Prof. dr hab. Jacek Gołaczyński
Uniwersytet Wrocławski

Recenzja rozprawy doktorskiej mgr Klaudii Maciejewskiej pt. „Prawne aspekty wykorzystania sztucznej inteligencji jako narzędzia podwyższającego efektywność i bezpieczeństwo systemów teleinformatycznych przetwarzających dane osobowe"

1. Uwagi wstępne

Tematyka rozprawy doktorskiej odnosząca się do sztucznej inteligencji w zakresie prawnych jej aspektów jako narzędzia podwyższającego efektywność i bezpieczeństwo systemów teleinformatycznych przetwarzających dane osobowe stanowi doniosłe zagadnienie prawne oraz informatyczne. Autorka słusznie zauważyła, że technologia i będące u jej podstaw, sztuczna inteligencja powoduje nowe zagrożenia i wyzwania dla organów regulacyjnych na całym świecie. Te wyzwania, a nawet zagrożenia obejmują ryzyko stronniczości i dyskryminacji, brak przejrzystości, wyjaśnialności i ludzkiego nadzoru, potencjalne szkody dla prywatności, podatność systemów sztucznej inteligencji na zagrożenia. Słusznie autorka wskazuje, że problemami związanymi z tytułowym wykorzystaniem narzędzi sztucznej inteligencji są także bezpieczeństwo, cyberbezpieczeństwo, ochrona danych osobowych, odpowiedzialność i kwestie związane z własnością intelektualną. Tymi zagadnieniami będzie się zajmowała w poszczególnych rozdziałach swojej rozprawy.

Autorka trafnie zauważa, że sztuczna inteligencja powoduje także zagrożenia, które mogą mieć negatywny wpływ na jednostki, grupy, organizacje, społeczności i społeczeństwo. Podobnie jak ryzyko związane z innymi rodzajami technologii, zagrożenia te mogą występować w różnej postaci i można je scharakteryzować jako długo- lub krótkoterminowe, o wysokim lub niskim prawdopodobieństwie wystąpienia, systemowe lub zlokalizowane oraz o dużym lub małym wpływie na rynek. Ryzyko to sprawia, że sztuczna inteligencja jest wyjątkowo trudną technologią do wdrożenia i wykorzystania zarówno w organizacjach. Stąd też prawidłowe spostrzeżenie autorki, że bez odpowiedniej kontroli, systemy AI mogą wzmacniać, utrwalać lub pogarszać niesprawiedliwe lub niepożądane skutki

dla osób z nich korzystających. Właściwa kontrola i wdrożenie zgodnie z *ethics by design*, systemy AI będą mogły łagodzić i zarządzać niesprawiedliwymi wynikami, jak również wykrywać niebezpieczeństwa, identyfikować podejrzane aktywności, tworzyć oprogramowanie, a także wykonywać wiele innych czynności. Coraz powszechniejsze stosowanie sztucznej inteligencji stanowi zmianę paradygmatu rozumienia i rozwoju oprogramowania oraz regulacji prawnych z tym związanych. Globalny krajobraz AI szybko ewoluuje, a nowe technologie są regularnie wprowadzane na rynek. Obecny ekosystem sztucznej inteligencji składa się z szerokiej gamy modeli i technik AI na różnych poziomach dojrzałości. W tym kontekście obowiązujące praktyki i procedury w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych są już dobrze ugruntowane i wykorzystywane do zabezpieczania tradycyjnych systemów opartych na oprogramowaniu oraz mają ograniczoną zdolność do radzenia sobie z szerszym zakresem zagrożeń wynikających ze stosowania systemów AI. Na poziomie międzynarodowym i europejskim trwają badania oraz wysiłki operacyjne mające na celu lepsze zrozumienie i zajęcie się tymi zagrożeniami, rozszerzenie obecnych praktyk i procedur oraz opracowanie nowych w celu zapewnienia bezpieczeństwa systemów sztucznej inteligencji. Stąd tez autorka zasadnie uznaje, że te wysiłki skutkują opracowaniem narzędzi zarządzania ryzykiem oraz definicją środków kontroli bezpieczeństwa, które są dostosowane do specyfiki zabezpieczania systemów AI, w tym odpowiednich wskaźników i środków łagodzących celem wyeliminowania luk w zabezpieczeniach specyficznych dla AI. Z tego punktu widzenia zarządzanie ryzykiem i jakością związane ze sztuczną inteligencją stanowi kluczowy element odpowiedzialnego rozwoju i użytkowania systemów AI. Odpowiedzialne praktyki sztucznej inteligencji mogą pomóc w dostosowaniu decyzji dotyczących projektowania, rozwoju i użytkowania systemów AI do zamierzonego celu i wartości. Słuszny jest także pogląd, że zarządzanie ryzykiem związanym z systemami AI może zwiększyć ich wiarygodność. Istnieje przy tym potrzeba całościowego rozważenia zarówno zagrożeń, jak i korzyści związanych z systemami sztucznej inteligencji w zakresie wyzwań regulacyjnych i etycznych.

Z tej perspektywy należy uznać, że temat rozprawy doktorskiej przedstawiony w tytule jest aktualny, i zmierza do rozwiązania istotnego pod względem jurydycznym zagadnienia, czyli opisu prawnych aspektów działania narzędzi sztucznej inteligencji dla zapewnienia efektywności systemów teleinformatycznych przetwarzających dane osobowe. Do tej pory w literaturze polskiej pojawiły się publikacje dotyczące prawnych aspektów sztucznej inteligencji, np. monografie pod red M. Świerczyńskiego i L. Lai, ale nie omawiały

zagadnienia efektywności narzędzi AI w zakresie systemów teleinformatycznych przetwarzających dane osobowe. Niniejsza praca zatem ma walor nowości.

Autorka formułuje następnie cele badawcze pracy(we wstępie rozprawy doktorskiej), a następnie w poszczególnych rozdziałów stara się je rozwijać.

Najważniejszym celem badawczym pracy jest ustalenie wpływu stosowania nowych technologii i usług cyfrowych dla koncepcji odpowiedzialności z perspektywy praw podstawowych. Rozważania zostały ograniczone do technologii AI, z uwzględnieniem uczenia maszynowego, sieci neuronowych, modeli AI ogólnego przeznaczenia, w tym generatywnej sztucznej inteligencji. Autorka stawia także hipotezę, że technologie sztucznej inteligencji dają już obecnie duże korzyści, przez zwiększenie wydajności, dokładności, terminowości i wygody świadczenia wielu usług.

Należy także odnotować, że opracowanie naukowe stanowiące rozprawę doktorską jest rezultatem prac badawczych oraz przeprowadzonej indukcyjnej i dedukcyjnej metody wnioskowania poświęconej analizie znaczenia sztucznej inteligencji dla bezpieczeństwa teleinformatycznego w inteligentnych sieciach i systemach, wykorzystywania inteligentnych systemów bezpieczeństwa (ang. *smart security*) w procesach technologicznych i społecznych, jak również wykorzystywania sztucznej inteligencji w tworzeniu bezpiecznych systemów teleinformatycznych, informatycznych, a także bezpiecznych systemów gromadzenia danych, weryfikacji, archiwizacji i przekazywania danych osobowych.

Obok zasadniczego zagadnienia badawczego, Autorka postawiła szereg tez pomocniczych:

1) zdiagnozowania zakresu zastosowania sztucznej inteligencji na potrzeby tworzenia inteligentnych sieci i systemów teleinformatycznych, w szczególności w zakresie bezpiecznych systemów gromadzenia danych;
2) zbadania wpływu systemów AI na pojęcie odpowiedzialności, w szczególności w zakresie, w jakim mogą one utrudniać korzystanie z praw człowieka i podstawowych wolności, oraz w kwestii odpowiedzialności za te zagrożenia i konsekwencje;
3) odzwierciedlenia stosowania sztucznej inteligencji w przepisach prawa powszechnie obowiązującego, na polu odpowiedzialności cywilnoprawnej za szkody wyrządzone przy wykorzystaniu systemów sztucznej inteligencji oraz ochrony własności intelektualnej;

4) ustalenia wartości wdrożeniowej dla przedsiębiorcy (Currenda Sp. z o.o.) działającego na rynku usług informatycznych zastosowania sztucznej inteligencji w systemach teleinformatycznych dla wymiaru sprawiedliwości i zawodów prawniczych.

Niniejsza praca nie ogranicza się zatem do przedstawienia i oceny obowiązujących oraz projektowanych przepisów prawa w obszarze sztucznej inteligencji, odpowiedzialności prawnej za szkody wyrządzone przy zastosowaniu sztucznej inteligencji, a także problematyki przetwarzania danych osobowych zaangażowanych w cały *life cycle* systemów AI przy zastosowaniu metody analityczno-porównawczej.

Na uwagę zasługuję, że efektem prowadzonych badań jest wdrożenie na rynek innowacyjnego systemu informacji prawnej do monitorowania zmian aktów prawnych przy wykorzystaniu sztucznej inteligencji, a także opracowanie u przedsiębiorcy (Currenda Sp. z o.o.) dokumentacji projektowej opartej na etycznej sztucznej inteligencji oraz sporządzeniu koncepcji audytowania systemów AI. Powyższe zagadnienia wynikają ze współpracy projektowej prowadzonej z zespołem programistów, ekspertów z dziedziny informatyki prawniczej, identyfikacji wyzwań etycznych relewantnych dla danego systemu sztucznej inteligencji oraz problematycznych zagadnień etycznych. Praca ma zatem walor wdrożeniowy, ponieważ na podstawie dokonanej analizy prawnej i stworzenia dokumentacji projektowej przedsiębiorca, w ramach działalności gospodarczej prowadzone były badanie naukowe doktorantki (doktorat wdrożeniowy), przygotował i wdrożył rozwiązanie opisane w niniejszej rozprawie doktorskiej.

2. Systematyka pracy i ocena metod badawczych

Autorka podzieliła rozprawę doktorską na rozdziały, w których występują mniejsze jednostki redakcyjne. Zawarła w rozprawie także wstęp obejmujący opis tematu rozprawy, i jego uzasadnienie, wskazanie głównego celu badawczego rozprawy oraz jej hipotez pomocniczych. Opis metod badawczych wykorzystywanych w rozprawie oraz opis treści poszczególnych rozdziałów wraz z uzasadnieniem takiej systematyki.

W mojej ocenie systematyka rozprawy doktorskiej jest prawidłowa. Rozdział I. Sztuczna inteligencja – zagadnienia podstawowe, Rozdział II. Zagrożenia związane z zastosowaniem rozwiązań sztucznej inteligencji w sieciach i systemach teleinformatycznych, Rozdział III. Odpowiedzialność prawna za szkody wyrządzone przy zastosowaniu sztucznej inteligencji, Rozdział IV. Ochrona własności intelektualnej systemów teleinformatycznych wytworzonych przez rozwiązania sztucznej inteligencji, Rozdział V. Wartość wdrożeniowa systemu „AIMON" jako przykładu zastosowania rozwiązań sztucznej inteligencji .

Autorka wychodzi od zagadnień wprowadzających, czyli analizy istoty sztucznej inteligencji – czym jest i jak działają oparte na niej technologie specyficzne dla danego obszaru i wykonywanego zadania. Zastosowanie w metody analitycznej i konstrukcji logicznej pozwoli skupić się na analizie pojęć i zwrotów w obszarze sztucznej inteligencji, uczenia maszynowego, sieci neuronowych AI generatywnej AI. Autorka uwzględniła aktualnie stosowaną terminologię techniczna, co pomaga w zrozumieniu – będących przedmiotem kolejnych części opracowania – aspektów prawnych ewoluujących w projektowanych i obowiązujących regulacjach Unii Europejskiej odnoszących się do sztucznej inteligencji.

Autorka zastosowała w tym zakresie metodę prawno-porównawczą i prawno-dogmatycznej, dokonują przeglądu, analizy i porównania strategii rozwoju AI, a także systemów prawnych regulujących AI w Stanach Zjednoczonych i w Chinach. Dobór jest reprezentatywny, ponieważ w tych krajach najszybciej rozwijają się narzędzia AI i następuje ich wykorzystanie w gospodarce. Dokonała przy tym oceny i diagnozy potencjalnych indywidualnych i zbiorowych zagrożeń bezpieczeństwa, a także negatywne indywidualne i zbiorowe konsekwencje, jakie może nieść ze sobą stosowanie zaawansowanych technologii cyfrowych w sieciach i systemach teleinformatycznych z perspektywy praw podstawowych, w tym przetwarzania danych osobowych i prawa do prywatności.

Autorka zastosowała także metodę aksjologiczną, za pomocą której omówiła takie zagadnienia, jak techniczna solidność i etyka godnej zaufania sztucznej inteligencji jako warunków koniecznych zwiększania cyberbezpieczeństwa, przejrzystości zabezpieczeń stosowanych w systemach AI, odporności tych systemów na działania naruszające poufność, integralność i dostępność oraz zapobiegania manipulacji danymi skierowanymi na modele i algorytmy AI. Przybliżony zostanie temat wytłumaczalności sztucznej inteligencji, która może wyjaśnić swoje wewnętrzne funkcje i umożliwić użytkownikom interpretację łańcucha logicznego prowadzącego do jej decyzji. Wytwarzanie bardziej zrozumiałych modeli AI, przy jednoczesnym zachowaniu wysokiego poziomu wydajności uczenia się, umożliwia użytkownikom zrozumienie systemów sztucznej inteligencji oraz pozwala im zaufać. Wykorzystanie technologii opartych na danych może zagrażać poszczególnym prawom, a także bardziej ogólnym wartościom i interesom zbiorowym. Kluczowe jest zapewnienie stosowania przez cały *life cycle* systemów AI autonomii i praw człowieka, zapobieganie szkodom i minimalizowanie zagrożeń oraz stosowanie odpowiednich środków technicznych i organizacyjnych. W tym przypadku istotne jest promowanie stosowania sztucznej inteligencji ukierunkowanej na człowieka, gwarantującej bezpieczeństwo informacji i wysoki poziom ochrony praw podstawowych, w tym w odniesieniu do prywatności i ochrony danych

osobowych. Podstawowe znaczenie ma również ustalenie, kto ponosi odpowiedzialność za negatywne konsekwencje wyrządzone przy zastosowaniu technologii cyfrowych. Szeroko zakrojone i potencjalnie poważne zagrożenia oraz ryzyko związane z rozwojem i stosowaniem systemów AI nieuchronnie rodzą ważne pytania o to, w jaki sposób należy rozdzielić odpowiedzialność za ich unikanie, zapobieganie i łagodzenie. Co więcej, jeśli ryzyko to przerodzi się w szkodę lub naruszenie praw materialnych i niematerialnych, to w jaki sposób należy przypisać odpowiedzialność za te konsekwencje i na jakich mechanizmach instytucjonalnych polegać w celu zapewnienia odpowiedniego egzekwowania i zadośćuczynienia?

W trzecim rozdziale dokonała identyfikacji i przedstawienie różnych modeli i zasad odpowiedzialności w prawie Unii Europejskiej, które można przyjąć w celu zarządzania alokacją i podziałem odpowiedzialności za różne rodzaje negatywnych skutków wynikających z działania lub zaniechania działania systemów sztucznej inteligencji. W tym rozdziale wykorzystała ponownie metodę formalno-dogmatyczna oraz komparystyczną, co ułatwiło zbadanie obowiązujących przepisów i oceny z rzeczywistością. Zasadnie zwróciła uwagę na pewne problemy, które wiążą się z wyzwaniami przy próbie przypisania odpowiedzialności za ryzyko i inne niekorzystne skutki wynikające z działania złożonych i współdziałających ze sobą systemów społeczno-technicznych, do których należą: 1) pojęcie produktu, 2) pojęcie wady, 3) pojęcie podmiotu odpowiedzialnego za szkody wyrządzone przy wykorzystaniu rozwiązań AI, 4) problem „wielu rąk", 5) interakcja człowiek – komputer i nadzór człowieka nad działaniem systemów AI, 6) nieprzewidywalny charakter interakcji między wieloma systemami algorytmicznymi, generującymi nowe i potencjalne zagrożenia, 7) postępowanie dowodowe i dochodzenie roszczeń z tytułu odpowiedzialności za szkody wyrządzone przez rozwiązania AI. Wszystkie te problemy wymagają dalszej uwagi, w szczególności w kontekście zharmonizowania ram odpowiedzialności cywilnej i skutecznego dochodzenia roszczeń, zgodnie z wymogami prawa unijnego i krajowego.

W kolejnych rozdziałach (czwartym i piątym) zajęła się, przy wykorzystaniu metody formalno-dogmatycznej oraz dogmatyczno-prawnej, oceną standardów prawa autorskiego i praw pokrewnych określonych przez ramy międzynarodowe i europejskie. Zauważyła bowiem, problem wynikający z uznania narzędzi sztucznej inteligencji jako podmiotu, przedmiotu praw własności intelektualnej oraz objęcia ochroną prawnoautorską rezultatów działania sztucznej inteligencji, a także naruszeń praw autorskich przez algorytmy AI. Omówiła także powyższe zagadnienie z perspektywy prawa i orzecznictwa Stanów Zjednoczonych oraz prawa Unii

Europejskiej. Większość państw demokratycznych podąża bowiem za wypracowanymi właśnie w tych dwóch systemach prawnych rozwiązaniami w zakresie nowych technologii· Podkreślić przy tym należy, że umiejscowienie rozwiązań sztucznej inteligencji w unijnym systemie prawa autorskiego powoduje zarówno weryfikację kluczowych pojęć prawa autorskiego, takich jak: twórca, utwór, program komputerowy, indywidualność i oryginalność dzieła, jak i stanowienie ram prawnych dla nowych, nieznanych dotąd obszarów. Należy do nich przede wszystkim udział twórczej działalności człowieka w procesie generowania wytworów przez systemy AI. Prawodawstwo europejskie słusznie ustala kierunek objęcia ochroną prawnoautorską dzieł, które powstały w wyniku czynności decyzyjnych człowieka. Podejście to odpowiada dotychczasowym poglądom europejskiej doktryny prawa, jak również ustawodawstwu amerykańskiemu, które zgodnie stoją na stanowisku wykluczenia rejestracji praw autorskich do dzieł niepochodzących od człowieka -twórcy. Słusznie tez zauważa, że takie rozwiązanie nie jest jednak pozbawione wad, ponieważ może okazać się, że oszacowanie wkładu ludzkiego i *sztucznej inteligencji* będzie trudne. Tym samym celem prawodawców jest ustandaryzowanie i ujednolicenie regulacji sztucznej inteligencji w obszarze działań twórczych oraz prawa autorskiego, co stanowi naturalną konsekwencję rozwoju technologicznego.

Autorka zajmuje się także opisem i oceną transformacji cyfrowej biznesu. Omówienie tego zagadnienia, ma istotne znaczenia dla tematu rozprawy doktorskiej oraz okoliczności, że doktorat ten ma charakter wdrożeniowy. Na podstawie raportów, badań i publikacji dokonała oceny wpływu sztucznej inteligencji na przedsiębiorców, tego, w jakich obszarach i zakresie jest ona wykorzystywana. W tym zakresie wykorzystała metodę analityczną, na podstawie której oceniała, jak rozwiązania AI mogą oddziaływać na automatyzację procesów, usprawnienie podejmowania decyzji, analizę oraz personalizację potrzeb użytkowników. Wskazane zostaną bariery, szanse, zagrożenia i cyberzagrożenia towarzyszące transformacji cyfrowej i automatyzacji. Przy wykorzystaniu badania empirycznego w dalszej części rozprawy przeprowadziła analizę zastosowania nowych technologii wykorzystujących AI w rozwiązaniach dla wymiaru sprawiedliwości i zawodów prawniczych. Przedmiotem badania były także zagadnienia, w jakim zakresie zastosowania sztucznej inteligencji na potrzeby tworzenia inteligentnych systemów dla omawianego obszaru. Narzędzia sztucznej inteligencji w skali światowej są wykorzystywane m.in. do rozstrzygania sporów, jako narzędzie wspomagające podejmowanie decyzji lub stanowiące wsparcie w analizie dokumentów, orzecznictwa czy też przepisów prawa. Konieczne jest zapewnienie, że nie podważają one gwarancji prawa dostępu do sędziego, prawa do rzetelnego procesu, prawa do prywatności i ochrony danych osobowych. Pod tym względem istnieje różnica pomiędzy Europą i Stanami

Zjednoczonymi w odniesieniu do prawa dostępu do algorytmów. Podczas gdy w Stanach Zjednoczonych organy sądowe niechętnie uznają to prawo w pełni i ważą interesy prywatne (w szczególności ochronę własności intelektualnej) z prawem do obrony, w Europie ramy są bardziej ochronne, z uwagi na przepisy odnoszące się do ochrony danych osobowych, które ustanawiają prawo do informacji na temat logiki podejmowanych decyzji przy użyciu algorytmów European Commission for the Efficiency of Justice (CEPEJ), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, adopted at the 31st plenary meeting of the CEPEJ). Kwestie związane z wprowadzaniem predykcyjnych narzędzi dla wymiaru sprawiedliwości i zawodów prawniczych są tak liczne i wieloaspektowe, że wymagają zrównoważonego podejścia ze strony ram legislacyjnych lub regulacyjnych oraz podmiotów wprowadzających je na rynek.

Autorka przedstawiła także stan polskiej legislacji w omawianym zakresie, a także opisała innowacyjne rozwiązanie sztucznej inteligencji do monitorowania zmian aktów prawnych, opracowane w ramach doktoratu wdrożeniowego.

Rozprawa kończy się wnioskami *de lege ferenda* odnoszące się do tworzenia regulacji prawnych dotyczących sztucznej inteligencji w sposób stopniowy, elastyczny, równoległy z rozwojem technologicznym. Regulacje prawne dotyczące AI powinny być wynikiem współpracy z ekspertami i zainteresowanymi stronami oraz uwzględniać międzynarodową i europejską normalizację i standaryzację. Dzięki zharmonizowanym przepisom prawa na poziomie europejskim oraz wdrożeniu odpowiedniej kontroli, systemy AI mogą stanowić narzędzia podwyższające efektywność i bezpieczeństwo przetwarzania danych osobowych.

3.Uwagi szczegółowe

Autorka trafnie zauważa, że sztuczna inteligencja powoduje korzyści w postaci szybszej i dokładniejszej analizy dużych zbiorów danych oraz automatyzację powtarzalnych czynności oraz, że projektowanie, rozwój, wdrożenie i wykorzystywanie systemów sztucznej inteligencji wpływa znacząco na jednostki, grupy jednostek i społeczeństwo, a złożoność technologii AI stwarza wyzwania związane z bezpieczeństwem informacji, przetwarzaniem danych osobowych, przejrzystością i wyjaśnialnością systemów AI.

Słusznie także zauważa, że różnorodność technologii sztucznej inteligencji dodatkowo zwiększa te wyzwania ze względu na wielość rodzajów modeli sztucznej inteligencji oraz danych. Stąd też słusznie uznaje, że należy dysponować skutecznymi i zgodnymi z prawem mechanizmami, które będą zapobiegać naruszeniom praw człowieka, biorąc pod uwagę szybkość i skalę, z jaką działa wiele zaawansowanych systemów AI. Konieczne jest, w tym zakresie, podejście prewencyjne jest szczególnie ważne, jeśli weźmie się pod uwagę, że takie

zagrożenia mogą poważnie osłabić fundamenty społeczne niezbędne dla moralnych i demokratycznych porządków, które są niezbędnymi warunkami wstępnymi korzystania z indywidualnej wolności, autonomii i praw człowieka. Autorka zauważa, że takie podejście obejmuje zarówno potrzebę opracowania zbiorowych mechanizmów składania skarg w celu ułatwienia skutecznej ochrony praw, jak i wzmocnienia i ożywienia istniejących koncepcji oraz rozumienia praw podstawowych. Konieczne jest także inicjowanie i wspieranie badań technicznych związanych z zapewnieniem odpowiedzialności za należyte poszanowanie wielu wartości leżących u podstaw praw człowieka. W tym celu należy prowadzić badania interdyscyplinarne przez zaangażowanie społeczności technicznej, prawa, nauk humanistycznych i społecznych, w celu pełniejszego określenia, w jaki sposób ochrona danych osobowych może być tłumaczona i wyrażana za pomocą technicznych mechanizmów ochrony wbudowanych w systemy sztucznej inteligencji.

Autorka zasadnie twierdzi, że dla efektywnej ochrony praw człowieka w globalnej erze cyfrowej konieczne jest dysponowanie zgodnymi z prawem mechanizmami oraz instrumentami zarządzania w celu monitorowania, ograniczania i nadzorowania odpowiedzialnego projektowania, rozwoju, wdrażania i utrzymania systemów AI. Wymaga to, co najmniej, zarówno uczestnictwa właściwych instytucji w procesie ustalania stosownych standardów, jak i istnienia niezależnych organów wyposażonych w odpowiednie uprawnienia do systematycznego gromadzenia informacji, badania niezgodności i sankcjonowania naruszeń, w tym uprawnień i umiejętności do badania i weryfikowania, czy systemy te są w rzeczywistości zgodne ze standardami i wartościami praw człowieka.

Słuszna jest konstatacja autorki, że przeprowadzona przez Nią analiza wykazała, że systemy AI, w tym systemy AI wysokiego ryzyka, mogą wprowadzać nowe zagrożenia dla podmiotów je wdrażających na rynek, z pozytywnymi lub negatywnymi konsekwencjami dla celów lub zmian w prawdopodobieństwie wystąpienia istniejących zagrożeń. Wymóg zapewnienia cyberbezpieczeństwa AI (uwzględniony w art. 15 i motywie 51 AIA), pod względem operacyjnym obejmuje cztery główne elementy. Po pierwsze, systemy sztucznej inteligencji, w tym systemy AI wysokiego ryzyka powinny być zaprojektowane tak, aby były odporne na próby zmiany ich użycia, zachowania i wydajności oraz naruszenia ich właściwości bezpieczeństwa przez złośliwe zachowania podmiotów trzecich. Po drugie, aby osiągnąć te cele, należy wdrożyć odpowiednie rozwiązania organizacyjne i techniczne, przy czym, rozwiązania techniczne powinny być odpowiednie do okoliczności i ryzyka. Po trzecie, w przypadku systemów AI wysokiego ryzyka należy

przeprowadzić ocenę ryzyka cyberbezpieczeństwa. Po czwarte, odpowiednie wydaje się, aby wszystkie systemy AI zdefiniowane w Akcie w sprawie sztucznej inteligencji musiały przechodzić ocenę zgodności i spełniać wymóg cyberbezpieczeństwa, zanim będą mogły być używane lub oddane do użytku na rynku Unii Europejskiej. Z uwagi na powyższe, za słuszne można by uznać wdrożenie opartego na ryzyku podejścia do identyfikacji, oceny i zrozumienia zagrożeń związanych z rozwiązaniami sztucznej inteligencji.

Chociaż stan wiedzy w zakresie zabezpieczania modeli sztucznej inteligencji ma ograniczenia, systemy AI mogą nadal osiągać zgodność z wymogami cyberbezpieczeństwa określonymi w Akcie w sprawie sztucznej inteligencji, o ile ich ryzyko dla cyberbezpieczeństwa jest skutecznie ograniczane za pomocą innych środków, które nie są wdrażane wyłącznie na poziomie modelu sztucznej inteligencji. Nie zawsze jest to jednak możliwe, a w przypadku niektórych systemów AI wysokiego ryzyka osiągnięcie zgodności z wymogiem cyberbezpieczeństwa określonym w AIA może być niewykonalne, chyba że system ten dodatkowo wprowadzi nowe kontrole cyberbezpieczeństwa i środki łagodzące o udowodnionej skuteczności. W efekcie uzasadniona stała się konkluzja, że systemy AI powinny podlegać wymogom dotyczącym: zarządzania ryzykiem, jakości i istotności wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości, wyjaśnialności, interpretowalności i przekazywania informacji podmiotom stosującym AI, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa.

System zarządzania ryzykiem powinien obejmować ciągły, iteracyjny proces, który jest planowany i realizowany przez cały cykl życia systemu AI. Proces ten powinien mieć na celu identyfikację i ograniczenie istotnego ryzyka, jakie systemy AI stwarzają dla bezpieczeństwa, praw podstawowych i przetwarzania danych osobowych. System zarządzania ryzykiem powinien podlegać regularnym przeglądom i aktualizacji, aby zapewnić jego stałą skuteczność, a także uzasadnienie i dokumentację wszelkich istotnych decyzji i podjętych działań. W systemie zarządzania ryzykiem należy przyjąć najbardziej odpowiednie środki zarządzania, zgodne ze stanem wiedzy technicznej w obszarze sztucznej inteligencji. Przy określaniu tych środków, dostawca AI powinien udokumentować i wyjaśnić dokonane wybory oraz – w stosownych przypadkach – zaangażować ekspertów i zewnętrzne zainteresowane strony.

Autorka dobrze identyfikuje zjawisko, że cykl życia zarządzania sztuczną inteligencją powinien z kolei obejmować szereg narzędzi i procesów, w tym: 1) utrzymywanie i promowanie świadomości na temat polityk oraz procesów zarządzania i narzędzi do

zarządzania sztuczną inteligencją 2) nadzorowanie strategii firmy w zakresie sztucznej inteligencji w sposób zaangażowany i świadomy; 3) utrzymywanie odpowiednich i wysokiej jakości danych, przy jednoczesnym przestrzeganiu najlepszych praktyk w zakresie zarządzania danymi; 4) rozważenie i podjęcie działań związanych z ryzykiem, prywatnością, cyberbezpieczeństwem, zgodnością i własnością intelektualną AI; 5) efektywne przydzielanie zasobów ludzkich i technologicznych, w tym niezbędnych narzędzi dla inicjatyw AI; 6) aktywne monitorowanie i ograniczanie ryzyka związanego ze stronami trzecimi i partnerami; 7) upewnienie się, że zespoły programistów AI i eksperci reprezentują różne środowiska i uwzględniają perspektywy interesariuszy; 8) wspieranie współpracy między zespołami i informacji zwrotnych na temat projektów sztucznej inteligencji; 9) wdrażanie wytycznych dotyczących strategii AI na poziomie zespołu projektowego i całego przedsiębiorstwa, zapewniając bezpośrednie raportowanie do kierownictwa wyższego szczebla w celu zapewnienia przejrzystości i odpowiedzialności; 10) zobowiązanie się do kompleksowego szkolenia i edukacji w zakresie AI dla wszystkich pracowników; 11) nawiązanie współpracy z grupami branżowymi, ośrodkami naukowymi w celu wniesienia wkładu i dostosowania się do standardów branżowych w zakresie odpowiedzialnej sztucznej inteligencji.

Systemy sztucznej inteligencji powinny być tym samym poddawane audytom wewnętrznym i zewnętrznym przez swój cały cykl życia. Podejście oparte na cyklu życia oznacza przestrzeganie obowiązków nałożonych na operatorów systemów AI, jak i same systemy AI: od planowania, projektowania, po wdrożenie, eksploatację, aż do wycofania z użytku, zapewniając tym samym kompleksowe podejście do potencjalnych zagrożeń i wyzwań. Powyższe wymaganie stanowiłoby zgodnie z Konwencją ramową w sprawie sztucznej inteligencji jeden z solidnych mechanizmów nadzoru i ram zarządzania celem zapewnienia odpowiedzialnego i etycznego wykorzystania sztucznej inteligencji, z czytelnymi zasadami odpowiedzialności i przejrzystości. Środki służące identyfikacji, ocenie, zapobieganiu i łagodzeniu zagrożeń stwarzanych przez systemy sztucznej inteligencji powinny być stopniowane i różnicowane stosownie do okoliczności. Powinny przy tym uwzględniać: 1) kontekst i zamierzone zastosowane systemów AI, 2) dotkliwość i prawdopodobieństwo potencjalnych skutków, 3) monitorowanie ryzyka i negatywnego wpływu na dane treningowe, walidacyjne, testowe, w tym przetwarzane dane osobowe, 4) przygotowanie odpowiedniej dokumentacji ryzyka, przedstawiającej rzeczywiste i potencjalne skutki stosowania systemów AI, w tym zarządzanie ryzykiem, 4) regularne testowanie systemów AI. Rozwój i wdrażanie rozwiązań sztucznej inteligencji na rynek europejski powinny być prowadzone w zgodności z

przepisami prawa, ustalonymi zasadami praw człowieka, prawem do prywatności i ochroną danych osobowych.

Dalej autorka dokonała analizy regulacji prawnych w zakresie odpowiedzialności za szkody wyrządzone przy zastosowaniu sztucznej inteligencji, dostrzegalna jest potrzeba wprowadzenia jednoznacznych i efektywnych przepisów prawa w tym obszarze. Zadaniem stojącym przed legislatorem europejskim jest ustalenie jasnego podziału odpowiedzialności, zapewniającego, że konkretne osoby lub podmioty zostaną pociągnięte do odpowiedzialności za działania i decyzje systemów AI. Odpowiedzialność ta powinna dotyczyć zarówno osób, jak i organizacji zaangażowanych w rozwój, wdrażanie i utrzymanie systemów AI. Podczas gdy aktualnie obowiązujące przepisy dotyczące odpowiedzialności oferują rozwiązania w odniesieniu do zagrożeń stwarzanych przez pojawiające się technologie cyfrowe, wyniki mogą nie zawsze wydawać się odpowiednie, biorąc pod uwagę: 1) brak spójnej i odpowiedniej reakcji systemu prawnego na zagrożenia dla interesów osób fizycznych, w szczególności dlatego, że ofiary szkód spowodowanych działaniem nowych technologii cyfrowych otrzymują mniejsze odszkodowanie lub nie otrzymują go wcale w porównaniu z ofiarami w funkcjonalnie równoważnej sytuacji obejmującej ludzkie zachowanie i konwencjonalną technologię; 2) brak skutecznego dostępu do wymiaru sprawiedliwości, w szczególności dlatego, że postępowanie sądowe dla ofiar staje się nadmiernie uciążliwe lub kosztowne.

Zauważyła dalej, że istotne jest rozważenie dostosowania i zmiany w zakresie odpowiedzialności w istniejących krajowych systemach prawnych odpowiedzialności. Należy pamiętać, że biorąc pod uwagę różnorodność pojawiających się technologii cyfrowych i odpowiednio zróżnicowany zakres zagrożeń, jakie mogą one stwarzać, niemożliwe jest znalezienie jednego, uniwersalnego rozwiązania odpowiedniego dla całego spektrum możliwych do wystąpienia szkód. Porównywalne ryzyka powinny być objęte podobnymi systemami odpowiedzialności, a istniejące między nimi różnice powinny zostać usunięte. Odpowiedzialność na zasadzie winy, jak również odpowiedzialność na zasadzie ryzyka i za wadliwe produkty, powinny nadal współistnieć. W zakresie, w jakim nakładają się one na siebie, oferując tym samym poszkodowanemu więcej niż jedną podstawę do dochodzenia odszkodowania od więcej niż jednej osoby, obowiązują zasady dotyczące wielu sprawców deliktów. Do celów odpowiedzialności nie jest przy tym konieczne nadawanie systemom autonomicznym osobowości prawnej, a surowa odpowiedzialność stanowi odpowiednią reakcję na zagrożenia stwarzane przez pojawiające się technologie cyfrowe, w tym rozwiązania wykorzystujące sztuczną inteligencję.

Autorka dalej zauważyła, że odpowiedzialność za szkody wyrządzone przez systemy AI powinna spoczywać na osobie, która kontroluje ryzyko związane z działaniem nowych technologii cyfrowych i która czerpie korzyści z ich działania (operator AI). Odpowiedzialność producenta odgrywa kluczową rolę w rekompensowaniu szkód spowodowanych przez wadliwe produkty i ich komponenty, niezależnie od tego, czy mają one postać materialną czy cyfrową. Producent jest podmiotem, który powinien ponosić ścisłą odpowiedzialność za wady powstających technologii cyfrowych, nawet jeśli wady te pojawiły się po wdrożeniu produktu na rynek, o ile producent nadal był w trakcie utrzymania i kontrolował aktualizacje lub ulepszał technologię. Nie można przy tym zapominać, że producenci powinni być zobowiązani do wyposażenia systemów sztucznej inteligencji wysokiego ryzyka w środki automatycznego rejestrowania informacji o ich działaniu zgodnie z wymogami prawa unijnego lub krajowego (motyw 46 AILD, art. 12 AIA, motyw 9, 66 i 91 AIA), jeżeli takie informacje są niezbędne do ustalenia, czy ryzyko związane z technologią zmaterializowało się, oraz jeżeli rejestrowanie jest odpowiednie i proporcjonalne, biorąc pod uwagę w szczególności techniczną wykonalność i koszty rejestrowania, dostępność alternatywnych środków gromadzenia takich informacji, rodzaj i skalę ryzyka stwarzanego przez technologię oraz wszelkie negatywne skutki, jakie rejestrowanie może mieć dla praw innych osób. Winno się odbywać się zgodnie z obowiązującymi przepisami prawa, (przepisami o ochronie danych osobowych i przepisami dotyczącymi ochrony tajemnic handlowych). W przypadku, gdy szkoda jest tego rodzaju, że zasady bezpieczeństwa miały na celu jej uniknięcie, nieprzestrzeganie takich zasad, w tym zasad dotyczących cyberbezpieczeństwa, powinno prowadzić do odwrócenia ciężaru dowodu. Jednak bez uszczerbku dla odwrócenia ciężaru dowodu, ciężar udowodnienia związku przyczynowego mógłby zostać zmniejszony w świetle wyzwań związanych z pojawiającymi się technologiami cyfrowymi, jeśli uzasadnia to wyważenie następujących czynników: 1) prawdopodobieństwo, że system AI przyczynił się do powstania szkody; 2) prawdopodobieństwo, że szkoda została spowodowana przez rozwiązanie AI; 3) ryzyko związane ze znaną wadą technologii, nawet jeśli jej faktyczny wpływ przyczynowy nie jest oczywisty; 4) stopień identyfikowalności *ex post* i zrozumiałość procesów w ramach zastosowanego systemu AI, które mogły przyczynić się do powstania przyczyny (asymetria informacyjna); 5) stopień dostępności *ex post* i zrozumiałość danych gromadzonych i generowanych przez technologię; 6) rodzaj i stopień potencjalnie oraz faktycznie wyrządzonej szkody.

Autorka zauważyła także, że przy planowaniu elementów przyszłych przepisów prawnych dla odpowiedzialności za szkody wyrządzone przy zastosowaniu sztucznej

inteligencji, istotne jest także ujednolicenie słownictwa stosowanego w AILD z Aktem w sprawie sztucznej inteligencji, w szczególności w zakresie terminu „użytkownik", jak również uwzględnienie w AILD pojęcia operatora i dystrybutora. Dostrzegalny jest przy tym problem rozumienia, co stanowi winę lub wadę produktu, w tym ustalenie, jakie wady projektowe systemów AI są niedopuszczalne.

Autorka odnosi te zagadnienia na pole ochrony danych osobowych, i wskazuje , że dostępność danych jest warunkiem niezbędnym do rozwoju sztucznej inteligencji, umożliwiając jej wykonywanie określonych zadań, które wcześniej były realizowane przez ludzi. Im więcej dostępnych danych, tym bardziej rozwiązania sztucznej inteligencji są w stanie udoskonalać modele AI, poprawiając ich zdolność predykcyjną. Zasadnie autorka w swojej pracy doktorskiej, analizuje zagadnienia prawa do prywatności i ochrony danych osobowych, i na tej podstawie stawia tezę, że Akt w sprawie sztucznej inteligencji i unijne przepisy o ochronie danych, w tym szczególności RODO, rozporządzenie 2018/1725, dyrektywa 2016/680, a także dyrektywa o prywatności i łączności elektronicznej, powinny być traktowane i interpretowane jako regulacje uzupełniające się i wzajemnie wzmacniające. Unijne prawo ochrony danych ma przy tym pełne zastosowanie do przetwarzania danych osobowych wykorzystywanych w całym cyklu życia systemów AI, co zostało wyraźnie podkreślone w art. 2 ust. 7 w zw. z motywem 9 i 10 AIA. Nadto wskazuje, że z art. 3 ust. 1 AIA, wynika, że przetwarzanie danych osobowych, które w systemach AI często jest związane z przetwarzaniem danych nieosobowych, może stwarzać wysokie ryzyko dla praw podstawowych. Należy też wskazać, że do tworzenia, testowania i walidacji wyszkolonych systemów AI wykorzystywane są treningowe, testowe i walidacyjne zbiory danych. Dane produkcyjne są z kolei testowane na już wyszkolonych modelach AI w celu tworzenia danych wyjściowych. Biorąc pod uwagę zdolność tych metod przetwarzania do ujawniania istniejącej dyskryminacji poprzez grupowanie lub klasyfikowanie danych odnoszących się do osób lub grup osób, interesariusze publiczni i prywatni powinni zapewnić, że metody te nie powielają ani nie pogłębiają takiej dyskryminacji oraz że nie prowadzą do deterministycznych analiz lub zastosowań.

Autorka zwraca także uwagę, że należy zachować ostrożność zarówno w fazie opracowywania, jak i wdrażania, zwłaszcza gdy przetwarzanie danych jest bezpośrednio lub pośrednio oparte na danych wrażliwych. Może to obejmować domniemane pochodzenie rasowe lub etniczne, pochodzenie społeczno-ekonomiczne, poglądy polityczne, przekonania religijne, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia lub dane dotyczące życia seksualnego

lub orientacji seksualnej. W ocenie wpływu systemów AI mogłaby pomóc dokumentacja dotycząca zbiorów danych wykorzystywanych w systemach sztucznej inteligencji, obejmująca swoim zakresem informacje o: 1) dostępności danych; 2) pochodzeniu zbioru danych; 3) ilości danych; 4) jakości danych; 5) kontroli dostępu do danych; 6) obszarach geograficznych objętych zbiorem danych; 7) przeglądzie danych i sposobie pozyskania i źródłach danych oraz kwestiach ich zgodności z przepisami prawa i zasadami etycznymi. Szczególne istotne są w tym kontekście procedura przygotowania danych, procedura zarządzania danymi, polityka wykorzystywania danych na potrzeby AI oraz procedura dokonywania zmian w systemach AI. Powyższe wymagania wypełniłyby lukę regulacji Aktu w sprawie sztucznej inteligencji, odnoszącą się do braku zobowiązania dostawców wysokiego ryzyka, dostawców modeli AI, importerów i dystrybutorów do udzielenia osobie poszkodowanej prawa dostępu do powyższych danych i informacji.

Słuszny jest także pogląd autorki, że zasada zgodności z prawem przetwarzania danych osobowych oraz obowiązek zapobiegania lub minimalizowania wpływu przetwarzania danych na prawa i podstawowe wolności osób, których dane dotyczą, wymuszają dokonanie uprzedniej oceny ryzyka. Konieczne jest wykorzystanie odpowiednich środków, w szczególności na etapie projektowania i domyślnie, w celu ograniczenia zidentyfikowanego ryzyka. Ponieważ dane osobowe muszą być przetwarzane w określonych i zgodnych z prawem celach, nie mogą być wykorzystywane niezgodnie z tymi celami, ani w sposób, który osoba, której dane dotyczą, może uznać za nieoczekiwany, niewłaściwy lub wątpliwy. Kwestia ponownego wykorzystywania danych osobowych i ich szerokiego udostępniania musi być zatem traktowana z najwyższą ostrożnością.

Prawidłowe są także rozważania autorki dotyczące ochrony własności intelektualnej w zakresie systemów teleinformatycznych wytworzonych przez rozwiązania sztucznej inteligencji, w oparciu o przepisy unijne, polskie oraz amerykańskie. Systemy AI oraz rozwiązania je wykorzystujące nie są rozumiane jako utwór. Stanowią one oprogramowanie wytworzone przez człowieka w rozumieniu dyrektywy w sprawie ochrony prawnej programów komputerowych, jak również ustawy o prawie autorskim i prawach pokrewnych. Tym samym podlegają ochronie prawami wyłącznymi. W celu uniknięcia wątpliwości, w europejskim i polskim systemie prawnym dzieło wytworzone wyłącznie przez rozwiązania wykorzystujące sztuczną inteligencję nie jest również przedmiotem ochrony prawa autorskiego. Inaczej ma się sytuacja w przypadku twórczego wkładu człowieka i jego oryginalności. Stąd też zasadny wniosek autorki, że objęcie systemów AI ochroną prawnoautorską jest możliwe, co potwierdza

rezolucja Parlamentu Europejskiego z 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji. Postuluje się w niej o ochronę twórczości technologicznej wygenerowanej przez sztuczną inteligencję w ramach praw własności intelektualnej oraz o przyjęcie, że wszelkie prawa własności intelektualnej powinny przysługiwać osobom fizycznym lub prawnym, które stworzyły utwór.

Odnosząc się natomiast do ochrony własności intelektualnej systemów teleinformatycznych wytworzonych przez rozwiązania sztucznej inteligencji, zgodnie z art. 15 Konwencji berneńskiej, art. 2 dyrektywy w sprawie ochrony prawnej programów komputerowych, art. 4 dyrektywy w sprawie ochrony prawnej baz danych oraz art. 8 ust. 1 i 2 u.p.a.p.p., autorka zauważyła, że narzędzia posługujące się sztuczną inteligencją nie są podmiotem praw własności intelektualnej. Jest nim osoba fizyczna lub grupa osób fizycznych, która stworzyła utwór, a także osoba prawna wskazana jako uprawniona na mocy obowiązujących przepisów prawa. Autorem z kolei jest ten, kto tworzy utwór. Na tle wyzwań związanych z twórczością generowaną przez rozwiązania sztucznej inteligencji, US Copyright Office wydało wytyczne w zakresie rejestracji praw autorskich utworów zawierających elementy wytworzone przez systemy i rozwiązania AI. Stanowczo przy tym wskazano, że dzieła pozbawione jakiegokolwiek elementu ludzkiej twórczości zostaną odrzucone przy rejestracji praw autorskich w USA. Obowiązujący stan prawny uniemożliwia przyjęcie stanowiska o celowości uznania autorstwa systemów sztucznej inteligencji.

Autorka słusznie zauważyła deficyt unijnych, międzynarodowych i polskich regulacji prawnych w zakresie relacji prawa autorskiego i sztucznej inteligencji powoduje, że decyzje w przedmiocie oceny: 1) autorstwa treści wytworzonych z wykorzystaniem rozwiązań AI; 2) własności dzieł stworzonych przez sztuczną inteligencję; 3) danych wykorzystanych przez systemy i rozwiązania AI oraz ich ochrony prawami własności intelektualnej; 4) danych wykorzystywanych przez systemy i rozwiązania AI a pochodzących z socialmediów i prywatnych kont osób fizycznych; 5) odpowiedzialności za naruszenia praw własności intelektualnej, w szczególności praw autorskich; 6) zakresu odpowiedzialności naruszyciela oraz ograniczenia jego odpowiedzialności; 7) środków prawnych przysługujących uprawnionemu z tytułu naruszenia praw własności intelektualnej, będą podejmowane przez sądy w prowadzonych postępowaniach. Istotne znaczenie ma ochrona interesów twórców, odpowiednia ocena wkładu ludzkiego, jak również ochrona danych osobowych. Celem zwiększenia przejrzystości danych wykorzystywanych do tworzenia i trenowania systemów AI, dostawcy tych systemów powinni udostępniać publicznie kompleksowe informacje odnoszące się do zakresu treści, które zostały użyte do trenowania

systemów i modeli AI. Strony mające uzasadniony interes prawny powinny natomiast mieć możliwość wykonywania i egzekwowania praw wynikających z ochrony prawnoautroskiej zagwarantowanej w Unii Europejskiej.

Badania objęte w niniejszej rozprawie doktorskiej wykazały, że systemy sztucznej inteligencji dla wymiaru sprawiedliwości i zawodów prawniczych mogą stanowić przykład wykorzystania rozwiązań AI jako narzędzia podwyższającego efektywność i bezpieczeństwo systemów teleinformatycznych przetwarzających dane osobowe. Jednakże, należy uznać, że przetwarzanie orzeczeń sądowych i danych musi służyć jasnym celom oraz pozostawiać w zgodzie z prawami podstawowymi gwarantowanymi przez Europejską Konwencję Praw Człowieka i Konwencję o ochronie danych osobowych. W sytuacji, kiedy narzędzia sztucznej inteligencji są wykorzystywane do rozstrzygania sporów lub służą jako narzędzie wspomagające podejmowanie decyzji sądowych bądź udzielające wskazówek społeczeństwu, konieczne jest zapewnienie, że nie podważają one gwarancji prawa dostępu do sędziego oraz prawa do rzetelnego procesu. Powinny być również stosowane z należytym poszanowaniem zasad praworządności i niezawisłości sędziów w procesie podejmowania decyzji.

Autorka zauważyła także, że dane oparte na orzeczeniach sądowych, które są wprowadzane do oprogramowania implementującego algorytm uczenia maszynowego, powinny pochodzić z certyfikowanych źródeł i nie powinny być modyfikowane, dopóki nie zostaną faktycznie wykorzystane przez mechanizm uczący. Cały proces musi być zatem identyfikowalny, aby zapewnić, że nie nastąpiła żadna modyfikacja danych w celu zmiany treści lub znaczenia przetwarzanej decyzji. Stąd tez konstatacja, że modele i algorytmy AI muszą powinny być przechowywane i trenowane w bezpiecznych środowiskach, tak aby zapewnić integralność i nienaruszalność systemu AI. Autonomia użytkownika powinna przy tym zostać zwiększona, a nie ograniczona. Użytkownik musi zostać poinformowany jasnym i zrozumiałym językiem o tym, czy rozwiązania oferowane przez narzędzia sztucznej inteligencji są wiążące, oraz o różnych dostępnych opcjach.

Odnośnie do zagadnienia wytłuaczalności AI, autorka zauważa zasadnie, że w przypadku stosowania narzędzi AI, proces selekcji oraz jakość i organizacja danych mają bezpośredni wpływ na fazę uczenia się modeli AI. Pierwszą opcją zapewnienia wytłumaczalności systemów AI jest zatem pełna przejrzystość techniczna, która może być ograniczona przez ochronę tajemnic handlowych. System AI mógłby być również wyjaśniony w jasnym i znanym języku, informując o charakterze oferowanych usług, opracowanych narzędziach, wydajności i ryzyku błędu. Autorka postuluje, aby niezależnym

organom lub ekspertom powierzyć zadanie certyfikacji i audytu metod przetwarzania lub wcześniejszego udzielania porad. Natomiast organy publiczne mogą udzielać certyfikatów systemom AI. Aby w pełni wykorzystać potencjał algorytmów i modeli AI, przy jednoczesnym przestrzeganiu zasad ochrony danych osobowych, należy zastosować zasadę ostrożności i wdrożyć polityki zapobiegawcze w celu przeciwdziałania potencjalnym zagrożeniom związanym z wykorzystaniem danych przetwarzanych przez te algorytmy oraz wpływem ich wykorzystania na osoby fizyczne i społeczeństwo.

4.Uwagi formalne

Pod względem formalnym praca nie budzi zastrzeżeń. Tematyka rozprawy doktorskiej ma uniwersalny zasięg, więc w sposób naturalny autorka musiała się oprzeć na literaturze , zarówno polskiej , jak i zagranicznej. Autora korzysta zatem z licznej literatury zagranicznej i polskiej, która dotyczy różnych obszarów praw, w tym prawa własności intelektualnej, prawa nowoczesnych technologii, informatyki itd. Nie budzą zastrzeż sposoby cytowania i wykorzystania poglądów innych autorów.

5. Wnioski końcowe

W mojej ocenie, przedstawiona do recenzji rozprawa doktorska pt. Prawne aspekty wykorzystania sztucznej inteligencji jako narzędzia podwyższającego efektywność i bezpieczeństwo systemów teleinformatycznych przetwarzających dane osobowe spełnia obecnie wymogi przewidzianych w art. 13 ust. 1 ustawy z 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce stawianym rozprawie doktorskiej. Rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego lub oryginalne rozwiązanie problemu w oparciu o opracowanie projektowe, konstrukcyjne, technologiczne, lub oryginalne dokonanie artystyczne, oraz wykazywać ogólną wiedzę teoretyczną kandydata w danej dyscyplinie naukowej lub artystycznej oraz umiejętność samodzielnego prowadzenia pracy naukowej lub artystycznej. Przedmiotowa rozprawa doktorska zawiera głębszą refleksję o naukowym charakterze na temat narzędzi sztucznej inteligencji służącym do podwyższenia efektywności i bezpieczeństwa systemów teleinformatycznych przetwarzających dane osobowe. Postawione tezy badawcze, wskazane we wstępie są rozwinięte i zmierzają do rozwiązania istotnego zagadnienia naukowego. Autorka opisała we wstępie jakie metody badawcze wykorzystała dla prowadzenia analizy zaproponowanych tez i hipotez badawczych, czyli metodę dogmatyczną, empiryczną, komparatystyczną oraz dogmatyczną analizę tekstu ustawy (aktu prawnego) i wykorzystując liczne poglądy judykatury dokonała własnych ocen, realizując cele badawcze rozprawy doktorskiej. Na szczególną uwagę zasługuję walor wdrożeniowy prowadzanych

badań naukowych. Wyniki bowiem pracy badawczej doktorantki zostały wykorzystane przez partnera gospodarczego, czyli Currenda spółkę z o.o., który wdrożył opracowanie.

Przedstawiona zatem do recenzji rozprawa doktorska może być przedmiotem dalszych kroków w przewodzie doktorskim.

Prof. dr hab. Jacek Gołaczyński

Wrocław, 8 listopada 2024r.