaje się, że podejście technorealizmu najbliższe jest prawidłowemu zdiagnozowaniu demokratycznej rzeczywistości w świecie nowych technologii, która dostarcza argumenty zarówno za pozytywnym, jak i negatywnym wpływem na demokrację.

[1] L. Koćwin, *Wyzwania i problemy kreacji społeczeństwa informacyjnego w Polsce*, [w:] *Praktyki komunikacyjne*, red. Jolanta Kędzior, Wrocław, 2019, s. 98-101.
[2] J. Rzuciło, *Elektroniczny rząd. Aspekty konstytucyjnoprawne*, Warszawa, 2015, s. 133.
[3] K. Brzoza, *Polskie posłanki VII kadencji Sejmu w sieci internetowej*, [w:] *Technopolityka w świecie nowych mediów*, red. M. K. Zwierżdżyński, M. Lakomy, K. Oświecimski , Kraków, 2015, s. 72-73.

Mimo kłopotów z jednoznaczną oceną, na ile wpływ nowych technologii jest dla państwa i stanu demokracji korzystny, nie budzi wątpliwości, że nowe technologie silnie oddziałują na sprawowanie władzy, komunikację czy prowadzenie kampanii politycznych[4]. Wyjątkową rolę na tym polu odgrywają portale społecznościowe i to głównie tym stronom internetowym zostaną poświęcone dalsze rozważania. W początkowym okresie wzrostu fenomenu mediów społecznościowych wiązano z nimi duże nadzieje na polepszenie stanu demokracji, ale dostrzegano też, że nie są one wolne od zagrożeń: „po okresie euforii, kiedy miano nadzieję, że media społecznościowe mogą zapoczątkować złoty okres globalnej demokracji, wielu badaczy zaniepokoiło się faktem, iż media te zaczną podważać demokrację, naruszać prawa i wolności człowieka, wpływać destrukcyjnie na stan debaty publicznej. […] Z jednej strony, media społecznościowe stały się ważnym instrumentem dla wykluczonych dotychczas z debaty przez media tradycyjne, pełniące role strażnika. Z drugiej jednak – media te niebędące ze swojej natury ani demokratycznymi, ani niedemokratycznymi stanowią atrakcyjne, tanie i anonimowe narzędzie wykorzystywane przez aktorów państwowych i niepaństwowych do rozpowszechniania szkodliwych treści”[5]. Obserwując debatę publiczną w mediach społecznościowych dostrzeżono zatem, że nie jest to idealny środek komunikacyjny oraz może on zostać wykorzystany zarówno w pozytywnym, jak i negatywnym oddziaływaniu na demokrację.

Relacja między rozwojem nowych technologii a funkcjonowaniem demokratycznego państwa wydaje się warta uwagi zwłaszcza dlatego, że proces przenoszenia ludzkich aktywności do sieci postępuje i nic nie wskazuje na to, by miał się zatrzymać. Istotności problemu zasługuje na przedstawienie i opisanie dostrzegalnych zalet i wad takiego stanu. To, że nie można już lekceważyć oddziaływania świata wirtualnego na polityczną rzeczywistość, raczej nie powinno budzić wątpliwości. Na to zjawisko nadal jednak zdaje się nie reagować prawo, które nie jest wystarczająco dostosowane zarówno do szans, jak i zagrożeń stwarzanych przez nowe technologie. Można odnieść wrażenie, że państwa tworząc prawo zapominają o postępie, jaki nowe technologie spowodowały w politycznej rzeczywistości. Portale społecznościowe, są szczególnie przez prawo niekontrolowane, pomimo ich zwiększającej się roli politycznej. Choć sfera politycznej partycypacji i aktywności obywateli jest co do zasady regulowana przez państwa tak, by respektowane były ważne

[4] T. Gajowniczek, *Internet w komunikowaniu politycznym*, Media - Kultura - Komunikacja Społeczna 2020, tom *2* nr 15, 53–67.
[5] A. Demczuk, *Wolność wypowiedzi w społeczeństwie informacyjnym*, Lublin, 2020, s. 266.

dla demokracji wartości (np. wolność słowa, pluralizm polityczny, prawa człowieka czy społeczeństwo obywatelskie), to regulacje te często nie nadążają za nowym internetowym światem oraz wyzwaniami ochrony demokracji w tym świecie. Warto więc przedstawić relację między rozwojem nowych technologii (ze szczególnym uwzględnieniem roli portalów społecznościowych) oraz standardami demokratycznymi, zastanawiając się nad oceną tych powiązań, a także nad tym, jak stosunki te powinny wpływać na prawo w demokratycznym państwie.

2. TECHNOLOGIE A NOWOCZESNE PAŃSTWO

Żyjąc w świecie niesamowicie nowoczesnym, wykorzystującym nowe technologie w tak wielu aspektach życia, nie można nie dostrzegać zalet jakie ze sobą niosą. Pozytywnych aspektów nie brakuje również, jeśli chodzi o wpływ nowych technologii na funkcjonowanie państwa oraz stan demokratycznych standardów. Docenić należy, że Internet dostarcza wielu narzędzi, które mogą posłużyć do usprawnienia i rozwinięcia komunikacji między państwem a obywatelami oraz do zwiększania zaangażowania obywateli w sprawy państwa. Ogromne znaczenie ma również zwiększenie dostępu do informacji, ułatwianie organizowania się społeczeństwa i intensyfikacja debaty publicznej. Wymienione możliwości są niezwykle istotne z punktu widzenia urzeczywistniania zasad demokratycznego państwa prawa oraz praw i wolności politycznych jednostki. W takim kontekście możemy mówić o powstaniu wspomnianej już elektronicznej demokracji, w której prawie każdy obywatel ma dostęp do treści prezentowanych przez partie polityczne oraz organizacje społeczne, jak również może wyrażać swoje opinie, komentarze i formułować propozycje dotyczące prezentowanych mu informacji[6], co jest bez wątpienia zjawiskiem bardzo pozytywnym. Uwypuklając korzystne cechy korzystania z nowych technologii, niektórzy wskazują nawet, że: „elektroniczna demokracja uważana jest za swoiste antidotum na negatywne zjawiska społeczne związane z kryzysem demokracji, takie jak malejąca frekwencja w wyborach, spadek zaufania do państwa, władzy czy partii politycznych”[7]. Szansa na zwiększenie uwagi obywateli co do spraw publicznych oraz ich partycypacji w sprawowaniu władzy jest realna, gdyż narzędzia internetowe pozwalają znacznie ograniczyć wysiłki, jakie zainteresowany musi włożyć. Wizja tego,

[6] W. M. Maziarz, *Społeczny wymiar społeczeństwa informacyjnego*, Szczecin, 2020, s. 106.
[7] *Ibidem,* s. 107.

że większość czynności związanych z uczestniczeniem w życiu politycznym może dokonać się bez wychodzenia z domu, może skutecznie zachęcać.

Wykorzystywanie nowych technologii sprzyja również zasadzie otwartego rządu. Zasada otwartego rządu, powiązana z tworzeniem się społeczeństwa obywatelskiego, służy realizacji bardzo ważnej zasady konstytucjonalizmu demokratycznego, jaką jest suwerenności narodu[8]. Władze, które chcą opierać swoje działania na tej zasadzie, muszą uwzględniać to, że obywatele powinni dysponować wiedzą, informacjami o sprawach publicznych oraz móc realnie kontrolować piastunów organów państwowych. W tym zakresie Internet staje się nieocenionym wsparciem, jako pole do komunikacji oraz źródło wiedzy, dziki czemu elitom sprawującym władze coraz trudniej ukryć cokolwiek przed społeczeństwem. Oprócz aspektu informacyjnego, pojęcie „otwartego rządu" obejmuje także partycypację w sprawowaniu władzy. Partycypacja ta jest znacznie łatwiejsza przy wykorzystaniu narzędzi, jakie dostarczają nowe technologie[9]. Można wyróżnić kilka płaszczyzn dzięki którym nowe technologie zwiększają szanse większej liczbie obywateli na realne uczestniczenie w sprawowaniu władzy. Po pierwsze portale społecznościowe pozwalają na stałe kontrolowanie i ocenianie polityków i przywódców politycznych, po drugie stwarzają szansę na grupowanie się i łączenie obywateli wokół wspólnych interesów, wreszcie dają impuls do rozważań nad wprowadzeniem internetowych metod partycypacji. Możliwości w tym zakresie są różne, dla przykładu może to być zorganizowanie internetowych referendów czy prowadzenie za pośrednictwem sieci konsultacji publicznych (jako przykład można wskazać inicjatywę rządu Finlandii, który stworzył portal konsultacyjny umożliwiający podmiotom rządowym i samorządowymi uzyskanie opinii obywateli[10]). Wykorzystanie Internetu może też sprzyjać zwiększeniu skuteczności korzystania z obywatelskiej inicjatywy ustawodawczej, a może nawet pozwolić zorganizować e-wybory, które mogłyby cieszyć się większą frekwencją niż te odbywające się w tradycyjny sposób. Wprowadzenie tak innowacyjnych rozwiązań na ten moment wydaje się trudnym wyzwaniem, głównie z racji tego, że wymagałoby to gruntownych zmian obowiązującego prawa, w dodatku często na poziomie konstytucyjnym. Jednak uwzględniając nieustanny postęp życia oraz to, że rozwiązania te stwarzają szanse na zwiększenie aktywności obywateli, a dodatkowo mogą nawet pozwolić na zminimalizowanie ekonomicznych

[8] J. Rzuciło, *op. cit.,* s. 35.
[9] *Ibidem*, s. 35-36.
[10] W. M. Maziarz, *op. cit.,* s. 109.

kosztów tych demokratycznych procedur[11], to należy zakładać, że władze ustawodawcze będą się starały wypracowywać korzystne zmiany prawa w przyszłości.

Celowe wydaje się rozwinięcie wątku zwiększenia aktywności politycznej obywateli oraz współdziałania ich ze sobą, zwłaszcza biorąc pod uwagę to, jak ważne jest, by w demokratycznym państwie mogły działać różne stowarzyszenia, ruchy społeczne i partie polityczne, skupiające ludzi o odmiennych poglądach i potrzebach. Demokratyczne państwo powinno umożliwiać obywatelom swobodne wypowiadanie się na ważne dla nich tematy oraz zabieranie głosu w dyskusji politycznej. Korzystanie z Internetu dostarcza wielu możliwości w tym zakresie, jak słusznie zauważono: „technologia informacyjno-komunikacyjna w poważnym stopniu zdefiniowała charakter aktywności politycznej obywateli, zwiększając zaangażowanie obywateli, nadając jej powszechny wymiar i umożliwiając rzeczywisty wpływ na funkcjonowanie społeczeństwa obywatelskiego. Jeszcze nie tak dawno aby zamanifestować swoje przekonanie polityczne, społeczne czy religijne, konieczne było osobiste uczestnictwo na różnego rodzaju manifestacjach czy zebraniach. Obecnie swoje poglądy każdy obywatel może przedstawić w sieci na forach dyskusyjnych, portalach czy serwisach społecznościowych, a ich odbiór będzie bardzo szeroki”[12]. W przywołanym fragmencie celnie wskazano, jak wiele upraszcza dostęp do internetowej polityki. Co więcej, dzięki portalom społecznościowym znacząco zwiększa się udział w polityce młodych ludzi, co daje nadzieje na wzrost odsetka zainteresowanych sprawami publicznymi w przyszłości oraz stopniową poprawę frekwencji podczas kolejnych wyborów powszechnych[13]. Przeniesienie partycypacji społeczeństwa do nowej sieciowej rzeczywistości to jednak nie tylko zalety, ale również ryzyko, że np. część ludzi zostanie wykluczona z racji swojego nieprzystosowania do korzystania z nowych technologii. Jak zauważono[14], mowa tu zwłaszcza o osobach starszych, dla przykładu, w Polsce część osób wciąż pozostaje poza wspólnotą ludzi aktywnych online lub ma niskie umiejętności korzystania z Internetu. Przy projektowaniu i rozwijaniu metod partycypacji politycznej obywateli w sieci, warto analizować

[11] Ł. Brzezicki, *Czy e-demokracja i rozwiązania znane ze świata biznesu są właściwymi kierunkami zmian politycznych w Polsce?*, Horyzonty Polityki 2021, tom 12 nr 39, s. 41-66.
[12] W. M. Maziarz, *op. cit.,* s. 106.
[13] M. Boyke, *Media społecznościowe a demokracja*, 2021, https://glospokolenia.pl/2021/02/media-spolecznosciowe-a-demokracja/ [dostęp: 20.05.2022 r.].
[14] G. Rydlewski, *Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji*, Warszawa, 2021, s. 54-55.

i uwzględniać nie tylko korzyści z nich płynące, ale również słabości, tak by nie doprowadzić do wykluczenia części społeczeństwa.

Podkreślenia wymaga też to, że w demokratycznym państwie bardzo ważny jest dostęp do zróżnicowanych i rzetelnych źródeł informacji. Znaczenie informacji dla prawidłowego działania demokratycznego państwa jest dostrzegane zarówno w Europie jak i na świecie. Przykładowo można wskazać, że w USA obowiązuje specjalny akt umożliwiający dostęp do informacji - Freedom of Information Act[15], z kolei w Polsce dostęp do informacji, zwłaszcza do informacji publicznej, przyznany jest obywatelom już na poziomie konstytucyjnym, mówią o nim art. 54 ust. 1 oraz art. 61 Konstytucji RP[16]. W tym zakresie Internet również jest przydatnym i korzystnym narzędziem, pozwalającym ponad granicami państw, bez udziału pośredników, pozyskiwać zróżnicowane informacje. Co więcej, daje także możliwość efektywniejszego korzystania z informacji publicznej, w tym z coraz liczniejszych internetowych rejestrów publicznych, co znacznie ułatwia kontrolę rządzących[17]. Jednak czerpanie wiedzy tylko za pośrednictwem nowych mediów, jakimi są między innymi portale społecznościowe, nie jest pozbawione poważnych wad i zagrożeń, o czym mowa w dalszej części artykułu. Nowoczesne techniki dają wiele narzędzi do sprawniejszego zarządzania państwem i mogą wspierać funkcjonowanie demokracji choćby przez opisany powyżej szeroki dostęp do informacji, o jakim przed dobą Internetu ciężko było marzyć. Niestety ponieważ taki sposób czerpania wiedzy nie jest wolny od negatywnych następstw, które zostaną wskazane w dalszej części, władze państwowe powinny odpowiednio szybko reagować odpowiednimi regulacjami prawa na pojawiające się nowinki techniczne i dbać, by nie zagrażały demokratycznemu społeczeństwu[18]. Niestety należy stwierdzić, że władze państwowe działają w tym zakresie ze znacznym opóźnieniem, co stwarza zagrożenie dla demokratycznych standardów.

3. INTERNET JAKO WIRTUALNE OKNO NA ŚWIAT

Jak już zostało to zaznaczone, w kontekście funkcjonowania demokratycznego państwa bardzo ważnym elementem jest dostęp do informacji.

[15] H. Izdebski, *4. Prawo dostępu do informacji publicznej* [w:] *Doktryny polityczno-prawne. Fundamenty współczesnych państw*, Warszawa, 2021, https://sip.lex.pl/#/monograph/369496157/63/izdebski-hubert-doktryny-polityczno-prawne-fundamenty-wspolczesnych-panstw?keyword=Freedom%20of%20Information%20Act&unitId=passage_20525 (dostęp: 06.12.2022).
[16] Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483).
[17] G. Rydlewski, *op. cit.,* s. 59-60.
[18] J. Rzuciło, *op. cit.,* s. 319-320.

Możliwości jakie daje Internet w zakresie dostępu do informacji są zdumiewające, zwłaszcza w porównaniu ze stanem sprzed doby Internetu. Rola tradycyjnych mediów coraz bardziej maleje w stosunku do siły jaką nabierają na tym polu strony internetowe. Zwłaszcza młodsze pokolenia czerpią informację przede wszystkim z sieci. I tutaj olbrzymią rolę pełnią portale społecznościowe, gdzie informacjami dzielą się ze społeczeństwem nie tylko dziennikarze, ale także politycy, naukowcy czy po prostu „zwykli ludzie". Zwiększa to bezpośredniość i szybkość dostępu do wiadomości ze świata oraz daje szanse na czerpanie tych wiadomości ze zróżnicowanych źródeł i środowisk. Niestety mimo ogromnych plusów jakie powoduje Internet w kwestii dostępu do informacji, nie brakuje istotnych minusów, które nie są obojętne dla utrzymywania demokratycznych standardów w tej sferze. Przyglądając się bliżej, okazuje się, że Internet nie jest tak rzetelnym, nienależnym i obiektywnym źródłem informacji, jak można by sądzić. Poniżej zostaną omówione negatywne zjawiska, jakie wiążą się czerpaniem wiedzy z Internetu.

Pierwszym z minusów wykorzystania portali sieciowych jako źródła informacji jest przeciążenie informacyjne i stres informacyjny[19]. Dostrzegalny jest ogromny problem z przyciągnięciem uwagi współczesnego odbiorcy wobec natłoku wiedzy jakiego dostarczają nowoczesne media. Skoro na co dzień jest się bombardowanym różnymi wieściami z całego świata, trudno skupić się i wychwycić informacje, które faktycznie są istotne dla danej osoby. Sytuacji nie ułatwiają internetowi dziennikarze, którzy chcąc skupić uwagę odbiorcy, wykorzystują popularne obecnie „klikbejty" (ang. *clickbait*). Są to nagłówki nacechowane skrajnymi emocjami, mające spełniać rolę „przynęty" dla internauty, z kolei dalsza część takiej publikacji znacząco odbiega od tego, co sugeruje taki nagłówek. Wykorzystywanie skandali i szokujących wypowiedzi stało się skuteczną i powszechną strategią w procesie przyciągania uwagi internautów[20]. Taki sposób zwracania uwagi odbiorców nie wpływa korzystnie na jakość dyskursu publicznego. Chwytliwe i kontrowersyjne nagłówki często wprowadzają w błąd oraz mogą sterować emocjami obiorców. Co więcej, wielu czytelników poprzestaje na przeczytaniu nagłówka będącego klikbejtem, nie zagłębiając się dalej w treść publikacji, co przyczynia się do tworzenia fałszywej wizji świata na ich postawie. Zjawisko to pogłębia też trend tzw. ramowania informacji (ang. *news framing*). Ramowanie to zabieg redakcyjny pozwalający na przekierowanie uwagi odbiorcy na wybrany

[19] W. M. Czerski, *Przeciążenie informacyjne wyzwaniem dla edukacji doby cyfrowej*, Przegląd Pedagogiczny 2020/2, s. 74-84.
[20] A. Demczuk, *op. cit.,* s. 35-36.

przekaz, a taka „zramowana" informacja, opublikowana na portalu internetowym, staje się klikbejtem i źródłem rozpowszechniania dezinformacji[21]. Odnosząc się do aspektu funkcjonowania państwa, warto mieć na uwadze, że wartość uzyskiwania informacji przez społeczeństwo nie powinna polegać jedynie na szybkim, prostym i wielotorowym jej obiegu, ale również na tym, by była ona rzetelna i pozwalała poznać prawdziwy obraz rzeczywistości. W dyskursie publicznym, w tym politycznym, takie zjawiska jak ramowanie i klikbejty odgrywają szczególnie niebezpieczną rolę, bo mogą mieć wymiar perswazyjny przez odpowiednie ukształtowanie obrazu rzeczywistości u odbiorców, według własnego uznania i aktualnych potrzeb politycznych danej grupy, a tym samym pozwalają sterować opinią publiczną.

Natłok informacji i ramowanie to niejedyny negatywny aspekt czerpania wiedzy za pośrednictwem Internetu. Dodatkowo warto zwrócić uwagę na pogląd, że Internet stał się wirtualną kabiną pogłosową[22]. Efekt kabiny pogłosowej oznacza sytuację, w której internauci dążą do wyszukiwania treści pokrywających się z ich poglądami, co sprzyja wzmacnianiu ich dotychczasowych poglądów. Takie zjawisko nie wpływa pozytywnie na pozyskiwanie rzetelnej informacji oraz zamyka obywateli na inne punkty widzenia, a tym samym ogranicza dyskurs, tak istotny dla funkcjonowania demokracji na wysokim poziomie. Tworzenie zamkniętych na inne poglądy grup jest ułatwione dzięki możliwościom platform internetowych do moderacji treści. David Beer wskazywał, że algorytmy służące pozycjonowaniu, sortowaniu i filtrowaniu treści mają wręcz społeczną władzę decydowania o tym, co jest w danym momencie promowane i znaczące[23]. Tym samym człowiek korzystający z mediów społecznościowych nie ma pełnej władzy na tym, co czyta i ogląda, a co za tym idzie, jakie wyobrażenie o świecie jest mu stwarzane. Również Eli Pariser zwracał uwagę na podobne niebezpieczeństwo tzw. baniek informacyjnych[24]. Według jego obserwacji różnorodności przekazu, który dociera do przeciętnego odbiorcy, ograniczana jest personalizacją wyświetlanych informacji, co oznacza, że platformy stale podpowiadają, co polubić lub co zobaczyć, tym samym zmykając człowieka we własnych bańkach informacyjnych. W takiej sytuacji odbiór rzeczywistości jest tylko cząstkowy i ograniczony do preferencji odbiorcy, określanych na podstawie

[21] *Ibidem*, s. 69.
[22] A. Demczuk*, op. cit.*, s. 132.
[23] J. Bednarek, *Problematyczność traktowania mediów społecznościowych jako źródeł informacji na przykładzie oblężenia wschodniego Aleppo w 2016 roku*, [w:] *Media Varia. Jednostki-Społeczeństwa-Technologie*, red. T. Gackowski, M. Patera, Warszawa, 2020, s. 194.
[24] *Ibidem*, s. 194.

dotychczasowej działalności w sieci. Nie jest to korzystne z perspektywy dążenia do wzorca dobrze poinformowanego i świadomego obywatela. Co ważne, traktując media społecznościowe jako źródło informacji, pozwala się, aby rolę filtra informacji, które docierają do społeczeństwa, pełniły algorytmy zaprojektowane przez prywatne korporacje, które − w przeciwieństwie do mediów tradycyjnych – nie mają odgórnie narzuconych zasad etycznych ani kompetencji serwisów informacyjnych[25], mogą mieć za to swoje prywatne interesy w tym, by pewne treści były premiowane kosztem innych.

Korzystając z internetowych sposobów uzyskiwania wiedzy, warto być świadomym zagrożeń jakie stwarzają, by nie skazać się na utratę zdolności uzyskiwania pełnych i rzetelnych wiadomości. Jest to istotne zwłaszcza dlatego, że czerpanie z Internetu informacji o ważnych wydarzeniach toczących się na świecie oraz o prezentowanych poglądach poszczególnych ludzi, przekłada się później na kształtowanie się sympatii politycznych oraz wybory polityczne. Czym bardziej poważne i dramatyczne wydarzenie jest relacjonowane za pośrednictwem portali społecznościowych, tym większe ryzyko, że wiadomości mogą być nacechowane emocjami a pozbawione merytorycznej wartości. Dobrym przykładem takich wydarzeń są konflikty zbrojne. Ryzyko jakie niesie za sobą traktowanie postów publikowanych w mediach społecznościowych jako źródeł informacji o konfliktach występujących na świecie, jest problematyczne przede wszystkim dlatego, że wiadomości pochodzące od osób bezpośrednio zaangażowanych w konflikt i pozbawionych dystansu, są subiektywnym przedstawieniem sytuacji, a nie tego oczekuje się od rzetelnego dziennikarstwa informacyjnego[26]. Dodatkowo materiały przedstawiane przez uczestników konfliktu nie są wolne od świadomych manipulacji, by zwiększyć sympatie i poparcie dla danej strony konfliktu. Przykładem może tu być dyskurs w mediach społecznościowych na temat wojny w Syrii[27], który odbywał się głównie w języku arabskim, natomiast treści anglojęzyczne, które adresowane były do zachodnich odbiorców, skupione były na cierpieniu niewinnych osób, podkreślaniu okrucieństwa wojsk rządowych i nawoływaniu zachodnich państw do pomocy, pomijając kontrowersyjne i niekorzystne dla nadawców treści. W tym kontekście zauważono[28], że media społecznościowe stwarzają niebezpieczną iluzję bezpośredniego przekazu

[25] *Ibidem,* s. 195.
[26] R. Wietoszko, *Ideologiczne narracje tożsamościowe w mediach–wymiar informacyjny i konsekwencje ekonomiczne*, Media Biznes, Kultura, 2018 (Numer 1 (4) 2018), s. 53-69.
[27] J. Bednarek, *op. cit.*, s. 189-192.
[28] *Ibidem,* s. 189-192.

informacji, a tak naprawdę są starannie nadzorowane przez siatki aktywistów, tak aby wytworzyć konkretne narracje. To wszystko utwierdza w przekonaniu, że do informacji pozyskanych w sieci należy podchodzić z odpowiednim dystansem, w innym przypadku łatwo o dezinformację i podziały społeczeństwa.

4. ZAGROŻENIE ALGORYTMAMI I GROMADZENIEM DANYCH

Zatem, jak można zauważyć, portale społecznościowe jako miejsce prowadzenia dyskursu publicznego, ścierania się poglądów czy jako źródło pozyskiwania informacji, nie jest wolne od manipulacji i zagrożeń, a ryzyko potęguje duża niezależność właścicieli platform w regulowaniu działalności użytkowników. Sytuacji nie ułatwia fakt, że współczesne państwa, by chronić obywateli, powinny prawnie uregulować wykorzystywanie nowoczesnych i wyspecjalizowanych narzędzi, których działanie może nie być do końca czytelne dla ciał ustawodawczych. Takim nie do końca uchwytnym narzędziem są algorytmy, wykorzystywane na szeroką skalę: „administratorzy internetowych wyszukiwarek i platform informacyjnych oraz kanałów komunikacyjnych uzyskują, za sprawą stosowanych algorytmów, w zasadzie nieograniczoną możliwość dokonywania wyboru, standaryzowania, pozycjonowania i strukturalizacji dostarczanych informacji. Dziś nie ulega wątpliwości, że korzystają z tej pozycji, postępując zgodnie ze swoimi interesami finansowymi”[29]. Stan takiego niekontrolowanego sterowania informacjami przy pomocy algorytmów wydaje się alarmujący. Ogromnym wyzwaniem dla dyskursu publicznego prowadzonego w demokratycznym państwie staje się więc infrastruktura manipulacyjna wykorzystywana do tworzenia i rozpowszechniania dezinformacji oraz współczesnej formy propagandy, jaką jest tzw. propaganda komputacyjna[30] oparta na oprogramowaniu komputerowym, które może być zorientowane ideologicznie, a zatem prezentować określoną perspektywę w debacie publicznej. Komputerowe techniki obliczeniowe stanowią potężną siłę w walce z konkurencją polityczną oraz mogą być z łatwością wykorzystywane do szerzenia fałszywych wiadomości. Dodatkowo algorytmy współtworzą wspomniane już bańki informacyjne, które odseparowują internautów o różnych poglądach. Algorytmizacja umożliwia dobór treści najbardziej atrakcyjnych dla internautów na podstawie dokonanych wcześniej wyborów, pozwala to na kształtowanie światopoglądu internautów, wywieranie

[29] G. Rydlewski, *op. cit.*, s. 61.
[30] A. Demczuk, *op. cit.*, s. 36-37.

wpływu na kreowanie wyobrażeń o otaczającej rzeczywistości oraz wyznaczanie, jakie informacje powinny być dla danego internauty ważne[31]. Należy uwzględnić, że używane algorytmy znajdują się w dyspozycji globalnych administratorów sieci i są podporządkowane realizacji zadań wskazanych przez ich twórców. Dodatkowy niepokój budzi to, że algorytmy są nietransparentnym mechanizmem selekcji informacji dla przeciętnego odbiorcy, a wywierają tak silny wpływ na filtrowanie rzeczywistości oraz monopolizowanie kierunków zainteresowań społeczeństwa. W świetle tego, ważna dla demokracji wartość wolności w Internecie, w tym wolność wyboru dokonywanego przez odbiorców internetowych, może okazywać się iluzją, a w praktyce internauci są skazani na wybory wynikając z preferencji administratorów wyszukiwarek i platform informacyjnych. Ponieważ w takich warunkach władza algorytmów przenika się z władzą polityczną, można stwierdzić, iż mając władzę nad algorytmami, uzyskuje się w pewnym stopniu władzę w sprawach dotyczących sfery publicznej[32]. Znaczenie algorytmów powinno być zatem uwzględniane w rządzeniu i tworzeniu prawa, tak by chronić demokratyczne wartości, szczególnie dlatego, że aktywność w sieci jest obecnie jednym z kluczowych elementów w trakcie wyborów politycznych i kształtowaniu wyborów społeczeństwa.

W kontekście szerokiego korzystania z internetowych portali nie można zapominać o tym, jak ważną wartością dla demokratycznego państwa jest wolność słowa: „wolność wypowiedzi jest podstawowym elementem konstytuującym pluralistyczny dyskurs publiczny, który jest kluczowym czynnikiem sprawczym w konstrukcji życia społecznego”[33]. W sieci, tak jak i w życiu rzeczywistym, nie brakuje jednak sytuacji przekraczania i nadużywania wolności słowa, a całkowita wolność słowa w Internecie to: „szlachetne marzenie, pełne optymizmu i wiary w człowieka”[34]. Problemem i wyzwaniem jest radzenie sobie z sytuacjami nadużywania wolności słowa, jednocześnie unikając cenzury i nie ograniczając dostępu do nowych mediów. By radzić sobie m.in. z mową nienawiści, szerzeniem fałszywych informacji, dyskryminacją i innymi negatywnymi zjawiskami, strony internetowe mają zwykle wprowadzone wewnętrzne regulacje. Procedury i zasady wprowadzane przez regulaminy portali społecznościowych często nie są jednak przejrzyste i nie wydają się wystarczające do radzenia sobie z tym problemem. Trudności z uregulowaniem

[31] A. Demczuk, *op. cit.*, s. 36-37.
[32] G. Rydlewski, *op. cit.,* s. 65.
[33] A. Demczuk, *op. cit.,* s. 17.
[34] F. Longchamps de Bérier, *Wolność słowa w internecie w świetle orzecznictwa Sądu Najwyższego Stanów Zjednoczonych*, [w:] *Prawo wobec nowoczesnych technologii*, red. P. Girdwoyń, Warszawa, 2008, s. 95.

patologii wynikających z działalności w sieci wynikają też z tego, że Internet i swoboda dostępu do niego są powszechnie uznawane za ogromną wartość, a próby ingerencji w tę sferę przez władze publiczne rodzą sprzeciw społeczny[35]. Co zaskakujące, społeczeństwo bardziej obawia się ingerencji władz państwowych, niż niewidzialnej na pierwszy rzut oka ingerencji prywatnych korporacji.

W kontekście stanu demokracji na uwagę zwraca również fakt, że w demokracji ważne jest poszanowanie podmiotowości uczestników dyskursu, które w wirtualnym świecie nie jest do końca respektowane. Ten problem dobrze opisują słowa Ryszarda Piotrowskiego: „demokracja jako debata, która służy zarówno poszukiwaniu prawdy, jak też porozumieniu i współdziałaniu, jest możliwa jedynie przy poszanowaniu podmiotowości uczestników dyskursu, co wymaga respektowania ich tożsamości, a więc tego, że mają władzę ustalania granic dostępu do swoich myśli oraz do informacji, w których przejawia się istnienie człowieka w świecie. We współczesnym społeczeństwie informacyjnym wyznacznikiem godności człowieka jest zdolność bycia podmiotem dotyczących go danych[…]. Niemal nieograniczona trwałość śladów, które jednostka pozostawia w sieci, a zarazem łatwość przejęcia kontroli nad cyfrowym odbiciem, które utrwalamy, uczestnicząc w różnych formach w wymianie informacji, wymaga regulacji, która […] nie poświęcałaby godności jednostki na rzecz interesu publicznego czy prywatnego”[36]. Ponadto wspomniany wyżej autor zauważa, że poddanie społeczeństwa inwigilacji i kontroli sprawowanej przez prywatne podmioty zarządzające danymi sprawia, że społeczeństwo traci zdolność do samoorganizacji niezależnej od dysponentów tych informacji i jest podatne na manipulacje[37]. Piotrowski zwraca również uwagę, że rozwój technologii informacyjnych, choć może być korzystny ze względu na nowe możliwości komunikacyjne, a przez to sprzyjanie budowaniu społeczeństwa obywatelskiego oraz ułatwianie niezależnej debaty publicznej, to zarazem stymuluje rezygnację z własnej prywatności użytkowników sieci, narzucając świat, w którym uczestnictwo w życiu społecznym staje się równoznaczne z rezygnacją z prywatności. Co dziwi i niepokoi, państwa nie mają szczególnie wpływu na to, co globalne korporacje robią z gromadzonymi danymi, a tak szeroki i niekontrolowany dostęp do wiedzy o obywatelach

[35] G. Rydlewski, *op. cit.,* s. 61.
[36] R. Piotrowski, *Prawo do tożsamości informacyjnej i jego znaczenie w ustroju demokratycznym*, [w:] *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka. Tom 1.*, Red. J. Jaskiernia, Warszawa, 2013, s. 479.
[37] *Ibidem,* s.483.

byłby szokujący dla suwerennego państwa z epoki przedinternetowej[38]. Na tego typu praktyki pozwala jednak słabość współczesnych państw w porównaniu z pozycją międzynarodowych korporacji oraz brak skutecznego sprzeciwu ze strony obywateli, którzy godzą się na oddanie swojej prywatności dla wygody[39]. Wątpliwe jest to, czy powinno to mieć miejsce w demokratycznym państwie, które co do zasady powinno chronić obywateli w tym zakresie.

5. POLITYKA W SIECI

Biorąc pod uwagę jak ogromny wpływ na codzienne wybory społeczeństwa wywiera działalność w sieci, nie dziwi fakt, że również politycy przenieśli swoją bieżącą działalność do Internetu. Prawdopodobnie trudno już sobie wyobrazić prowadzenie polityki poza siecią, bez korzystania z portali społecznościowych, które są istotną przestrzenią choćby przez sam fakt posiadania tak licznego audytorium[40] i bezpośredniości przekazu. Właśnie dzięki mediom społecznościowym zmianie uległ model komunikowania politycznego, który stał się bardziej dwukierunkowy. Politycy już nie tylko komunikują coś swoimi odbiorcom, ale mogą prowadzić z nimi aktywny dialog[41], co wydaje się zjawiskiem pozytywnym, pozwalającym obywatelom lepiej poznać polityków, doprowadzić do wymiany zdań. Korzyści płynące z polityki w sieci spowodowały rozpowszechnienie tej formy jej prowadzenia, dlatego zgodzić należy się z tezą mówiącą o tym, że obecnie sukces wyborczy nie zależy już od rozwieszenia plakatów na ulicy i rozdania ulotek[42]. Aktualnie, jeśli jest się osobą publiczną, w tym politykiem, a nie korzysta się z mediów społecznościowych, to pozbawia się „istnienia" dla bardzo dużej części społeczeństwa, gdyż media społecznościowe, są obecnie jednym z głównych źródeł wiedzy na temat polityków[43]. Politycy zauważając siłę takiej formy prowadzenia kampanii wyborczych oraz promowania swojej osoby, nie bagatelizują tego sposobu prowadzenia polityki i to niezależnie od wieku (choć oczywiście łatwiej się przystosować osobom młodym, dla których środowisko Internetu jest bardziej naturalne).

[38] *Ibidem,* s. 485-486.
[39] *Ibidem*, s. 488.
[40] G. Kowalczyk, *Social media w samorządowej kampanii wyborczej,* [w:] *Media Varia. Jednostki-Społeczeństwa-Technologie*, red. T. Gackowski, M. Patera, Warszawa, 2020, s. 131.
[41] K. Piórecka, *Wybory do polskiego Sejmu i Senatu 2019. Kampania wyborcza na Twitterze*, [w:] *Media Varia. Jednostki-Społeczeństwa-Technologie*, red. T. Gackowski, M. Patera, Warszawa, 2020, s. 158.
[42] K. Nowak, *Facebookowa walka o samorządy*, [w:] *Technopolityka w świecie nowych mediów*, red. M. K. Zwierżdżyński, M. Lakomy, K. Oświecimski, Kraków, 2015, s. 238.
[43] *Ibidem*, s. 256-257.

W Polsce siła Internetu w dotarciu do władzy została zwłaszcza uwidoczniona podczas pierwszej kampanii wyborczej prezydenta Andrzeja Dudy[44], który korzystał wówczas z mediów społecznościowych na szeroką skalę, a w dniu zaprzysiężenia połączył się na żywo z internautami za pomocą facebookowej aplikacji – *Live for Facebook Mentions*[45]. Otwarcie się na prowadzenie kampanii wyborczej w sieci było poważnym czynnikiem decydującym o przewadze Andrzeja Dudy nad konkurującym z nim Bronisławem Komorowskim. Przykład kampanii wyborczej podczas polskich wyborów prezydenckich w 2015 r. doskonale obrazuje, jaką polityczną siłę ma Internet.

Głównymi portalami wykorzystywanymi przez polityków są Facebook i Twitter[46]. Facebook jest przestrzenią skupiającą bardzo duże audytorium, ale nie tak upolitycznioną jak Twitter. Twitter zaś jest platformą skupiającą głównie osoby zajmujące się polityką bądź aktywnością publiczną zawodowo[47]. Polityczne wykorzystanie Twittera jest zachęcające dlatego, że to zwłaszcza on stwarza poczucie bezpośredniości kontaktu, skracając dystans komunikacyjny między użytkownikami. Powoduje to, że w teorii każdy obywatel może nawiązać kontakt najważniejszymi osobami tego świata[48]. Pomimo popularności, portalom tym można oczywiście postawić zarzuty manipulowania odbiorcą. Z punktu widzenia bezpieczeństwa i przejrzystości działalności politycznej w sieci, istotne jest wskazanie, że operatorzy kluczowych internetowych platform komunikacyjnych stali się kreatorami debaty publicznej, a świat algorytmów wkroczył do sfery polityki i jest narzędziem kształtowania postaw politycznych, robiąc to w sposób arbitralny, nieprzejrzysty i pozbawiony kontroli zewnętrznej[49]. W tym kontekście obawy budzą wykorzystywane techniki mikrotargetingu (ang. *microtargeting*) oraz profilowania z wykorzystaniem algorytmów prognostycznych. Mikrotargeting jest znaną w kampaniach wyborczych techniką polegającą na przeszukiwaniu rynku po to, by odnaleźć potencjalnych wyborców i do nich skierować pasujący do nich przekaz. Dzięki politycznemu mikrotargetingowi umożliwia się tworzenie precyzyjnie

[44] R. Zyzik, *Błędy poznawcze w decyzjach politycznych: perspektywa nowych mediów* [w:] *Technopolityka w świecie nowych mediów*, red. M. K. Zwierżdżyński, M. Lakomy, K. Oświecimski, Kraków, 2015, s. 311.
[45] *Facebook z transmisjami na żywo w Mentions. Andrzej Duda przemówi do internautów*, https://www.wirtualnemedia.pl/artykul/facebook-z-transmisjami-na-zywo-w-mentions-andrzej-duda-przemowi-do-internautow, [dostęp: 14.12.2022].
[46] K. Stefanowicz, *Portale społecznościowe jako narzędzie wpływu politycznego*, Nowe Media. Czasopismo Naukowe, 2011/2, s. 55-68.
[47] G. Kowalczyk, *op. cit.,* s. 134-135.
[48] K. Piórecka, *op. cit.,* s. 162.
[49] G. Rydlewski, *op. cit.,* s. 62.

dopasowanych treści skierowanych do odpowiednich kategorii odbiorców, co ułatwia partiom politycznym dopasowanie się do docelowych wyborców[50]. Z tego powodu odbiorcy wytwarzają w swojej głowie obrazy czy opinie na podstawie tego, co sugerują im algorytmy.

Z taką polityczną działalnością w sieci wiążą się też inne poważne zagrożenia. Wątpliwości budzi przestrzeganie zasad pluralizmu politycznego w kontekście arbitralnego blokowania pewnych kontrowersyjnych treści oraz usuwania z portali społecznościowych kont dużych graczy politycznych. Doskonale obrazuje to przykład aktywności w mediach społecznościowych Donalda Trumpa. Okazuje się, że decydując się na komunikację ze społeczeństwem za pomocą portalów społecznościowych, politycy muszą się liczyć z możliwością zablokowania swoich kont przez administratorów komunikatorów internetowych. Tak stało się w przypadku byłego prezydenta USA, który został zablokowany na Facebooku[51], a na Twitterze (również w okresie wyborów prezydenckich w USA w listopadzie 2020 r.) jego tweety były regularnie blokowane[52]. Podobne doświadczenia spotkały w Polsce polityków Konfederacji, którym usunięto partyjne konto na Facebooku[53]. Nie oceniając zasadności kierowanych przeciwko powyższym politykom zarzutów i podstaw zablokowania tych profili, budzi wysoki niepokój fakt, że bez wyroku sądu, na podstawie wewnętrznej decyzji portalu, zablokowane zostały konta legalnie funkcjonujących polityków, którzy, biorąc pod uwagę rolę i znaczenie mediów społecznościowych, muszą w nich uczestniczyć, by nie skazać się na polityczny niebyt.

Warto zwrócić też uwagę na fakt, jak arbitralne decyzje portali społecznościowych lub niekontrolowane szerzenie się fałszywych informacji, bazujące choćby na przywołanych już wcześniej „klikbejtach", staje się niebezpieczne w czasie kampanii wyborczych, których okres powinien być pod szczególną ochroną. W tym kontekście można przytoczyć raport Freedom House z 2019 r. [54], w którym opisano trzy modele możliwej internetowej ingerencji w wybory:

[50] A. Demczuk, *op. cit.,* s. 48-49.
[51] *Facebook zablokował Trumpa na dwa lata*, https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8181856,facebook-zablokowal-trumpa-na-dwa-lata.html, [dostęp: 13.12.2022].
[52] G. Rydlewski, *op. cit.,* s. 143.
[53] A. Mierzyńska, *Konfederacja usunięta z Facebooka za propagandę antyszczepionkową i mowę nienawiści*, https://oko.press/konfederacja-usunieta-z-facebooka-za-propagande-antyszczepionkowa/, [dostęp: 19.05.2022].
[54] G. Rydlewski, *op. cit.,* s. 153-154.

1. oparte na środkach informacyjnych, dyskretne i coraz bardziej inteligentne manipulowanie treściami na korzyść określonych państw lub sił politycznych;
2. ograniczanie dostępu do niezależnych źródeł wiadomości i narzędzi komunikacji, blokowanie i hakowanie określonych stron, odcinanie dostępu do Internetu;
3. wprowadzania ograniczeń w dostępie do Internetu oraz karanie za ujawnianie w komunikacji elektronicznej negatywnego stanowiska wobec rządzących[55].

W wyżej wskazanym raporcie zdiagnozowano również zjawisko „autorytaryzmu cyfrowego", który zagraża wolności internetowej. Jak wskazano w raporcie: „Media społecznościowe pozwalają zwykłym ludziom, grupom obywatelskim, i dziennikarzom docierać do szerokiego grona odbiorców przy niewielkich lub zerowych kosztach, ale stanowią także niezwykle użyteczną i niedrogą platformę dla operacji wywierania złego wpływu przez podmioty zagraniczne i krajowe"[56]. Jak zatem można zauważyć, raport słusznie przedstawił to, że uwzględniając zalety kampanii wyborczych w sieci, nie można zapominać o negatywnych aspektach tej praktyki. Celnie wskazuje się nawet, że: „wybory coraz częściej odbywają się w warunkach internetowej wojny informacyjnej, w której biorą udział poszczególne państwa, siły polityczne i indywidualnie politycy"[57]. Dlatego tym bardziej uwidacznia się potrzeba przyjęcia regulacji, które zapanują nad tą ważną dla demokratycznego państwa sferą.

Mówiąc o procesach demokratycznych przebiegających w Internecie oraz o przestrzeganiu prawa i standardów konstytucyjnych w tym kontekście, warto poruszyć jeszcze inną interesującą kwestię. Podczas wyborów polski Kodeks wyborczy[58] w art. 107 wymaga zachowania tzw. ciszy wyborczej. W czasach wirtualnej debaty publicznej trudne jest do skontrolowania i oceny, co stanowi jej naruszenie. Jak wskazują obserwatorzy życia publicznego, kampania wyborcza w sieci trwa cały czas, również w dniu wyborów[59]. Można zadać sobie pytanie, czy wystarczy „polajkowanie" wpisu na Facebooku czy Twitterze, czyniąc go widocznym dla większej grupy osób, aby złamać ciszę wyborczą? Sytuacja jest trudna do oceny, a to nie jedyny dylemat, innym

[55] *Ibidem,* s. 153-154.
[56] G. Rydlewski, *op. cit.,* s. 63.
[57] *Ibidem,* s. 149.
[58] Ustawa z dnia 5 stycznia 2011 r. - Kodeks wyborczy (t.j. Dz. U. z 2022 r. poz. 1277 z późn. zm.).
[59] V. Makarenko, *Cisza wyborcza w internecie to fikcja. Zobacz, jak wygląda na forach i w sieciach społecznościowych*, 2015, https://biqdata.wyborcza.pl/biqdata/7,159116,22075698,cisza-wyborcza-w-internecie-to-fikcja-zobacz-jak-wyglada-na.html [dostęp: 19.05.2022 r.].

przykładem może być udostępniane humorystycznych obrazków, rebusów lub znaków, które jednoznacznie są kojarzone z określoną preferencją wyborczą, mimo że nie mówią tego wprost. Biorąc pod uwagę siłę oddziaływania takich czynów, wydaje się, że definicja ciszy wyborczej powinna ulec zmianie, ale polska Państwowa Komisja Wyborcza zdaje się tego nie dostrzegać[60]. W ten sposób państwa mając trudności z nadążaniem za nowymi technologiami i nowym sposobem prowadzenia debaty publicznej, nie dostosowując przepisów do nowej rzeczywistości, tworzą luki, które pozwalają naruszać standardy demokratyczne.

6. PRAWO W ODPOWIEDZI NA NOWE TECHNOLOGIE

Liczne kontrowersje powiązane z używaniem nowoczesnych technologii wskazują na to, że aktualnie obowiązujące prawo nie jest do końca przystosowane do realiów jakie stwarzają i nie chroni skutecznie wartości demokratycznych w wirtualnej debacie politycznej. Potrzebne są nowe rozwiązania, adekwatne do tego jak wygląda rzeczywistość w sieci. Zrozumiały jest fakt, że konsekwencje wprowadzania nowych technologii musiały się najpierw uwidocznić w praktyce by można było podjąć sensowne decyzje ustawodawcze[61]. Jednak obecnie władze ustawodawcze demokratycznych państw mogą bazować na wystarczająco utartej praktyce korzystania z sieci oraz posiadają informacje o zidentyfikowanych zagrożeniach, dlatego nie powinny dalej zwlekać z poddaniem kontroli państwowej tych negatywnych zjawisk. Brak dostatecznych regulacji prawnych przerzuca rolę w wyznaczaniu standardów działalności w Internecie na krajowe i międzynarodowe sądownictwo[62] oraz na prywatne korporacje. Wydaje się, że nadszedł moment i potrzeba na interwencje przy pomocy prawa stanowionego. Zwłaszcza, że biorąc pod uwagę zdolność algorytmów do kształtowania odbioru rzeczywistości, coraz trudniej zaakceptować to, by były one tajne, układane w sposób niepodlegający odpowiedzialności oraz kontroli publicznej[63]. Warto podkreślić, że na konieczność podjęcia aktywniejszej polityki władz publicznych w dziedzinie przeciwdziałania i zwalczania fałszywych wiadomości zaapelował nawet sam twórca

[60] *Cisza wyborcza jest łamana, nawet gdy lajkujemy*, 2020, https://www.prawo.pl/prawo/lamanie-ciszy-wyborczej-w-sieci-i-w-realu,501615.html [dostęp: 19.05.2022r.].
[61] A. Demczuk, *op. cit.,* s. 205.
[62] *Ibidem,* s. 194.
[63] T. G. Ash, *Wolne słowo. Dziesięć zasad dla połączonego świata*, przekł.: M. Godyń, F. Godyń, Kraków, 2018, s. 592-593.

platformy Facebook[64]. Dość oczywistym jest, że samo wprowadzenie konkretnych przepisów nie zmieni całkowicie rzeczywistości i nie uzdrowi w pełni internetowej przestrzeni. Jednak już samo istnienie pewnych ustanowionych standardów zwiększy szansę na weryfikację działalności w sieci oraz pokaże, że władze publiczne dostrzegają ten aspekt działalności politycznej.

Od jakiegoś czasu nad zwiększeniem kontroli nad cyberprzestrzenią pracuje Unia Europejska. W 2018 r. Komisja Europejska, w ramach zwalczania dezinformacji w Internecie, przedstawiła unijny kodeks ws. dezinformacji, który przewiduje m.in. wyeliminowanie przychodów z reklam na kontach i stronach internetowych wprowadzających w błąd, ujawnianie reklam politycznych, prowadzenie konkretnej i publicznie dostępnej polityki w zakresie tożsamości i botów internetowych oraz podejmowanie działań na rzecz zamykania fałszywych kont[65]. Na poziomie krajowym przykład działania daje niemieckie ustawodawstwo – powstała tam ustawa o polepszeniu egzekwowania prawa w sieciach społecznościowych[66], mająca zastosowanie do dużych platform, takich jak Facebook, Twitter i Youtube[67]. Odpowiedzią na zdiagnozowane problemy z wirtualną rzeczywistością mają być procedowane obecnie na poziomie Unii Europejskiej nowe przepisy regulujące usługi cyfrowe. W tym celu wypracowano dwie regulacje - akt o rynkach cyfrowych (*Digital Markets Act – DMA*) oraz akt o usługach cyfrowych (*Digital Services Act – DSA*)[68]. Mają one stanowić standardy dla funkcjonowania Internetu na najbliższe lata. Uwagę zwraca szereg zakazów, które przewiduje *DMA* w kwestii ograniczenia nadużyć wobec użytkowników jeśli chodzi o profilowanie i zmuszanie do korzystania z określonych rozwiązań. Z kolei akt o usługach cyfrowych reguluje zagadnienia związane z moderacją treści, targetowaniem reklam i wykorzystywaniem algorytmów do rekomendowania określonych treści. Dodatkowo, nowe przepisy mają pomóc chronić użytkowników przed nielegalnymi i szkodliwymi treściami dostępnymi w Intrenecie poprzez usprawnienie procedury zgłaszania naruszeń. W dodatku decyzje o usunięciu danej treści z sieci mają

[64] A. Demczuk, *op. cit.,* s. 412.
[65] *Ibidem*, s. 393.
[66] *Niemiecka ustawa o mediach społecznościowych – dobre chęci, nieprzewidziane skutki*, https://bezprawnik.pl/niemiecka-ustawa-o-mediach-spolecznosciowych-dobre-checi-nieprzewidziane-skutki/, [dostęp: 13.12.2022r.].
[67] A. Demczuk, *op. cit.,* s. 406-409.
[68] A. Wittenberg, *Koniec dyktatu Google i Apple. Unijny bat na technologicznych gigantów wchodzi w życie*, https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/8592988,dsa-dma-wchodzi-w-zycie-digital-service-act-google-iphone.html, [dostęp: 13.12.2022r.].

zapadać w sposób bardziej przejrzysty[69]. Projektowane przepisy zdają się odpowiadać na część zdiagnozowanych problemów, co należy ocenić pozytywnie. Optymizmem napawa fakt, że problem arbitralności i nieprzejrzystości portali społecznościowych jest coraz bardziej zauważalny przez władze ustawodawcze na poziomie unijnym oraz przez władze poszczególnych państw. Również w Polsce debata nad tymi problemami jest aktualna[70] i należy mieć nadzieję, że przyniesie oczekiwane skutki.

7. ZAKOŃCZENIE

Ryzyko, że w mediach społecznościowych dochodzi do manipulacji opinią publiczną, sterowania wyborami i ograniczania praw ważnych z perspektywy standardów demokratycznych, rzeczywiście istnieje. Opisana zależność między rozwojem życia politycznego i społecznego w wirtualnym świecie a przestrzeganiem zasad demokracji pokazuje, że świat ten stwarza zagrożenia, m.in. z uwagi na brak kontroli nad algorytmami, arbitralnymi decyzjami administratorów portali społecznościowych czy doprowadzaniem do dezinformacji. Nie demonizując jednak nazbyt nowych technologii oraz doceniając liczne zalety jakie wnoszą do demokratycznego państwa, konieczny jest dyskurs poświęcony temu, by zapobiegać zagrożeniom, a jednocześnie wykorzystywać szanse na doskonalenie demokratycznych procedur. Władze, obserwując jakie skutki wywierają nowe media, powinny interweniować adekwatnymi rozwiązaniami ustawodawczymi. Państwa nie powinny na poziomie stanowienia prawa dłużej udawać, że życie polityczne nie toczy się również w sieci i że nie trzeba go tam uregulować. Oczywiście kroki powinny być wywarzone, by przy okazji regulacji chroniących opisane wartości demokratyczne, które są zagrożone przez działalność w obszarach sieci, nie doprowadzić do ograniczenia innych praw i wolności, zwłaszcza poprzez zbyt restrykcyjne przepisy, które byłyby cenzurujące lub zamykające rynek nowych mediów. Bardzo ważna jest również edukacja społeczeństwa, uczulanie obywateli na zagrożenia oraz oddziaływanie miękkimi metodami, by promować dobre praktyki i uświadamiać z jaką rzeczywistością mają do czynienia. Przed współczesnymi demokracjami stoi wyzwanie, by demokratyczne wartości i praktyki dostosować do warunków jakie stwarzają nowe technologie i by „dogonić" postępy

[69] W. Pikusa, *UE zmienia świat online! O DMA i DSA słów kilka.,* https://srdk.pl/publikacje/ue-zmienia-swiat-online-o-dma-i-dsa-slow-kilka/ [dostęp: 20.05.2022r.].

[70] Cyfryzacja KPRM, profil na portalu Linkedin, https://www.linkedin.com/posts/ministerstwo-cyfryzacji_facebook-dezinformacja-przeciwdziaagkanie-activity-6933486185386274816-7wdN?utm_source=linkedin_share&utm_medium=ios_app [dostęp: 22.05.2022].

techniki odpowiednimi regulacjami prawa. Nowe technologie rozwijają się błyskawicznie, a fenomen portali społecznościowych intensywnie oddziałuje na polityczną sferę. Warto zatem zadbać, by prawo nie było wobec tego „spóźnione" i adekwatnie odpowiadało na wyzwania nowej rzeczywistości.

BIBLIOGRAFIA

Akty prawne

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483).

Ustawa z dnia 5 stycznia 2011 r. - Kodeks wyborczy (t.j. Dz. U. z 2022 r. poz. 1277 z późn. zm.).

Publikacje

Ash T. G., *Wolne słowo. Dziesięć zasad dla połączonego świata*, przekł.: M. Godyń, F. Godyń, Kraków 2018.

Bednarek J., *Problematyczność traktowania mediów społecznościowych jako źródeł informacji na przykładzie oblężenia wschodniego Aleppo w 2016 roku*, [w:] *Media Varia. Jednostki-Społeczeństwa-Technologie*, red. T. Gackowski, M. Patera, Warszawa 2020.

Boyke M., *Media społecznościowe a demokracja*, 2021, https://glospokolenia.pl/2021/02/media-spolecznosciowe-a-demokracja/ [dostęp: 20.05.2022].

Brzoza K., *Polskie posłanki VII kadencji Sejmu w sieci internetowej*, [w:] *Technopolityka w świecie nowych mediów*, red. M. K. Zwierżdżyński, M. Lakomy, K. Oświecimski, Kraków 2015.

Brzezicki Ł., Czy e-demokracja i rozwiązania znane ze świata biznesu są właściwymi kierunkami zmian politycznych w Polsce?, Horyzonty Polityki 2021, tom 12 nr 39.

Czerski W.M., *Przeciążenie informacyjne wyzwaniem dla edukacji doby cyfrowej*, Przegląd Pedagogiczny 2020/2.

Demczuk A., *Wolność wypowiedzi w społeczeństwie informacyjnym*, Lublin, 2020.

Gajowniczek, T. *Internet w komunikowaniu politycznym*, Media - Kultura - Komunikacja Społeczna 2020, tom 2 nr 15.

Izdebski H., *4. Prawo dostępu do informacji publicznej*, [w:] *Doktryny polityczno-prawne. Fundamenty współczesnych państw*, Warszawa 2021, https://sip.lex.pl/#/monograph/369496157/63/izdebski-hubert-doktryny-polityczno-prawne-fundamenty-wspolczesnych-panstw?keyword=Freedom%20of%20Information%20Act&unitId=passage_20525 (dostęp: 06.12.2022).

Koćwin L., *Wyzwania i problemy kreacji społeczeństwa informacyjnego w Polsce,* [w:] *Praktyki komunikacyjne*, red. Jolanta Kędzior, Wrocław 2019.

Kowalczyk G., *Social media w samorządowej kampanii wyborczej,* [w:] *Media Varia. Jednostki-Społeczeństwa-Technologie*, red. T. Gackowski, M. Patera, Warszawa 2020.

Longchamps de Bérier F., *Wolność słowa w internecie w świetle orzecznictwa Sądu Najwyższego Stanów Zjednoczonych*, [w:] *Prawo wobec nowoczesnych technologii*, red. P. Girdwoyń, Warszawa 2008.

Makarenko V., *Cisza wyborcza w internecie to fikcja. Zobacz, jak wygląda na forach i w sieciach społecznościowych*, 2015, https://biqdata.wyborcza.pl/biqdata/7,159116,22075698,cisza-wyborcza-w-internecie-to-fikcja-zobacz-jak-wyglada-na.html [dostęp: 19.05.2022].

Maziarz W. M., *Społeczny wymiar społeczeństwa informacyjnego*, Szczecin 2020.

Mierzyńska A., *Konfederacja usunięta z Facebooka za propagandę antyszczepionkową i mowę nienawiści*, https://oko.press/konfederacja-usunieta-z-facebooka-za-propagande-antyszczepionkowa/ [dostęp: 19.05.2022 r.].

Nowak K., *Facebookowa walka o samorządy*, [w:] *Technopolityka w świecie nowych mediów*, red. M. K. Zwierżdżyński, M. Lakomy, K. Oświecimski , Kraków 2015.

Pikusa W., *UE zmienia świat online! O DMA i DSA słów kilka,* https://srdk.pl/publikacje/ue-zmienia-swiat-online-o-dma-i-dsa-slow-kilka/ [dostęp: 20.05.2022].

Piotrowski R., *Prawo do tożsamości informacyjnej i jego znaczenie w ustroju demokratycznym*, [w:] *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka. Tom 1.*, Red. J. Jaskiernia, Warszawa 2013.

Piórecka K., *Wybory do polskiego Sejmu i Senatu 2019. Kampania wyborcza na Twitterze*, [w:] *Media Varia. Jednostki-Społeczeństwa-Technologie*, red. T. Gackowski, M. Patera, Warszawa 2020.

Rydlewski G., *Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji*, Warszawa 2021.

Rzuciło J., *Elektroniczny rząd. Aspekty konstytucyjnoprawne*, Warszawa 2015.

Stefanowicz K., *Portale społecznościowe jako narzędzie wpływu politycznego*, Nowe Media. Czasopismo Naukowe 2011/2.

Wietoszko R., *Ideologiczne narracje tożsamościowe w mediach–wymiar informacyjny i konsekwencje ekonomiczne*, Media Biznes, Kultura 2018, nr 1 (4).

Wittenberg A., *Koniec dyktatu Google i Apple. Unijny bat na technologicznych gigantów wchodzi w życie*, https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/8592988,dsa-dma-wchodzi-w-zycie-digital-service-act-google-iphone.html [dostęp: 13.12.2022].

Zyzik R., *Błędy poznawcze w decyzjach politycznych: perspektywa nowych mediów,* [w:] *Technopolityka w świecie nowych mediów*, red. M. K. Zwierżdżyński, M. Lakomy, K. Oświecimski, Kraków 2015.

Źródła internetowe

Cisza wyborcza jest łamana, nawet gdy lajkujemy, 2020, https://www.prawo.pl/prawo/lamanie-ciszy-wyborczej-w-sieci-i-w-realu,501615.html [dostęp: 19.05.2022].

Cyfryzacja KPRM, profil na portalu Linkedin, https://www.linkedin.com/posts/ministerstwo-cyfryzacji_facebook-dezinformacja-przeciwdziaagkanie-activity-6933486185386274816-7wdN?utm_source=linkedin_share&utm_medium=ios_app [dostęp: 22.05.2022].

Facebook zablokował Trumpa na dwa lata, https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8181856,facebook-zablokowal-trumpa-na-dwa-lata.html, [dostęp: 13.12.2022].

Facebook z transmisjami na żywo w Mentions. Andrzej Duda przemówi do internautów, https://www.wirtualnemedia.pl/artykul/facebook-z-transmisjami-na-zywo-w-mentions-andrzej-duda-przemowi-do-internautow, [dostęp: 14.12.2022].

Niemiecka ustawa o mediach społecznościowych – dobre chęci, nieprzewidziane skutki, https://bezprawnik.pl/niemiecka-ustawa-o-mediach-spolecznosciowych-dobre-checi-nieprzewidziane-skutki/, [dostęp: 13.12.2022].

DEMOCRACY IN THE WORLD OF NEW TECHNOLOGIES - POLITICAL ROLE OF SOCIAL MEDIA AND THE LAW

Summary: The article outlines the impact of new technologies, especially social media, on the functioning of a democratic state, with a particular focus on the formation of public opinion and policy-making through them. The article describes the risks posed by new technologies in the context of the proper functioning of democracy and respect for democratic values. The author presents the advantages and disadvantages of the political use of social media and calls for changes in the law so that values such as freedom of speech and political pluralism are respected in social media.

Keywords: democracy, new technologies, social media, politics, algorithms

PATRYCJA KULAK
UNIWERSYTET WROCŁAWSKI

PRAWO W OBLICZU NFT

Abstrakt: W dzisiejszych czasach popularność zdobywają nowe technologie. Uczestnicy Sieci stale poszukują nowych form inwestycji swojego kapitału. Jak kiedyś kryptowaluty, tak i teraz na rynku pojawiły się tokeny NFT. Ludzie tokenizują i wystawiają na sprzedaż najmniej oczekiwane rzeczy, takie jak: swoje ciało, czy uczucie miłości. Na pozór brzmi abstrakcyjnie, jednak kwoty jakie są płacone za różnego rodzaju tokeny NFT sięgają kilkudziesięciu milionów dolarów. Czym zatem jest token NFT i co sprawia, że jego wartość jest tak wysoka? Token NFT to niewymienialne, unikatowe aktywo o charakterze cyfrowym, funkcjonujący w Sieci Blockchain. Co zatem jest przedmiotem zbycia tokenu NFT? Dokładnie to, co strony postanowią w umowie. Przedmiot umowy zależy wyłącznie od indywidualnego przypadku, czy będzie to wyłącznie prawo dostępu do cyfrowego aktywa, czy może niewyłączna licencja. Problematyka NFT nie została jeszcze wprost uregulowana w przepisach powszechnie obowiązujących w Rzeczpospolitej Polskiej. Wobec powyższego, niezbędnym jest umiejscowienie tokenów NFT w ramach obecnie istniejących instytucji prawnych, jak przykładowo w instytucji znaków legitymacyjnych.

Słowa klucze: NFT, prawo, nowe technologie, inwestowanie

1. WPROWADZENIE

NFT stanowi nowe, technologiczne rozwiązanie i jest efektem postępu w XXI wieku. Stanowi też źródło dochodu, czasem nawet bardzo wysokiego. Stąd nie budzi wątpliwości, iż powinno zostać uregulowane prawnie, zwłaszcza na gruncie podatkowym. Obywatel powinien wiedzieć i znać system podatkowy i sposób rozliczenia swojego dochodu, nawet tak nowoczesnego, jakim jest przychód uzyskany z NFT. Z drugiej jednak strony, ustawodawca potrzebuje czasu, aby zapoznać się z nowinkami technologicznymi, które pojawiły się na rynku, sprawdzić ich działanie i wtedy dopiero móc stworzyć

odpowiednie regulacje. Implementacja niesprawdzonych rozwiązań ustawodawczych nie jest też dobrym rozwiązaniem, gdyż spotka się z wieloma nowelizacjami, rozłożonymi w krótkim czasie, co spowoduje chaos dla obywateli, jak również dla egzekwujących takie prawo.

Tym bardziej istotne, aby w naukowych rozważaniach, pochylać się nad tematami nowymi, które nie do końca znalazły jeszcze swoje odzwierciedlenie w przepisach prawnych. Niniejsza praca ma na celu przybliżenie tematyki NFT, wskazanie czym NFT jest i jak aktualnie jest postrzegane, zarówno od strony technologiczno- biznesowej, jak również prawnej, porównanie NFT z walutami wirtualnymi, jak również tokenem użytkowym oraz nakreślenie ich miejsca w systemie prawnym, zwłaszcza jeśli chodzi o dziedzinę prawa autorskiego, prawa konsumenckiego, czy prawa podatkowego. Autorka niniejszych rozważań przytoczy również interpretacje prawa podatkowego, w których organy podatkowe wyrażają swoje stanowisko w przedmiocie regulacji prawno- podatkowej NFT. Całość pracy zostanie również wsparta o przykłady i refleksje pochodzące z praktyki zawodowej.

W ocenie autorki niniejszej pracy, nie sposób NFT zakwalifikować jako waluty wirtualnej, ponieważ NFT nie odpowiada przesłankom definicyjnym waluty wirtualnej, o której w ustawie o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu[1], między innymi takim jak: wymienialność na inne prawne środki płatnicze, jak w przypadku walut wirtualnych, czy brak funkcji umarzania zobowiązań. W tak skomplikowanym stanie faktycznym, jakim są NFT, istotne byłoby, aby wskazać precyzyjnie, jakie obecne już w systemie prawnym przepisy prawne, można zastosować do NFT. Niniejsze rozważania są czynione na dzień 6 czerwca 2022 r., a z uwagi na dynamikę rozwoju nowoczesnych technologii, nakreślenie ram czasowych jest niezbędne.

2. NFT A WALUTY WIRTUALNE

Nowe technologie stanowią prawdziwe wyzwanie dla ustawodawców, tj. nie tylko polskiego, ale również dla ustawodawcy unijnego. Wszystko bowiem co nowe, potrzebuje czasu na weryfikację i stworzenie przepisów prawnych, pozwalających na skonstruowanie wyczerpującej regulacji prawnej. Zjawisko obrotu kryptowalutami pokazuje jak proces regulowania nowych technologii następuje, tj. w pierwszej kolejności, gdy prawo nie wprowadza jeszcze definicji pewnych zjawisk, doktryna i praktyka podejmuje wysiłki,

[1] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U.2022.593 t.j. z dnia 2022.03.15.

celem zakwalifikowania takich zjawisk do aktualnie obowiązujących instytucji prawnych. Taka sytuacja też miała miejsce w przypadku kryptowalut. Do momentu wprowadzenia przez ustawodawcę definicji legalnej waluty wirtualnej w ustawie o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, kryptowaluty były kwalifikowane jako znaki legitymacyjne, na podstawie art. 921 [15] Kodeksu cywilnego (dalej jako „kc")[2]. Definicja legalna jednak została zaimplementowana do polskiego porządku prawnego i zgodnie z nią waluta wirtualna to „cyfrowe odwzorowanie wartości, które nie jest:

a) prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,
b) międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
c) pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,
d) instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
e) wekslem lub czekiem

- oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego"[3]. Z uwagi na konieczność zachowania precyzji, autora niniejszych rozważań, wskazuje wprost definicję waluty wirtualnej, przytoczoną powyżej.

Ww. definicja legalna została wprowadzona do porządku prawnego dnia 13 lipca 2018 r. Już kilka lat wcześniej, tj. przed wprowadzeniem do systemu prawnego, definicji legalnej waluty wirtualnej, kryptowaluty były bardzo popularne. Jak zostało powyżej wspomniane, do momentu wprowadzenia do porządku prawnego ww. definicji legalnej, kryptowaluty były postrzegane jako znaki legitymacyjne, zgodnie z 921 [15] kc. W sytuacji, gdy prawo nie wprowadzało bezpośredniej regulacji, dotyczącej waluty wirtualnej, należało skorzystać z instytucji prawnych, najlepiej odwzorowujących istotę walu wirtualnych. Podobnie aktualnie sytuacja wygląda z tokenami NFT, brak regulacji wymusza niejako „wpisanie" tokenów NFT w instytucje prawne, najbardziej zbliżone do istoty tokenu NFT[4].

[2] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz.U.2020.1740 t.j. z dnia 2020.10.08.
[3] Art. 2 ust. 2 pkt 26 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.
[4] Komentarz autorki, na podstawie praktyki zawodowej.

3. KRYPTOAKTYWA I TOKEN UŻYTKOWY

Analizując problematykę obrotu tokenami NFT należy na wstępie wyjaśnić czym właściwie jest token i w jaki sposób postrzegać go przez pryzmat regulacji prawnych. Ogólnie pojęte tokeny są już przedmiotem zainteresowania ustawodawcy, jak również organów państwowych, stąd jest więcej możliwości przytoczenia opinii organów państwowych w kwestii tokenów w ogólności czy nawet kryptoaktywów, aniżeli konkretnie na temat tokenów NFT (choć wiele aktualnie dostępnych w obrocie tokenów NFT wykazuje cechy tokenów użytkowych, o czym poniżej). W tym celu autorka niniejszych rozważań, posłuży się stanowiskiem Urzędu Komisji Nadzoru Finansowego (w dalszej części pracy zwany również jako „KNF") w sprawie wydawania i obrotu kryptoaktywami z dnia 10 grudnia 2020 r.[5]. Zgodnie z wyżej przytoczonym stanowiskiem KNF, kryptoaktywo jest rozumiane jako cyfrowe odwzorowanie stosunku funkcjonującego pomiędzy podmiotami uczestniczącymi w sieci DLT[6], a który posiada różnego rodzaju uprawnienia. Kryptoaktywo może być przedmiotem obrotu na rynku. Kryptoaktywem może być przykładowo token[7].

Trzeba mieć jednak na uwadze, iż stanowisko KNF nie jest aktem prawa powszechnie obowiązującego, może stanowić jedynie wskazówkę interpretacyjną, ale nie mogą być wydawane na jego podstawie, przykładowo decyzje administracyjne, ponieważ stanowisko organu nie jest źródłem prawa. Niemniej jednak, na potrzeby naukowe, warto przedstawić stanowisko organów w kwestii postrzegania kryptoaktywów[8].

Następnym pojęciem, które z punktu widzenia niniejszych rozważań w przedmiocie problematyki obrotu tokenami NFT warto przedstawić jest token użytkowy (eng- *utility token*). Wiele tokenów NFT dostępnych aktualnie w obrocie, posiada cechy tego kryptoaktywa (nie można jednoznacznie stwierdzić, czy każdy token NFT posiada takie cechy, bowiem po pierwsze token NFT nie jest równy żadnemu innemu tokenowi NFT, a po drugie

[5] Komisja Nadzoru Finansowego, *Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami* https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf, (dostęp: 06.06.2022).

[6] Technologia rozproszonego rejestru (również „Technologia rozproszonych rejestrów"[1], ang. Distributed Ledger Technology, DLT) – rodzaj technologii wspierającej rozproszone rejestrowanie zaszyfrowanych danych[2], https://pl.wikipedia.org/wiki/Technologia_rozproszonego_rejestru, (dostęp: 06.06.2022).

[7] Komisja Nadzoru Finansowego, *op. cit.*, (dostęp: 06.06.2022).

[8] Art. 87 Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U.1997.78.483 z dnia 1997.07.16.

nie istnieje definicja legalna tokenu NFT, aby można było jednoznacznie stwierdzić w jaki sposób ustawodawca pojmuje tego rodzaju kryptoaktywa)[9].

W świetle powyższych rozważań, token użytkowy to jeden z najbardziej znanych tokenów, nie sposób wymienić wszystkich rodzajów tokenów, bowiem token może tworzyć różnego rodzaju uprawnienia, stąd nazwanie wszystkich ze względu na korzyści z nich płynące, nie jest możliwe. Zgodnie z ww. stanowiskiem KNF token użytkowy przyznaje nabywcom możliwość pozyskiwania w zamian za niego, różnego rodzaju towarów lub usług (najczęściej są to towary i usługi oferowane przez samego emitenta tokenów). KNF podkreśla, iż tego rodzaju tokeny wykazują podobieństwo do kuponów rabatowych, przeznaczonych na realizację zakupu towarów lub usług, jak również są zbliżone do kart podarunkowych, czy różnego rodzaju bonów lub voucherów, które uprawniają posiadacza do zamiany na inny towar lub usługę. Ponadto, KNF zwraca uwagę również na prawne aspekty tokenów użytkowych. Warto w tym miejscu wziąć pod uwagę art. 919 kc i kolejne przepisy kodeksu cywilnego[10].

Art. 919 kc reguluje instytucję przyrzeczenia publicznego. Zgodnie z ww. przepisem prawnym, każdy, kto ogłosił publicznie, że przyrzeka przyznać nagrodę za wykonanie konkretnej czynności, zobowiązany jest takiego przyrzeczenia dotrzymać. Przyrzeczenie jednak może zostać odwołane dopóki żaden podmiot wykona czynności i pod warunkiem, że nie zostało określone, że przyrzeczenie nie jest nieodwołalne oraz nie określono terminu końcowego wykonania przyrzeczonej czynności[11]. Instytucja ta może być stosowana do emitentów tokenów użytkowych, w sytuacji gdy, emitenci przyrzekają publicznie, iż określone tokeny „X" będą możliwe do zamiany na towary, np. książki, roboty kuchenne albo na usługę masażu w konkretnym salonie masażu. Najczęściej powyższe uzyskanie przykładowo książki, czy robota kuchennego, jest uzależnione od nabycia tokenu. W takiej sytuacji, emitenci tokenów użytkowych są zobowiązani do dotrzymania przyrzeczenia i zapewnienia nabywcom tokenów możliwości otrzymania konkretnych dóbr. Jak zostało już wspomniane w kontekście walut wirtualnych, tak i tokeny użytkowe z uwagi na podobieństwo do voucherów czy bonów, są postrzegane jako znaki legitymacyjne, na podstawie art. 921 [15] k.c.[12] Zgodnie z ww. podstawą prawną, przepisy dotyczące papierów wartościowych należy stosować

[9] Komisja Nadzoru Finansowego, *op. cit.,* (dostęp: 06.06.2022).
[10] Art. 919 Kodeksu cywilnego.
[11] *Ibidem.*
[12] Art. 921 [15] Kodeksu cywilnego.

odpowiednio również do znaków legitymacyjnych. Odpowiednie stosowanie stanowi bardzo szerokie stwierdzenie, bowiem jak wskazał KNF, powołując się na wyrok Sądu Najwyższego z dnia 15 lutego 2008 r., w sprawie o sygnaturze I CSK 357/07[13], odpowiednie stosowanie przepisów można pojmować w różny sposób, bowiem może to oznaczać, stosowanie przepisów bezpośrednio, tj. bez jakichkolwiek modyfikacji, do innych sytuacji, jak również może to oznaczać stosowanie przepisów z pewnymi modyfikacjami albo nieużywanie takich przepisów w ogóle do żadnych innych sytuacji. Powyższe wskazuje, iż zakres interpretacji ww. klauzuli jest istotnie obszerny. KNF jednak wskazał, iż w przedmiotowym przypadku tokenów użytkowych, odpowiednie stosowanie przepisów dotyczących papierów wartościowych ma znaczenie dla formy dokumentów, przenoszenia uprawnień z nich, czy w kontekście zasad ich działania. Przedmiotowa kwalifikacja tokenów użytkowych jako znaków legitymacyjnych ma doniosłe znaczenie, bowiem taki obrót nie będzie podlegał nadzorowi Komisji Nadzoru Finansowego, co niewątpliwie ma duże znaczenie dla przedsiębiorców, tworzących projekty z udziałem tokenów użytkowych[14].

Warto podjąć również kwestię kierowania tokenów użytkowych do nieograniczonej liczby odbiorców, bowiem tokeny NFT są podobnie oferowane nieoznaczonemu kręgowi adresatów. Taka sytuacja, tj. oferowanie tokenów do nieograniczonej ilości adresatów, nie podlega przepisom ustawy o obrocie instrumentami finansowymi[15], z wyjątkiem sytuacji, gdy tokeny będą mieć charakter hybrydowy i będą się przykładowo charakteryzowały również cechami tokenów inwestycyjnych, co jednak z punktu widzenia tokenów NFT nie jest konieczne dla niniejszych rozważań[16].

Podsumowując powyższe rozważania, obserwując obrót tokenami NFT można stwierdzić, iż w wielu przypadkach stanowią tokeny użytkowe, które to w świetle obowiązujących przepisów prawnych są uznawane za znaki legitymacyjne i nie podlegają nadzorowi Komisji Nadzoru Finansowego.

[13] Wyrok Sądu Najwyższego z dnia 15 lutego 2008 r., w sprawie o sygnaturze I CSK 357/07, OSNC 2009/4/62.
[14] Komisja Nadzoru Finansowego, *op. cit.*, dostęp: dnia 6 czerwca 2022 r.
[15] Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, Dz.U.2022.861 t.j. z dnia 2022.04.21.
[16] Komisja Nadzoru Finansowego, *op. cit.*, (dostęp: 06.06.2022).

4. TOKEN NFT- WPROWADZENIE

Jedną z najnowszych i najpopularniejszych aktualnie nowinek technologicznych jest token NFT. Kiedyś ktoś powiedział - „wszystko jest na sprzedaż"- w ślad za tym powstało NFT (NonFungible Token), w taki oto sposób wszelkie pytania o to, czy uczucia, takie jak miłość, da się kupić, zostały rozwiązane. Media społecznościowe obiegła informacja, iż jedna z polskich influencerek, Pani Marta Rentel dokonała zbycia swojej miłości w formie NFT[17]. Takie informacje są aktualnie powszechne w Sieci. W pierwszej jednak kolejności należy wyjaśnić czym jest token NFT. Na dzień sporządzania niniejszej pracy, tj. na dzień 6 czerwca 2022 r., nie istnieje legalna definicja tokenu NFT.

NFT można pojmować jako niewymienny, unikatowy token, funkcjonujący w oparciu o technologię Blockchain[18]. Niektórzy podkreślają jego zastosowanie, tj. „unikatowa, cyfrowa jednostka danych oparta na architekturze Blockchain, którą użytkownicy protokołu mogą między sobą handlować, reprezentująca szeroką gamę przedmiotów materialnych i niematerialnych, takich jak kolekcjonerskie karty sportowe, wirtualne nieruchomości lub wirtualne dzieła sztuki"[19]. Podsumowując powyższe rozważania, można uznać NFT za konkretny zapis w sieci Blockchain, która to technologia dzięki swojemu rozproszeniu, zapewnia unikatowość zapisu tokenu NFT. W porównaniu zatem z walutą wirtualną- nie są one wymienialne w obrocie gospodarczym, co właśnie ma im zapewnić oryginalność i wyjątkowość. Brak możliwości

[17] Wprost.pl, *Polska celebrytka sprzedała swoją miłość za milion złotych. Skorzystała z tokenu NFT. „Sama dokładnie nie potrafię wytłumaczyć, co to jest"* https://biznes.wprost.pl/technologie/internet/10469958/marta-rentel-albo-marti-renti-sprzedala-swoja-milosc-w-formie-tokenu-nft-zarobila-milion-zlotych.html, (dostęp: 06.06.2022).

[18] Blockchain, (pl. łańcuch bloków) – jeden z rodzajów technologii DLT, rejestr rozproszony i zdecentralizowany, działający w modelu open source, umożliwiający wykonywanie transakcji w modelu komunikacji p2p bez podmiotu centralnego zatwierdzającego transakcje lub przechowującego informacje. Technologia ta zapewnia niezaprzeczalność transakcji oraz pozwala na przechowywanie o nich informacji publicznie w ramach funkcjonujących węzłów z wykorzystaniem zabezpieczeń kryptograficznych. Skutkuje to znacznym utrudnieniem jakiejkolwiek modyfikacji informacji o transakcjach już zapisanych w łańcuchu bloków. Blockchain wykorzystuje jednocześnie funkcje kryptograficzne i algorytmiczne do zapisu oraz synchronizacji danych w ramach sieci w stały sposób. Należy wskazać, że nie każdy rejestr rozproszonych danych wykorzystuje technologię łańcucha bloków. Blockchain, ze względu na swoje cechy może być – oprócz przechowywania danych transakcyjnych – wykorzystywany również do innych celów, chociażby przechowywania dokumentacji czy prowadzenia głosowań. Możemy obecnie wyróżnić Blockchain publiczny, prywatny i hybrydowy w oparciu o to, jak określono zasady dostępu do informacji przetwarzanych na Blockchain. https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf, (dostęp: 06.06.2022).

[19] *Niewymienny token*, https://pl.wikipedia.org/wiki/Niewymienny_token, (dostęp: 06.06.2022).

ich powielenia, powoduje, że zyskują na wartości[20]. Warto również skupić uwagę wokół określenia wymienialności, bowiem jest to najistotniejsza część definicji tokenu NFT. Istotę wymienialności najlepiej zaprezentować na przykładzie wymienialności pieniądza, tj. w obrocie gospodarczym funkcjonuje wiele banknotów o nominale- 100 złotych, a pożyczając podmiotowi trzeciemu 100 zł, nikt nie oczekuje, iż otrzyma zwrot dokładnie tego samego banknotu, bowiem nie ma to dla niego znaczenia, wartość wynika z samej waluty, a nie tego konkretnego banknotu, ponadto istnieje w obiegu wiele banknotów 100 złotowych i nikt nie przywiązuje uwagi do konkretnego egzemplarza. Pieniądze są przykładem rzeczy oznaczonych co do gatunku, a więc dla nikogo nie ma znaczenia, czy zostanie zwrócony ten sam banknot, czy takiego samego rodzaju banknot. Podobnie jest również w przypadku kryptowalut, dlatego w ich definicji legalnej wprost uregulowano, iż są wymienialne. Odmiennie jednak sytuacja wygląda w przypadku tokenów NFT. Nie sposób bowiem wymienić jednego NFT na inny, bowiem są one odmienne, mają inny zapis w sieci Blockchain, dlatego nie sposób ich skopiować, czy powielić. Technologia Blockchain uniemożliwia takie działanie, tj. powielanie tego samego zapisu ciągu bloków, składających się na token NFT[21].

Podsumowując zatem, czym właściwie jest token NFT? Sam token NFT sprowadza się do unikatowego (nie ma drugiego takiego samego) zapisu w sieci Blockchain. Taki zapis może uprawniać do konkretnego cyfrowego pliku, przykładowo do grafiki, wideo czy nawet rzeczywistej usługi, tj. dostęp do prestiżowej grupy czy możliwość uczestnictwa w elitarnym wydarzeniu (tak naprawdę token NFT może uprawniać do wszystkiego, a ograniczeniem jest wyłącznie ludzka wyobraźnia, powyżej wskazano na najbardziej popularne uprawnienia, jakie niesie za sobą token NFT). Token NFT czyli zapis w blockchainie jest powiązany za pomocą smart contractu z grafiką, czy utworem, który dokładnie określa jakie uprawnienia zyska nabywca tokenu NFT. Często ten zapis zawiera link do zewnętrznego serweru, na którym można zapoznać się lub pobrać cyfrową grafikę (lub coś innego, do czego token NFT uprawnia). Co za tym idzie, sam token NFT nie stanowi utworu, nabywca najczęściej kupuje sam zapis i ma uprawnienia do tego zapisu, tj. wyłącznie tych metadanych, a nie tego, do czego token NFT uprawnia i z czym jest

[20] J. Kubalski, A. Czubek, *Obrót NFT, a prawa własności intelektualnej*, https://ssw.solutions/pl/obrot-nft-a-prawa-wlasnosci-intelektualnej/, (dostęp: 05.06.2022).

[21] Binance, *Kto Jest Właścicielem Praw Autorskich do NFT, Twórcy czy Nabywcy?* https://www.binance.com/pl/blog/nft/kto-jest-w%C5%82a%C5%9Bcicielem-praw-autorskich-do-nft-tw%C3%B3rcy-czy-nabywcy-421499824684902084, (dostęp: 06.06.2022).

powiązany- kwestie prawa autorskiego zostały opisane poniżej- niemniej jednak istotne jest nakreślenie ich już w tym miejscu, aby zrozumieć istotę tokenu NFT. Prawna regulacja tokenów NFT byłaby zbyt prosta, gdyby nie odstępstwa, bowiem można również na rynku zaobserwować takie tokeny NFT, w których już sam zapis w sieci Blockchain zawiera jakiś utwór, przykładem może być zapis utworu muzycznego- w takiej sytuacji sam token NFT może stanowić utwór w rozumieniu prawa autorskiego, a tworzenie nowych tokenów (eng. *minting*), będzie w takiej sytuacji prowadził do zwielokrotniania utworu[22].

Mimo iż główny trend nabywania tokenu NFT można zaobserwować od poprzedniego roku, tj. 2021 r., NFT istniało już wcześniej, bowiem w 2014 r. pojawił się pierwszy token o charakterze niewymienialnym, a więc aż 7 lat przed tym, gdy pojawiła się prawdziwa moda na NFT. Swoją popularność NFT zdobywało dzięki grze komputerowej o nazwie CryptoKitties. Reguły ww. gry nakazywały graczom kupno tokenu NFT wirtualnego zwierzęcia w zamian za uzyskanie korzyści w grze[23]. Powyższe wskazuje na typowo użytecznościową cechę tego tokenu, bowiem w zamian za nabycie tokenu, posiadacz uzyskiwał bezpośrednie korzyści w grze komputerowej[24].

NFT w ostatnich latach zdobyło bardzo dużą popularność, a konsumenci kupują praktycznie wszystko- wszystko oczywiście w wersji cyfrowej. Stało się tak niewątpliwie dzięki hasłom reklamowym podkreślającym ich wyjątkowość i niepowtarzalność. NFT służy aktualnie przede wszystkim do nabywania dzieł sztuki, ciekawym przypadkiem jest artysta Banksy, który jedno ze swoich dzieł w formie materialnej, istniejących fizycznie, zniszczył, jednak wcześniej zdigitalizował je, tworząc NFT, a następnie zbył wersję cyfrową tego dzieła[25]. Za najlepsze i najciekawsze ekspozycje można zapłacić nawet kilka milionów. Zapłacić, ale za co konkretnie? Otóż w przypadku nabycia NFT, nabywający nie zawsze zyskuje majątkowe prawa autorskie, to znaczy między innymi, że nie będzie mógł rozpowszechniać dzieła, czy wykorzystywać go do celów komercyjnych. W takim przypadku co konkretnie jest przedmiotem nabycia NFT? Co do zasady - nabywający NFT kupują zapis tokenu

[22] T. Targosz, *NFT w prawie autorskim,* https://www.traple.pl/nft-w-prawie-autorskim/?fbclid=IwAR1qzBinpoVAVoBZYj9milnRZqznVupsefh0Dc1lw0S1PkLiB1zFF0yosPk, (dostęp: 28.11.2022).

[23] Binance, *NFT – Gdzie Kupić?*, https://www.binance.com/pl/blog/nft/nft--gdzie-kupi%C4%87-421499824684902675,m (dostęp: 05.06.2022).

[24] Komentarz autorski.

[25] Newonce, *Tego jeszcze nie było - obraz Banksy'ego został spalony, zdigitalizowany i wystawiony w formie NFT*, https://newonce.net/artykul/tego-jeszcze-nie-bylo-obraz-banksyego-zosta-spalony-zdigitalizowany-i-wystawiony-w-formie-nft, (dostęp: 05.06.2022).

NFT w sieci Blockchain oraz powiązany z nim dostęp do pliku cyfrowego, przykładowo dzieła sztuki, co powoduje, że ich możliwości korzystania z tego dzieła są niewielkie, niemniej jednak każda transakcja tokenem NFT jest inna, a przedmiotem umowy mogą być odmienne uprawnienia. Dlatego nie można wprost określić, co jest przedmiotem nabycia tokenu NFT, bowiem za każdym razem mogą to być odmienne korzyści dla nabywającego[26].

Zgodnie z badaniami prowadzonymi przez Qin Wang, Rujia Li, Qi Wang, Shiping Chen, przede wszystkim jego wynikami, przedstawionymi w dziele, pt. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges „w chwili pisania tego tekstu (maj 2021 r.) łączna suma środków pieniężnych wykorzystanych w ramach zakończonej sprzedaży NFT osiągnęła 34 530 649,86 USD. Tysiąckrotny zwrot z rosnącego rynku przyciąga ogromną uwagę na całym świecie. Jednak rozwój ekosystemu NFT jest wciąż na wczesnym etapie, a technologie NFT są przedwczesne. Z powodu braku systematycznych podsumowań nowicjusze mogą się pogubić w ich szalonym rozwoju"[27]. Zatem rok później kwota ta musiała zwiększyć się co najmniej kilkakrotnie, biorąc pod uwagę popularność, jaką aktywa tego rodzaju, cieszą się na rynku[28].

Tokeny NFT stają się coraz bardziej popularne nie tylko z uwagi na potencjalne możliwości inwestycyjne. Nabywcy tokenów NFT upatrują w nich możliwość zabezpieczenia dzieł sztuki, takich jak grafik, zapisów utworów muzycznych, czy plików wideo, właśnie ze względu na możliwości tokenów NFT, niemożność stworzenia jego kopii. Artyści zauważają szansę w potencjale tokenów NFT[29]. „Jest to atut dla twórców, rynek wtórny był wcześniej bardzo trudny do wyegzekwowania praw do wynagrodzenia. Powszechne są nadal problemy z pobieraniem ustawowego wynagrodzenia droit de suite, nawet przez znanych twórców. Ze względu na niezamienność „kontraktu NFT", za każdym razem, gdy aktywo NFT jest sprzedawane pomiędzy różnymi stronami, strony nie mogą „wycofać się" z postanowień umownych zaszytych w NFT"[30].

[26] M. Sewastianowicz, *Wszystko można kupić, tyle że w NFT - z praktycznym wykorzystaniem nieco gorzej*, https://www.prawo.pl/prawo/nft-a-prawo-autorskie-i-wlasnosc,513011.html, (dostęp: 06.06.2022); J. Kubalski, A. Czubek, *op. cit.*

[27] Qin Wang, Rujia Li, Qi Wang, Shiping Chen, *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges*, https://arxiv.org/abs/2105.07447 (dostęp: 05.06.2022).

[28] Komentarz autorski.

[29] J. Kubalski, A. Czubek, *op. cit.*

[30] *Ibidem.*

Każda rzecz czy usługa może zostać stokenizowana i sprzedana jako token NFT. Daje to potencjał dla rozwoju tego cyfrowego zapisu[31]. Niemniej jednak, unikatowy jest sam zapis w sieci Blockchain, a ważne, aby również powiązane z nim dobro lub usługa była unikatowa. Niewątpliwie, odbiorcom zależy właśnie na tym. Jeśli bowiem unikalny będzie jedynie kod, który jednak będzie powiązany z utworem, który może zostać kupiony przez nieograniczoną liczbę odbiorców, NFT- w ocenie autorki niniejszych rozważań- może stracić w niedługim czasie na znaczeniu[32].

Z analizy praktyki zawodowej, można wywnioskować, iż co do zasady token NFT posiada dwa elementy, tj. element zewnętrzny i wewnętrzny- usługowo- cyfrowy. Oprócz bowiem grafiki czy nagrania, emitenci tokenów NFT coraz częściej oferują konsumentom różnego rodzaju usługi, przykładowo, możliwość dołączenia do elitarnej grupy, uczestnictwa w jakimś wydarzeniu i inne. To właśnie często ta usługa powoduje, że konsumenci przejawiają zainteresowanie nabyciem tokenów NFT. Obserwując rynek projektów z udziałem tokenów NFT, nie można jednak wprost stwierdzić, iż dwuskładnikowe tokeny NFT są zasadą. Rzeczywiście występują często w takiej formie i zdaniem autorki przedmiotowych rozważań, emitenci tokenów NFT wybiorą właśnie tę ścieżkę emisji ww. tokenów, zachęcając tym samym potencjalnych nabywców do zakupu NFT. Dostęp do elitarnej grupy, spotkanie ze światowej sławy aktorem, czy możliwość udziału w prestiżowym wydarzeniu, jest i będzie bezpośrednim motorem dla zakupu NFT[33].

5. PROBLEMATYKA PRAWNA TOKENÓW NFT

5.1. Swoboda umów

Po krótkim omówieniu czym jest token NFT, warto zastanowić się nad prawnymi regulacjami tego rodzaju tokenu. Jak zostało wcześniej wspomniane, nie istnieją aktualnie regulacje prawne wprost odwołujące się do tokenu NFT. Warto zatem na podstawie znanych nam instytucji prawnych, zastanowić się czym token NFT w świetle prawa jest i w jaki sposób następuje prawny obrót tego typu aktywem na rynku. Na pierwszym planie pojawia się najpopularniejsza z umów, tj. umowa sprzedaży, w oparciu o art. 535 par. 1 kc, zgodnie z którym „przez umowę sprzedaży sprzedawca zobowiązuje

[31] J. Kubalski, A. Czubek, *op. cit.*
[32] Komentarz autorki.
[33] Komentarz autorki poparty praktyką zawodową.

się przenieść na kupującego własność rzeczy i wydać mu rzecz, a kupujący zobowiązuje się rzecz odebrać i zapłacić sprzedawcy cenę". Zgodnie jednak z art. 45 Kodeksu cywilnego, „rzeczami w rozumieniu niniejszego kodeksu są tylko przedmioty materialne". Jak podkreśla M. Balwicka-Szczyrba „zgodnie z art. 45 rzeczami są przedmioty materialne. A contrario dobra niematerialne nie mogą otrzymać takiego statusu, pomimo że niekiedy dóbr tych (np. energii czy utworów) dotyczy stosunek cywilnoprawny. (…) Z powyżej wskazanych względów rzeczami nie są również prawa, pomimo że także ich, może dotyczyć obrót cywilnoprawny (np. cesja praw)"[34]. Skoro token NFT jest cyfrową jednostką danych, cyfrowym zapisem- materii zatem nie posiada, stąd nie sposób uznać go jako rzecz. W świetle powyższego, umowa sprzedaży, z uwagi na przedmiot obrotu, tj. niematerialna, cyfrowa wartość, nie może mieć zastosowania do obrotu gospodarczego. Niemniej jednak ww. przedstawicielka doktryny stwierdziła wprost, iż dobra niematerialne mogą być przedmiotem obrotu gospodarczego, a więc tokeny NFT mogłyby być zbywane w ramach takiej umowy[35].

Oprócz powyższego rozwiązania, istnieje również inny sposób, chętnie wykorzystywany przez podmioty, nabywające tokeny NFT. Ww. zbycie może również nastąpić na podstawie art. 353 [1] kc[36], tj. w oparciu o zasadę swobody umów, czyli jednej z naczelnych zasad prawa cywilnego- swobody kontraktowania. Zgodnie z powyższą zasadą, strony mogą w dowolny sposób ułożyć swoje relacje biznesowe, nie mogą one jednak stać w sprzeczności z naturą takiego stosunku gospodarczego, literą prawa, czy zasadami współżycia społecznego. Warto podkreślić, iż nie tylko treść takiego stosunku gospodarczego nie może naruszać ww. wartości, ale również jego cel. Mając na uwadze powyższe, możliwym jest dokonywanie obrotu tokenami NFT w oparciu o zasadę swobody umów, która to zgodnie z twierdzeniami K. Czub, „jest wyrazem autonomii woli stron stosunków obligacyjnych. Fundamentem nowożytnej wolności kontraktowej jest zasada pacta sunt servanda. W polskim systemie prawnym koncepcja swobody umów przyjmuje postać zasady prawnej, zarówno w ujęciu opisowym (określenie typu ukształtowania instytucji prawnej), jak i dyrektywalnym (dyrektywa postępowania, norma prawna)"[37].

[34] M. Balwicka-Szczyrba, A. Sylwestrzak (red.), *Kodeks cywilny. Komentarz*, art. 45, WKP 2022.
[35] *Ibidem*.
[36] Art. 353 [1] Kodeksu cywilnego.
[37] M. Balwicka-Szczyrba (red.), A. Sylwestrzak (red.), *op. cit*.

5.2. Oferta nabycia tokenów NFT

Kolejno, należy wyjaśnić co jest przedmiotem zbycia tokenu NFT, tj. jakie prawa zyskuje nabywca tokenu NFT. Powyższe- jak zostało już w tekście niniejszej pracy wspomniane- w dużej mierze zależy od konkretnej umowy, co zostanie przedstawione poprzez zaprezentowanie kilku ofert nabycia NFT, dostępnych na giełdzie kryptowalut Binance[38]. Przedstawiciele zawodów prawniczych wskazują, iż nabywcy NFT zyskują przede wszystkim dostęp do cyfrowej wersji konkretnego dobra, przykładowo obrazka lub szeroko ujmując, określonego aktywa. Czasem przedmiotem zbycia może być niewyłączna licencja do korzystania z NFT, natomiast raczej nie będą to majątkowe prawa autorskie do konkretnego NFT[39]. Ponadto, wskazuje się, aby dostrzegać różnicę pomiędzy nabyciem na własność zdigitalizowanego aktywa, a majątkowych praw autorskich do konkretnego utworu, co można klarownie przedstawić na przykładzie obrazu znanego malarza. Jeśli obraz zostanie stokenizowany, możliwym jest sprzedanie cyfrowej wersji obrazu podmiotom trzecim. W takiej sytuacji nadal autorskie prawa majątkowe będą należeć do autora, a podmiot trzeci nie będzie miał uprawnień do powielania jego treści czy komercjalizacji[40]. Każdorazowo przy zakupie NFT warto zapoznać się z opisem oferty oraz regulaminu giełdy, czy *whitepaper*, ponieważ to one wyznaczają, co jest przedmiotem umowy. Tylko umowa o przeniesienie autorskich praw majątkowych będzie umożliwiała nabywcy NFT posługiwanie się autorskimi prawami majątkowymi. Musi ona jednak zostać zawarta, tj. automatycznie nie zostaną przeniesione autorskie prawa majątkowe, jeśli umowa nie reguluje takiej kwestii[41].

Przykładowo, jedna z ofert nabycia NFT zawiera następujący opis, tj. „stworzona przez Globe Photos, ta kolekcja 1/1 NFT to Twoja szansa na posiadanie wyjątkowego kawałka historii. Ten NFT pełni również funkcję bezpiecznego cyfrowego Certyfikatu Autentyczności, w którym posiadacz tego NFT będzie mógł ubiegać się o rzeczywiste fizyczne zdjęcie zabytkowe o wymiarach 25 cm na 20 cm, które zostanie wysłane bezpośrednio do niego. Aby uzyskać więcej informacji, śledź @GlobeEntMedia na Twitterze”[42]. Powyższe wskazuje, iż oprócz dostępu do cyfrowego obrazka, nabywca będzie

[38] Binnace, https://www.binance.com/pl/about, (dostęp: 06.06.2022).
[39] M. Sewastianowicz, *op.cit*.
[40] J. Kubalski, A. Czubek, *op. cit.*
[41] Komentarz autorki.
[42] Binance, *Marilyn Vintage Press Print #6*, https://www.binance.com/en/nft/goods/detail?productId=61831260&isProduct=1, (dostęp: 05.06.2022).

mógł żądać wydania rzeczywistego zdjęcia, które autor tej oferty, nazywa zabytkowym. Nie zostało natomiast wskazane czy dojdzie do przeniesienia autorskich praw majątkowych, a więc nie zostaną one przetransferowane. Podsumowując, nabywca nie będzie mógł rozpowszechniać takiego NFT, ani ww. zdjęcia czy komercjalizować go[43].

Z kolei inna oferta, w taki oto sposób opisuje token NFT, tj. „twój przyjazny galaktyczny kosmiczny wojownik przybył! BUBBLES to unikalna kolekcja sztucznych, komicznych mechanoidalnych NFT, mogących przybierać różne formy. Każdy BUBBLES przechodzi przez bardzo drobiazgowy proces projektowania i pielęgnacji, aby zapewnić jego rzadkość. Posiadacze będą mogli brać udział w ekskluzywnych wydarzeniach organizowanych przez naszą społeczność: loteriach, zrzutach, Gachaponach i nie tylko! Posiadanie BUBBLES daje Ci również wyłączne prawa twórcze i komercyjne do Twoich BUBBLES"[44]. Nabywca tokenu NFT, zgodnie z powyższym opisem otrzyma inne uprawnienia, aniżeli na podstawie poprzedniej oferty. Mianowicie przedmiotowa oferta nie nadaje nabywcy żadnych fizycznych przedmiotów, oprócz cyfrowego obrazka, nabywca otrzymuje dostęp do społeczności, w której będą organizowane różnego rodzaju loterie, czy gry. Ostatnie zdanie może wskazywać na przeniesienie również majątkowych praw autorskich do tego NFT lub przynajmniej udzielenie formy licencji na korzystanie w celach komercyjnych z takiego NFT, a więc w celach nastawionych na czerpanie zysku z ww. obrazka[45].

Z kolei opis poniższego tokenu NFT, tj. „special DICE NFT to pierwsza limitowana edycja ITEM NFT gry DICAST P2E ze specjalnymi zdolnościami. Specjalne NFT DICE na normalnym poziomie będą miały następujące statystyki i korzyści. [KORZYŚCI] - Specjalne kości (normalne) - 1000 klejnotów - 27 000 złota [EFEKT KOŚCI] [EKSKLUZYWNY JACK POTWORA/BOHATERA] Zdobądź 1 kartę poniżej co 7 tur. [PÓŁTARCZA], [KOŚCI 1], [KOŚCI 6]"[46], wskazuje na otrzymanie dostępu do cyfrowej wersji obrazka jak również dodatkowych uprawnień w powyższe grze.

Celem przytoczenia powyższych ofert nabycia tokenów NFT jest wskazanie, iż tokeny NFT nie są sobie równe, a nabywając je, jeden podmiot może otrzymać jedynie dostęp do cyfrowej wersji obrazka, drugi z kolei może zyskać

[43] *Ibidem*.
[44] Binance, *BĄBELKI #1132*, https://www.binance.com/en/nft/goods/detail?productId=63066802&isProduct=1, (dostęp: 06.06.2022).
[45] *Ibidem*.
[46] Binance, *Special DICE NFT – Normal*, https://www.binance.com/en/nft/goods/detail?productId=63657687&isProduct=1, (dostęp: 06.06.2022).

uprawnienia do komercyjnego rozpowszechniania tokenu NFT oraz dobra z nim powiązanego. Przykładowo, kolejny token NFT nadaje następujące uprawnienia jego nabywcom, tj. „tajemnicze pudełko z Dark Throne of Epic League. Jego właściciel dostanie totem box do ponownego otwarcia. Rozpakowanie pudełka z totemem jest dostępne w Epic League Hub. Każdy totem może być używany we wszystkich grach z serii Epic League i ma swoją własną rzadkość, wygląd i cechy". Celem ww. tokenów NFT jest przekazanie nabywcy- totemu w powyższej grze komputerowej, które to totemy mają na celu urozmaicenie ww. gry[47].

Oferta zbycia NFT, która precyzyjnie wskazuje co jest jej przedmiotem, tj. jakie uprawnienia nabywca tokenu zyskuje na skutek nabycia tokenu NFT (posługując się jednocześnie językiem prawniczym), to choćby propozycja Mike Shinoda, członka zespołu Linkin Park, który zaoferował klip pt. „Happy Endings" w postaci NFT, w taki sposób opisał warunki zbycia NFT: „udzielane są jedynie ograniczone prawa do osobistego, niekomercyjnego użytku oraz odsprzedaży NFT i nie masz prawa do udzielania licencji, komercyjnego wykorzystania, reprodukcji, dystrybucji, przygotowywania prac zależnych, publicznego wykonywania lub publicznego wyświetlania NFT lub muzyki czy też dzieła sztuki w nim zawartego. Wszelkie prawa autorskie i inne prawa są zastrzeżone i nie są udzielane"[48]. W świetle powyższej oferty nabycia NFT, przedmiotowy token mógłby służyć wyłącznie celom prywatnym, kolekcjonerskim, ewentualnie mógłby zostać odsprzedany innemu podmiotowi, żadne inne uprawnienia, tj. komercyjne wykorzystanie, czy nawet tworzenie dzieł zależnych, nie jest możliwe[49].

W świetle przytoczonych powyżej ofert nabycia tokenów NFT, wprost jest widoczne, iż token NFT tokenowi NFT nie jest równy (zresztą to jest ich cechą, tj. unikatowość, wyjątkowość), a zakres nabywanych uprawnień zależy wyłącznie od treści umowy, co zresztą wpisuje się w zasadę swobody kontraktowania. Za każdym razem, gdy dokonujemy zakupu NFT, warto również zapoznać się z regulaminem serwisu giełdy, na której nabywamy tokeny NFT- akty te również powinny regulować kwestię zbycia tokenów NFT i są przedmiotem umowy pomiędzy nabywcą a zbywcą. Być może, gdy zostanie uregulowane zbycie NFT na poziomie ustawowym (a obrót NFT będzie możliwy nie tylko na podstawie ogólnej zasady swobody umów), ustawodawca

[47] *Dark Throne*, https://darkthrone.epicleague.io/, (dostęp: 05.06.2022).
[48] M. Shinoda, *Warunki NFT*, https://www.mikeshinoda.com/NFTTerms, (dostęp: 05.06.2022).
[49] *Ibidem*.

ureguluje osobno umowę zbycia tokenów NFT i wskaże odgórnie jakiego rodzaju uprawnienia taką umową przechodzą na nabywcę. Na chwilę obecną, kupujący muszą zachować szczególną ostrożność i każdorazowo zapoznać się z przedmiotem zakupu, tym bardziej, gdy nie zawiera on precyzyjnych określeń prawniczych. W takiej sytuacji konsumentowi może być trudno pozyskać informację, co jest dokładnie przedmiotem umowy. Nie sposób również nie zauważyć, iż praktycznie wszystko może zostać stokenizowane i tym samym stać się tokenem NFT. Przytoczone w niniejszej pracy przykłady wskazują, iż nie tylko dzieła sztuki podlegają tokenizacji. Rynek tokenów NFT jest aktualnie tak popularny, że ich przedmiotem może stać się dosłownie wszystko[50].

Brak przejrzystej regulacji prawnej dotyczącej zbywania tokenów NFT jest niebezpieczny dla konsumentów i ochrony ich praw. Może się bowiem okazać, iż na skutek niedoczytania warunków umowy, które to mogą być dostępne nie tylko w treści oferty zbycia tokenów NFT, lecz również- jak zostało powyżej wskazane- w różnego rodzaju regulaminach serwisów internetowych, czy *whitepaper*- konsumenci nie nabędą żadnych praw do zakupionego tokenu NFT. W ocenie autorki przedmiotowego opracowania, nie ulega wątpliwości, że konsument, który wydaje niejednokrotnie duże środki pieniężne na zakup NFT, ma prawo spodziewać się, że otrzyma w zamian konkretne uprawnienia, a nie tylko prawo korzystania z grafiki czy nagrania, które są powiązane z NFT. Takie sytuacje są sprzeczne z zasadami współżycia społecznego i nie powinny mieć miejsca- tym bardziej, biorąc pod uwagę, iż NFT jest nowym rozwiązaniem technologicznym. Niestety, z drugiej właśnie strony, dlatego, że NFT jest nowe, nieuregulowane przez ustawodawcę, opierające się właściwie jedynie na zasadzie swobody umów, ciężko jest chronić konsumenta. W takich sytuacjach (zanim ustawodawca wprowadzi pakiet przepisów prawnych), zaleca się konsumentom zachowanie ostrożności przy zakupie tokenów NFT, bardzo szczegółowe zapoznanie się z warunkami ich nabycia, upewnienie się, jakie regulacje łączą ich z emitentem tokenów NFT (np. oferta nabycia tokenu oraz regulamin, albo umowa elektroniczna i oferta nabycia- mogą być różne konfiguracje)[51].

[50] A. Ziębicki, *NFT - na czym polega, prawo, przykłady*, https://www.infor.pl/prawo/prawa-konsumenta/konsument-w-sieci/5404200,NFT-na-czym-polega-prawo-przyklady.html, (dostęp: 05.06.2022).
[51] Komentarz autorki.

5.3. Prawo autorskie a tokeny NFT

Zanim przejdę do rozważań prawnych na temat przeniesienia autorskich praw majątkowych i udzielenia licencji, należy na wstępie wyjaśnić co jest tak naprawdę przedmiotem rozważań prawnoautorskich. Jak zostało już wspomniane powyżej, token NFT jest to unikatowy zapis na Blockchainie. Sam zapis nie jest rozważany w kontekście prawa autorskiego, gdyż nie stanowi utworu. W kontekście prawa autorskiego analizujemy to, co jest powiązane z zapisem na Blockchainie[52]. Tym samym istotne jest, aby odróżnić uprawnienia do samego zapisu (do samego tokenu NFT), a uprawnienia do tego, z czym NFT się wiąże, np. grafiki. Można bowiem uzyskać prawa do odsprzedania tokenu NFT, ale nie posiadać uprawnienia do rozpowszechniania czy reprodukcji grafiki lub wideo, co sprowadzi się do tego, że podmiot będzie mógł zbyć jedynie zapis w sieci Blockchain. Autorskie prawa majątkowe, jak również udzielenie licencji wymaga odpowiednich postanowień w umowie - bez nich bowiem nie przechodzą na nabywcę ani majątkowe prawa autorskie ani licencyjne, co w praktyce sprowadza się jedynie do możliwości korzystania z jakiegoś prawa[53].

Mając na uwadze prawne uwarunkowania tokenów NFT, tj. nabycie przez nabywcę tokenu NFT, autorskich praw majątkowych w aktualnie obowiązującej, polskiej rzeczywistości prawnej, nie jest możliwe, bowiem zgodnie z art. 53 Prawa autorskiego i praw pokrewnych[54], umowa o przeniesienie autorskich praw majątkowych wymaga zachowania formy pisemnej pod rygorem nieważności. Jak wskazuje jednak A. Niewęgłowski „surogat zwykłej formy pisemnej, o której wyżej mowa, wymienia ustawodawca w przepisie art. 781 § 2 k.c. Chodzi o elektroniczną formę czynności prawnej. Ażeby jej dochować, konieczne jest, po pierwsze, przygotowanie umowy w postaci pliku cyfrowego. Po drugie, w tym pliku strony składają kwalifikowane podpisy elektroniczne. Trzeba podkreślić, że materiałem do oceny, czy podpisy elektroniczne są autentyczne, nie jest wówczas wydruk komputerowy. Oryginalnym dokumentem jest wyłącznie plik cyfrowy utrwalający umowę autorską”[55]. Powyższe może stanowić pewnego rodzaju rozwiązanie, jednakże godziłoby to w sens funkcjonowania NFT w oparciu

[52] T. Targosz, *op. cit.*, (dostęp: 28.11.2022).
[53] J. Kubalski, A. Czubek, *op. cit.*
[54] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U.2021.1062 t.j. z dnia 2021.06.14.
[55] A. Niewęgłowski, *Prawo autorskie. Komentarz*, art. 53, WKP 2021.

o sieć Blockchain, która to ma zapewnić anonimowość tym podmiotom. Z drugiej jednak strony najczęstszymi elementami umowy, jaka łączy nabywcę ze zbywcą tokenów NFT jest regulamin, whitepaper, ewentualnie inne umowy. Nie występuje dwustronna tradycyjna umowa, którą strony podpisują ręcznie lub podpisami kwalifikowanymi, stąd takie rozwiązanie może nie być wystraczające do panującej rzeczywistości zbywania tokenów NFT.

Dobrym rozwiązaniem zatem byłaby modyfikacja ww. przepisu, która pozwalałaby na przeniesienie na nabywcę tokenu NFT, autorskich praw majątkowych, przykładowo poprzez użycie formy dokumentowej. W ocenie autorki niniejszego opracowania, z racji rozwoju technologicznego, przeniesienie autorskich praw majątkowych winno być możliwe na skutek zastosowania formy dokumentowej, postęp technologiczny potrzebuje prostej formy zbycia takich praw[56].

Innym rozwiązaniem ww. sytuacji jest udzielenie licencji. Niestety nie ma możliwości, aby zawrzeć umowę licencji wyłącznej, bowiem zgodnie z art. 67 ust. 5 Ustawy o Prawach autorskich i prawach pokrewnych, umowa licencyjna wyłączna wymaga zachowania formy pisemnej pod rygorem nieważności, zastosowanie znajdzie argumentacja jak powyżej, w przypadku przeniesienia autorskich praw majątkowych [57]. Podsumowując ww. rozważania, najszersze uprawnienia jakie są możliwe do przeniesienia na nabywcę tokenu NFT stanowi aktualnie licencja niewyłączna, bowiem współcześnie obowiązujące polskie przepisy powszechnie obowiązujące, wprowadzając rygor formy pisemnej umowy dla przeniesienia autorskich praw majątkowych oraz udzielenia licencji wyłącznej, uniemożliwiają transfer tych uprawnień na nabywcę tokenu NFT (oczywiście mając również na uwadze jak wygląda w praktyce zbycie tokenów NFT). Pewnym rozwiązaniem byłaby również modyfikacja przepisów, regulujących formę ww. czynności prawnych lub wprowadzenie wyjątku dla obrotu NFT. Jednakże druga możliwość byłaby dostępna dopiero, gdy tokeny NFT zostaną uregulowane bezpośrednio w akcie prawnym i gdy prawo zacznie je wprost dostrzegać. Trzeba mieć jednak na uwadze, iż nie w każdym kraju, ustawodawca wprowadza pisemną formę dla umowy przeniesienia autorskich praw majątkowych lub udzielenia licencji wyłącznej. W takich przypadkach

[56] Komentarz autorki.
[57] Art. 67 ust. 5 Ustawy Prawo autorskie i prawa pokrewne.

możliwym byłoby zaprogramowanie smart contractu w taki sposób, aby zawierał przeniesienie autorskich praw majątkowych do NFT[58].

Podsumowując zatem rozważania na temat praw autorskich w przypadku tokenu NFT, należy odróżnić prawa do tokenu NFT, tj. jako cyfrowego aktywa od posiadania autorskich praw majątkowych do dzieła, z którym NFT jest powiązane. O ile nabywca tokenu NFT, w większości przypadków, otrzyma na własność konkretny token NFT rozumiany jako cyfrowe aktywo, o tyle może to nie znaleźć odwzorowania w prawie autorskim dotyczących tego, z czym token NFT jest powiązany[59].

5.4. Ochrona konsumentów a tokeny NFT

Rynek tokenów NFT nie jest zrozumiały dla wszystkich uczestników obrotu gospodarczego, wręcz przeciwnie - wiele jego podmiotów niedostatecznie skrupulatnie dokonuje weryfikacji tego, co kupuje i to wcale nie za niskie kwoty. W tym miejscu może dojść do naruszenia wielu praw konsumenckich, tj. niewłaściwego opisu oferty przez co konsumenci tak naprawdę nie wiedzą, co kupują. Wyżej wymienione oferty tokenów NFT wskazują, iż nie zawsze opis konkretnej oferty jest precyzyjny. Ponadto, w Sieci wiele osób rekomenduje i reklamuje oferty nabycia tokenów NFT- w wielu przypadkach dochodzi do naruszenia praw konsumenckich, między innymi wprowadzenia konsumentów w błąd co do przedmiotu nabycia[60]. Mając na uwadze powyższe, sytuacji postanowił przyjrzeć się Prezes Urzędu Ochrony Konkurencji i Konsumentów, tj. szeroko pojętej akcji polskich influencerów, zachęcających swoich fanów do zakupu produktów, które nie posiadają cech, o których ci zapewniają. Takie zachowanie wprowadza w błąd konsumentów i powinno być stale monitorowane przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów[61]. W przypadku tokenów NFT bardzo łatwo wprowadzić odbiorców w błąd, a szkoda (biorąc pod uwagę za jakie kwoty są sprzedawane tokeny NFT) może być bardzo wysoka. Powyższe było widoczne choćby podczas akcji funkcjonującej pod nazwą Fancy Bears Metaverse, organizowanej przez

[58] M. Nosowski, *NFT a prawo, czyli co przepisy mówią o tokenach niewymienialnych*, https://www.wsroddanych.pl/post/nft-a-prawo-czyli-co-przepisy-m%C3%B3wi%C4%85-o-tokenach-niewymienialnych, (dostęp: 05.06.2022).

[59] M. Staniszewski, *Jak NFT wpłynie na prawo własności intelektualnej?,* https://nowymarketing.pl/a/36285,jak-nft-wplynie-na-prawo-wlasnosci-intelektualnej, (dostęp: 05.06.2022).

[60] M. Sewastianowicz, *op.cit*.

[61] M. Frączak, *UOKiK przygląda się akcji promocyjnej „misiowej" kolekcji NFT firmy Fanadise*, https://www.politykabezpieczenstwa.pl/pl/a/uokik-przyglada-sie-akcji-promocyjnej-misiowej-kolekcji-nft-firmy-fanadise (dostęp: 05.06.2022).

przedsiębiorcę działającego pod nazwą Fanadise[62]. W ww. akcji marketingowej wzięła udział między innymi Pani Magdalena Gessler, która postanowiła zareklamować token NFT w taki oto sposób- cytując wprost: „ten miś to cyfrowa wersja mnie. Jestem podekscytowana nie tylko byciem częścią tego klubu, ale również możliwościami, jakie technologia NFT daje artystom. Nie jest to coś, co do końca rozumiem, ale czuję, że na naszych oczach dzieje się rewolucja. Poza tym sama jestem malarką, więc jest to coś co odczuwam na bardzo personalnym poziomie"[63]. Pytanie rodzi się jedno, czy powinniśmy akceptować, aby znane w Sieci osoby zwane influencerami, reklamowały coś, czego mechanizmu funkcjonowania same nie rozumieją? Grono odbiorców takich influencerów należy rozumieć jako przeciętnych konsumentów.

Ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym traktuje przeciętnego konsumenta jako podmiot, który posiada dostateczny poziom poinformowania, jest również ostrożny i uważny, podczas podejmowania decyzji, ponadto jest to podmiot, który ocenia rzeczywistość przez pryzmat elementów kulturowych, czy społecznych, jak również ze względu na przynależność do grup konsumenckich, które ww. akt prawny traktuje jako „dającą się jednoznacznie zidentyfikować grupę konsumentów, szczególnie podatną na oddziaływanie praktyki rynkowej lub na produkt, którego praktyka rynkowa dotyczy, ze względu na szczególne cechy, takie jak wiek, niepełnosprawność fizyczna lub umysłowa". Zgodnie z wyrokiem Sądu Najwyższego (dalej jako „SN"), „poziom uwagi i ostrożności przeciętnego konsumenta na użytek oceny przesłanki wprowadzenia w błąd różni się w szczególności w zależności od natury reklamowanego produktu, częstotliwości jego zakupu oraz ceny. Poziom uwagi konsumenta może być zatem niższy, w zależności od tego, jakich produktów dotyczy dana oferta oraz w jakich okolicznościach są one nabywane"[64]. Biorąc pod uwagę naturę tokenu NFT oraz fakt, iż stanowi on swoistą nowinkę technologiczną, nie tak prostą do zrozumienia przez osobę, która nie interesuje się branżą kryptowalut, czy szeroko pojętymi nowymi technologiami, opis tokenu NFT powinien być wyczerpujący, a przede wszystkim należy wprost sformułować, jakie korzyści nabywca tokenu NFT, uzyska. W świetle przytoczonego powyżej wyroku SN, w przypadku tokenów NFT, poziom uwagi i ostrożności konsumenta można spodziewać się, że będzie niższy, aniżeli w przypadku lepiej znanych produktów,

[62] Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym, Dz.U.2017.2070 t.j. z dnia 2017.11.09.
[63] M. Frączak, *op. cit.*
[64] Wyrok Sądu Najwyższego z dnia 5 maja 2021 r., I NSKP 7/21, LEX nr 3225327.

stąd należy konsumentowi wyczerpująco przedstawić ofertę nabycia tokenu NFT. Ponadto, Sąd Apelacyjny w Warszawie zwraca uwagę, iż tzw. przeciętny konsument nie posiada wiedzy specjalistycznej w konkretnej dziedzinie[65]. W ocenie autorki niniejszej pracy, wiedza z zakresu nowych technologii oraz prawa (mowa przecież głównie o przeniesieniu autorskich praw majątkowych czy udzieleniu licencji), to wiedza o charakterze specjalistycznym, której nie posiada przeciętny konsument. Z kolei „jako praktykę wprowadzającą w błąd należy kwalifikować każdą praktykę, która w jakikolwiek sposób, w tym również przez swoją formę wywołuje skutek w postaci, co najmniej możliwości wprowadzenia w błąd przeciętnego konsumenta, do którego jest skierowana i która może zniekształcić jego zachowanie rynkowe"[66], zatem już sama możliwość zrozumienia komunikatu reklamowego w sposób niezgodny z rzeczywistym stanem sprawy, może być uznana za wprowadzającą w błąd konsumenta informację.

Podsumowując rozważania w przedmiocie praw konsumenta i tokenów NFT, konsumenci powinni zachować szczególną ostrożność i czujność, jeśli zamierzają inwestować w tokeny NFT, w tym nie powinni ulegać reklamom influencerów, ponieważ może się okazać, iż nie wszystkie informacje, które oni przekazują, są zgodne ze stanem faktycznym oferty nabycia tokenu NFT. Z kolei, osoby znane, skupiające wokół siebie tzw. *followersów*, powinny bardzo ostrożnie podchodzić do kwestii reklamowania projektów, których same nie rozumieją i których samodzielnie nie zweryfikowały- w końcu swoim wizerunkiem udzielają pewnej rękojmi społecznej dla takich projektów.

5.5. Prawo podatkowe a tokeny NFT

5.5.1. Podatek dochodowy

W świetle przytoczonej powyżej definicji waluty wirtualnej, umiejscowionej w ustawie o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, w ocenie autorki niniejszych rozważań, token NFT nie spełnia przesłanek definicyjnych waluty wirtualnej, tj. nie jest wymienialny, co zostało wprost zaakcentowane w definicji legalnej waluty wirtualnej, stąd też przepisy ustaw podatkowych, odnoszące się do walut wirtualnych- według autorki

[65] Wyrok Sądu Apelacyjnego w Warszawie z dnia 24 kwietnia 2018 r., VII AGa 247/18, LEX nr 2668905.
[66] Wyrok Sądu Apelacyjnego w Warszawie z dnia 22 marca 2017 r., VI ACa 1863/15, LEX nr 2308678.

niniejszego opracowania- nie powinny być automatycznie stosowane wobec tokenów NFT. Analiza dotyczy przepisów zarówno ustawy o podatku dochodowym od osób fizycznych[67], jak również ustawy o podatku dochodowym od osób prawnych[68]. Z uwagi na fakt, iż w praktyce nabycia NFT dokonuje się za pośrednictwem waluty wirtualnej, warto wspomnieć o regulacjach podatkowych również waluty wirtualnej. Z uwagi na wprowadzenie do polskiego porządku prawnego definicji waluty wirtualnej i zaimplementowania jej do ustaw podatkowych, określenie skutków obrotu walutami wirtualnymi nie powoduje takich trudności, jak w czasach, gdy definicji legalnej nie było w systemie prawnym.

Zgodnie z art. 7b ust. 1 pkt 6 lit. f ustawy o podatku dochodowym od osób prawnych, przychody z wymiany walut wirtualnych na środek płatniczy, towar, usługę lub prawo majątkowe inne niż waluta wirtualna lub z regulowania innych zobowiązań walutą wirtualną, stanowią przychód z zysków kapitałowych. Analogiczny przepis prawny funkcjonuje w ustawie o podatku dochodowym od osób fizycznych, bowiem przychody z kapitałów pieniężnych stanowią przychody z odpłatnego zbycia waluty wirtualnej.

Tokeny NFT nie są walutami wirtualnymi, niemniej jednak powyższe rozważania mają duży wpływ na obrót NFT, bowiem- jak zostało wspomniane- NFT nabywa się najczęściej właśnie za waluty wirtualne. Niemniej jednak, pozostawiając na uboczu regulacje dotyczące waluty wirtualnej, tokeny NFT w świetle ustaw podatkowych, mogą zostać uznane za prawa majątkowe, a przychód uzyskany z NFT może stanowić przychód z praw majątkowych (tak samo były kwalifikowane kryptowaluty przed wprowadzeniem do porządku prawnego ich legalnej definicji). Ustawy podatkowe w przedmiocie podatku dochodowego nie wprowadzają jednak definicji legalnej prawa majątkowego, a zatem koniecznym jest sięgniecie do doktryny. P. Małecki i M. Mazurkiewicz wprost przyznają, iż „przedmiotem obrotu mogą być także prawa majątkowe. Ustawa nie zawiera również definicji praw majątkowych. Bez wątpienia są one rodzajem praw podmiotowych, uwarunkowanych interesem ekonomicznym podatnika. Mogą to być zatem prawa rzeczowe, wierzytelności bądź też prawa na dobrach niematerialnych (prawa autorskie, prawa wynikające z przepisów o wynalazczości, o ochronie topografii układów scalonych, o znakach towarowych itp.). Szczególnym rodzajem praw majątkowych mogą być również

[67] Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, Dz.U.2021.1128 t.j. z dnia 2021.06.24.
[68] Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych, Dz.U.2021.1800 t.j. z dnia 2021.10.04.

prawa spadkowe i rodzinne. Prawa majątkowe mogą przynosić przychody bądź przez ich wykonywanie, bądź z tytułu ich sprzedaży"[69].

Zgodnie z art. 18 ustawy o podatku dochodowym od osób fizycznych, „za przychód z praw majątkowych uważa się w szczególności przychody z praw autorskich i praw pokrewnych w rozumieniu odrębnych przepisów, praw do projektów wynalazczych, praw do topografii układów scalonych, znaków towarowych i wzorów zdobniczych, w tym również z odpłatnego zbycia tych praw"[70]. Ww. katalog pozostaje otwarty, a zaprezentowane przykłady nie wypełniają definicji prawa majątkowego (z uwagi na użycie stwierdzenia „w szczególności"). Przepis ten szeroko obejmuje wszelkie uprawnienia, mające charakter majątkowy. Tokeny NFT mogą wpisywać się właśnie w taką interpretację jako nieposiadające materii, cyfrowe aktywa, przynoszące jednak przychód. Mimo iż pojawia się coraz więcej indywidualnych interpretacji podatkowych, nadal tokeny NFT są nowym zjawiskiem i trzeba mieć na uwadze, iż stanowisko organów podatkowych dopiero się kształtuje. Zwłaszcza gdy chodzi o nowe technologie, takie jak NFT zajęcie jednoznacznego stanowiska, jest w praktyce czasochłonne.

5.5.2. Podatek od towarów i usług

Również w przypadku rozważań prawnych w przedmiocie podatku od towarów i usług, należy podkreślić ponownie, iż tokeny NFT nie realizują przesłanek definicyjnych waluty wirtualnej, przynajmniej nie w takim kształcie jak je aktualnie postrzegamy (ze względu na cechę niewymienialności), do których zastosowanie znajdzie zwolnienie z podatku od towarów i usług, bowiem zgodnie z art. 43 ust 1. ww. ustawy, przewidującym zwolnienia od przedmiotowego podatku, podatkowi nie podlegają transakcje, „łącznie z pośrednictwem, dotyczące walut, banknotów i monet używanych jako prawny środek płatniczy, z wyłączeniem banknotów i monet będących przedmiotami kolekcjonerskimi, za które uważa się monety ze złota, srebra lub innego metalu oraz banknoty, które nie są zwykle używane jako prawny środek płatniczy lub które mają wartość numizmatyczną"[71], ani też „usługi w zakresie depozytów środków pieniężnych, prowadzenia rachunków

[69] P. Małecki, M. Mazurkiewicz, *CIT. Podatki i rachunkowość. Komentarz*, wyd. XII, art. 14, WKP 2021.
[70] Art. 18 ustawy o podatku dochodowym od osób fizycznych.
[71] Art. 43 ust. 1 pkt 7 Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług, Dz.U.2022.931 t.j. z dnia 2022.04.29.

pieniężnych, wszelkiego rodzaju transakcji płatniczych, przekazów i transferów pieniężnych, długów, czeków i weksli oraz usługi pośrednictwa w świadczeniu tych usług”[72]. Powyższe zwolnienia mają zastosowanie do walut wirtualnych, a contrario- skoro token NFT, nie jest walutą wirtualną, zwolnieniu na podstawie ww. przepisu prawnego (ani żadnego innego), nie będzie podlegał. Podsumowując zatem rozważania na tle ustawy podatku od towarów i usług, podatek ten wystąpi w podstawowej stawce 23% w przypadku zbycia tokenów NFT[73].

Fakt, iż wymiana walut wirtualnych na NFT będzie opodatkowana podatkiem od towarów i usług potwierdza praktyka organów podatkowych, wyrażona w indywidualnej interpretacji przepisów prawa podatkowego, wydanej w sprawie o sygnaturze: 0112-KDIL1-3.4012.279.2022.2.KK, tj. „opisane przez Wnioskodawcę świadczenia, polegające na transakcji sprzedaży tokenów NFT za X (walutę wirtualną) wypełnią definicję odpłatnego świadczenia usług, o którym mowa w art. 8 ust. 1 ustawy, i jako takie stanowić będą czynności podlegające opodatkowaniu podatkiem od towarów i usług. (…) W przedmiotowej sprawie, w przypadku sprzedaży tokenów w zamian za X (walutę wirtualną) będziemy mieli do czynienia ze świadczeniem za wynagrodzeniem – usługi za usługę. (…) W konsekwencji transakcja sprzedaży tokenów NFT będzie podlegała opodatkowaniu podatkiem VAT na podstawie art. 5 ust. 1 pkt 1 ustawy, jako odpłatne świadczenia usług w rozumieniu art. 8 ust. 1 ustawy, i nie będzie korzystała ze zwolnienia od podatku od towarów i usług”[74]. Trzeba mieć jednak na uwadze, iż stany faktyczne z udziałem tokenów NFT, będące przedmiotem wydawanych interpretacji indywidualnych przez Dyrektora Krajowej Informacji Skarbowej są bardzo różne i każdorazowo należy dokonać oceny *ad casum*.

W niektórych indywidualnych interpretacjach prawa podatkowego można zauważyć, iż organy podatkowe nie chcą dokonywać oceny w przedmiocie tego, czy tokeny NFT spełniają przesłanki waluty wirtualnej, wymagając określenia tego faktu przez wnioskodawcę. Przykładem takiej indywidualnej interpretacji może być sprawa o sygnaturze 0111-KDIB1-1.4010.224.2022.2.SH. Powyższe wskazuje, iż potrzeba wprowadzenia precyzyjnej regulacji jest niezbędna, organy stosujące prawo nie powinny

[72] Art. 43 ust. 1 pkt 40 Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług.
[73] Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług.
[74] Dyrektor Krajowej Informacji Skarbowej, *Interpretacja indywidualna*, 0112-KDIL1-3.4012.279.2022.2.KK, https://eureka.mf.gov.pl/informacje/podglad/512331;keyWords=NFT, (dostęp: 28.11.2022).

zmagać się z takimi problemami, tj. „na wstępie należy zaznaczyć, że w niniejszej sprawie jako element opisu stanu zdarzenia przyszłego przyjęto wskazanie Wnioskodawcy, że stworzone i wyemitowane przez Wnioskodawcę tokeny NFT nie spełniają definicji waluty wirtualnej w rozumieniu art. 4a pkt 22a ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (Dz. U. z 2021 r. poz. 1800 ze zm., dalej „ustawa o CIT"). Ta okoliczność nie była tym samym przedmiotem oceny Organu"[75]. Ciężar ten nie powinien być przenoszony na wnioskodawcę, który składając wniosek o wydanie indywidualnej interpretacji przepisów prawa podatkowego poszukuje rozwiązania problemu sposobu rozliczania podatku, zwłaszcza gdy kwalifikacja w tym przypadku NFT jako waluty wirtualnej ma decydujące znaczenia pod względem podatkowym. Obywatel bowiem może nie znać przesłanek ustawowych waluty wirtualnej, a do wydania interpretacji powinien być wystarczający sam opis zdarzenia, bez prawnej kwalifikacji NFT jako waluty wirtualnej. Obywatel bowiem w ocenie autorki niniejszej pracy, nie jest nawet podmiotem uprawnionym do wydawania takich osądów. Ten obowiązek należy do organów państwowych, w tym do ustawodawcy. Niestety w czasach niepewności legislacyjnej i braku tak potrzebnej dla obrotu (w tym konsumenckiego) regulacji prawnej, są podejmowane próby obarczenia tym brakiem tych, którzy powinni być najbardziej chronieni- obywateli.

6. ZAKOŃCZENIE

Na wstępie niniejszej pracy, przedstawiono w jaki sposób token NFT jest definiowany w świetle technologiczno- biznesowym, bowiem definicji legalnej tokenu NFT polski system prawny jeszcze nie zna. Przeprowadzono również analizę porównawczą tokenu NFT do waluty wirtualnej oraz tokenu użytkowego. Autorka niniejszych rozważań stwierdziła, iż token NFT nie powinien być kwalifikowany jako waluta wirtualna, bowiem nie spełnia przesłanek definicyjnych waluty wirtualnej pod warunkiem, że token NFT rozumiemy przez pryzmat jego niewymienialności. Token NFT bardziej przypomina swoimi cechami token użytkowy. Następnie, pochylono się nad prawną analizą tokenu NFT i tego, co jest przedmiotem jego obrotu, tj. jakie korzyści uzyskuje nabywca tokenu NFT. Jednak z uwagi na brak jakichkolwiek regulacji prawnych dotyczących wprost NFT, polegając wyłącznie na zasadzie swobody

[75] Dyrektor Krajowej Informacji Skarbowej, *Interpretacja indywidualna*, 0111-KDIB-1-1.4010.224.2022.2.SH, https://eureka.mf.gov.pl/informacje/podglad/511149;keyWords=NFT, (dostęp: 28.11.2022).

umów, każdorazowo obrót NFT należy zweryfikować pod względem treści umowy pomiędzy nabywcą, a zbywcą. Kolejno, przedstawiono możliwości zbycia tokenów NFT i powiązanych z nimi dóbr w kontekście prawa autorskiego, tj. udzielenie licencji lub przeniesienie autorskich praw majątkowych. Pracę zamyka analiza prawa podatkowego, tj. w jaki sposób rozliczać podatek dochodowy oraz podatek od towarów i usług w przypadku nabycia tokenów NFT, przytoczono także stanowiska organów podatkowych, dotyczących tokenów NFT.

Mając na uwadze powyższe, należy stwierdzić, iż cele pracy, postawione na wstępie, zostały osiągnięte. Niniejsza praca pokazała jak istotne jest, aby nowinki technologiczne, jakim niewątpliwie są tokeny NFT, odnalazły swoje miejsce w porządku prawnym. Brak bowiem regulacji prawnej, generuje ryzyko i niebezpieczeństwo obrotu dla nabywających tokeny NFT. System prawny ma na celu ochronę praw słabszych podmiotów. W tym przypadku niewątpliwie są nimi podmioty nabywające tokeny NFT - w dużej mierze konsumenci. Zwłaszcza na początku, gdy mechanizmów prawnych brakuje, a organy egzekwujące prawo same nie wiedzą, jakie przepisy powinny stosować, konsument musi liczyć przede wszystkim na siebie i zachować szczególną ostrożność i rozsądek, nabywając tokeny NFT. Zanim jednak powstaną konkretne przepisy, dotyczące tokenów NFT i zanim ustawodawca zaproponuje definicję legalną tokenu NFT, powinniśmy zakwalifikować mechanizm tokenu NFT do istniejących instytucji prawnych. I o ile, można zrozumieć ustawodawcę, że regulacja nowego rozwiązania technologicznego wymaga trochę czasu, tak zakwalifikowanie przejściowo NFT do istniejących rozwiązań prawnych, powinno nastąpić o wiele szybciej. Podobny problem był z walutami wirtualnymi, co zostało opisane na początku niniejszych rozważań- warto zatem byłoby, aby ustawodawca bazując na tamtym doświadczeniu nie zwlekał z regulacją tak długo i aby zaproponował przejściowe przepisy (kwalifikację pod istniejące już rozwiązania prawne)- brak bowiem jakichkolwiek wytycznych rodzi chaos i nie chroni praw tych, o których powinien dbać.

Niewątpliwie rozważaniom na temat tokenów NFT towarzyszą zapytania na temat celu nabywania tokenów NFT za tak duże kwoty. Tak naprawdę w tym momencie należałoby zapytać tych, którzy wydali już bajońskie sumy na cyfrowe aktywa. Niewątpliwie wyjątkowość i oryginalność egzemplarza przemawia do nabywających. Czy jednak nie kryje się za tym głębszy cel? Z pewnością podmioty nabywające tak drogie tokeny NFT oczekują zysku z odsprzedaży ich za jakiś czas za kwotę wyższą, aniżeli którą uiścili celem nabycia tokenu NFT (cel inwestycyjny). Ponadto, oprócz oczywistych chęci

zysku, nabywcy zapewne pragną być częścią elitarnej społeczności, nabywając konkretne tokeny NFT. Dodatkowo popyt na tokeny NFT zwiększają znani twórcy, ich historie, sława czy ponadczasowość albo szeroko pojęta moda. Nie rzadko kupowane tokeny NFT mają pomagać graczom wygrywać pojedynki w wirtualnej rzeczywistości i wzbogacają metawersum. To, co konkretny token NFT może zaoferować, praktycznie nie ma granic- za wyjątkiem ludzkiej wyobraźni. Pytanie jednak, czy będą to korzyści, jakich spodziewali się ci, którzy zdecydowali się nabyć tokeny NFT za tak duże sumy? Jak zatem pogodzić prawo i nowe technologie? Trzeba być z nimi przede wszystkim na bieżąco.

BIBLIOGRAFIA

Akty prawne:

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U.1997.78.483 z dnia 1997.07.16

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz.U.2020.1740 t.j. z dnia 2020.10.08.

Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, Dz.U.2021.1128 t.j. z dnia 2021.06.24.

Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych, Dz.U.2021.1800 t.j. z dnia 2021.10.04.

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U.2021.1062 t.j. z dnia 2021.06.14.

Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług, Dz.U.2022.931 t.j. z dnia 2022.04.29.

Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, Dz.U.2022.861 t.j. z dnia 2022.04.21.

Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym, Dz.U.2017.2070 t.j. z dnia 2017.11.09.

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U.2022.593 t.j. z dnia 2022.03.15.

Źródła internetowe:

Binance, *BĄBELKI #1132*, https://www.binance.com/en/nft/goods/detail?productId=63066802&isProduct=1 (dostęp: 06.06.2022).

Binance, *Kto Jest Właścicielem Praw Autorskich do NFT, Twórcy czy Nabywcy?* https://www.binance.com/pl/blog/nft/kto-jest-w%C5%82a%C5%9Bcicielem-praw-autorskich-do-nft-tw%C3%B3rcy-czy-nabywcy-421499824684902084 (dostęp: 06.06.2022).

Binance, *NFT – Gdzie Kupić?* https://www.binance.com/pl/blog/nft/nft--gdzie-kupi%C4%87-421499824684902675 (dostęp: 05.06.2022).

Dark Throne, https://darkthrone.epicleague.io/ (dostęp: 05.06.2022).

Dyrektor Krajowej Informacji Skarbowej, interpretacja indywidualna, 0112-KDIL-1-3.4012.279.2022.2.KK, https://eureka.mf.gov.pl/informacje/podglad/512331;keyWords=NFT, (dostęp: 28.11.2022).

Dyrektor Krajowej Informacji Skarbowej, interpretacja indywidualna, 0111-KDIB-1-1.4010.224.2022.2.SH, https://eureka.mf.gov.pl/informacje/podglad/511149;keyWords=NFT,(dostęp: 28.11.2022).

Frączak M., *UOKiK przygląda się akcji promocyjnej „misiowej" kolekcji NFT firmy Fanadise*, https://www.politykabezpieczenstwa.pl/pl/a/uokik-przyglada-sie-akcji-promocyjnej-misiowej-kolekcji-nft-firmy-fanadise (dostęp: 05.06.2022).

Kubalski J., Czubek A.*, Obrót NFT, a prawa własności intelektualnej*, https://ssw.solutions/pl/obrot-nft-a-prawa-wlasnosci-intelektualnej/ (dostęp: 05.06.2022).

Marilyn Vintage Press Print #6, https://www.binance.com/en/nft/goods/detail?productId=61831260&isProduct=1 (dostęp: 05.06.2022).

Newonce, *Tego jeszcze nie było - obraz Banksy'ego został spalony, zdigitalizowany i wystawiony w formie NFT*, https://newonce.net/artykul/tego-jeszcze-nie-bylo-obraz-banksyego-zosta-spalony-zdigitalizowany-i-wystawiony-w-formie-nft (dostęp: 05.06.2022).

Niewymienny token, https://pl.wikipedia.org/wiki/Niewymienny_token (dostęp: 06.06.2022).

Nosowski M., *NFT a prawo, czyli co przepisy mówią o tokenach niewymienialnych*, https://www.wsroddanych.pl/post/nft-a-prawo-czyli-co-przepisy-m%C3%B3wi%C4%85-o-tokenach-niewymienialnych (dostęp: 05.06.2022).

Qin Wang, Rujia Li, Qi Wang, Shiping Chen, Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges, https://arxiv.org/abs/2105.07447 (dostęp: 05.06.2022).

Sewastianowicz M., *Wszystko można kupić, tyle że w NFT - z praktycznym wykorzystaniem nieco gorzej,* https://www.prawo.pl/prawo/nft-a-prawo-autorskie-i-wlasnosc,513011.html (dostęp: 06.06.2022).

Shinoda M., *Warunki NFT*, https://www.mikeshinoda.com/NFTTerms (dostęp: 05.06.2022).

Special DICE NFT – Normal, https://www.binance.com/en/nft/goods/detail?productId=63657687&isProduct=1 (dostęp: 06.06.2022).

Staniszewski M., *Jak NFT wpłynie na prawo własności intelektualnej?*, https://nowymarketing.pl/a/36285,jak-nft-wplynie-na-prawo-wlasnosci-intelektualnej (dostęp: 05.06.2022).

Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf (dostęp: 06.06.2022).

Targosz T., *NFT w prawie autorskim*, https://www.traple.pl/nft-w-prawie-autorskim/?fbclid=IwAR1qzBinpoVAVoBZYj9milnRZqznVupsefh0Dc1lw0S1PkLiB1zFF0yosPk, (dostęp: 28.11.2022).

Wprost.pl, *Polska celebrytka sprzedała swoją miłość za milion złotych. Skorzystała z tokenu NFT. „Sama dokładnie nie potrafię wytłumaczyć, co to jest"* https://biznes.wprost.pl/technologie/internet/10469958/marta-rentel-albo-marti-renti-sprzedala-swoja-milosc-w-formie-tokenu-nft-zarobila-milion-zlotych.html (dostęp: 06.06.2022).

Ziębicki A., *NFT - na czym polega, prawo, przykłady*, https://www.infor.pl/prawo/prawa-konsumenta/konsument-w-sieci/5404200,NFT-na-czym-polega-prawo-przyklady.html (dostęp: 05.06.2022).

Orzecznictwo:

Wyrok Sądu Najwyższego z dnia 15 lutego 2008 r., w sprawie o sygnaturze I CSK 357/07, OSNC 2009/4/62

Wyrok Sądu Najwyższego z dnia 5 maja 2021 r., I NSKP 7/21, LEX nr 3225327.

Wyrok Sądu Apelacyjnego w Warszawie z dnia 22 marca 2017 r., VI ACa 1863/15, LEX nr 2308678.

Wyrok Sądu Apelacyjnego w Warszawie z dnia 24 kwietnia 2018 r., VII AGa 247/18, LEX nr 2668905.

Literatura:

Balwicka-Szczyrba M., Sylwestrzak A. (red.), *Kodeks cywilny. Komentarz, art. 45,* WKP 2022.

Małecki P., Mazurkiewicz M., *CIT. Podatki i rachunkowość. Komentarz, wyd. XII, art. 14*, WKP 2021.

Niewęgłowski A., *Prawo autorskie. Komentarz, art. 53*, WKP 2021.

LAW IN THE FACE OF NFT

Abstract: Nowadays, new technologies are gaining popularity. Network participants are constantly looking for new forms of investing their capital. Like cryptocurrencies in the past, NFT tokens have now appeared on the market. People tokenize and put up for sale the least expected things, such as their body or feelings of love. On the surface it sounds abstract, but the amounts paid for various types of NFT tokens reach tens of millions of dollars. So what is an NFT token and what makes its value so high? An NFT token is a non-exchangeable, unique digital asset, functioning on the Blockchain Network. So what is the subject of the NFT token divestment? Exactly what the parties decide in the contract. The subject matter of the contract depends entirely on the individual case, whether it be solely the right to access the digital asset or perhaps a non-exclusive licence. The issue of NFT has not yet been directly regulated by generally applicable regulations in the Republic of Poland. In view of the above, it is necessary to place NFT tokens in currently existing legal institutions, such as, for example, the institution of ID tokens.

Keywords: NFT, law, new technologies, investing,

ISBN: 978-83-67527-55-2