Uniwersytet Łódzki
Wydział Prawa i Administracji

Julita Skowrońska

Prawnokarne aspekty technologii wykorzystującej sztuczną inteligencję ze szczególnym uwzględnieniem kwalifikacji prawnej, przypisaniem sprawstwa i odpowiedzialności twórcy

Rozprawa doktorska przygotowana
w Katedrze Prawa Karnego Wykonawczego
pod kierunkiem
prof. UŁ dr hab. Aldony Nawój-Śleszyński
w dyscyplinie nauki prawne

Łódź 2024

Spis treści

Wykaz skrótów

AGI	Artificial General Intelligence (PL: Ogólna Sztuczna Inteligencja)
AI	Artificial Intelligence (PL: SSztuczna Inteligencja)
ASI	Artificial Superintelligence (PL: Superinteligencja Sztuczna)
CFPB	Consumer Financial Protection Bureau (PL: Biuro Ochrony Finansowej Konsumentów)
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions (PL: System profilowania zarządzania przestępcami w celu alternatywnych sankcji)
DDoS	Distributed Denial of Service (PL: Rozproszona odmowa usługi)
DOJ	Department of Justice (PL: Departament Sprawiedliwości)
DRM	Digital Rights Management (PL: Zarządzanie prawami cyfrowymi)
EEOC	Equal Employment Opportunity Commission (PL: Komisja ds. Równych Szans Zatrudnienia)
FTC	Federal Trade Commission (PL: Federalna Komisja Handlu)
G7	Grupa siedmiu (międzynarodowe forum gospodarcze)
GDPR	General Data Protection Regulation (PL: Ogólne rozporządzenie o ochronie danych, RODO)
IoT	Internet of Things (PL: Internet Rzeczy)
NHTSA	National Highway Traffic Safety Administration (PL: Krajowa Administracja Bezpieczeństwa Ruchu Drogowego)
NLP	Natural Language Processing (PL: Przetwarzanie Języka Naturalnego)
OECD	Organisation for Economic Co-operation and Development (PL: Organizacja Współpracy Gospodarczej i Rozwoju)
ONZ	Organizacja Narodów Zjednoczonych
PIA	Privacy Impact Assessment (PL: Ocena wpływu na prywatność)
RPA	Robotic Process Automation (PL: Automatyzacja Procesów Robotycznych)
SI	Sztuczna Inteligencja (ANG: AI - Artificial Intelligence)
TOR	The Onion Router (PL: Cebulowy Router)
UE	Unia Europejska (ANG: EU - European Union)
UNESCO	United Nations Educational, Scientific and Cultural Organization (PL: Organizacja Narodów Zjednoczonych do spraw Oświaty, Nauki i Kultury)
USA	United States of America (PL: Stany Zjednoczone Ameryki)

VPN	Virtual Private Network (PL: Wirtualna sieć prywatna)

Wstęp

Nauka od wieków jest tym elementem, który może inicjować proces zmian, porządkować lub pozwalać lepiej go zrozumieć. To właśnie wiedza jest tym za czym podążamy i co chcemy następnie wykorzystywać, czy to w życiu prywatnym czy zawodowym. Świadomość jest elementem odkrywania i przygody, w którą zaprasza nas życie. Wyzwaniem współczesnej nauki staje się dogłębna analiza odkryć dokonanych lub zapoczątkowanych przez naszych poprzedników. Innym wyzwaniem jest interdyscyplinarne podejście, które daje nowe pole badawcze w różnych dziedzinach, dzięki wykorzystaniu odkryć z innych dyscyplin. Zawsze będziemy mieli do czynienia z procesem przyczynowo-skutkowym. Czasami praca naukowa będzie dogłębną analizą danego tematu, innym razem otworzy nowe pole badawcze, a jeszcze w innych przypadkach może stanowić podstawę do zakwestionowania dotychczasowego punktu widzenia. W moim przypadku mamy do czynienia z pierwszą sytuacją, w której należy wnikliwie zbadać temat i gruntownie się nad nim zastanowić.

Wobec powyższego, podejmuję pracę nad problematyką związaną ze sztuczną inteligencją, będącą zarówno obszarem moich zainteresowań, jak i wynikającą z mojej działalności zawodowej. Zagadnienia nowych technologii oraz towarzyszących im wyzwań i zagrożeń poruszałam już na etapie pracy magisterskiej, gdzie analizowałam sieć TOR stanowiącą element sieci ukrytej (ang. dark web) w Internecie. Nowe technologie stanowią dla mnie coś niezwykłego, niewątpliwie zmieniającego nasz świat i umożliwiającego korzystanie z rzeczy, o których moim zdaniem, nawet nie śniły poprzednie pokolenia. Nie należę do zwolenników lęku przed rozwojem, a raczej kieruję się myślą przypisywaną Henry'emu Fordowi, który zapytany o wynalazek samochodu, miał odpowiedzieć: „*Gdybym zapytał ludzi, czego chcą, powiedzieliby szybciej poruszające się konie*"[1]. Choć autentyczność tego cytatu jest często kwestionowana i brak bezpośrednich dowodów na to, że Ford rzeczywiście wypowiedział te słowa, to odzwierciedla on pewną ideę przyświecającą innowatorom. Rozumiem, że innowacje mogą budzić obawy, podobnie jak wszystko nowe wykracza poza naszą strefę komfortu, w której panuje przekonanie „*to znam i wiem, jak się z tym obchodzić*". Są to naturalne procesy myślowe. Tym samym moją rolę naukową rozumiem jako element układanki w procesie innowacji i zmiany świata. Jej celem jest dogłębne zbadanie tej części, która przyczyni się do

[1] Ford H., *Moje życie i dzieło*, Wydawnictwo Naukowe PWN 2022, s. 147.

lepszej wiedzy odbiorców na temat innowacji będącej przedmiotem mojej pracy, co może przełożyć się na zmniejszenie obawy przed zmianą. To właśnie stanowi moją motywację do podjęcia badań naukowych.

Wybrany przeze mnie temat pracy doktorskiej "*Prawnokarne aspekty technologii wykorzystującej sztuczną inteligencję ze szczególnym uwzględnieniem kwalifikacji prawnej, przypisania sprawstwa i odpowiedzialności twórcy*" niewątpliwie wpisuje się w obszar moich zainteresowań nowymi technologiami. Dziedzina ta zaczyna już wprowadzać interdyscyplinarne zmiany na świecie. Zmiany te rodzą nowe możliwości rozwoju, ale również obawy i zagrożenia. Powyższe odpowiada moim motywacjom, które stymulują mnie do pracy. Istotnym czynnikiem jest również fakt, że w mojej działalności zawodowej kilka lat temu rozpoczęłam pracę przy tworzeniu technologii wykorzystującej sztuczną inteligencję do opracowywania nowych usług rynkowych. To właśnie w trakcie tej pracy zaczęłam zastanawiać się, z jaką odpowiedzialnością będzie musiała się zmierzyć firma, dla której pracowałam. Nie znajdując prostej odpowiedzi, dostrzegłam obszar wymagający pogłębionej analizy, której efektem jest moja rozprawa doktorska.

Podejmując pracę nad tematem rozprawy, pomocnym aspektem było moje zawodowe doświadczenie w obszarze prawa i technologii. Umożliwiło mi to wprowadzenie do dziedziny prawa umiejętności i wiedzy nabytej dzięki praktykowaniu z nowymi technologiami. W rezultacie zwróciłam uwagę na problematykę, z którą boryka się sektor gospodarczy, nieznajdujący odpowiedzi w obowiązujących regulacjach prawnych. Innymi słowy, rozwój nowych technologii nie znajduje wsparcia w przepisach prawa, które umożliwiłyby ich postęp w sposób bardziej efektywny i zgodny z innymi dziedzinami. Moją największą satysfakcją jest podjęcie tematu wypełniającego interdyscyplinarnie tę lukę.

Biorąc powyższe pod uwagę, celem niniejszej pracy doktorskiej jest dogłębne zbadanie prawnokarnych aspektów wykorzystania sztucznej inteligencji, ze szczególnym uwzględnieniem kwestii związanych z kwalifikacją prawną, przypisaniem odpowiedzialności oraz identyfikacją twórców tych systemów. Praca ma na celu rozpoznanie istniejących luk prawnych, wyzwań oraz potencjalnych rozwiązań, które mogą przyczynić się do opracowania bardziej efektywnej i sprawiedliwej regulacji prawnej dotyczącej technologii SI.

Założenia dysertacji są następujące:

1. analiza obecnego stanu prawa

niniejsza rozprawa ma na celu przegląd oraz analizę obecnych regulacji prawnych dotyczących sztucznej inteligencji, tak aby zbadać, w jaki sposób obowiązujące prawo radzi sobie z nowymi wyzwaniami wynikającymi z postępu technologii SI;

2. kwalifikacja prawna działań SI

   głównym celem tej pracy jest również zrozumienie, w jaki sposób działania sztucznej inteligencji są obecnie interpretowane przez system prawny, zwłaszcza w kontekście prawa karnego, oraz jakie konsekwencje to niesie dla sprawiedliwości i odpowiedzialności;

3. przypisanie sprawstwa i odpowiedzialność twórcy

   badania realizowane w ramach rozprawy mają na celu zrozumienie, w jaki sposób prawo karne określa winę i odpowiedzialność za czyny sztucznej inteligencji, zarówno w kontekście bezpośredniej odpowiedzialności twórcy, jak i ogólniejszych aspektów prawnych;

4. propozycje reform prawnych

   po dokładnym zbadaniu, celem pracy będzie także znalezienie sposobów na lepsze radzenie sobie z problemami związanymi z sztuczną inteligencją poprzez rozważenie ewentualnych zmian w przepisach prawa karnego, w tym propozycje modyfikacji kwalifikacji prawnej i systemów odpowiedzialności;

5. interdyscyplinarny i porównawczy charakter analizy

   badanie dokonywane na potrzeby niniejszej rozprawy zakłada wykorzystanie podejścia interdyscyplinarnego, które obejmuje obszary prawa, etyki oraz technologii. Ponadto, przewiduje analizę porównawczą różnych systemów prawnych w celu zrozumienia różnorodnych podejść do regulacji sztucznej inteligencji na całym świecie.

Poprzez koncentrację na tych celach i założeniach, rozprawa ma na celu wniesienie wkładu do literatury naukowej w obszarze prawa karnego i technologii poprzez dostarczanie zarówno teoretycznych analiz, jak i praktycznych zaleceń dla ustawodawców, projektantów sztucznej inteligencji oraz społeczeństwa.

W dysertacja przyjęłam model, w którym kolejno prowadzę czytelnika przez dwanaście rozdziałów, zakładając, że nie musi on mieć wiedzy fachowej z zakresu wielu dyscyplin, przez

które przechodzi się, aby dotrzeć do wyników istotnych dla dziedziny prawa, gdyż rozdziały te wyposażają czytelnika w wiedzę, którą uznałam za niezbędną dla spójności pracy i jej właściwego odbioru. W rozdziale pierwszym, który rozpoczyna część teoretyczną rozprawy doktorskiej, przedstawiam podstawową wiedzę z zakresu sztucznej inteligencji, aby głębiej dostrzec różnice w tej tematyce oraz szerzej zrozumieć funkcjonowanie tej technologii. Drugi rozdział stanowi wprowadzenie technologii sztucznej inteligencji do obszaru prawa, pokazując wspólne pole badawcze dla dziedziny prawa karnego i technologii, zaś w rozdziale trzecim zaczynam już porządkować wspólny obszar dla tych dziedzin. W wymienionych rozdziałach pojawia się również temat etyki, która w mojej ocenie jest nierozłącznym elementem sztucznej inteligencji, dlatego w rozdziale czwartym omawiam ten temat szczegółowo dla lepszego zrozumienia tej problematyki i wzajemnego wpływu prawa, etyki i sztucznej inteligencji na siebie. Rozdział piąty omawia problematykę zmian, badając potrzeby i lukę, której efektem są dalsze rozdziały prowadzące do wyników. W tym miejscu pojawia się również szersze ujęcie twórcy sztucznej inteligencji jako podmiotu, którego badam pole odpowiedzialności. To właśnie te podmioty, zajmujące się tworzeniem innowacyjnych technologii, dostrzegają potrzebę odpowiedzi na pytanie, gdzie ich odpowiedzialność się zaczyna, a gdzie kończy w kontekście nowatorskich rozwiązań, nad którymi prowadzą prace. Nie tylko pozwala im to czuć się zabezpieczonym przez prawo w możliwości tworzenia, ale również daje świadomość ryzyk, jakie niesie ze sobą ich działalność twórcza. Oczywiście pojawia się tu również problematyka nieograniczania swobody prac rozwojowych i negatywnego wpływu regulacji prawnych na postęp technologiczny. W dalszej części dysertacji, czyli w rozdziale siódmym, aby lepiej zobrazować sytuacje, z jakimi już się stykamy, przedstawiam przykłady naruszeń w siedmiu wybranych przeze mnie dziedzinach. Wybór ten, w mojej ocenie, wnosi ciekawy walor percepcyjny, gdyż przykłady dotyczą często naszej codziennej aktywności, oferując tym samym perspektywę praktyczną. W empirycznej części pracy zostaną szczegółowo omówione fundamentalne pojęcia i teorie związane z pojęciem sprawstwa oraz odpowiedzialności w kontekście prawnym. Przedstawione zostaną również różnorodne modele odpowiedzialności, które mogą być stosowane w przypadku systemów sztucznej inteligencji, obejmujące zarówno ryzyko, przyczynowość, jak i koncepcje winy i zawinienia. Dalsze rozdziały przedstawiają cel i założenie pracy, metodologię badawczą, wyniki, dyskusję z wynikami, a w następstwie prowadzą do podsumowania całej pracy.

Przyjęta przeze mnie metodyka przeprowadzania badań opiera się na interdyscyplinarnym podejściu, które łączy analizę prawną z aspektami technicznymi i etycznymi funkcjonowania systemów sztucznej inteligencji. Wykorzystałam metodę dogmatyczną, analizę przypadków oraz przegląd literatury przedmiotu w celu uzyskania wszechstronnego spojrzenia na problematykę. Szczególny nacisk położyłam w mojej dysertacji na dynamiczny rozwój sztucznej inteligencji, skupiając badania na najnowszych precedensach prawnych, dyskusjach doktrynalnych oraz obecnych trendach technologicznych. Metodyka użyta w niniejszej pracy doktorskiej ma na celu zbadanie aspektów prawnokarnych technologii SI poprzez interdyscyplinarne podejście, które łączy analizę prawną, etyczną i technologiczną. Aby osiągnąć cele badawcze, wykorzystane zostaną następujące strategie:

1. analiza prawna

   przeprowadzę dokładną analizę obowiązujących przepisów prawnych oraz orzecznictwa dotyczącego sztucznej inteligencji, skupiając się głównie na prawie karnym. Analiza obejmie zarówno przepisy krajowe (w tym Polski), jak i międzynarodowe, takie jak dyrektywy Unii Europejskiej oraz standardy Organizacji Narodów Zjednoczonych;

2. przegląd literatury przedmiotu

   wykorzystam już dostępne materiały naukowe, takie jak artykuły z recenzowanych czasopism, książki oraz raporty międzynarodowych organizacji dotyczące wykorzystania sztucznej inteligencji i regulacji prawnych. Przeprowadzenie analizy literatury przedmiotu pozwoli na odkrycie braków w wiedzy oraz istniejących rozwiązań badawczych;

3. studia przypadków

   przegląd wybranych przypadków, w których sztuczna inteligencja była tematem analizy prawniczej. Te przykłady posłużą jako konkretne przykłady potencjalnych problemów prawnych i etycznych wynikających z działalności SI;

4. metoda porównawcza

   zostanie dokonana analiza porównawcza regulacji dotyczących sztucznej inteligencji w różnych jurysdykcjach. Skupienie się na różnicach i podobieństwach w podejściach prawnych pomoże zrozumieć, jak różne systemy prawne radzą sobie z wyzwaniami, jakie stawia sztuczna inteligencja;

5. wywiady i konsultacje

   planuję przeprowadzenie rozmów z profesjonalistami z obszaru prawa, etyki i technologii sztucznej inteligencji, w tym prawnikami, naukowcami i twórcami technologicznymi, aby lepiej zrozumieć kwestie oraz możliwe sposoby ich rozwiązania;

6. analiza etyczna

   rozważenia etyczne będą integralną częścią badania, gdzie każdy aspekt prawny zostanie oceniony także z punktu widzenia etyki aplikacyjnej, koncentrując się na implikacjach moralnych wynikających z użycia SI w społeczeństwie.

Przyjęte strategie badawcze umożliwią holistyczne podejście do analizy różnorodnych aspektów prawnych technologii sztucznej inteligencji, co pozwoli na formułowanie trafnych wniosków i rekomendacji dla decydentów oraz społeczeństwa.

Rozprawa doktorska uwzględnia stan prawny na dzień 01.05.2024 r.

Rozdział I. Podstawy teoretyczne, definicja i klasyfikacja sztucznej inteligencji

Rozwój technologii, szczególnie w obszarze sztucznej inteligencji, stawia przed nami wiele pytań, nie tylko praktycznych, ale przede wszystkim teoretycznych. Kluczowe jest zrozumienie funkcjonowania nowoczesnych algorytmów, ich założeń i ograniczeń, aby pełniej pojąć implikacje ich zastosowań zarówno w kontekście prawnym jak i społecznym czy etycznym.

W epoce cyfrowej rewolucji, kiedy technologia przenika niemal każdy aspekt naszego życia codziennego, termin „*sztuczna inteligencja*" (SI, ang. artificial intelligence- AI) staje się coraz bardziej popularny. Niemniej jednak, czy zawsze go w pełni rozumiemy? Pomimo powszechnej obecności sztucznej inteligencji w naszym życiu codziennym, jej definicja często pozostaje niejasna i wieloznaczna. Często traktowana jest jako synonim innowacyjności i postępu, jednakże, aby dokładniej poznać jej wpływ na różne sfery życia konieczne jest dogłębne zrozumienie definicji oraz klasyfikacji tej pasjonującej dziedziny nauki.

Niniejszy rozdział ma na celu zbadać oraz wyjaśnić kluczowe koncepcje związane ze sztuczną inteligencją celem dostarczenia czytelnikowi solidnej podstawy do dalszego zrozumienia treści niniejszej pracy. Przedstawione zostaną różnorodne definicje SI zaproponowane na przestrzeni lat ukazujące ewolucję tego pojęcia oraz różnorodność perspektyw pod którymi można je analizować. Omówiona zostanie również klasyfikacja sztucznej inteligencji ułatwiająca zrozumienie różnych form i aplikacji SI a także ujawniająca potencjalne wyzwania i możliwości wynikające z rozwoju tej dziedziny.

1.1 Ewolucja pojęcia sztucznej inteligencji

1.1.1 Początki i rozwój koncepcji SI

Sztuczna inteligencja, mimo że obecnie jest zaawansowaną i powszechnie stosowaną technologią, wywodzi się z głęboko zakorzenionych tradycji filozoficznych i technicznych. Początki koncepcji SI można znaleźć już w starożytności, gdy ludzie marzyli o stworzeniu maszyn zdolnych do naśladowania ludzkich umiejętności i zachowań[2]. Mitologia grecka opowiada o mechanicznych robotach, takich jak złote automaty Hefajstosa czy brązowy

[2] McCorduck P., *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence*, A K Peters/CRC Press 2004.

olbrzym Talos. W średniowieczu i renesansie wynalazcy oraz filozofowie, tacy jak Ramon Llull czy Leonardo da Vinci, tworzyli mechaniczne automaty mające imitować pewne ludzkie funkcje.

W XVII i XVIII wieku, wraz z pojawieniem się pierwszych mechanicznych automatów i maszyn, takich jak znane automaty Jaqueta Droza, zaczęto rozważać koncepcję maszyn zdolnych imitować działania i zachowania ludzkie[3].

Prawdziwy rozwój sztucznej inteligencji zaczęto rozważać w XX wieku. Alan Turing, brytyjski matematyk i kryptolog, często uznawany za jednego z pionierów sztucznej inteligencji, przedstawił znany test Turinga, który miał na celu ustalenie, czy maszyna może „*myśleć*" w sposób nie do odróżnienia od człowieka[4].

W latach 50. XX wieku, dzięki zaangażowaniu naukowców takich jak John McCarthy czy Marvin Minsky, sztuczna inteligencja zaczęła być traktowana jako istotna dziedzina badawcza. Konferencja w Dartmouth w 1956 roku jest powszechnie uznawana za moment narodzin sztucznej inteligencji jako oddzielnej gałęzi nauki[5].

Postęp w dziedzinie technologii komputerowej w latach 60. i 70. pozwolił na realizację pierwszych projektów SI, takich jak ELIZA[6] czy SHRDLU[7], które mimo swoich ograniczeń, były ważnym etapem na drodze do rozwoju bardziej zaawansowanych systemów[8].

---

[3] Riskin J., *The Defecating Duck, Or, the Ambiguous Origins of Artificial Life*, "Critical Inquiry" 2003, Vol. 29, No. 4, s. 599-633.

[4] Turing A. M., *Computing Machinery and Intelligence*, "Mind" 1950, Vol. 59, No. 236, s. 433-460.

[5] McCarthy J., Minsky M. L., Rochester N., Shannon C. E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955*, "AI Magazine" 2006, Vol. 27, No. 4, s. 12.

[6] **ELIZA** - program komputerowy stworzony przez Josepha Weizenbauma w latach 60. XX wieku uważany jest często za pierwszego „chatbota". ELIZA potrafiła prowadzić podstawowe rozmowy w języku naturalnym, udając terapeutę poprzez przekształcanie wypowiedzi użytkownika i zadawanie dodatkowych pytań, co dawało wrażenie zrozumienia i empatii, mimo braku rzeczywistego rozumienia języka czy zdolności do prowadzenia sensownej dyskusji.

[7] **SHRDLU** - program komputerowy opracowany przez Terry'ego Winograda w latach 60. XX wieku miał na celu pokazanie, jak maszyny mogą przetwarzać język naturalny. SHRDLU działał w specjalnie stworzonym „świecie bloków", interpretując polecenia użytkownika wyrażone w języku angielskim i wykonując akcje, takie jak przesuwanie bloków. Chociaż był ograniczony do konkretnego kontekstu, SHRDLU demonstruje zdolność do rozumienia i reagowania na pytania użytkownika, co sprawia, że jest ważnym punktem odniesienia w dziedzinie sztucznej inteligencji i przetwarzania języka naturalnego.

[8] Weizenbaum J., *ELIZA—a computer program for the study of natural language communication between man and machine*, "Communications of the ACM" 1966, Vol. 9, No. 1, s. 36-45.

1.1.2 Kluczowe momenty w historii sztucznej inteligencji

Historia sztucznej inteligencji jest pełna przełomowych momentów, które miały wpływ na jej rozwój i postrzeganie przez społeczeństwo. Od wczesnych koncepcji automatów i maszyn zdolnych do wykonywania zadań typowych dla ludzi, aż po współczesne technologie, historia SI to fascynująca podróż przez różne epoki i paradygmaty[9].

Jednym z istotnych momentów w historii SI był rozwój maszyn Turinga oraz wprowadzenie testu Turinga, który stał się kluczowym „*kamieniem milowym*" w rozwoju tej dziedziny, dostarczając ramy do oceny zdolności maszyn do „*myślenia*" na sposób ludzki[10].

Kolejnym ważnym etapem był okres często określany jako „*złoty wiek*" sztucznej inteligencji, obejmujący lata 50. i 60. XX wieku. W tym czasie, dzięki wsparciu finansowemu ze strony rządu USA, dziedzina ta przechodziła dynamiczny rozwój, a naukowcy byli pełni optymizmu co do przyszłości i możliwości SI[11].

Jednak entuzjazm ten został stłumiony podczas tzw. „*chłodnej fazy SI*", która miała miejsce w latach 70. i 80., kiedy wiele projektów SI nie spełniło oczekiwań, prowadząc do ograniczenia finansowania oraz zainteresowania ze strony rządu i przemysłu.[12].

Współczesna era, często nazywana „*renesansem SI*", charakteryzuje się znaczącymi postępami w dziedzinie uczenia maszynowego, głębokiego uczenia oraz dostępności dużych zbiorów danych. To wszystko wspólnie umożliwiło osiągnięcie znaczących sukcesów w różnych obszarach zastosowań SI takich jak rozpoznawanie obrazów, czy przetwarzanie języka naturalnego albo autonomiczna jazda[13].

1.1.2.1 Współczesne rozumienie SI

Współczesne rozumienie sztucznej inteligencji ma swoje korzenie w dziedzinie informatyki, ale korzysta również z wielu innych nauk, takich jak psychologia, neurobiologia, matematyka, lingwistyka i inne. SI nie jest już tylko postrzegana jako narzędzie do naśladowania ludzkiej

[9] McCorduck P., *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence*, A K Peters/CRC Press 2004.
[10] Turing A. M., *Computing Machinery and Intelligence*, "Mind" 1950, Vol. 59, No. 236, s. 433-460.
[11] Crevier D., *AI: The Tumultuous History of the Search for Artificial Intelligence*, Basic Books 1993.
[12] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[13] Goodfellow I., Bengio Y., Courville A., Bengio Y., *Deep Learning*, Vol. 1, MIT Press Cambridge 2016.

inteligencji lub przewyższania jej, ale także jako technologia wspierająca i poszerzająca ludzkie możliwości[14].

Współczesne podejście do SI skupia się głównie na praktycznych zastosowaniach i potencjalnych korzyściach tej technologii. Na przykład systemy rekomendacji stosowane przez platformy e-commerce do personalizacji ofert dla użytkowników czy systemy rozpoznawania mowy używane przez asystentów wirtualnych to tylko kilka przykładów[15].

Etyka i odpowiedzialność są równie istotnymi elementami współczesnej sztucznej inteligencji. W miarę postępującego rozwoju technologicznego pojawiają się kwestie dotyczące odpowiedzialności, bezpieczeństwa oraz wpływu SI na społeczeństwo. Pojęcie „*odpowiedzialnej SI*" odgrywa kluczową rolę w debatach dotyczących przyszłości tej technologii[16].

Rozwój sztucznej inteligencji jest ściśle powiązany z dostępnością danych potrzebnych do trenowania modeli. Kwestie prywatności i ochrony danych stają się coraz bardziej istotne wraz z postępem technologicznym, a regulacje prawne takie jak *Ogólne Rozporządzenie o Ochronie Danych* (dalej: GDPR)[17] nabierają znaczenia w kontekście wykorzystywania oraz rozwoju sztucznej inteligencji.[18].

1.2 Definiowanie sztucznej inteligencji

1.2.1 Techniczne aspekty definicji SI

Sztuczna inteligencja to obszar informatyki, który od dawna przyciąga uwagę i ciekawość naukowców, technologów i filozofów. Techniczne aspekty SI często koncentrują się na jej

[14] Por.:Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[15] Goodfellow I., Bengio Y., Courville A., Bengio Y., *Deep Learning*, Vol. 1, MIT Press Cambridge 2016.
[16] Por.:Floridi L., Cowls J., *A Unified Framework of Five Principles for AI in Society*, "Harvard Data Science Review" 2019.
[17] **Ogólne Rozporządzenie o Ochronie Danych (GDPR)** - Przepis prawniczy przyjęty przez Unię Europejską i obowiązujący od 25 maja 2018 roku, mający na celu kontrolowanie przetwarzania danych osobowych przez firmy i organizacje w UE. GDPR zwiększa prawa jednostek w zakresie ochrony prywatności danych, wprowadzając szereg wymagań, które firmy muszą spełnić podczas gromadzenia, przetwarzania i przechowywania danych osobowych. To rozporządzenie niesie także za sobą poważne kary finansowe za złamanie zasad dotyczących ochrony danych.
[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

zdolności do wykonywania zadań, które normalnie wymagałyby ludzkiej inteligencji do ich wykonania[19].

Jednym z kluczowych elementów technicznych SI jest możliwość uczenia się, czyli dostosowywanie się do nowych danych i sytuacji poprzez zmianę wewnętrznych parametrów. Algorytmy uczenia maszynowego, takie jak sieci neuronowe, są powszechnie stosowane do tego celu, umożliwiając „*maszynom uczenie się*" (ang. machine learning) z danych i doskonalenie swoich działań w miarę zdobywania nowych doświadczeń[20].

Innym istotnym technicznym aspektem jest przetwarzanie języka naturalnego (NLP), które pozwala maszynom na rozumienie i generowanie ludzkiego języka, co jest istotne dla interakcji między człowiekiem a maszyną[21].

Z kolei umiejętność rozpoznawania wzorców zarówno w danych wizualnych, jak i innych formach danych stanowi kolejny ważny element techniczny uwzględniany często w definicjach SI. To umożliwia maszynom „*rozumienie*" oraz interpretację danych sensorycznych[22][23].

1.2.2 Filozoficzne podejście do definicji SI

Rozważania filozoficzne na temat sztucznej inteligencji często dotyczą głębokich kwestii związanych z naturą umysłu, świadomości i tym, co oznacza być „*inteligentnym*". Alan Turing, uważany powszechnie za twórcę sztucznej inteligencji, przedstawił słynny test Turinga jako miarę inteligencji maszynowej pytając, czy maszyna może działać w sposób nierozróżnialny od człowieka[24].

Jednakże filozoficzne zagadnienia dotyczące SI sięgają znacznie dalej, rozważając możliwość posiadania przez maszyny świadomości czy zdolności „*myślenia*" w prawdziwym sensie tego

[19] Por.:Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[20] Więcej: Goodfellow I., Bengio Y., Courville A., Bengio Y., *Deep Learning*, Vol. 1, MIT Press Cambridge 2016.
[21] Patrz: Jurafsky D., Martin J. H., *Speech and Language Processing*, Cambridge University Press 2019.
[22] **Dane sensoryczne** - Informacje pobierane z otoczenia za pomocą czujników lub urządzeń, które potrafią wykrywać bodźce fizyczne, mogą obejmować różnorodne dane, takie jak obrazy i filmy wizualne, dźwięki i muzykę słyszalną, tekstury i ciśnienie odczuwane dotykiem oraz temperaturę mierzalną. W dziedzinie sztucznej inteligencji dane sensoryczne są często analizowane i przetwarzane w celu identyfikacji wzorców, klasyfikacji informacji oraz podejmowania decyzji na podstawie sygnałów z otoczenia. (Murphy, K. P.. Machine Learning: A Probabilistic Perspective. MIT Press) 2012.
[23] Bishop C. M., *Pattern Recognition and Machine Learning*, Springer 2006.
[24] Turing A. M., *Computing Machinery and Intelligence*, "Mind" 1950, Vol. 59, No. 236, s. 433-460.

słowa. John Searle w swoim eksperymencie myślowym „*Pokój Chiński*”[25] argumentuje, że nawet perfekcyjnie symulowane zachowania inteligentne nie są równoważne z prawdziwym rozumieniem, czy świadomością.[26].

Z kolei dla filozofów takich jak Daniel Dennett ludzki umysł jest rodzajem maszyny, a świadomość oraz myśli są formą algorytmu. To sugeruje teoretycznie możliwość bycia przez maszyny inteligentnymi lub nawet świadomymi[27].

Filozoficzne dyskusje na temat SI często koncentrują się na pytaniach o naturę umysłu, wartości etycznych i moralną odpowiedzialność maszyn. Prowadzi to do głębszych refleksji nad tym, jak definiowane i rozumiane są koncepcje oraz definicje SI.

1.2.3 Wyzwania związane z definiowaniem SI

Definiowanie sztucznej inteligencji stanowi długotrwałe wyzwanie dla naukowców i filozofów, głównie z powodu trudności w samym zdefiniowaniu inteligencji[28].

Pierwszym problemem, na jaki się natrafia, jest różnorodność dziedzin i zastosowań SI, które obejmują obszary tak różnorodne jak rozpoznawanie wzorców, uczenie maszynowe, rozumowanie, planowanie czy interakcje między ludźmi a maszynami. Każda z tych dziedzin może wymagać własnego określenia i kryteriów oceny inteligencji[29].

Kolejnym aspektem do rozważenia jest kwestia świadomości i zrozumienia. Czy maszyna zdolna do symulowania ludzkich zachowań i reakcji faktycznie „*rozumie*” wykonywane

[25] **Pokój Chiński** - Eksperyment myślowy zaproponowany przez Johna Searle'a ma na celu podważenie idei, że maszyny lub komputery mogą posiadać prawdziwe rozumienie lub świadomość. W tym eksperymencie osoba nieznająca języka chińskiego siedzi w pokoju i korzysta z szczegółowych instrukcji (lub “programu"), aby odpowiadać na pytania zadawane w języku chińskim, nawet jeśli nie rozumie tego języka. Searle argumentuje, że nawet jeśli odpowiedzi są trudne do odróżnienia od odpowiedzi osoby faktycznie znającej język chiński, to osoba (lub maszyna) w pokoju nie rozumie języka w prawdziwym znaczeniu, ponieważ jej brakuje świadomości i zrozumienia znaczenia tych symboli; patrz: (Searle, J. R. (1980). Umysły, mózgi i programy. Behavioral and Brain Sciences” 1980, No 3(3), 417-457).

[26] Searle J. R., *Minds, Brains, and Programs*, “Behavioral and Brain Sciences” 1980, Vol. 3, No. 3, s. 417-457.

[27] Dennett D. C., *Consciousness Explained*, Little, Brown and Co 1991.

[28] Legg S., Hutter M., *A Collection of Definitions of Intelligence*, “Frontiers in Artificial Intelligence and Applications” 2007, Vol. 157, s. 17.

[29] Poole D., Mackworth A., Goebel R., *Computational Intelligence: A Logical Approach*, Oxford University Press 1998.

zadania czy też po prostu imituje obserwowane zachowania? To pytanie - często określane jako „*trudny problem świadomości*" - stanowi przedmiot intensywnych debat i badań[30].

Na koniec warto podkreślić etyczne i moralne dylematy związane z definiowaniem SI. Jakie prawa oraz obowiązki powinny być przyznane maszynom wykazującym pewien stopień „*inteligencji*"? Czy maszyna zdolna do symulowania emocji lub odczuwania bólu powinna być chroniona przed „*krzywdą*"?[31].

1.3 Klasyfikacja sztucznej inteligencji

Wraz z postępem technologii sztucznej inteligencji i jej coraz większą powszechnością, rośnie potrzeba klarownego opisu i klasyfikacji tych systemów. Ustalenie jasnych kategorii pozwala lepiej zrozumieć różnorodność SI, ich potencjalne zastosowania oraz wynikające z nich wyzwania etyczne i prawne. Niniejszy rozdział ma na celu przedstawienie różnych podejść do klasyfikacji systemów SI, skupiając się na różnych kryteriach, takich jak stopień autonomii, zdolności poznawcze, sposób uczenia się czy praktyczne wykorzystanie.

Klasyfikacja ta nie tylko ułatwia zrozumienie technicznej strony sztucznej inteligencji, ale także pomaga w identyfikacji obszarów wymagających regulacji prawniczej i nadzoru. Zrozumienie tych systemów oraz ich podziałów jest istotne dla prawników, decydentów politycznych oraz badaczy, aby efektywnie reagować na dynamiczny rozwój tej technologii i przewidywać konsekwencje jej implementacji.

W dalszej części rozdziału omówione zostaną główne kategorie sztucznej inteligencji podzielone według współczesnych kryteriów klasyfikacyjnych, które ukazują kompleksowość i różnorodność tego szybko ewoluującego obszaru.

1.3.1 Sztuczna inteligencja słaba (narrow AI) vs. silna (strong AI)

Rozróżnienie pomiędzy sztuczną inteligencją słabą (ang. narrow AI) a silną (ang. strong AI) jest kluczowe dla zrozumienia różnic w podejściach i celach w dziedzinie sztucznej inteligencji. Sztuczna inteligencja słaba, znana również jako narrow AI, odnosi się do systemów SI, które zostały zaprojektowane i przeszkolone do wykonywania określonych zadań bez posiadania

[30] Chalmers D. J., *Facing Up to the Problem of Consciousness*, "Journal of Consciousness Studies" 1995, Vol. 2, No. 3, s. 200-219.
[31] Gunkel D. J., *The Machine Question: Critical Perspectives on AI, Robots, and Ethics*, MIT Press 2012.

ogólnej inteligencji. Przykładowo, systemy rozpoznawania mowy, rekomendacji produktów czy autonomiczne pojazdy są przykładami narrow AI[32]. Mimo, że te systemy mogą wydawać się inteligentne i zaawansowane w swoich specyficznych obszarach, ich możliwości są ściśle ograniczone do konkretnego zakresu zadań.

Z kolei sztuczna inteligencja silna, zwana także generalną SI, to rodzaj maszynowej inteligencji teoretycznej posiadający zdolność do rozumienia, uczenia się i stosowania wiedzy w różnych obszarach poprzez symulację zdolności poznawczych człowieka. Strong AI nie tylko jest zdolna do wykonywania zadań, ale także posiada umiejętność rozumowania oraz samoświadomość[33].

Debata na temat możliwości osiągnięcia strong AI jest szeroka i obejmuje różnorodne perspektywy – zarówno optymistyczne jak i sceptyczne – dotyczące przyszłości sztucznej inteligencji. Podczas gdy niektórzy naukowcy i filozofowie tak jak Ray Kurzweil przewidują nadejście epoki, w której maszyny będą posiadały pełen zestaw ludzkich zdolności poznawczych[34], inni tacy jak Hubert Dreyfus czy John Searle wyrażają poważne zastrzeżenia co do tego czy maszyny kiedykolwiek będą zdolne osiągnąć prawdziwą świadomość, czy zrozumienie[3536].

1.3.2 Sztuczna inteligencja ogólna (AGI) vs. specjalizowana (ASI)

Analizując różne rodzaje sztucznej inteligencji, często dochodzi się do dyskusji na temat ich zakresu i specjalizacji. W kontekście tego zagadnienia istnieją dwie główne kategorie, które są zwykle analizowane: ogólna sztuczna inteligencja (AGI) oraz specjalizowana sztuczna inteligencja (ASI).

Ogólna Sztuczna Inteligencja (AGI), określana czasem jako „*wszechstronna sztuczna inteligencja*", odnosi się do zdolności maszyny do wykonywania dowolnego zadania intelektualnego, które może być zrealizowane przez ludzki umysł. AGI nie jest ograniczona do jednej konkretnej dziedziny, czy zadania, ale potrafi rozumieć, uczyć się i stosować wiedzę

[32] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[33] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.
[34] K Kurzweil R., *The Singularity Is Near: When Humans Transcend Biology*, Viking 2005.
[35] Dreyfus H. L., *What Computers Still Can't Do: A Critique of Artificial Reason*, MIT Press 1992.
[36] Searle J. R., *Minds, Brains, and Programs*, "Behavioral and Brain Sciences" 1980, Vol. 3, No. 3, s. 417-457.

w różnych obszarach, co sprawia, że jest wszechstronna i elastyczna w różnych kontekstach i sytuacjach[37].

Natomiast sztuczna inteligencja Specjalizowana (ASI), czasami nazywana „*superinteligencją*" (ang. superintelligence), odnosi się do systemów SI, które przewyższają ludzką inteligencję we wszystkich istotnych aspektach, łącznie z kreatywnością, umiejętnością rozwiązywania problemów oraz zdolnościami społecznymi. ASI teoretycznie miałaby zdolność przewyższania najlepszych ludzkich umysłów we wszystkich dziedzinach, obejmując naukę, sztukę oraz interakcje społeczne[38].

Wyzwania związane z osiągnięciem AGI i ASI są kolosalne i obejmują nie tylko bariery technologiczne, lecz także etyczne oraz filozoficzne dylematy. Na przykład jak zagwarantować zgodność rozwijającej się inteligencji z wartościami i interesami ludzkimi? Jakie środki bezpieczeństwa i kontroli powinny być wprowadzone, aby zapewnić bezpieczne rozwijanie i wdrażanie AGI lub ASI?[39].

1.3.3 Klasyfikacja według zdolności do uczenia się

Klasyfikacja sztucznej inteligencji z uwzględnieniem zdolności uczenia się stwarza ciekawe pole do rozmów i analizy, skupiając się na tym, w jaki sposób różne systemy SI dostosowują się i rozwijają w reakcji na nowe dane i doświadczenia. Klasyfikacja ta prezentuje się następująco:

1. uczenie nadzorowane i nienadzorowane

   Uczenie maszynowe jest dziedziną sztucznej inteligencji, którą można ogólnie podzielić na uczenie nadzorowane i nienadzorowane. W przypadku uczenia nadzorowanego model jest trenowany na podstawie danych z etykietami, co oznacza, że każdy przykład treningowy jest powiązany z odpowiedzią, którą model ma się nauczyć przewidywać[40]. Natomiast uczenie nienadzorowane polega na analizowaniu danych bez etykiet, gdzie algorytm stara się odkryć ukryte wzorce lub struktury w danych[41].

[37] Goertzel B., Pennachin C. (Eds.), *Artificial General Intelligence*, Springer 2007.
[38] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.
[39] Russell S., Dewey D., Tegmark M., *Research Priorities for Robust and Beneficial Artificial Intelligence*, "AI Magazine" 2015, Vol. 36, No. 4, s. 105-114.
[40] Bishop C. M., *Pattern Recognition and Machine Learning, Spri*nger 2006.
[41] Hinton G. E., Sejnowski T. J., *Unsupervised Learning: Foundations of Neural Computation*, MIT Press 1999.

2. uczenie przez wzmacnianie

   Nauka przez wzmacnianie to metoda, w której modele uczą się podejmować sekwencje decyzji poprzez interakcję ze środowiskiem i otrzymywanie informacji zwrotnej na temat swoich wyborów w postaci pozytywnych lub negatywnych sygnałów[42]. Stanowi to kluczowy element dla systemów, które muszą nauczyć się funkcjonować w zmiennych warunkach, takich jak gry komputerowe, czy robotyka.

3. uczenie głębokie

   Głębokie uczenie, które wykorzystuje zaawansowane sieci neuronowe, umożliwia modelom przetwarzanie i zrozumienie ogromnych zbiorów danych, co często prowadzi do imponujących wyników w dziedzinach takich jak rozpoznawanie obrazów, mowy czy analiza tekstu[43].

4. transfer wiedzy i uczenie wielozadaniowe

   Przekazywanie informacji i uczenie się wielozadaniowe to techniki, które umożliwiają modelom wykorzystać zdobytą wiedzę podczas rozwiązywania jednego zadania do rozwiązania innych problemów z nim związanych. Taka praktyka może przyspieszyć i usprawnić proces uczenia się[44].

1.4 Formy i aplikacje sztucznej inteligencji. Algorytmy i maszyny uczące się

Algorytmy oraz techniki uczenia maszynowego stanowią istotny składnik sztucznej inteligencji, pozwalając systemom na analizę danych, wyciąganie wniosków z praktyki i adaptację do nowych informacji. Podział ze względu na formy i aplikacje sztucznej inteligencji, przedstawia się następująco:

1. klasyfikacja algorytmów uczenia maszynowego

[42] Sutton R. S., Barto A. G., *Reinforcement Learning: An Introduction*, MIT Press 2018.
[43] Goodfellow I., Bengio Y., Courville A., Bengio Y., *Deep Learning*, Vol. 1, MIT Press Cambridge 2016.
[44] Pan S. J., Yang Q., *A Survey on Transfer Learning*, "IEEE Transactions on Knowledge and Data Engineering" 2010, Vol. 22, No. 10, s. 1345-1359.

Istnieje wiele rodzajów algorytmów uczenia maszynowego, które można sklasyfikować na różne sposoby, na przykład pod względem rodzaju uczenia (nadzorowanego, nienadzorowanego, półnadzorowanego i przez wzmacnianie) oraz zdolności do uczenia w czasie rzeczywistym online lub offline w trybie wsadowym[45].

2. drzewa decyzyjne i lasy losowe

   „*Drzewa decyzyjne*" oraz „*lasy losowe*" są powszechnie używanymi algorytmami do rozwiązywania problemów klasyfikacji i regresji, oferując czytelne i graficzne przedstawienie procesów podejmowania decyzji[46].

3. sieci neuronowe

   Sieci neuronowe, inspirowane strukturą i funkcjonowaniem ludzkiego mózgu, są podstawą wielu zaawansowanych technik uczenia głębokiego, co umożliwia rozpoznawanie wzorców i klasyfikację w skomplikowanych zbiorach danych[47].

4. algorytmy oparte na danych

   Algorytmy, takie jak SVM czy regresja logistyczna, które koncentrują się na wyznaczaniu granic decyzyjnych w danych, są używane w różnych dziedzinach, począwszy od analizy finansowej aż po diagnostykę medyczną[48].

5. algorytmy optymalizacyjne

   Algorytmy optymalizacyjne, takie jak algorytmy ewolucyjne lub algorytmy roju, są stosowane do rozwiązywania problemów polegających na wyborze najlepszego rozwiązania spośród wielu możliwości, na przykład w projektowaniu sieci czy planowaniu produkcji[49].

6. robotyka i autonomizacja

[45] Alpaydin E., *Introduction to Machine Learning*, MIT Press 2014.
[46] Breiman L., *Random Forests*, "Machine Learning" 2001, Vol. 45, No. 1, s. 5-32.
[47] Goodfellow I., Bengio Y., Courville A., Bengio Y., *Deep Learning*, Vol. 1, MIT Press Cambridge 2016.
[48] Vapnik V., *The Nature of Statistical Learning Theory*, Springer 1995.
[49] Yang X. S., *Nature-Inspired Metaheuristic Algorithms*, Luniver Press 2010.

Robotyka i autonomizacja to obszary, które znacząco wspierają rozwój technologiczny poprzez łączenie sztucznej inteligencji w celu stworzenia maszyn zdolnych do samodzielnego funkcjonowania oraz podejmowania decyzji[50].

7. robotyka przemysłowa

   Technologie sztucznej inteligencji wykorzystywane w robotyce przemysłowej zmieniają sposób, w jaki odbywają się procesy produkcyjne, wprowadzając automatyzację i efektywność w różnorodnych branżach przemysłu. Roboty przemysłowe są zdolne do wykonywania zadań z precyzją i konsekwencją, które często sprawiają trudności ludziom, takie jak montaż czy spawanie[51].

8. autonomiczne pojazdy

   Pojazdy autonomiczne, takie jak samochody, drony czy statki, wykorzystują zaawansowane algorytmy sztucznej inteligencji do poruszania się, omijania przeszkód i podejmowania decyzji w różnorodnych środowiskach. To stwarza nowe możliwości oraz problemy do rozwiązania, zarówno techniczne, jak i etyczne[52].

9. roboty społeczne i opiekuńcze

   Roboty towarzyskie i opiekuńcze, takie jak roboty asystujące czy towarzyszące, korzystają z sztucznej inteligencji do komunikacji z ludźmi, oferując pomoc, wsparcie i towarzystwo, a także pomagając w codziennych obowiązkach, takich jak rozmowy, czy opieka nad osobami starszymi[53].

[50] Tkacz S., *Robotyka i autonomizacja - wpływ na rozwój technologiczny*, w: Knosala R. (red.), „Innowacje w zarządzaniu i inżynierii produkcji" 2018, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, t.1, s. 471.
[51] Nof S. Y. (Ed.), *Handbook of Industrial Robotics*, Wiley 1999.
[52] Maurer M., Gerdes J. C., Lenz B., Winner H. (Eds.), *Autonomous Driving: Technical, Legal and Social Aspects*, Springer 2016.
[53] Broadbent E., *Interactions with Robots: The Truths We Reveal about Ourselves*, "Annual Review of Psychology" 2017, Vol. 68, s. 627-652.

10. robotyka medyczna

Technologia medyczna wykorzystująca robotykę integruje sztuczną inteligencję w celu ułatwienia dokładnych zabiegów chirurgicznych, diagnostyki i terapii, co może skutkować poprawą rezultatów terapeutycznych oraz zmniejszeniem ryzyka dla pacjentów[54].

11. autonomizacja procesów biznesowych

Wykorzystanie robotów do automatyzacji procesów biznesowych (RPA) i innych technologii sztucznej inteligencji umożliwia przedsiębiorstwom lepsze zarządzanie zadaniami i procesami, co prowadzi do obniżenia kosztów i zwiększenia efektywności operacyjnej[55].

12. systemy ekspertowe

Systemy ekspertowe to programy komputerowe, które imitują zdolności podejmowania decyzji eksperta ludzkiego w określonej dziedzinie. Korzystają z bazy wiedzy zawierającej fakty i reguły, aby rozwiązywać konkretne problemy w danej dziedzinie ekspertyzy[56]:

13. asystenci wirtualni

Asystenci wirtualni, korzystając z technologii sztucznej inteligencji, takich jak przetwarzanie języka naturalnego (NLP) i uczenie maszynowe, potrafią rozumieć i odpowiadać na pytania użytkowników, często prowadząc naturalne rozmowy[57].

1.5 Etyczne i filozoficzne implikacje sztucznej inteligencji

1.5.1 SI a świadomość i samoświadomość

Badanie związku między sztuczną inteligencją a pojęciami świadomości i samoświadomości stawia przed nami fundamentalne pytania dotyczące istoty umysłu, świadomości oraz tego, co oznacza „*bycie świadomym*". Biorąc powyższe pod uwagę należy wyróżnić aspekty, które należy rozważać mówiąc o SI w kontekście świadomości i samoświadomości:

[54] Rosen J., Hannaford B., Satava R. M., *Surgical Robotics: Systems Applications and Visions*, Springer 2019.
[55] Lacity M. C., Willcocks L. P., Robotic Process Automation and Risk Mitigation: The Definitive Guide, SB Publishing 2016.
[56] Durkin J., *Expert Systems: Design and Development*, Macmillan Publishing Co 1994.
[57] McTear M., Callejas Z., Griol D., The Conversational Interface: Talking to Smart Devices, Springer 2016.

1. definiowanie świadomości

   Często uważana za wyjątkową cechę istot ludzkich, świadomość obejmuje zdolność do doświadczania, percepcji i refleksji nad własnymi stanami umysłowymi. W ramach sztucznej inteligencji pojawia się pytanie: czy maszyny mogą posiadać formę świadomości, czy też są jedynie zaawansowanymi systemami przetwarzania informacji[58]?

2. SI i świadomość

   Istnieje wiele dyskusji na temat możliwości osiągnięcia przez sztuczną inteligencję poziomu świadomości. Jedni twierdzą, że maszyny mogą jedynie imitować świadomość, nie posiadając jej faktycznie, podczas gdy inni sugerują, że zaawansowana SI może potencjalnie rozwijać pewną formę świadomości[59].

3. samoświadomość maszyn

   Samoświadomość, czyli umiejętność analizy własnych stanów mentalnych i istnienia, jest kolejnym stopniem złożoności. W przypadku sztucznej inteligencji, samoświadomość oznacza możliwość systemu do rozpoznawania i refleksji nad własnymi procesami decyzyjnymi oraz „*myślowymi*”[60].

4. etyczne implikacje świadomej SI

   Jeśli rozważymy perspektywę istnienia sztucznej inteligencji świadomej, pojawiają się istotne kwestie moralne. Jakie prawa powinny być przyznane świadomym maszynom? Jakie zobowiązania i odpowiedzialności mamy wobec nich oraz jakie konsekwencje to niesie dla naszego pojmowania moralności i etyki[61]?

1.5.2 Moralność i etyka maszyn

W obliczu rosnącego wpływu sztucznej inteligencji na społeczeństwo, zagadnienia związane z moralnością i etyką maszyn stają się coraz bardziej istotne. Dyskusje skupiają się na

[58] Chella A., Manzotti R., *Artificial Consciousness: Theoretical and Practical Issues*, "Frontiers in Robotics and AI" 2020, Frontiers Media SA, vol. 7, s. 1.
[59] Searle J. R., *Minds, Brains, and Programs*, “Behavioral and Brain Sciences” 1980, Vol. 3, No. 3, s. 417-457.
[60] Metzinger T., Being No One: The Self-Model Theory of Subjectivity, MIT Press 2003.
[61] Gunkel D. J., The Machine Question: Critical Perspectives on AI, Robots, and Ethics, MIT Press 2012.

wyzwaniach etycznych związanych z tworzeniem i wdrażaniem SI oraz filozoficznych implikacjach potencjalnej moralności maszyn[62]. Do tych wyzwań należą:

1. etyczne wyzwania w projektowaniu SI

   Projektowanie sztucznej inteligencji stawia przed nami wiele pytań moralnych, takich jak sprawiedliwość, przejrzystość i odpowiedzialność. Osoby zajmujące się tworzeniem sztucznej inteligencji muszą zastanowić się nad tym, jak zapewnić uczciwość i bezstronność systemów oraz jakie środki odpowiedzialności powinny zostać wprowadzone[63].

2. maszyny a moralność

   Czy komputery mogą posiadać moralność? Czy mogą podejmować decyzje, opierając się na normach etycznych? Te kwestie prowadzą do głębokich refleksji na temat natury moralności oraz pytają, czy może ona być odtwarzana lub nawet autentycznie doświadczana przez maszyny[64].

3. autonomia moralna maszyn

   Autonomia moralna oznacza zdolność do podejmowania samodzielnych decyzji moralnych. W kontekście sztucznej inteligencji pojawia się pytanie, czy maszyny kiedykolwiek będą w stanie osiągnąć autentyczną autonomię moralną, czy też zawsze będą polegać na wartościach i zasadach narzuconych przez ludzi[65].

4. etyczne implikacje autonomicznej SI

   Rozwój sztucznej inteligencji autonomicznej, która jest zdolna do samodzielnego podejmowania decyzji, stawia przed nami wiele pytań dotyczących etyki, takich jak: kwestie odpowiedzialności, kontroli i praw maszyn oraz jak powinniśmy radzić sobie z etycznymi konsekwencjami decyzji podejmowanych przez maszyny[66]?

---

[62] Bostrom N., Yudkowsky E., *The Ethics of Artificial Intelligence*, "The Cambridge Handbook of Artificial Intelligence" 2014, Cambridge University Press, s. 316.
[63] Vincent, J. (2019). *Ethics in the Age of Artificial Intelligence*. Oxford University Press.
[64] Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.
[65] Bryson J. J., *Robots should be slaves*, red. Y. Wilks, in: "Close Engagements with Artificial Companions: Key Social, Psychological, Ethical and Design Issues", John Benjamins Publishing Company, Vol. 8, s. 63-74, https://doi.org/10.1075/nlp.8.11bry (dostęp: 10.06.2024 r.)
[66] Bostrom N., Yudkowsky E., *The Ethics of Artificial Intelligence*, red. Keith Frankish, William Ramsey, "Cambridge Handbook of Artificial Intelligence" 2014.

1.5.3 Autonomia decyzyjna SI a wolna wola

Temat autonomii decyzyjnej sztucznej inteligencji (SI) oraz kwestii wolnej woli stanowi głęboko zakorzeniony element dyskusji filozoficznych i etycznych dotyczących roli i znaczenia SI w społeczeństwie. Zrozumienie wpływu autonomii maszyn na nasze postrzeganie wolnej woli jest kluczowe dla kształtowania przyszłości technologii. Należy przy tym uwzględnić:

1. autonomię decyzyjną SI

   Autonomia decyzyjna sztucznej inteligencji oznacza zdolność systemów do podejmowania decyzji bez bezpośredniego nadzoru ludzkiego. Wraz z postępem technologii SI, maszyny stają się coraz bardziej niezależne w podejmowaniu decyzji, co rodzi szereg wyzwań etycznych i prawnych[67].

2. wolną wolę a SI

   Czy możliwe jest, aby maszyny, nawet te o dużej autonomii, posiadały coś w rodzaju „*wolnej woli*", czyli zdolności do podejmowania decyzji niezależnie od zewnętrznych czynników? Koncepcja wolnej woli jest głęboko zakorzeniona w ludzkiej świadomości i moralności[68].

3. etyczne i prawne implikacje autonomicznej SI

   Technologiczne systemy autonomiczne, które mają zdolność podejmowania decyzji bez ingerencji ludzi, stawiają przed nami wiele trudnych pytań z zakresu etyki. Jakie powinny być ograniczenia odpowiedzialności maszyn oraz w jaki sposób możemy zapewnić, że ich działania są zgodne z naszymi przekonaniami i standardami moralnymi[69]?

4. Przyszłość autonomii SI

   Rozważania na temat przyszłości autonomii sztucznej inteligencji skupiają się na kwestiach związanych z ewolucją tej technologii oraz potencjalnymi skutkami

[67] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach, Pearson* 2016.
[68] Dennett D. C., *Freedom Evolves*, Viking 2003.
[69] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.

wprowadzenia coraz bardziej autonomicznych systemów do różnorodnych obszarów naszego społeczeństwa[70].

1.6 Przyszłość sztucznej inteligencji

1.6.1 Prognozy i scenariusze rozwoju SI

Rozważania na temat przyszłości sztucznej inteligencji są równie intrygujące, jak i niezwykle skomplikowane, biorąc pod uwagę dynamiczny postęp technologii i jej wpływ na różne obszary społeczeństwa i gospodarki. Przewidywania oraz wizje rozwoju SI często stanowią przedmiot spekulacji, ale także poważnych analiz naukowych i technologicznych, należą do nich przede wszystkim:

1. technologiczne prognozy rozwoju SI

   Postęp sztucznej inteligencji ściśle wiąże się z rozwojem dziedzin takich jak machine learning, przetwarzanie języka naturalnego i robotyka. Nadchodzące lata mogą przynieść rozwój w tych obszarach, ale także wprowadzenie nowych paradygmatów i technologii71.

2. społeczno-ekonomiczne scenariusze

   Wpływ sztucznej inteligencji na społeczeństwo i gospodarkę jest już zauważalny i obejmuje obszary takie jak rynek pracy, bezpieczeństwo czy ochrona prywatności. Przyszłe scenariusze mogą uwzględniać różne ścieżki wpływu SI na te dziedziny, biorąc pod uwagę różnorodne możliwości regulacyjne i adaptacyjne[72].

3. etyczne i moralne wyzwania przyszłości

   Rozwój sztucznej inteligencji w przyszłości prawdopodobnie stanie przed nami nowymi problemami etycznymi i moralnymi, takimi jak autonomia maszyn, prawa maszyn, czy wpływ na ludzką autonomię i wolność. Odpowiedź społeczeństwa na te wyzwania będzie kluczowym pytaniem w nadchodzących latach[73].

[70] Scharre P., *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton & Company 2018.
[71] Kurzweil R., *The Singularity Is Near: When Humans Transcend Biology*, Viking 2005.
[72] Brynjolfsson E., McAfee A., *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company 2014.
[73] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.

4. SI a przyszłość ludzkości

Rozmyślenia na temat przyszłości sztucznej inteligencji często dotyczą również kluczowych kwestii dotyczących dalszych losów ludzkości, roli człowieka w świecie coraz bardziej podporządkowanym technologii oraz tego, jakie znaczenie w społeczeństwie będą miały maszyny[74].

5. SI a Prawo

a. regulacje prawne dotyczące SI

Rozwój sztucznej inteligencji stwarza nowe wyzwania dla ustawodawców, którzy muszą dostosować obecne przepisy do zmieniającej się rzeczywistości, aby zapewnić ochronę praw jednostek i zapewnić sprawiedliwość wobec systemów autonomicznych[75].

b. odpowiedzialność prawna SI

Kwestia odpowiedzialności prawnej za czyny wykonywane przez sztuczną inteligencję jest ważnym zagadnieniem. Jak można określić, kto odpowiada za decyzje podejmowane przez maszyny? Jakie zmiany w przepisach są potrzebne, aby skutecznie rozwiązać te problemy[76]?

c. prawa maszyn

Czy należy przyznać maszynom prawa? Jakie prawa mogą one posiadać i jaki wpływ będą miały na nasz system prawny oraz społeczeństwo? To pytania, które prawdopodobnie nabiorą coraz większego znaczenia wraz z postępem technologii[77].

d. SI a prawa człowieka

Jak zagwarantować, że rozwój i wdrożenie sztucznej inteligencji będą zgodne z fundamentalnymi prawami człowieka, takimi jak prawo do prywatności czy wolność

[74] Harari Y. N., *Homo Deus: A Brief History of Tomorrow*, Harper 2017.
[75] Solum Lawrence B., *Legal Personhood for Artificial Intelligences*, "North Carolina Law Review" 1992.
[76] Vladeck D. C., *Machines Without Principals: Liability Rules and Artificial Intelligence*, "Washington Law Review" 2014.
[77] Bryson J. J., Diamantis M. E., Grant T. D., *Of, for, and by the people: the legal lacuna of synthetic persons*, "Artificial Intelligence and Law" 2017.

słowa? Jakie środki kontroli i regulacji mogą być konieczne do ochrony tych praw w kontekście sztucznej inteligencji[78]?

1.6.2 Potencjalne zagrożenia i wyzwania

Mimo imponującego potencjału i korzyści, jakie może przynieść sztuczna inteligencja w różnych dziedzinach, towarzyszy jej wiele potencjalnych zagrożeń i wyzwań, które muszą być uwzględnione i rozwiązane przez naukowców, praktyków oraz decydentów. Należą do nich:

1. zagrożenia związane z autonomią SI

   Autonomia sztucznej inteligencji może prowadzić do sytuacji, w których maszyny podejmują decyzje niezgodne z etyką lub prawem, co rodzi pytania o kontrolę nad tymi systemami oraz mechanizmy zabezpieczające[79].

2. bezpieczeństwo i ochrona danych

   Z rosnącym potencjałem sztucznej inteligencji w zakresie przetwarzania i analizy danych pojawiają się wątpliwości dotyczące bezpieczeństwa informacji oraz ochrony prywatności danych osobowych[80].

3. ekonomiczne i społeczne konsekwencje

   Postęp sztucznej inteligencji może mieć wpływ na sytuację na rynku pracy, nierówności społeczne i ekonomiczne, a także na struktury społeczne, co wymaga zbadania i ewentualnej interwencji ze strony decydentów politycznych[81].

[78] Gavaghan C., *Defining the Challenge for 21st Century NZ: Robots and the Law*, New Zealand Law Foundation 2016.
[79] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.
[80] Zarsky T. Z., *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making, Science*, "Technology, & Human Values" 2016.
[81] Brynjolfsson E., McAfee A., *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company 2014.

4. etyczne i moralne dylematy

   Etyczne dylematy, takie jak sprawiedliwość algorytmiczna, uprzedzenia w danych czy etyczność decyzji podejmowanych przez sztuczną inteligencję, stanowią temat intensywnych analiz i debat w środowisku naukowym i przemyśle[82].

1.6.3 Kierunki dalszych badań i rozwoju technologii SI

Postęp technologii sztucznej inteligencji rozwija się dynamicznie i stale ewoluuje, co otwiera nowe perspektywy, jednakże generuje również nowe dylematy i zagadnienia dla naukowców oraz praktyków. Dlatego wyróżnia się kierunki, jakie powinny podlegać badaniom i rozwojowi towarzyszących sztucznej inteligencji, tj.:

1. eksploracja nowych architektur i algorytmów

   Wraz z postępem technologii sztucznej inteligencji, badacze starają się odkryć innowacyjne struktury i metody, które mogą zapewnić doskonalsze rezultaty oraz być bardziej wydajne pod względem obliczeniowym i energetycznym[83].

2. bezpieczeństwo i odporność SI

   Problemy związane z bezpieczeństwem i odpornością systemów sztucznej inteligencji na różnorodne formy ataków, takie jak ataki adwersarialne, stają się istotnym obszarem badań, mającym na celu zapewnienie niezawodności i bezpieczeństwa technologii[84].

3. badania nad wpływem SI na społeczeństwo

   Przyszłe studia powinny także koncentrować się na dochodzeniu, jak sztuczna inteligencja wpływa na społeczeństwo, gospodarkę oraz kulturę, aby lepiej zrozumieć i przewidzieć ewentualne zmiany i wyzwania, które mogą wyniknąć z powszechnego stosowania tych technologii[85].

---

[82] Mittelstadt B., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, Big Data & Society 2016.
[83] LeCun Y., Bengio Y., Hinton G., *Deep learning*, "Nature" 2015, Vol. 521, No. 7553, s. 436-444.
[84] Papernot N., McDaniel P., Goodfellow I., Jha S., Celik Z. B., Swami A., *Practical black-box attacks against machine learning*, Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security 2018.
[85] Susskind R., Susskind D., *The Future of the Professions: How Technology Will Transform the Work of Human Experts*, Oxford University Press 2015.

4. zbadanie etycznych dylematów SI

   Przyszłe badania powinny skupić się na badaniu moralnych wyzwań związanych z sztuczną inteligencją, takich jak autonomia, odpowiedzialność i sprawiedliwość, aby lepiej zrozumieć rozwój i zastosowanie tych technologii w sposób etyczny i sprawiedliwy[86].

5. interdyscyplinarność badań nad SI

   Rozwój sztucznej inteligencji wymaga podejścia interdyscyplinarnego, które integruje wiedzę z dziedzin informatyki, psychologii, filozofii, prawa oraz innych obszarów, aby skutecznie reagować na złożoność i różnorodność wyzwań związanych z tą technologią[87].

1.7 Podsumowanie

Podsumowując dyskusję z rozdziału dotyczącego podstaw teoretycznych sztucznej inteligencji, warto zwrócić uwagę na kilka kluczowych punktów, które wynikają z przeprowadzonej analizy.

1. skomplikowana definicja SI - określenie sztucznej inteligencji jest zadaniem skomplikowanym i wielopłaszczyznowym, obejmującym różnorodne perspektywy techniczne, filozoficzne oraz praktyczne aspekty technologii[88].

2. złożoność i wielopłaszczyznowość SI - sztuczna inteligencja jako dziedzina jest głęboko wielopłaszczyznowa i skomplikowana, obejmująca różnorodne aspekty techniczne, etyczne oraz społeczne, które wymagają dalszej analizy i refleksji[89].

3. rozwój i klasyfikacja SI - historia oraz rozwój sztucznej inteligencji pokazują dynamiczny postęp tej dziedziny od prostych algorytmów do zaawansowanych systemów zdolnych do wykonywania skomplikowanych zadań oraz uczenia się[90].

[86] Vincent J., *Ethical Dimensions of AI*, in Proceedings of the International Conference on Ethics and AI 2019.
[87] Vincent C., Bengio Y., *Evolutionary Architectures for Learning to Learn*, in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2019.
[88] Russell S., Norvig P., *Artificial Intelligence: A Modern Ap*proach, Pearson 2016.
[89] Kaplan A., *Where Does Artificial Intelligence Stand?*, "Proceedings of the International Conference on Artificial Intelligence" 2016.
[90] McCorduck P., *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence*, A K Peters/CRC Press 2004.

4. etyczne i filozoficzne wyzwania - kwestie etyczne i filozoficzne dotyczące SI takie jak autonomia decyzyjna, świadomość czy moralność maszyn są tematem istotnych dyskusji oraz badań mających na celu zrozumienie oraz radzenie sobie z potencjalnymi implikacjami technologicznymi[91].

5. ciągły rozwój i adaptacja - w miarę jak technologia SI będzie ewoluować konieczna będzie nieustanna adaptacja metod badawczych, regulacji prawnych oraz strategii implementacyjnych, aby efektywnie reagować na nowe wyzwania oraz możliwości[92].

6. przyszłość SI - przyszłość sztucznej inteligencji jest tematem wielu spekulacji i prognoz uwzględniających różnorodne scenariusze rozwoju potencjalnie zagrożenia a także kierunki dalszych badań oraz rozwoju technologicznego[93].

7. prawne wyzwania - sztuczna inteligencja stawia przed prawodawcami i ekspertami z dziedziny prawa liczne wyzwania, wynikające przede wszystkim z jej złożoności i ciągłej ewolucji. Kluczowe kwestie prawne, które pojawiają się w kontekście SI, obejmują:

   a. definicje i normy prawne - pierwszym krokiem w skutecznej regulacji jest ustalenie klarownych definicji kluczowych terminów związanych ze sztuczną inteligencją oraz wprowadzenie norm prawnych odnoszących się do aktualnego stanu wiedzy i technologii.

   b. odpowiedzialność - w kontekście SI pojawiają się pytania dotyczące przypisania odpowiedzialności, zarówno prawniczej, jak i moralnej, za działania podejmowane przez systemy sztucznej inteligencji. Konieczne jest określenie momentu, kiedy odpowiedzialność spoczywa na twórcy, użytkowniku lub samym systemie SI.

   c. prywatność i ochrona danych - kwestie związane z zbieraniem, przetwarzaniem i wykorzystywaniem danych przez systemy SI wymagają szczególnej uwagi w ramach przepisów dotyczących ochrony danych osobowych oraz prywatności.

[91] Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.
[92] Dignum V., Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way,"Nature" 2019, Springer.
[93] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.

d. wpływ na rynek pracy - automatyzacja i systemy sztucznej inteligencji mogą znacząco wpłynąć na rynek pracy, co stawia pytania dotyczące społecznych konsekwencji oraz potrzebę dostosowania systemów ubezpieczeń społecznych.

e. etyka i standardy postępowania - sztuczna inteligencja stwarza nowe wyzwania etyczne, takie jak pojęcie sztucznej świadomości, autonomii czy moralności maszyn, które potrzebują opracowania nowych norm postępowania oraz etycznych wytycznych.

f. adaptacja prawa do ciągłej ewolucji - prawo powinno być dostosowywalne, aby nadążać za szybkim tempem rozwoju technologii sztucznej inteligencji, co wymaga regularnego przeglądu i aktualizacji regulacji.

g. przyszłość i niepewność - przyszłość sztucznej inteligencji i jej wpływ na społeczeństwo, gospodarkę oraz system prawny jest niezwykle trudna do przewidzenia, co utrudnia tworzenie długoterminowych regulacji. Decydenci muszą być przygotowani na różnorodne sytuacje, łącznie z nieoczekiwanymi wyzwaniami.

Wyzwania te wymagają współpracy między prawnikami, informatykami, etykami oraz innymi ekspertami w celu skutecznego zarządzania wpływem SI na społeczeństwo i gospodarkę. Istotne jest także utrzymywanie otwartego dialogu z szeroką społecznością w celu zapewnienia przejrzystości i akceptacji nowych regulacji prawnych.

Rozdział II. Prawo karne a technologia - wprowadzenie do relacji pomiędzy technologią a prawem karnym

2.1 Ewolucja technologii a zmiany w prawie karnym

Rozwój technologii, szczególnie w obszarze informatyki, zawsze był ściśle związany z ewolucją prawa karnego. Początki informatyki, chociaż skromne w porównaniu do dzisiejszych osiągnięć, już wtedy stawiały wyzwanie dla prawa, które musiało dostosować się do nowej rzeczywistości.

Początki rozwoju informatyki, takie jak czas wynalezienia pierwszych komputerów i sieci, były świadkami pojawienia się pierwszych form przestępczości komputerowej. Na przykład w latach 60. i 70. XX wieku, gdy komputery stawały się bardziej powszechne, zaczęły pojawiać się pierwsze przypadki nieautoryzowanego dostępu lub kradzieży danych[94].

Wprowadzenie technologii informatycznych do codziennego życia społeczeństwa oraz funkcjonowania instytucji państwowych i firm spowodowało konieczność dostosowania prawa do nowych wyzwań. Zostały wprowadzone pierwsze regulacje prawne, takie jak *Ustawa o Przestępczości Komputerowej*[95] w Stanach Zjednoczonych w 1986 roku, mająca na celu zwalczanie nowych rodzajów przestępstw[96].

W miarę postępu technologicznego, zwłaszcza sztucznej inteligencji, prawo karne musiało zmierzyć się z problemami dotyczącymi odpowiedzialności prawnej. Pojawienie się sztucznej inteligencji podejmującej decyzje wcześniej zastrzeżone dla ludzi rodziło pytania dotyczące odpowiedzialności i winy[97].

Ewolucja technologii od początkowych komputerów po zaawansowane systemy sztucznej inteligencji wymagała i nadal wymaga dostosowywania prawa karnego tak aby mogło ono skutecznie reagować na nowe formy przestępstw oraz wyzwania związane z odpowiedzialnością prawną.

---

[94] Levy S., *Hackers: Heroes of the Computer Revolution*, Doubleday 1984.

[95] Ustawa o Przestępczości Komputerowej Stanów Zjednoczonych z dnia 29 października 1986 r. w sprawie zwalczania przestępstw komputerowych oraz ochrony systemów informatycznych (Computer Fraud and Abuse Act, 18 U.S.C. § 1030).

[96] Kerr O. S., *Computer Crime Law* (5th ed.), West Academic Publishing 2021.

[97] Ashley K. D., *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambridge University Press 2017.

Wraz z postępem technologii, system prawny będzie musiał ciągle się rozwijać, aby sprostać nowym wyzwaniom.

2.2 Wyzwania i możliwości technologiczne w kontekście prawa karnego

Technologia jako czynnik stymulujący rozwój, stawia przed prawem karnym zarówno wyzwania, jak i możliwości. W dobie cyfryzacji i wzrostu znaczenia sztucznej inteligencji w różnych dziedzinach społeczeństwa, system prawny musi dostosować się do nowej rzeczywistości technologicznej[98].

Wyzwania dla prawa karnego:

1. odpowiedzialność prawna - ustalenie, kto ponosi odpowiedzialność prawną za działania podejmowane przez systemy sztucznej inteligencji, stanowi istotne wyzwanie. Skomplikowana natura algorytmów oraz samodzielność podejmowania decyzji przez SI mogą sprawić trudności w określeniu odpowiedzialności prawnej[99].

2. prywatność - ochrona prywatności i danych osobowych w dzisiejszym świecie cyfrowym stanowi kolejne wyzwanie. Nowoczesne technologie, takie jak identyfikacja twarzy czy analiza ogromnych zbiorów danych (ang. big data), mogą stwarzać zagrożenie dla prywatności poszczególnych osób[100].

3. bezpieczeństwo cyfrowe - zagrożenia związane z cyberprzestępczością, takie jak ataki hakerskie czy ransomware, wymagają ciągłego doskonalenia zarówno przepisów prawnych, jak i technologii w celu skutecznego przeciwdziałania nim[101].

Możliwości technologiczne w kontekście prawa karnego:

[98] Ashley K. D., *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambridge University Press 2017.
[99] Kerr O. S., *Computer Crime Law* (5th ed.), West Academic Publishing 2021.
[100] Goldsmith J., Wu T., *Cybercrime: Digital Cops in a Networked Environment*, NYU Press 2006.
[101] Albanese J. S., *Transnational Crime and the 21st Century: Criminal Enterprise, Corruption, and Opportunity,* Oxford University Press 2011.

1. ściganie przestępstw - technologia oferuje narzędzia, które mogą być używane w celu zwalczania przestępczości, na przykład analiza danych czy sztuczna inteligencja mogą wspierać organy ścigania w identyfikacji i zapobieganiu przestępczości[102].

2. prewencja - technologia sztucznej inteligencji może być używana do analizy wzorców przestępczych oraz prognozowania potencjalnych zagrożeń, co może wspomóc w zapobieganiu przestępczości[103].

3. cyberbezpieczeństwo - postęp technologiczny pozwala również na tworzenie coraz bardziej zaawansowanych rozwiązań bezpieczeństwa, które pomagają w zwalczaniu zagrożeń związanych z cyberprzestępczością[104].

Podsumowując, technologia stawia przed prawem karnym pewne wyzwania ale jednocześnie otwiera drogę do wielu nowych możliwości, które mogą być wykorzystane w walce z przestępczością i podnoszeniu poziomu bezpieczeństwa w świecie cyfrowym. Kluczowe jest jednak, aby rozwój legislacyjny nadążał za postępem technologicznym i zapewniał równowagę między ochroną praw jednostek a skutecznością działań antyprzestępczych.

2.3 Technologia jako narzędzie przestępczości

2.3.1 Formy cyberprzestępczości

Cyberprzestępczość, będąca efektem postępu technologicznego, jest obecnie jednym z kluczowych wyzwań dla współczesnego prawa karnego. To zjawisko obejmuje różnorodne formy nielegalnej działalności, które wykorzystują technologię cyfrową zarówno jako narzędzie jak i cel przestępstwa[105].

Jedną z najpopularniejszych form przestępstw internetowych jest phishing, który polega na wyłudzaniu informacji osobistych i finansowych od użytkowników poprzez podszywanie się pod zaufane instytucje, takie jak banki czy urzędy administracji publicznej. Inne rodzaje

[102] Holt T. J., Bossler A. M., Seigfried-Spellar K. C., *Cybercrime and Digital Forensics: An Introduction*, Routledge 2014.
[103] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[104] Goodman M., Brenner S. W., *The Emerging Consensus on Criminal Conduct in Cyberspace*, International Journal of Law and Information Technology 2002, Vol. 10, No. 2, s. 135-223.
[105] Kerr O. S., *Computer Crime Law* (5th ed.), West Academic Publishing 2021.

ataków, np. ataki DDoS, mają na celu uniemożliwienie dostępu do konkretnych zasobów internetowych poprzez przeciążenie serwerów[106].

Cyberprzestępczość to nie tylko tradycyjne formy przestępstw, takie jak oszustwa czy kradzieże, ale także nowe rodzaje nielegalnych działań charakterystyczne dla świata cybernetycznego, takie jak ataki na kluczową infrastrukturę czy wykorzystanie botnetów do przeprowadzania ataków[107].

Warto również podkreślić, że cyberprzestępczość często wykazuje cechy transgraniczne, co sprawia, że jest szczególnie trudna do zwalczania i wymaga współpracy międzynarodowej w dziedzinie prawa[108].

2.3.2 Wykorzystanie SI i innych technologii w działaniach przestępczych

Technologie takie jak sztuczna inteligencja, pomimo swojego potencjału w przynoszeniu korzyści społeczeństwu, stwarzają również nowe wyzwania dla prawa karnego poprzez swoje wykorzystanie w działaniach przestępczych. Przestępcy korzystają z SI do automatyzacji i efektywnego skalowania swoich działań, takich jak ataki cybernetyczne, oszustwa czy szerzenie dezinformacji[109].

Przykładem może być zastosowanie tzw. „*głęboka mistyfikacja*" (ang. deepfake) - technologii opartej na sztucznej inteligencji, która umożliwia manipulowanie obrazem i dźwiękiem w celu tworzenia przekonujących fałszywych materiałów wideo lub audio[110]. Głębokie mistyfikacje mogą być wykorzystywane do oszustw, szantażu, a także do wprowadzania w błąd organów ścigania oraz sądów[111].

---

[106] Albanese J. S., *Transnational Crime and the 21st Century: Criminal Enterprise, Corruption, and Opportunity,* Oxford University Press 2011.

[107] Holt T. J., Bossler A. M., Seigfried-Spellar K. C., *Cybercrime and Digital Forensics: An Introduction*, Routledge 2014.

[108] Gercke M., *Understanding Cybercrime: A Guide for Developing Countries*, ITU 2012.

[109] Buchanan B., Grant T., *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*, IGI Global 2018.

[110] Chesney R., Citron D., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, "California Law Review" 2018, Vol. 107, s. 1753-1819.

[111] Westerlund M., *The Emergence of Deepfake Technology: A Review*, "Technology Innovation Management Review" 2020 Vol. 10, No. 11, s. 14-26.

Kolejnym przykładem jest wykorzystanie algorytmów do przeprowadzania zaawansowanych ataków cybernetycznych, które są bardziej złożone i trudniejsze do wykrycia dla standardowych systemów bezpieczeństwa[112].

Należy także zwrócić uwagę na korzystanie z technologii blockchain do przeprowadzania nielegalnych transakcji w sposób anonimowy, co stanowi trudność dla organów ścigania w zakresie śledzenia i identyfikacji osób popełniających przestępstwa[113].

2.3.3 Walka z cyberprzestępczością i jej wyzwania

Walka z przestępczością internetową staje się coraz trudniejsza wraz z postępem technologii i zdobywaniem przez przestępców nowych umiejętności[114]. Wyzwania, które stawiają przed sobą organy ścigania w kontekście cyberprzestępczości, są różnorodne i obejmują aspekty takie jak wykrywanie, ściganie oraz zapobieganie tego rodzaju działaniom[115].

Jednym z głównych wyzwań stanowi transgraniczny charakter cyberprzestępczości, co komplikuje ściganie winowajców ze względu na rozbieżności w przepisach prawnych poszczególnych państw oraz trudności z ekstradycją[116]. Dodatkowo, zachowanie anonimowości dzięki pewnym technologiom, takim jak sieci VPN czy technologia blockchain, sprawia trudności w identyfikacji sprawców[117].

Wyjątkowym wyzwaniem staje się dynamiczny postęp technologiczny, który zmusza do nieustannego dostosowywania i aktualizacji metod zwalczania cyberprzestępczości w odpowiedzi na zmieniające się warunki[118]. Wymaga to regularnego szkolenia personelu, inwestowania w nowoczesne narzędzia, a także promowania współpracy międzynarodowej i wymiany doświadczeń[119].

---

[112] Goodman M., Brenner S. W., *The Emerging Consensus on Criminal Conduct in Cyberspace*, International Journal of Law and Information Technology 2002, Vol. 10, No. 2, s. 135-223.
[113] Foley S., Karlsen J. R., Putniņš T. J., *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?*, "The Review of Financial Studies" 2019, Vol. 32, No. 5, s. 1798-1853.
[114] Wall D. S., *Cybercrime: The Transformation of Crime in the Information Age,* "Polity" 2007.
[115] Brenner S. W., *Cybercrime: Criminal Threats from Cyberspace*, "ABC-CLIO" 2010.
[116] Grabosky P., *Virtual Criminals: Old Wine in New Bottles?*, "Social & Legal Studies" 2001, Vol. 10, No. 2, s. 243-249.
[117] Tavani H. T., Grodzinsky F. S., *Cyberstalking, Personal Privacy, and Moral Responsibility*, "Ethics and Information Technology" 2002, Vol. 4, No. 2, s. 123-132.
[118] Goodman M., *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*, Doubleda, 2015.
[119] Choo K. K. R., *The Cyber Threat Landscape: Challenges and Future Research Directions*, "Computers & Security 2011", Vol. 30, No. 8, s. 719-731

2.4 Technologia jako obiekt ochrony prawa karnego

2.4.1 Przestępstwa przeciwko danym i systemom informatycznym

Przestępstwa popełniane przeciwko danym i systemom informatycznym są obecnie jednym z głównych problemów, z którymi boryka się współczesne prawo karnego[120]. W epoce cyfryzacji dane osobowe, poufne informacje firm i instytucji oraz kluczowa infrastruktura stają się coraz częstszym celem ataków cyberprzestępców[121].

Przestępstwa tego rodzaju przybierają różne postaci, takie jak włamania do systemów komputerowych, ataki ransomware oraz kradzież danych[122]. Warto zaznaczyć, że motywacje tych przestępstw mogą być różnorodne – od dążenia do zysku materialnego, poprzez chęć pozyskania informacji, aż po pobudki polityczne czy ideologiczne[123].

W kontekście prawa karnego, wyzwanie polega nie tylko na zidentyfikowaniu sprawców, ale także na właściwym ukaraniu ich działań, co często jest utrudnione przez brak spójnych regulacji prawnych na arenie międzynarodowej oraz ograniczenia jurysdykcyjne[124]. Dodatkowo, należy również brać pod uwagę aspekty prewencji, które mogą obejmować zarówno działania prawne, jak i techniczne środki zapobiegawcze[125].

2.4.2 Ochrona własności intelektualnej w erze cyfrowej

W epoce cyfrowej ochrona własności intelektualnej staje się coraz większym wyzwaniem, biorąc pod uwagę łatwość kopiowania i dystrybuowania treści cyfrowych[126]. Naruszenia praw autorskich, patenty oraz inne formy własności intelektualnej są powszechne w świecie online,

[120] Casey E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press 2011.
[121] Brenner S. W., *Cybercrime: Criminal Threats from Cyberspace*, "ABC-CLIO" 2010.
[122] Goodman M., *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*, Doubleday 2015.
[123] Wall D. S., *Cybercrime: The Transformation of Crime in the Information Age*, "Polity" 2007.
[124] Grabosky P., *Virtual Criminals: Old Wine in New Bottles?*, "Social & Legal Studies" 2001, Vol. 10, No. 2, s. 243-249.
[125] Choo K. K. R., *The Cyber Threat Landscape: Challenges and Future Research Directions*, "Computers & Security" 2011, Vol. 30, No. 8, s. 719-731
[126] Lessig L., *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, Penguin 2004.

często przybierając postać piractwa cyfrowego, nielegalnego udostępniania oprogramowania czy naruszania praw do baz danych[127].

W kontekście prawa karnego, ochrona własności intelektualnej w środowisku cyfrowym obejmuje zarówno aspekty prawne, jak i techniczne. Z jednej strony, istnieje potrzeba tworzenia i dostosowywania przepisów prawa, które skutecznie będą chronić prawa autorskie w dobie nowoczesnych technologii[128]. Z drugiej strony, istotne jest także rozwijanie oraz implementacja rozwiązań technicznych mających na celu zabezpieczenie treści, takich jak systemy zarządzania prawami cyfrowymi (DRM), czy narzędzia do wykrywania i zwalczania nielegalnego rozpowszechniania materiałów[129].

Ochrona własności intelektualnej w kontekście technologii cyfrowych nie jest jednak jednoznaczna i stawia wiele pytań dotyczących etyki oraz prawa, na przykład równowagi między prawami autorskimi a prawem do dostępu do kultury i wiedzy[130]. Dlatego też, konieczna jest analiza prawnicza i etyczna różnych aspektów ochrony własności intelektualnej w kontekście technologii cyfrowych, aby zrozumieć i skutecznie rozwiązać te złożone zagadnienia.

2.4.3 Zabezpieczenia prawne i technologiczne przed atakami cybernetycznymi

W obliczu rosnącej liczby incydentów związanych z bezpieczeństwem cybernetycznym, aspekty prawne i technologiczne odgrywają istotną rolę w zapewnieniu ochrony jednostek, firm oraz integralności systemów informacyjnych na arenie międzynarodowej[131]. Ataki tego rodzaju mogą przybierać różnorodne formy, jak na przykład ransomware, phishing czy ataki DDoS i mogą być wymierzone w różnorakie cele, obejmujące zarówno infrastrukturę kluczową, dane osobowe jak i poufne informacje handlowe[132].

Ramy prawne związane z bezpieczeństwem cybernetycznym różnią się na poziomie krajowym i międzynarodowym, ale ich głównym celem jest zapewnienie ochrony przed atakami

[127] Litman J., *Digital Copyright*, Prometheus Books 2001.
[128] Suter T., Hugenholtz P. B., *Copyright and Digital Rights Management, in Handbook on the Economics of Copyright: A Guide for Students and Teachers*, Edward Elgar Publishing 2005.
[129] Rosenblatt B., *Digital Rights Management: Business and Technology*, M&T Books 2005.
[130] Boyle J., *The Public Domain: Enclosing the Commons of the Mind*, Yale University Press 2008.
[131] Goodman M., *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It,* Doubleday 2015.
[132] Wall D. S., *Cybercrime: The Transformation of Crime in the Information Age*, "Polity" 2007.

internetowymi oraz określenie odpowiedzialności prawnej za naruszenia bezpieczeństwa danych[133]. W niektórych obszarach prawnych, takich jak Unia Europejska, istnieją przepisy wymagające od firm zgłaszania incydentów bezpieczeństwa oraz podejmowania konkretnych działań w celu zabezpieczenia danych[134].

Technologie zapewniające bezpieczeństwo, takie jak zapory sieciowe, programy antywirusowe i systemy wykrywania oraz zapobiegania intruzom, stanowią pierwszą linię obrony przed atakami cybernetycznymi[135]. Dodatkowo, metody takie jak szyfrowanie informacji oraz uwierzytelnianie wielopoziomowe są kluczowe dla ochrony danych i zapewnienia bezpieczeństwa transakcji internetowych[136].

Mimo obecności ram prawnych i dostępności zaawansowanych technologii, wciąż pojawiają się trudności, takie jak dynamicznie rozwijające się metody ataków, niewystarczająca świadomość cyberbezpieczeństwa wśród użytkowników oraz kwestie związane zabezpieczeniem Internetu Rzeczy (IoT)[137]. W związku z tym konieczne jest kontynuowanie badań i rozwoju w obszarze cyberbezpieczeństwa zarówno pod kątem prawnym, jak i technologicznym, aby skutecznie stawić czoła tym wyzwaniom.

2.5 Technologia jako narzędzie egzekwowania prawa karnego

2.5.1 Cyfrowe środki dowodowe i ich ważność w procesie karnym

W erze cyfrowej, gdzie dane są przechowywane i przesyłane za pomocą elektronicznych nośników, cyfrowe dowody stają się istotnym elementem postępowania karnego[138]. Wykorzystanie technologii w systemie sądowym otwiera nowe perspektywy, ale także niesie ze sobą wyzwania, które wymagają dogłębnej analizy i uregulowania prawnego.

Cyfrowe dowody obejmują różnorodne elementy, takie jak e-maile, logi serwerów, dane z dysków twardych czy informacje z mediów społecznościowych. Mogą one dostarczyć

[133] Brenner S. W., *Cybercrime: Criminal Threats from Cyberspace*, "ABC-CLIO" 2010.
[134] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informacyjnych w Unii, 2016 (Dz.U. L 194 z 19.7.2016).
[135] Stallings W., Brown L., *Computer Security: Principles and Practice*, Pearson, 2015.
[136] Pfleeger C. P., Pfleeger S. L., *Security in Computing*, Prentice Hall 2006.
[137] Weber R. H., *Internet of Things – New security and privacy challenges*, "Computer Law & Security Review" 2010, Vol. 26, No. 1, s. 23-30.
[138] Casey E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press 2011.

istotnych informacji w sprawach karnych[139]. Wartość tych dowodów jest często kluczowa dla wyjaśnienia sprawy, jednak konieczne jest zachowanie ich autentyczności i integralności przez cały proces sądowy.

Ważność elektronicznych dowodów często staje się tematem sporów sądowych, w których strony mogą podważać ich autentyczność, integralność oraz sposób pozyskania[140]. Dlatego ważne jest, aby proces pozyskiwania, przechowywania i prezentowania dowodów elektronicznych był zgodny z obowiązującymi przepisami i standardami[141].

Wprowadzenie elektronicznych dowodów do postępowania karnego stwarza pewne trudności. Sprawy związane z prywatnością, dostępem do danych oraz technicznymi aspektami analizy dowodów stawiają przed sądami i praktykami prawnymi nowe pytania oraz wyzwania etyczne[142].

Z uwagi na dynamiczny postęp technologiczny, system prawa karnego i procesowego będzie musiał dostosować się do nowych form dowodów oraz metod ich analizy. Badania nad bezpieczeństwem cyfrowych dowodów oraz rozwój technologii zapewniających ich autentyczność i integralność stanowią kluczowe elementy dla przyszłości egzekwowania prawa karnego w świecie cyfrowym[143].

2.5.2 Wykorzystanie technologii do ścigania przestępstw

Technologia, zwłaszcza w obszarze informatyki śledczej i analizy danych, jest teraz nieodłączną częścią dzisiejszych metod zwalczania przestępczości[144]. W obliczu wzrostu liczby przestępstw cyfrowych i wykorzystania technologii w tradycyjnej przestępczości, narzędzia technologiczne odgrywają kluczową rolę w identyfikacji, analizie i reagowaniu na zagrożenia kryminalne.

Informatyka śledcza, czyli wykorzystanie metod i technik informatycznych do zbierania dowodów, jest kluczowym narzędziem w zwalczaniu przestępczości internetowej oraz

[139] Volonino L., Anzaldua R., Godwin J., *Computer Forensics: Principles and Practices*, Pearson 2014.
[140] Kerr, O. S., *Search Warrants in an Era of Digital Evidence*, "Mississippi Law Journal" 2005, No 75, s. 85-123.
[141] Kołecki H., *Dowody elektroniczne - przepisy i standardy*, "Prokuratura i Prawo" 2013, nr 6, s. 177.
[142] Brenner, S. W., *Law in an Era of "Smart" Technology*, Oxford University Press 2007.
[143] Goodison, S. E., Davis, R. C., & Jackson, B. A., *Digital Evidence and the U.S. Criminal Justice System,* RAND Corporation 2015.
[144] Casey E*., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press 2011.

w analizie materiałów cyfrowych[145]. Wprowadzenie technologii do procedury dochodzeniowej umożliwia skuteczne i dokładne przetwarzanie danych, które mogą mieć kluczowe znaczenie dla sprawy.

Technologie analizy danych, takie jak algorytmy uczenia maszynowego, czy sztuczna inteligencja, są używane do wykrywania wzorców zachowań przestępczych i przewidywania potencjalnych zagrożeń[146]. Takie systemy mogą pomóc organom ścigania w alokacji zasobów i zapobieganiu przestępczości.

Technologia pomaga także w codziennej pracy funkcjonariuszy poprzez dostarczanie narzędzi takich jak systemy identyfikacji twarzy, drony czy technologie biometryczne, które znajdują zastosowanie w różnych obszarach działań policyjnych[147].

Wprowadzenie technologii do ścigania przestępstw wiąże się z szeregiem trudności, takich jak zagadnienia związane z prywatnością, etyką oraz potencjalnymi błędami algorytmicznymi, które mogą wpłynąć na proces podejmowania decyzji w obszarze prawa karnego[148].

2.5.3 Etyczne i prawne wyzwania związane z użyciem technologii przez organy ścigania

Wprowadzenie technologii do dziedziny prawnej i śledczej, chociaż niewątpliwie przynosi wiele zalet, stwarza również szereg problemów etycznych i prawnych[149]. W szczególności w kontekście prawa karnego, gdzie często na szali znajduje się wolność jednostki, te wyzwania stają się szczególnie istotne. Jak obserwuje się w literaturze przedmiotu można wyróżbnić następujące wyzwania etyczne i prawne związane z użyciem technologii przez organy ścigania:

1. prywatność i nadzór

   Wdrożenie technologii, takich jak systemy identyfikacji twarzy czy analizy danych, przez organy ścigania stawia przed nimi istotne dylematy związane z prywatnością

[145] Volonino L., Anzaldua R., Godwin J., *Computer Forensics: Principles and Practices*, Pearson 2014.
[146] Perry W. L., McInnis B., Price C. C., Smith S. C., Hollywood J. S., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation 2013.
[147] Taylor E., Lee M., Willis M., Gannoni A., *Real-time monitoring of offenders: The high-tech future of crime prevention?*, "Trends & Issues in Crime and Criminal Justice" 2017, No. 532, s. 1-16.
[148] Ferguson A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, NYU Press 2017.
[149] Lyon D., *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination*, Routledge 2003.

i nadzorem[150]. Znalezienie równowagi między zapewnieniem bezpieczeństwa a poszanowaniem praw obywatelskich stanowi kluczowe wyzwanie.

2. błędy i „*bias*" w technologii

   Technologie, takie jak prognozy algorytmiczne czy sztuczna inteligencja, mogą zawierać niedoskonałości lub uprzedzenia (*bias*[151]), które mają potencjał wpływać na procesy podejmowania decyzji w obszarze prawa karnego.[152].

3. dostęp do dowodów cyfrowych

   Dostęp do informacji cyfrowych, na przykład danych przechowywanych na serwerach za granicą, stanowi także trudność z punktu widzenia przestrzegania jurysdykcji i norm międzynarodowych[153].

4. Etyka i odpowiedzialność

   Kwestie moralne, takie jak jasność i odpowiedzialność za decyzje podejmowane przez algorytmy, również stwarzają znaczące wyzwanie, szczególnie w kontekście decyzji dotyczących przestępstw[154].

2.6 Perspektywy i wyzwania przyszłości

Przyszłość prawa karnego w obliczu postępujących innowacji technologicznych, takich jak rozwój sztucznej inteligencji, otwiera przed nami zarówno obiecujące możliwości, jak i istotne wyzwania. Możemy przewidywać, że technologia będzie rozwijać się coraz bardziej, co może skutkować pojawieniem się nowych form przestępstw, takich jak zaawansowane oszustwa

[150] Brkan M., Psychogiopoulou E., The Future of Privacy Certification in Europe: An Exploration of the GDPR Provisions on Criteria and Procedures for Certification, European Journal of Law and Technology 2018, Vol. 9, No. 1.

[151] Bias to systematyczne odchylenie od normy lub rzeczywistości, które prowadzi do błędnych wniosków, ocen lub decyzji. W kontekście sztucznej inteligencji, bias może prowadzić do dyskryminacji pewnych grup społecznych lub utrwalania stereotypów. Przykładowo, algorytmy uczenia maszynowego mogą wykazywać tendencyjność, jeśli są trenowane na niezrównoważonych lub niereprezentacyjnych danych. Dlatego ważne jest, aby dążyć do minimalizacji biasu w systemach SI poprzez odpowiednie projektowanie, testowanie i monitorowanie modeli. Zob. Mehrabi N., Morstatter F., Saxena N., Lerman K., Galstyan A., *A Survey on Bias and Fairness in Machine Learning*, "ACM Computing Surveys" 2021, vol. 54, no. 6, s. 1-2.

[152] O'Neil C., Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, 2016.

[153] Svantesson D. J. B., Clarke R., *Privacy and consumer risks in cloud computing*, "Computer Law & Security Review" 2010, Vol. 26, No. 4, s. 391-397.

[154] Mittelstadt B., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, "Big Data & Society" 2016.

internetowe, manipulacja danymi czy nawet działania szkodliwe podejmowane autonomicznie i nieprzypisywalne bezpośrednio żadnej konkretnej osobie fizycznej.

Wyzwanie tkwi w utrzymaniu równowagi między promowaniem innowacji a zapewnieniem bezpieczeństwa społecznego oraz ochroną praw jednostki. Prawo karne będzie musiało opracować nowe strategie regulacyjne, które będą skutecznie reagować na zagrożenia związane z nadużyciami technologii sztucznej inteligencji i zapewnić odpowiedzialność za takie działania[155].

Kolejnym ważnym zagadnieniem jest konieczność zapewnienia ochrony praw cyfrowych obywateli w obliczu coraz większej roli sztucznej inteligencji w naszym codziennym życiu. Dotyczy to zarówno kwestii prywatności, jak i nowych wyzwań związanych z prawem do „*cyfrowego spokoju*", czy „*cyfrowej autonomii*"[156].

Ponadto, postęp sztucznej inteligencji rodzi pytanie o rolę i pozycję człowieka w ramach systemu prawnego? W jaki sposób technologia wpłynie na pracę prawników, sędziów oraz organów ścigania? Czy sztuczna inteligencja będzie wspierać procesy podejmowania decyzji, czy może zastąpi ludzi w pewnych funkcjach[157]?

2.6.1 Prognozy rozwoju technologii i potencjalne implikacje dla prawa karnego

Wraz z postępem technologii sztucznej inteligencji i jej coraz powszechniejszym zastosowaniem, prognozowane jest, że będzie ona miała coraz większe znaczenie dla różnych obszarów społeczeństwa, w tym także prawa karnego. W nadchodzących latach możemy przewidzieć:

Automatyzację procesówów sądowych - postęp w dziedzinie sztucznej inteligencji może przyczynić się do większej automatyzacji zbierania dowodów, analizy dokumentów oraz nawet procesów wydawania wyroków. Chociaż może to podnieść efektywność i zmniejszyć

[155] Hallevy Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, "Journal of Criminal Law and Criminology" 2011, Vol. 101, No. 2.
[156] Lynskey O., *The Foundations of EU Data Protection Law*, Oxford University Press 2017.
[157] Susskind R., Susskind D., *The Future of the Professions: How Technology Will Transform the Work of Human Experts*, Oxford University Press 2015.

obciążenie systemów sądowych, rodzi to też wątpliwości dotyczące przejrzystości i uczciwości procedur prawnych.

Zmianę paradygmatu odpowiedzialności - tradycyjne zasady odpowiedzialności karnej mogą potrzebować przewartościowania w kontekście decyzji podejmowanych przez maszyny. W szczególności, trzeba będzie rozważyć, w jaki sposób zastosować obecne definicje intencji, winy i niedbalstwa do działalności sztucznej inteligencji.

Rozwój cyberprzestępczości - wraz z postępem technologicznym należy spodziewać się wzrostu zaawansowania i subtelności cyberprzestępczości. Prawo karne będzie musiało sprostać nowym formom ataków, takich jak zaawansowane oszustwa algorytmiczne, manipulowanie danymi czy tworzenie i wykorzystywanie sztucznych identyfikatorów.

Prawa i ochrona osobowa maszyn – w miarę postępu technologicznego należy spodziewać się bardziej złożonych i subtelnych form cyberprzestępczości. System prawny będzie musiał odpowiedzieć na nowe metody ataków, takie jak zaawansowane oszustwa algorytmiczne, manipulacja danymi czy tworzenie oraz wykorzystywanie sztucznych tożsamości.

Etyczne i prawne ramy dla SI - aby odpowiedzieć na dylematy etyczne związane z sztuczną inteligencją, konieczne będzie ustanowienie i wdrożenie międzynarodowych ram regulacyjnych, które będą nadzorować projektowanie, rozwój i wykorzystanie systemów SI, aby zapewnić ich zgodność z humanistycznymi wartościami i społecznymi normami.

2.6.2 Adaptacja prawa karnego do nowych technologii

Wprowadzenie zmian w systemie prawnym w odpowiedzi na postęp technologiczny powinno skupić się na kilku istotnych kwestiach:

1. aktualizacji definicji przestępstwa - dostosowanie opisów obecnie istniejących przestępstw w taki sposób, aby uwzględniały działania podejmowane przez sztuczną inteligencję. Na przykład, można rozważyć wprowadzenie terminu „*przemoc cybernetyczna*” jako nowej kategorii przestępstw związanych z wykorzystaniem SI;

2. ustanowieniu nowych kategorii odpowiedzialności - wprowadzenie nowych kategorii odpowiedzialności prawnej, które bardziej adekwatnie odzwierciedlą złożoność i naturę działań podejmowanych przez systemy sztucznej inteligencji;

3. prawnych ramach dla autonomicznych systemów - utworzenie ram prawnych dla autonomicznych systemów, które będą regulować sposób kontroli i audytu sztucznej inteligencji, a także określą wymagane standardy etyczne i techniczne;

4. zasadach wprowadzania SI do praktyki prawnej - przygotowanie wytycznych dotyczących wdrożenia sztucznej inteligencji w praktyce prawniczej, w tym w systemach wymiaru sprawiedliwości, uwzględniając potencjalne dylematy etyczne i prawne;

5. rozwoju procedur ścigania cyberprzestępczości - rozwijanie procedur zwalczania cyberprzestępczości, podnoszenie kwalifikacji organów ścigania w dziedzinie technologii informatycznych oraz wzmacnianie współpracy międzynarodowej w tej sferze;

6. edukacji i świadomości prawnej - inwestowanie w rozwój edukacji i podnoszenie świadomości prawnej społeczeństwa w obszarze nowoczesnych technologii ma na celu lepsze przygotowanie obywateli do identyfikowania i reagowania na zagrożenia związane z sztuczną inteligencją;

7. współpracy międzysektorowej - zachęcanie do współpracy między przedstawicielami prawa, technologii i etyki w celu opracowania spójnych i zharmonizowanych rozwiązań prawnych dla wyzwań związanych z sztuczną inteligencją.

Propozycje te powinny być przedmiotem dogłębnej dyskusji i konsultacji, zarówno na arenie krajowej, jak i międzynarodowej, aby zagwarantować dostosowanie prawa karnego do nowych technologii w sposób staranny i zrównoważony.

2.6.3 Znaczenie badań interdyscyplinarnych i współpracy międzynarodowej

W obliczu dynamicznego rozwoju technologii i jej coraz większego wpływu na różne dziedziny życia, w tym na sferę prawa karnego, niezwykle istotne staje się prowadzenie badań interdyscyplinarnych oraz zacieśnianie współpracy międzynarodowej. Złożoność i wieloaspektowość wyzwań, jakie stawia przed nami postęp technologiczny, wymaga zaangażowania specjalistów z różnych dziedzin oraz wymiany doświadczeń i wiedzy ponad granicami państw.

Badania interdyscyplinarne, łączące w sobie perspektywy nauk prawnych, informatycznych, socjologicznych, psychologicznych czy etycznych, pozwalają na pełniejsze zrozumienie

zjawisk znajdujących się na styku prawa i technologii[158]. Taka wielowymiarowa analiza umożliwia identyfikację potencjalnych zagrożeń, wypracowanie skutecznych rozwiązań i sformułowanie rekomendacji uwzględniających różne aspekty problemu[159]. Współpraca międzynarodowa z kolei, w dobie globalizacji i transgranicznego charakteru wielu przestępstw związanych z technologią, staje się nieodzowna dla efektywnego ścigania sprawców i zapewnienia bezpieczeństwa obywatelom[160].

Dostrzegając fundamentalne znaczenie badań interdyscyplinarnych i współpracy międzynarodowej dla kształtowania przyszłości prawa karnego w kontekście rozwoju technologii, w niniejszym punkcie należy zauważyć, że mają one znaczenie dla:

Badania interdyscyplinarne i współpraca międzynarodowa moją fundamentalne znaczenie dla:

1. budowania zrozumienia, bowiem interdyscyplinarność badań umożliwia połączenie kompetencji z dziedziny informatyki, prawa, etyki oraz socjologii w celu lepszego zrozumienia wpływu sztucznej inteligencji na społeczeństwo oraz sposobów, w jakie system prawny może adekwatnie reagować na te zmiany;

2. tworzenia zintegrowanych rozwiązań, bowiem praca badaczy z różnych dziedzin jest korzystna dla opracowywania kompleksowych rozwiązań prawnych, które biorą pod uwagę zarówno techniczne funkcje sztucznej inteligencji, jak i społeczne oraz etyczne skutki jej wykorzystania;

3. standardów międzynarodowych, bowiem współpraca międzynarodowa odgrywa kluczową rolę w ustanawianiu norm dotyczących sztucznej inteligencji, które będą powszechnie akceptowane na całym świecie. Dzięki niej możliwe jest stworzenie spójnych ram prawnych i zapobieżenie „*wyścigowi na dno*" w zakresie regulacji;

4. zapobiegania konfliktom prawnym, bowiem międzynarodowe umowy i konwencje mogą przyczynić się do uniknięcia sporów prawnych i jurysdykcyjnych, które mogą wynikać

[158] Chynoweth P., *Legal research in the built environment: a methodological framework*, "International Journal of Law in the Built Environment" 2009, vol. 1, no. 1, s. 30.
[159] Brownsword R., Scotford E., Yeung K. (eds.), *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press 2017, s. 6-7.
[160] Grabosky P., *Cybercrime*, "Oxford Handbook of Crime and Public Policy" 2011, Oxford University Press, s. 472-473.

z transgranicznego charakteru funkcjonowania systemów sztucznej inteligencji i cyfrowych;

5. wymiany doświadczeń, bowiem wymiana informacji między różnymi krajami pomaga lepiej zrozumieć potencjalne trudności i skuteczniej się nimi zająć, uwzględniając różnorodność kontekstów społecznych i prawnych;

6. rozwoju praw człowieka, bowiem współpraca pomiędzy krajami przyczynia się do rozwoju i aktualizacji międzynarodowych standardów dotyczących praw człowieka w erze technologicznej, co jest kluczowe w obliczu rosnących wyzwań, jakie niesie za sobą sztuczna inteligencja.

Rozdział III. Prawnokarne aspekty sztucznej inteligencji

W poprzednim podrozdziale wywiedziono, że rozwój sztucznej inteligencji stanowi jedno z najważniejszych osiągnięć dzisiejszej technologii, niosąc zarówno ogromne możliwości, jak i wyzwania dla legislacji na całym globie. W obszarze prawa karnego, technologie SI rzucają nowe światło głównie na zagadnienia takie jak: kwalifikacja prawna, sprawstwo oraz odpowiedzialność twórców i operatorów tych systemów. Zrozumienie i właściwe rozwiązanie tych problemów wymaga dogłębnej analizy oraz być może przedefiniowania pewnych podstawowych zasad prawa karnego.

Dla prawa karnego, które tradycyjnie skupia się na ludzkich czynach i winie, społecznej szkodliwości czynu, bezprawności i karalności, pojawienie się procesu podejmowania przez maszyny korzystające z SI stawia pytania o przypisanie odpowiedzialności: czy twórca systemu SI powinien ponosić konsekwencje karnoprawne za nieprzewidziane skutki zachowania jego dzieła? Jak należy traktować sytuacje z udziałem sztucznej inteligencji prowadzące do naruszeń prawa lub nawet czynów przestępnych?

Te pytania nabierają szczególnego znaczenia w obliczu zdolności SI do samodzielnego uczenia się i podejmowania decyzji bez bezpośredniego nadzoru człowieka. Staje się oczywiste, że tradycyjne podejścia do legislacji mogą okazać się niewystarczające do regulowania działań i skutków generowanych przez te zaawansowane systemy. W rezultacie przed naukowcami prawa, ustawodawcami oraz społecznością międzynarodową staje zadanie zrozumienia tych nowych technologii i dostosowania ram prawnych w sposób zapewniający ochronę jednostek i społeczeństwa przy jednoczesnym wspieraniu innowacji technologicznej.

3.1 Wprowadzenie do prawnych wyzwań stawianych przez SI

3.1.1 Definicja i zakres sztucznej inteligencji w kontekście prawnokarnym.

Sztuczna inteligencja, pomimo iż to pojęcie nie jest nowe, ciągle się rozwija i staje coraz ważniejsza w różnych obszarach życia społecznego, gospodarczego, a teraz także prawnego. W kontekście prawa, definicja oraz zakres sztucznej inteligencji wymagają szczególnego podejścia ze względu na specyficzne wyzwania, które stawia przed systemem prawnym.

Sztuczna inteligencja to umiejętność maszyn do wykonywania zadań, które wymagają ludzkiej inteligencji, takie jak: rozumowanie, uczenie się, percepcja i interakcja językowa[161]. Ta obszerna definicja obejmuje zarówno proste algorytmy, jak i zaawansowane systemy zdolne do samodzielnego uczenia się i adaptacji, co znacząco utrudnia kwestie prawne dotyczące odpowiedzialności za działania SI.

W kontekście prawnym, obszar sztucznej inteligencji podlegający regulacji obejmuje systemy autonomiczne i półautonomiczne, które są zdolne do podejmowania decyzji bez bezpośredniej ingerencji ludzkiej. Pytania dotyczące odpowiedzialności za działania podejmowane przez SI, zwłaszcza gdy prowadzą one do naruszeń zakazanych przez prawo, wynikają z ich zdolności do samodzielnego działania[162].

Próba uregulowania znaczenia i miejsca stosowania sztucznej inteligencji w prawie karnym wymaga dokładnego określenia samej technologii oraz zrozumienia sposobów jej wykorzystania i potencjalnych zagrożeń z nią związanych. Istotne jest także rozróżnienie między różnymi poziomami autonomii sztucznej inteligencji, co ma istotne konsekwencje dla przypisywania odpowiedzialności prawnej[163].

Analizując definicję i zakres sztucznej inteligencji w kontekście prawnym, nie można pominąć szybkiego postępu technologicznego i jego wpływu na przyszłe kształtowanie się prawa. Dla prawników i ustawodawców stanowi to wyzwanie nie tylko w dostosowaniu obecnych regulacji, ale także w przewidywaniu rozwoju technologii SI oraz ich potencjalnego znaczenia dla przypisania konsekwencji prawnych[164].

3.1.2 Przegląd aktualnych dyskusji na temat regulacji SI.

W ostatnich latach rozwój technologii opartych na sztucznej inteligencji przyniósł znaczące postępy w różnych dziedzinach życia, ale jednocześnie generuje nowe wyzwania prawne, zwłaszcza w kontekście prawa karnego. Szybkie wprowadzanie SI w obszary takie jak medycyna, transport, finanse i bezpieczeństwo publiczne budzą pytania dotyczące legalności

[161] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[162] Scherer M. U., *Regulating Artificial Intelligence Systems: Risks, Challenges*, *Competencies, and Strategies*, "Harvard Journal of Law & Technology" 2016, Vol. 29, No. 2, s. 353-400.
[163] Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.
[164] Casey B., *Rethinking the Boundaries of Law in the Age of SI*, "Columbia Law Review" 2019, Vol. 119, s. 1743-1782.

działań podejmowanych przez systemy SI, identyfikacji winnych za ich działania oraz karalności osób odpowiedzialnych za rozwój i implementację tych technologii.

Analiza obecnych debat na temat regulacji SI podkreśla skomplikowaną naturę zagadnień prawnych związanych z dynamicznym rozwojem technologicznym. Uczestnicy dyskusji koncentrują się na kilku kluczowych obszarach problemowych tj.:

1. kwalifikacja prawna działań SI - w powszechnym rozumieniu prawa karnego przyjmuje się, że za zachowanie prowadzące do złamania norm prawnych ponosi odpowiedzialność człowiek. Natomiast sztuczna inteligencja, działając na podstawie algorytmów i uczenia maszynowego, może doprowadzić do skutków prawnych trudnych do przypisania konkretnej osobie;

2. Przypisanie sprawstwa – kwestia odpowiedzialności za działania sztucznej inteligencji jest tematem gorącej debaty. Rozważane są różne podejścia, począwszy od przypisywania winy ludziom (osobom fizycznym) tj. twórcom, operatorom, aż po koncepcje prawno-filozoficzne rozszerzające pojęcie podmiotowości na niehumanoidalne istoty, takie jak zaawansowane systemy SI;

3. odpowiedzialność twórców i operatorów SI - pytania dotyczące odpowiedzialności za szkody powstałe w wyniku działań systemów SI stawiane są w kontekście zakresu odpowiedzialności ich twórców i operatorów. Dyskusja skupia się na sposobach ustanowienia ram prawnych umożliwiających skuteczne określenie odpowiedzialności, przy jednoczesnym zachowaniu swobody dla innowacji technologicznych.

Rozmowa ta ma miejsce na różnych platformach - od środowisk akademickich, przez sektor technologiczny, aż po organy ustawodawcze i międzynarodowe organizacje, takie jak Unia Europejska, która aktywnie pracuje nad opracowaniem regulacji dotyczących sztucznej inteligencji, co jest widoczne w proponowanych aktach prawnych, jak na przykład rozporządzenie dotyczące sztucznej inteligencji (AI Act).[165].

Podczas analizy literatury przedmiotu związanej z tematem warto skupić się na tekstach autorstwa Russell'a i Norviga, którzy w swojej kluczowej pracy „*Sztuczna inteligencja:*

[165] Komisja Europejska, 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, COM(2021) 206 final, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (dostęp: 10.06.2024 r.).

Nowoczesne podejście"[166] poruszają kwestie etyczne i prawne związane z sztuczną inteligencją. Również prace Franka Pasquale oraz jego analiza „*Społeczeństwo Czarnych Skrzynek*"[167] akcentują istotne zagadnienia dotyczące odpowiedzialności i przejrzystości funkcjonowania algorytmów.

Zapoznanie się z wyzwaniami prawnymi związanymi z SI jest kluczowym elementem analizy prawnokarnych aspektów technologii SI, podkreślając konieczność ciągłego dostosowywania regulacji prawnych do szybko rozwijających się technologii oraz znaczenie interdyscyplinarnego podejścia, które integruje wiedzę prawniczą, etyczną i technologiczną.

3.2 Regulacje międzynarodowe i krajowe dotyczące SI

3.2.1 Regulacje międzynarodowe SI

W odpowiedzi na rosnące zainteresowanie i wdrożenie technologii sztucznej inteligencji na całym świecie, pojawia się konieczność opracowania spójnych regulacji prawnych, które będą w stanie sprostać wyzwaniom związanym z odpowiedzialnością prawną, etyką i bezpieczeństwem. Międzynarodowe przepisy odgrywają tutaj istotną rolę, stanowiąc podstawę dla krajowych ustaw oraz wytyczając kierunki dla globalnych standardów postępowania z SI. W tej części zostaną omówione kluczowe inicjatywy międzynarodowe dotyczące regulacji SI, ze szczególnym uwzględnieniem ich wpływu na prawo karne:

1. Inicjatywy Organizacji Narodów Zjednoczonych (ONZ) - Narody Zjednoczone za pośrednictwem swoich agend, takich jak UNESCO, aktywnie uczestniczą w opracowywaniu zasad etycznych i regulacyjnych dotyczących sztucznej inteligencji. Przykładem jest „*Zalecenie dotyczące etyki SI*", które ma na celu promowanie zrównoważonego rozwoju i ochronę praw człowieka w kontekście rosnącego wykorzystania SI[168];

[166] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[167] Pasquale F., *The Black Box Society*, Harvard University Press 2015.
[168] UNESCO, *Rekomendacja w sprawie etyki sztucznej inteligencji*, https://unesdoc.unesco.org/ark:/48223/pf0000373434 (dostęp: 10.06.2024 r.).

2. Deklaracja G7 o SI - kraje należące do Grupy G7 przyjęły oświadczenie dotyczące stosowania sztucznej inteligencji, podkreślając konieczność międzynarodowej współpracy w badaniu wpływu SI na społeczeństwo, włączając w to kwestie prawne i etyczne[169];

3. Zasady OECD dotyczące SI - Organizacja Współpracy Gospodarczej i Rozwoju (OECD) stworzyła zestaw zasad służących jako fundament dla rozwoju i wykorzystania Sztucznej Inteligencji przez instytucje rządowe i firmy. Zasady te skupiają się na transparentności, bezpieczeństwie oraz odpowiedzialności, a także na poszanowaniu praw człowieka oraz demokratycznych wartości[170];

4. Europejski Akt o SI - Unia Europejska stoi na czele regulacji sztucznej inteligencji na arenie międzynarodowej, wprowadzając kompleksowy zbiór przepisów mających na celu kontrolę ryzyka związanego z różnymi zastosowaniami SI. Akt dotyczący SI skupia się szczególnie na klasyfikacji systemów SI według poziomu ryzyka, nakładając surowsze wymagania na systemy uznane za „*wysokiego ryzyka*”[171].

Analiza tych inicjatyw pokazuje, w jaki sposób różnorodne podejścia i działania na scenie międzynarodowej wpływają na regulacje prawne dotyczące sztucznej inteligencji, stawiając przed twórcami, użytkownikami i regulatorami nowe wyzwania i pytania. W kontekście prawa karnego, międzynarodowe przepisy dotyczące SI mają za zadanie nie tylko ochronę społeczeństwa przed potencjalnymi naruszeniami prawa, ale także zapewnienie, że rozwój technologii będzie się odbywał w sposób etyczny i odpowiedzialny, z poszanowaniem podstawowych praw i wolności.

3.2.2 Regulacje krajowe SI

Polska wprowadziła „*Strategię Rozwoju Sztucznej Inteligencji w Polsce od 2020 roku*”, która ma na celu pomóc społeczeństwu, przedsiębiorstwom, środowiskom naukowym i administracji

[169] *G7 Leaders' Statement on the Hiroshima AI Process, The White House, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/(dostęp: 10.06.2024 r.)*.

[170] OECD, *OECD AI Principles overview*, https://oecd.ai/en/ai-principles (dostęp: 10.06.2024 r.).

[171] Komisja Europejska, 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, COM(2021) 206 final, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (dostęp: 10.06.2024 r.).

publicznej w korzystaniu z potencjału rozwoju SI, przy jednoczesnym zapewnieniu ochrony praw człowieka i zachowaniu uczciwej konkurencji[172].

Ta strategia zakłada przeprowadzenie różnorodnych działań mających na celu wspieranie rozwoju sztucznej inteligencji w Polsce, takich jak:

- zwiększenie znaczenia Polski jako jednego z beneficjentów gospodarki opartej na analizie danych,
- pomoc polskim firmom zajmującym się sztuczną inteligencją poprzez stworzenie sposobów finansowania ich rozwoju oraz zachęcanie do współpracy startupów z rządem,
- wsparcie polskiego środowiska naukowego i badawczego w obszarze sztucznej inteligencji, między innymi poprzez utworzenie katedr SI oraz przyznawanie grantów dla naukowców,
- inicjatywy edukacyjne mające na celu podniesienie umiejętności cyfrowych społeczeństwa,
- międzynarodowa współpraca w dziedzinie rozwoju i promocji polskiej technologii sztucznej inteligencji,
- implementacja SI w sektorze publicznym w celu usprawnienia działania administracji oraz ułatwienia dostępu do danych publicznych.

„*Polityka dotycząca rozwoju sztucznej inteligencji w Polsce od 2020 roku*" reprezentuje ważny krok w kierunku uregulowań prawnych związanych z sztuczną inteligencją na poziomie krajowym, wpisując się w szersze regulacje europejskie i międzynarodowe. Dokument ten przyczynia się do przygotowania rozwiązań prawnych w Polsce, szczególnie poprzez określenie głównych działań mających na celu wsparcie rozwoju i stosowania technologii SI w sposób zrównoważony i etyczny. Dokument zwraca szczególną uwagę na:

1. wpływ na świadomość i edukację społeczeństwa

[172]Rada Ministrów RP, Polityka rozwoju SI w Polsce przyjęta przez Radę Ministrów – co dalej?, Portal Gov.pl, *https://www.gov.pl/web/govtech/polityka-rozwoju-ai-w-polsce-przyjeta-przez-rade-ministrow--co-dalej* (dostęp: 10.06.2024 r.).

Jednym z kluczowych elementów tego podejścia jest zwiększenie świadomości społecznej na temat sztucznej inteligencji oraz związanych z nią kwestii etycznych, prawnych i technologicznych. Inicjatywy edukacyjne i informacyjne promowane w ramach tej polityki, mają na celu przygotowanie społeczeństwa do korzystania z SI, zrozumienie potencjalnych zagrożeń oraz sposobów ich minimalizacji.

2. wsparcie dla innowacyjnych firm i startupów

   Polityka stawia duży nacisk na pomoc dla krajowych firm i startupów rozwijających sztuczną inteligencję poprzez wprowadzanie różnych form wsparcia, w tym finansowania, regulacyjnych platform do testowania oraz innych form pomocy. Dzięki temu tworzone są warunki sprzyjające rozwojowi innowacyjnych rozwiązań, które są zgodne z obowiązującymi przepisami prawnymi i jednocześnie podnoszą konkurencyjność Polski na światowym rynku technologii opartych na sztucznej inteligencji.

3. Współpraca międzynarodowa i dostosowanie do standardów

   Polityka podkreśla ważność współpracy międzynarodowej i dostosowania się do europejskich oraz globalnych norm w dziedzinie regulacji sztucznej inteligencji. Te działania mają na celu promowanie polskich przedsiębiorstw związanych z sztuczną inteligencją za granicą, a także zapewnienie, że polskie przepisy i standardy będą zgodne z międzynarodowymi wymaganiami, co jest kluczowe dla ułatwienia transgranicznego handlu i współpracy w obszarze sztucznej inteligencji.

4. Rozwój nauki i badań nad SI

   Poprzez wsparcie środowiska naukowego i badawczego w Polsce w obszarze sztucznej inteligencji, polityka przyczynia się do rozwoju bezpiecznych, etycznych i efektywnych technologii SI. Inwestycje w badania i rozwój, przyznawanie grantów badaczom oraz współpraca między uczelniami a biznesem sprzyjają tworzeniu innowacyjnych rozwiązań, które mogą być następnie wdrożone zgodnie z obowiązującymi przepisami prawnymi.

5. Znaczenie dla regulacji prawnych

   „*Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*” odgrywa istotną rolę w kształtowaniu przyszłych uregulowań prawnych związanych z SI w Polsce. Poprzez ustalenie priorytetów i kierunków działań, stanowi podstawę dla tworzenia konkretnych

przepisów prawnych, które będą regulować rozwój i stosowanie SI. Dodatkowo, wspomaga publiczną dyskusję na temat potrzeb regulacyjnych w tym dynamicznie rozwijającym się obszarze.

Wprowadzenie tej strategii jest ważnym krokiem w budowaniu wszechstronnego i spójnego systemu prawnego dotyczącego sztucznej inteligencji w Polsce, co ma kluczowe znaczenie dla zapewnienia, że rozwój i wykorzystanie SI będą odbywać się w sposób zrównoważony, etyczny i zgodny z przepisami prawa.

Polska, podobnie jak inne kraje członkowskie Unii Europejskiej, musi dostosować swoje przepisy krajowe do wymagań unijnych, zwłaszcza w obszarze regulacji dotyczących sztucznej inteligencji. To dostosowanie jest konieczne ze względu na pierwszeństwo prawa unijnego nad krajowym oraz potrzebę spójnego stosowania przepisów we wszystkich państwach członkowskich. Proces ten obejmuje zarówno rewizję istniejących przepisów, jak i wprowadzenie nowych regulacji zgodnych z normami unijnymi.

Europejski akt dotyczący sztucznej inteligencji, podobnie jak wcześniejsze Rozporządzenie Ogólne o Ochronie Danych (RODO), nakłada na państwa członkowskie obowiązek podjęcia działań legislacyjnych w celu zapewnienia pełnej zgodności z jego postanowieniami. Oznacza to, że Polska jest zobowiązana do przeprowadzenia analizy obecnych przepisów prawnych i praktyk regulacyjnych oraz wprowadzenia ewentualnych zmian lub uzupełnień, aby dostosować krajowe regulacje do standardów i wymogów określonych na poziomie unijnym.

Dopasowanie polskiego prawa do europejskiego aktu dotyczącego sztucznej inteligencji będzie kluczowe dla zapewnienia, że rozwój i implementacja technologii SI w Polsce będzie odbywać się w sposób bezpieczny, zgodny z zasadami etycznymi oraz respektującymi podstawowe prawa i wolności obywatelskie. Proces ten może obejmować także wprowadzenie konkretnych mechanizmów nadzoru, procedur oceny zgodności oraz systemów rekompensat i odpowiedzialności za ewentualne szkody spowodowane przez systemy SI.

Mimo, że szczegóły procesu dostosowania będą zależeć od ostatecznego kształtu europejskiego aktu dotyczącego sztucznej inteligencji, Polska, tak jak inne kraje UE, będzie musiała ściśle współpracować z instytucjami unijnymi, sektorem prywatnym oraz społeczeństwem obywatelskim, aby skutecznie wdrożyć te regulacje. To proces, który wymaga szerokiego dialogu i współpracy między różnymi interesariuszami, aby zapewnić, że przepisy będą

wspierać innowacje i rozwój technologiczny, jednocześnie chroniąc interesy oraz prawa użytkowników i obywateli.

W polskim systemie prawnym, zarówno w obszarze prawa cywilnego, jak i karnego, obecnie nie istnieją specjalne przepisy dedykowane wyłącznie regulacji działań związanych z udziałem sztucznej inteligencji. Niemniej jednak aktualne przepisy mogą być interpretowane oraz stosowane w taki sposób, aby uwzględniać pewne aspekty funkcjonowania SI, szczególnie pod kątem zapewnienia ochrony przed niepożądanymi i nielegalnymi działaniami tych technologii.

W obszarze prawa cywilnego, zabezpieczenie przed potencjalnie szkodliwymi działaniami sztucznej inteligencji może być zapewnione poprzez stosowanie ogólnych zasad odpowiedzialności cywilnej, takich jak odpowiedzialność za czyny niedozwolone (delikty) oraz odpowiedzialność umowna. Na przykład, jeśli działanie sztucznej inteligencji spowoduje szkodę, poszkodowany ma prawo dochodzić roszczeń na podstawie ogólnych przepisów dotyczących odpowiedzialności za wyrządzone szkody (np. artykuł 415 i kolejne Kodeksu cywilnego[173]).

W dziedzinie prawa karnego nie ma specjalnych przepisów dotyczących sztucznej inteligencji, ale istnieją obowiązujące regulacje, które mogą być stosowane w przypadku działań z użyciem sztucznej inteligencji, naruszających prawo. Na przykład, jeśli niewłaściwe wykorzystanie sztucznej inteligencji prowadzi do naruszenia dóbr osobistych lub danych osobowych, albo gdy sztuczną inteligencję wykorzystuje się do popełnienia przestępstwa (np. oszustwa), to mogą zostać zastosowane odpowiednie przepisy Kodeksu karnego[174].

Warto jednak zaznaczyć, że rosnące znaczenie technologii sztucznej inteligencji oraz jej coraz szersze zastosowanie w różnych dziedzinach życia społecznego i gospodarczego mogą wymagać bardziej szczegółowych uregulowań prawnych. Dlatego trwają dyskusje na poziomie Unii Europejskiej oraz w poszczególnych państwach członkowskich na temat konieczności wprowadzenia dedykowanych regulacji prawnych dotyczących sztucznej inteligencji. Celem tych przepisów miałoby być nie tylko zapewnienie ochrony przed negatywnymi skutkami zastosowania SI, ale również stworzenie korzystnych warunków dla rozwoju i stosowania technologii SI w sposób etyczny i bezpieczny.

[173] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2023 r. poz. 1610 z późn. zm.).
[174] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2024 r. poz. 17 z późn. zm.)

W kontekście międzynarodowym i europejskim, przygotowany „*Europejski Akt o Sztucznej Inteligencji*”[175] ma na celu ustanowienie wszechstronnych regulacji dla SI w Unii Europejskiej, co z kolei będzie wymagać dostosowania krajowych systemów prawnych do nowych przepisów. To z kolei może prowadzić do wprowadzenia konkretnych przepisów w polskim prawie regulujących, gdzie mogą wystąpić konsekwencje prawne przy działaniach związanych z użyciem sztucznej inteligencji.

3.2.3 Analiza przepisów prawnych dotyczących SI w wybranych jurysdykcjach

Rozwój technologii sztucznej inteligencji stwarza nowe wyzwania dla ustawodawców, wymagające przemyślanej i skoordynowanej reakcji prawniczej. Przepisy dotyczące SI różnią się w zależności od jurysdykcji, odzwierciedlając lokalne priorytety, cele polityczne oraz poziomy zaawansowania technologicznego. Ta analiza skupia się na regulacjach dotyczących SI w Unii Europejskiej, Stanach Zjednoczonych i Chinach, aby ukazać zróżnicowane podejścia do regulacji tego dynamicznie rozwijającego się obszaru.

1. Unia Europejska

   Unia Europejska dąży do stworzenia „*ekosystemu zaufania*” wokół sztucznej inteligencji, poprzez proponowanie regulacji mających na celu zapewnienie bezpiecznego i etycznego wykorzystania SI, jednocześnie wspierając innowacyjność. Kluczowym dokumentem w tej kwestii jest projekt „*Ustawy o Sztucznej Inteligencji*” (AI Act), która wprowadza spójne zasady dla SI w krajach członkowskich UE[176].

2. Stany Zjednoczone

   Stany Zjednoczone stosują bardziej zdecentralizowane i sektorowe podejście do regulacji sztucznej inteligencji, koncentrując się na promowaniu innowacji i konkurencyjności. Rząd federalny opublikował szereg wytycznych mających na celu kierowanie rozwojem

[175]Komisja Europejska, *Artificial Intelligence Act*, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, (dostęp 10.06.2024 r.).

[176] Komisja Europejska, 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, COM(2021) 206 final, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (dostęp: 10.06.2024 r.).

i wdrażaniem SI w sektorze publicznym i prywatnym, ale bez wprowadzania surowych regulacji na poziomie federalnym[177].

3. Chiny

Chiny szybko opracowują strategie i polityki mające na celu osiągnięcie pozycji światowego lidera w dziedzinie sztucznej inteligencji do 2030 roku[178]. Chiński rząd wprowadził wiele inicjatyw i programów, które wspierają badania nad SI, rozwój talentów oraz stosowanie SI w różnych sektorach gospodarki[179], jednocześnie zwiększając kontrolę państwa nad rozwojem i wykorzystaniem sztucznej inteligencji[180].

Reasumując każdy z opisanych wyżej podmiotów prawa międzynarodowego ma swoje własne podejście do regulacji odnoszącej się do sztucznej inteligencji, odzwierciedlające różne cele polityczne i społeczno-ekonomiczne. Unia Europejska koncentruje się na ochronie praw podstawowych i promowaniu etycznych aspektów SI, Stany Zjednoczone skupiają się na innowacyjności i konkurencyjności, natomiast Chiny stawiają sobie za cel szybkie zdobycie globalnego przywództwa w dziedzinie technologii SI przy jednoczesnym zwiększaniu kontroli państwowej.

W aspekcie prawnym, różnice w podejściach mają istotne konsekwencje dla ustalenia statusu prawnej osoby, przypisania winy oraz odpowiedzialności twórców Sztucznej Inteligencji. Analiza ta sugeruje konieczność międzynarodowej współpracy w dziedzinie regulacji SI w celu skutecznego rozwiązania problemów transgranicznych i ustanowienia wspólnych norm etycznych i prawnych.

---

[177] Executive Office of the President, National Science and Technology Council, Committee on Technology, *Preparing for the Future of Artificial Intelligence*, Washington, D.C., https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (dostęp: 10.06.2024 r.).

[178] State Council of the People's Republic of China, *New Generation Artificial Intelligence Development Plan* 2017.

[179] Ding J., *Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI*, "Future of Humanity Institute" 2018, University of Oxford, s. 12-13.

[180] Roberts H., Cowls J., Morley J., Taddeo M., Wang V., Floridi L., *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*, "AI & Society" 2021, vol. 36, s. 63-64.

3.2.4 Przegląd regulacji międzynarodowych dotyczących SI w ujęciu prawa karnego

Obecnie na całym świecie toczą się intensywne debaty na temat regulacji prawnych dotyczących sztucznej inteligencji, w tym w kontekście prawa karnego[181]. Wiele systemów prawnych opracowuje lub już wprowadziło regulacje prawne mające na celu kontrolowanie wykorzystania SI[182]. Niemniej jednak bezpośrednie przepisy prawne dotyczące SI w prawie karnym są rzadkością, a częściej prawo karne odnosi się do SI pośrednio, poprzez uregulowania dotyczące odpowiedzialności za czyny popełnione z wykorzystaniem technologii lub nadużycia jej, bez jasnego wskazania, że odnosi się to do użycia sztucznej inteligencji[183].

1. Przykład Singapuru

   Singapur to jeden z krajów, które aktywnie angażują się w opracowywanie przepisów dotyczących sztucznej inteligencji, zwłaszcza w kontekście odpowiedzialności i etyki. Model „*Governance Framework for Artificial Intelligence in Singapore*"[184] stanowi przełomową próbę uregulowania kwestii związanych z etycznym wykorzystaniem SI, aczkolwiek bardziej jest to zestaw wytycznych niż surowe przepisy prawne.

2. Unia Europejska

   Unia Europejska pracuje nad „*Aktem dotyczącym Sztucznej Inteligencji*"[185] (Artificial Intelligence Act), który ma na celu ustanowienie kompleksowego systemu regulacyjnego dla SI, będącego pierwszym tego rodzaju na świecie[186]. Regulacje obejmują różnorodne zagadnienia związane z wykorzystaniem SI, w tym odpowiedzialność i nadzór[187]. Mimo, że projekt skupia się głównie na aspektach cywilnoprawnych i rynkowych, jego wpływ

[181] Hallevy G., *Liability for Crimes Involving Artificial Intelligence Systems*, Springer International Publishing 2015, s. 1-2.
[182] Barfield W., Pagallo U. (eds.), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing 2018, s. 37-38.
[183] Hallevy G., *Liability for Crimes Involving Artificial Intelligence Systems*, Springer International Publishing 2015, s. 3-4.
[184] Infocomm Media Development Authority (IMDA), *Model Governance Framework for Artificial Intelligence in Singapore*, 2nd ed., "Infocomm Media Development Authority" 2020.
[185] Komisja Europejska, *Artificial Intelligence Act*, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (dostęp 10.06.2024 r.)
[186] Komisja Europejska, *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206, (dostęp: 13.06.2023).
[187] Ibidem, art. 1,3,16,17.

może także objąć obszar prawa karnego, szczególnie w kontekście potencjalnych nadużyć lub szkód powodowanych przez systemy SI[188].

3. Stany Zjednoczone

W USA nie ma spójnego podejścia federalnego do regulacji sztucznej inteligencji, chociaż niektóre stany, takie jak Kalifornia, podejmują kroki w celu uregulowania konkretnych zastosowań SI, takich jak rozpoznawanie twarzy. Na poziomie federalnym istnieją różne inicjatywy, ale brakuje jednolitej, ogólnokrajowej polityki regulacyjnej dotyczącej SI. Na przykład, Kalifornia wprowadziła przepisy[189], które wymagają od firm informowania konsumentów o zbieraniu ich danych biometrycznych, w tym rozpoznawania twarzy, oraz umożliwiają konsumentom rezygnację (ang. opt-out) z takiego przetwarzania danych. Proces opt-out polega na tym, że konsumenci mają prawo zażądać, aby ich dane biometryczne nie były gromadzone ani wykorzystywane przez firmę. Firmy są zobowiązane do udostępnienia łatwego sposobu na zgłoszenie takiej rezygnacji, na przykład poprzez link na stronie internetowej o nazwie „*Do Not Sell My Personal Information*"[190]. Dodatkowo istnieją działania na szczeblu federalnym mające na celu rozwiązanie konkretnych problemów związanych z SI, takich jak dyskryminacja algorytmiczna, chociaż nie ograniczają się one wyłącznie do kontekstu prawnego. W 2023 roku administracja Prezydenta Bidena wydała kilka istotnych dokumentów, w tym „*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*"[191], który podkreśla potrzebę zajęcia się dyskryminacją algorytmiczną i zapewnienia sprawiedliwego oraz odpowiedzialnego stosowania SI. W szczególności administracja wspomniała o konieczności zapewnienia, aby nowe technologie nie pogłębiały istniejących nierówności ani nie wprowadzały nowych form dyskryminacji[192].

---

[188] Sellier A.L., *The impact of the Artificial Intelligence Act on criminal law*, "EU Law Live" 2021, no. 91, s. 2-3, https://eulawlive.com/weekend-edition/weekend-edition-no91/, (dostęp: 13.06.2023).

[189] California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (dostęp 10.06.2024 r.).

[190] State of California Department of Justice, *California Consumer Privacy Act (CCPA),* https://www.oag.ca.gov/privacy/ccpa (dostęp: 10.06.2024 r.).

[191] Rozporządzenie Wykonawcze Prezydenta USA z dnia 30 października 2023 r. w sprawie bezpiecznego, pewnego i godnego zaufania rozwoju oraz użycia sztucznej inteligencji, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (dostęp 10.06.2024 r.).

[192] Allen, N., Barrett, M. N., Millendorf, S. M., Moore, S., & Zhang, R. R. , *Highlights From the Biden Administration Executive Order on AI*, Foley & Lardner LLP, https://www.foley.com/insights/publications/2023/11/highlights-biden-administration-executive-order-ai/ (dostęp: 10.06.2024 r.).

Ponadto, Federalna Komisja Handlu (FTC), Departament Sprawiedliwości (DOJ), Komisja Równych Szans Zatrudnienia (EEOC) i Biuro Ochrony Finansów Konsumenckich (CFPB) wydały wspólne oświadczenie dotyczące zwalczania dyskryminacji związanej z zastosowaniem sztucznej inteligencji[193]. Oświadczenie to podkreśla, że istniejące prawa ochrony konsumentów i prawa antydyskryminacyjne mają zastosowanie do technologii SI, a agencje federalne zobowiązują się do monitorowania i egzekwowania tych przepisów w kontekście nowych technologii[194].

Podsumowując można stwierdzić, iż obecnie, bezpośrednie przepisy prawne dotyczące sztucznej inteligencji w kontekście prawa karnego są stosunkowo rzadkie, a większość państw nadal pracuje nad opracowaniem odpowiednich regulacji. Większość tych regulacji skupia się na kwestiach odpowiedzialności cywilnej, etyki i nadzoru nad SI, co pośrednio wpływa na zagadnienia związane z prawem karnym poprzez ustanawianie standardów odpowiedzialnego wykorzystania technologii SI. W miarę postępu technologii i jej coraz szerszego zastosowania można spodziewać się dalszego rozwoju i specjalizacji przepisów prawnych dotyczących SI, również w obszarze prawa karnego.

3.2.5 Przegląd Aktu o Sztucznej Inteligencji UE

Projekt „*Ustawy o Sztucznej Inteligencji*”[195] przygotowywany przez Unię Europejską stanowi pierwszą próbę kompleksowego uregulowania technologii SI na arenie międzynarodowej. Istotne zagadnienia obejmują: ustalenie zasad odpowiedzialności za systemy SI, ocenę ryzyka związanego z różnymi zastosowaniami SI, szczegółowe regulacje dotyczące systemów wysokiego ryzyka, wymogi dotyczące przejrzystości oraz danych używanych do szkolenia SI, a także mechanizmy nadzoru i egzekwowania przestrzegania prawa. Celem inicjatywy jest budowanie zaufania do technologii SI poprzez zapewnienie jej bezpiecznego rozwoju i stosowania w Europie[196].

---

[193] EEOC, DOJ, FTC, & CFPB, *Joint Statement on Artificial Intelligence and Algorithmic Bias*, Federal Trade Commission, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf (dostęp 10.06.2024 r.).

[194] Goodman, M. E., Shinohara, T. K., De, R., Kourinian, A., *US FTC, DOJ, EEOC, and CFPB Release Joint Statement on AI, Discrimination and Bias*, Mayer Brown, https://www.mayerbrown.com/en/insights/publications/2023/04/us-ftc-doj-eeoc-and-cfpb-release-joint-statement-on-ai-discrimination-and-bias (dostęp: 10.06.2024 r.).

[195] Komisja Europejska, *Artificial Intelligence Act*, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, (dostęp 10.06.2024 r.).

[196] Komisja Europejska, *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i*

Rozwój sztucznej inteligencji w Europie i na świecie stwarza nowe wyzwania i możliwości dla społeczeństwa oraz gospodarki. Unia Europejska, dążąc do zachowania swojej pozycji lidera w dziedzinie technologicznej, jednocześnie pragnie zapewnić, że rozwój SI będzie przebiegał zgodnie z europejskimi wartościami, prawami podstawowymi i zasadami etycznymi[197]. „*Akt o Sztucznej Inteligencji*" jest kluczowym elementem europejskiej strategii w tym zakresie, wprowadzającym regulacje prawne, które mają na celu wspieranie innowacji i jednoczesne przeciwdziałanie potencjalnym zagrożeniom związanym z wykorzystaniem SI[198].

Mechanizmy i zabezpieczenia prawne w prawie Unii Europejskiej dotyczące sztucznej inteligencji koncentrują się na regulacji systemów SI o wysokim ryzyku. Obejmują one systemy wykorzystywane do identyfikacji biometrycznej, zarządzania krytyczną infrastrukturą, edukacji, zatrudnienia, a także dostępu do usług publicznych i prywatnych. Ponadto, regulacje te dotyczą także zastosowań w egzekwowaniu prawa oraz administracji sądowej.

Kluczowym aspektem jest konieczność przeprowadzenia przez dostawców systemów sztucznej inteligencji oceny ryzyka, która obejmuje identyfikację i ocenę potencjalnych negatywnych skutków funkcjonowania tych systemów. Dostawcy muszą także zapewnić odpowiednie środki zaradcze w celu zminimalizowania wykrytych zagrożeń. W dokumencie szczegółowo opisano również wymagania dotyczące dokumentacji technicznej, które mają na celu zwiększenie przejrzystości i ułatwienie nadzoru nad systemami sztucznej inteligencji[199].

Przyjęcie „*Akt o Sztucznej Inteligencji*"[200] jest kluczowe dla utrzymania zaufania społeczeństwa do technologii SI i zachowania konkurencyjności europejskiej gospodarki. Poprzez

zmieniającego niektóre akty ustawodawcze Unii, COM/2021/206 final, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0012.02/DOC_1&format=PDF (dostęp: 13.06.2023).

[197] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Sztuczna inteligencja dla Europy*, COM(2018) 237 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018DC0237 (dostęp: 13.06.2023).

[198] Komisja Europejska, *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*, COM/2021/206 final, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0012.02/DOC_1&format=PDF (dostęp: 13.06.2023).

[199] Komisja Europejska, *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*, COM/2021/206 final, art. 9, 11, 12, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0012.02/DOC_1&format=PDF, (dostęp: 13.06.2023).

[200] Komisja Europejska, *Artificial Intelligence Act*, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (dostęp 10.06.2024 r.).

wprowadzenie klarownych i spójnych zasad, Unia Europejska dąży do stworzenia bezpiecznego środowiska sprzyjającego rozwojowi oraz wdrożeniu SI, przy jednoczesnym szacunku dla praw i wolności obywatelskich. Komisja Europejska podkreśla, że równie istotne jest wspieranie innowacji i zapewnienie, aby regulacje nie ograniczały postępu technologicznego, ale promowały rozwijanie etycznych oraz bezpiecznych rozwiązań w dziedzinie SI[201].

Dlatego akt dotyczący sztucznej inteligencji w Unii Europejskiej jest istotnym krokiem w kierunku zrównoważonego rozwoju technologii SI, który uwzględnia potrzeby zarówno gospodarki, jak i społeczeństwa, a także ochronę podstawowych praw[202]. Konieczne będą dalsze dyskusje i konsultacje z zainteresowanymi stronami, aby dostosować i doskonalić przepisy w taki sposób, aby skutecznie reagować na dynamicznie zmieniający się krajobraz technologiczny[203].

3.3 Prawa i obowiązki użytkowników systemów SI

3.3.1 Przegląd praw i obowiązków użytkowników korzystających z systemów SI

Wzrost wykorzystania systemów opartych na sztucznej inteligencji powoduje konieczność precyzyjnego określenia praw i obowiązków osób korzystających z tych technologii. W tym kontekście, użytkownicy systemów SI to nie tylko pojedynczy klienci, ale także firmy i instytucje publiczne, które wykorzystują te technologie do różnorodnych celów, począwszy od automatyzacji procesów po analizę dużych zbiorów danych[204].

Prawa użytkowników systemów SI obejmują, ale nie są ograniczone prawem do:

[201] European Parliament, Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai (dostęp: 10.06.2024 r.).

[202] Komisja Europejska, *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*, COM/2021/206 final, preambuła, punkty 1-5, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206, (dostęp: 13.06.2023).

[203] European Parliament, *Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice*, (2020/2013(INI)), https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_EN.html (dostęp: 13.06.2023).

[204] Lee, K., *SI Superpowers: China, Silicon Valley, and the New World Order*, Houghton Mifflin Harcourt 2018.

1. transparentności działania systemów SI - użytkownicy mają pełne prawo do uzyskania informacji na temat funkcjonowania oraz podstawowych zasad decyzyjnych systemów sztucznej inteligencji, z których korzystają[205].

2. ochrony prywatności - podczas zbierania i przetwarzania informacji przez systemy sztucznej inteligencji, należy zapewnić ochronę użytkowników przed nieuprawnionym dostępem i wykorzystaniem ich danych osobowych[206].

3. niezawodności i bezpieczeństwa - systemy sztucznej inteligencji powinny działać w sposób niezawodny i bezpieczny, ograniczając ryzyko popełnienia błędów i awarii, które mogą prowadzić do szkód finansowych lub niemajątkowych[207].

Obowiązki użytkowników systemów SI to między innymi:

1. odpowiedzialne korzystanie - użytkownicy powinni korzystać z systemów sztucznej inteligencji w sposób odpowiedzialny, z zachowaniem obowiązujących przepisów prawa oraz norm etycznych[208].

2. zapewnienie ochrony danych - podczas korzystania z systemów sztucznej inteligencji do przetwarzania danych osobowych, użytkownicy (w szczególności firmy i instytucje) są zobowiązani do zapewnienia adekwatnego poziomu ochrony tych informacji[209].

3. podnoszenie świadomości i edukacja - użytkownicy, zwłaszcza ci pracujący w sektorze publicznym i biznesie, powinni starać się zwiększać świadomość na temat potencjałów oraz ograniczeń systemów sztucznej inteligencji, a także edukować pracowników i klientów na temat bezpiecznego korzystania z tych technologii[210].

Ważne jest przestrzeganie tych zasad i obowiązków, nie tylko w celu ochrony poszczególnych użytkowników, lecz także dla zapewnienia stabilności oraz bezpieczeństwa społecznego i gospodarczego w dobie cyfryzacji[211]. Należy kontynuować rozwój ram prawnych, które

[205] Zittrain, J., *The Future of the Internet and How to Stop It*, Yale University Press2008.
[206] Whitley, E. A., *Information Privacy, Consent and the „Control" of Personal Data*, "Information Security Technical Report" 2009, Vol. 14, No. 3, Elsevier.
[207] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.
[208] Russell S., *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking 2019.
[209] Edwards L., *Law, Policy, and the AI Dilemma*, Routledge 2022.
[210] Ng A., *Deep Learning*, "DeepLearning.AI" 2021.
[211] Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji - Europejskie podejście do doskonałości i zaufania*, COM(2020) 65 final, s. 3, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pl.pdf (dostęp: 13.06.2023).

skutecznie regulują dynamicznie zmieniającą się dziedzinę sztucznej inteligencji, jednocześnie wspierając innowacje oraz ochronę podstawowych praw obywatelskich[212]. Te normy są kluczowe zarówno dla zapewnienia prawnego bezpieczeństwa użytkowników, jak i osób trzecich, które mogą być pośrednio lub bezpośrednio dotknięte działaniem sztucznej inteligencji[213].

3.3.2 Problematyka ochrony danych i prywatności w kontekście interakcji z SI

W miarę postępu technologii sztucznej inteligencji, ochrona danych osobowych i prywatności użytkowników staje przed nowymi wyzwaniami. Korzystanie z systemów opartych na SI generuje dużą ilość informacji, które mogą być używane w sposób pożyteczny lub potencjalnie niebezpieczny. Dlatego ważne jest, aby zrozumieć i przestrzegać praw użytkowników oraz podkreślić obowiązki twórców i operatorów systemów SI w kontekście ochrony prywatności.

Kluczowe wyzwania to:

1. **przejrzystość i zrozumienie działania SI** - użytkownicy powinni być informowani o sposobie wykorzystywania ich danych przez systemy sztucznej inteligencji oraz o zastosowanych mechanizmach decyzyjnych. Często występujący problem braku przejrzystości (ang. black box) w algorytmach sztucznej inteligencji sprawia, że trudno jest zrozumieć i kontrolować sposób przetwarzania danych osobowych[214];

2. zbieranie i wykorzystanie danych bez wyraźnej zgody - Zbieranie informacji w sposób niejawny, bez wyraźnej zgody użytkowników, budzi kontrowersje dotyczące legalności i moralności takich działań. Konieczne jest ustanowienie klarownych reguł dotyczących zgody na przetwarzanie danych osobowych[215];

---

[212] Parlament Europejski, *Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii*, (2020/2012(INL)), preambuła, punkt F, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PL.html (dostęp: 13.06.2023).

[213] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, s. 11, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, (dostęp: 13.06.2023).

[214] Art. 29 Grupa Robocza ds. Ochrony Danych, *Wytyczne w sprawie przejrzystości na mocy rozporządzenia 2016/679*, 2018, https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf&ved=2ahUKEwjB-sDijdGGAxW8KRAIHWRMBu4QFnoECBUQAQ&usg=AOvVaw3THJIYxE3qtBg7knfbycpt (dostęp: 10.06.2024 r.).

[215] Solove D., *Understanding Privacy*, Harvard University Press 2008.

3. zabezpieczenie przed nieautoryzowanym dostępem - wzrost zaawansowania SI niesie ryzyko cyberataków mających na celu wykradzenie lub manipulację danymi. Ochrona przed takimi atakami wymaga skutecznych rozwiązań w zakresie cyberbezpieczeństwa[216];

4. odpowiedzialność za naruszenia danych - w kontekście prawnym istotne jest określenie, kto ponosi odpowiedzialność za ewentualne naruszenia ochrony danych osobowych spowodowane przez systemy sztucznej inteligencji. Sprawa ta dotyczy zarówno osób tworzących, jak i korzystających z tych systemów, a jej rozwiązanie wymaga precyzyjnych przepisów regulujących kwestię odpowiedzialności[217];

Prawa użytkowników w kontekście SI obejmują:

- prawo do pełnej informacji na temat przetwarzania danych, w tym celów, metod i algorytmów stosowanych przez systemy sztucznej inteligencji,
- możliwość sprawdzenia i poprawienia swoich danych przechowywanych przez system sztucznej inteligencji, w tym prawo do dostępu do nich,
- prawo do bycia zapomnianym oznacza możliwość usunięcia swoich danych z systemów informatycznych w przypadku ich zbędności lub gdy użytkownik wycofa zgodę na ich przetwarzanie,
- możliwość żądania ograniczenia przetwarzania danych przez system informatyczny, zwłaszcza gdy dane są przetwarzane w sposób niepoprawny lub niezgodny z prawem,
- użytkownicy mają uprawnienia do przenoszenia swoich informacji osobistych z jednej platformy cyfrowej na drugą poprzez korzystanie z prawa do transferu danych.

Obowiązki twórców i operatorów SI są następujące:

- zapewnienie jasności w procesach podejmowania decyzji przez sztuczną inteligencję, co pozwala użytkownikom zrozumieć, w jaki sposób ich dane są wykorzystywane,

[216] Cavoukian A., *Privacy by Performance: The 7 Foundational Principles*, https://www.datatilsynet.no/globalassets/global/english/7foundationalprinciples_anncavoukian2.pdf (dostęp: 10.06.2024 r.)

[217] Koops B.-J., *The Trouble with European Data Protection Law*, "International Data Privacy Law" 2014, Vol. 4, No. 4, s. 250–261.

- ważne jest, aby użytkownicy jasno wyrazili zgodę na przetwarzanie swoich danych, co wymaga przejrzystej komunikacji i możliwości udzielenia zgody,
- wdrożenie zaawansowanych środków bezpieczeństwa danych w celu ochrony przed dostępem nieupoważnionym, ujawnieniem lub innymi formami nadużyć,
- promowanie etycznych praktyk i odpowiedzialnego podejścia do korzystania z informacji osobowych, w tym poprzez szkolenia, edukację użytkowników i ciągłe doskonalenie metod ochrony prywatności.

Współpraca między ustawodawcami, twórcami technologii, użytkownikami i organami regulacyjnymi jest kluczowa dla rozwiązania problemów związanych z ochroną danych i prywatności w erze sztucznej inteligencji. Istotne jest, aby światowe standardy ochrony danych były elastyczne i dostosowywalne do dynamicznego rozwoju technologii SI, jednocześnie wspierając innowacyjność i respektując podstawowe prawa i wolności.

3.4 Podsumowanie głównych problemów i wyzwań prawnokarnych związanych z SI

Podczas badania kwestii prawnych związanych z technologią opartą na sztucznej inteligencji pojawia się wiele istotnych problemów i wyzwań, które wymagają dogłębnego rozważenia oraz reakcji ze strony ustawodawców, prawników i społeczności naukowej. Problemy te odnoszą się do następujących kwestii:

1. kwalifikacja czynów dokonanych przez SI jako przestępstw - istotnym zagadnieniem jest pytanie, czy i w jakich sytuacjach sztuczna inteligencja może być traktowana jako podmiot zdolny do popełnienia czynu zabronionego oraz jakie konsekwencje to niesie dla tradycyjnych kategorii prawnokarnych[218];

2. przypisanie sprawstwa i odpowiedzialności - pytanie o sprawstwo i odpowiedzialność za działania sztucznej inteligencji stawia przed nami nowe wyzwania, które wymykają się spod znanych dotąd definicji i teorii sprawstwa w prawie karnym. Rozważane są różne modele

[218] Scherer M. U., Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, "Harvard Journal of Law & Technology" 2016, Vol. 29, No. 2, s. 353-400.

odpowiedzialności - od bezpośredniej odpowiedzialności twórców i operatorów po nowe formy odpowiedzialności prawnej.[219];

3. ochrona danych i prywatności - w obszarze sztucznej inteligencji ochrona danych osobowych i prywatności użytkowników staje się istotnym wyzwaniem, ze względu na zdolność SI do przetwarzania informacji w dużych ilościach i tworzenia profili w celu obsługi różnorodnych zastosowań, w tym tych o charakterze prawnym[220];

4. autonomia decyzyjna SI i etyczne implikacje - systemy decyzyjne działające autonomicznie stawiają pytania dotyczące granic autonomii sztucznej inteligencji oraz kwestii etycznych związanych z ich użyciem, takich jak ryzyko nadużyć i dyskryminacji, co ma istotny wpływ na obszar prawa karnego i jego praktyczne zastosowanie[221];

5. międzynarodowe i krajowe regulacje prawne - różnice w podejściu do regulacji sztucznej inteligencji na różnych szczeblach legislacyjnych - od lokalnych po międzynarodowe - prowadzą do powstania zróżnicowanego środowiska prawno-regulacyjnego, co może stanowić wyzwanie dla skutecznego zarządzania ryzykiem związanym ze sztuczną inteligencją oraz prowadzić do sporów dotyczących jurysdykcji[222].

Podsumowując, postęp technologii sztucznej inteligencji stwarza nowe wyzwania dla systemu prawnego, które wymagają przemyślanych, zrównoważonych i dostosowanych do szybko zmieniającego się środowiska technologicznego rozwiązań. Konieczne jest dążenie do stworzenia regulacji prawnych, które zapewnią skuteczną ochronę praw jednostek oraz umożliwią kontynuację rozwoju i innowacji w obszarze sztucznej inteligencji.

[219] Vladeck D. C., *Machines Without Principals: Liability Rules and Artificial Intelligence*, "Washington Law Review" 2014.
[220] Bygrave L. A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International 2002.
[221] Bostrom N., *Ethical Issues in Advanced Artificial Intelligence*, Cognitive, "Emotive and Ethical Aspects of Decision Making in Humans and in Artificial Intelligence" 2003, Vol. 2.
[222] Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.

Rozdział IV. Prawo karne a etyka w kontekście sztucznej inteligencji

Etyczny aspekt rozwoju sztucznej inteligencji podważa tradycyjne pojęcia karnoprawnej odpowiedzialności, autonomii i moralności, co wymusza konieczność nowych regulacji w zakresie prawa karnego.

Znaczenie etyki w kontekście sztucznej inteligencji nie ogranicza się jedynie do abstrakcyjnych koncepcji moralnych. Ma ono rzeczywiste odzwierciedlenie w praktyce prawa karnego, gdzie muszą być rozstrzygane kwestie odpowiedzialności za działania lub zaniechania związane ze sztuczną inteligencją. Etyka wykracza więc poza filozoficzne debaty, stając się integralnym elementem procesu formułowania prawa oraz jego egzekwowania[223][224].

W kontekście prawa karnego, ocena wpływu sztucznej inteligencji na jego kształt i funkcjonowanie wymaga zrozumienia, w jaki sposób istniejące przepisy prawa karnego mogą być zastosowane do działań wynikających z działania algorytmów lub systemów autonomicznych. Ten temat dotyczy zarówno definicji popełnienia przestępstwa, jak i możliwości ustalenia odpowiedzialności[225][226].

Istotne pytanie, które pojawia się przy tej okazji, dotyczy możliwości dostosowania tradycyjnych kategorii prawnych, takich jak wina, zamiar czy nieumyślność, do kontekstu sztucznej inteligencji. Czy i w jaki sposób twórca lub operator systemu SI może ponosić odpowiedzialność karną za działania maszyny? W jaki sposób można określić i uregulować „*etykę algorytmów"* zgodnie z wymogami prawa karnego[227]?

Odpowiedzi na te pytania wymagają holistycznego podejścia, które łączy wiedzę z dziedzin informatyki, prawa, filozofii i etyki. Należy również uwzględnić dynamiczny postęp

[223] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.
[224] Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.
[225] Hildebrandt M., *The new laws of robotics: Defending human expertise in the age of AI*, Harvard University Press 2016.
[226] Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.
[227] Goodman R., *A guide to the ethics of autonomous cars*, Ethics and Information Technology 2016, Vol. 18, No. 3, s. 179-191.

technologiczny oraz konieczność elastyczności przepisów, aby móc skutecznie reagować na zmieniające się wyzwania[228].

Przy próbie zrozumienia i uregulowania relacji między etyką a prawem karnym w kontekście sztucznej inteligencji, konieczne jest wyjście poza ustalone ramy i poszukiwanie nowych, adekwatnych do zmieniającej się rzeczywistości, normatywnych rozwiązań.

4.1 Wprowadzenie do tematyki etyki i prawa karnego w kontekście SI

Sztuczna inteligencja, poruszająca się na granicy informatyki i etyki, wprowadza nowe elementy w obszarze prawa karnego. Rozwój technologii SI nie tylko otwiera możliwości pozytywnych zmian, ale także niesie ze sobą ryzyko oraz wyzwania, przed którymi muszą stanąć legislatorzy i praktycy prawa. W kontekście etycznym szczególne znaczenie nabiera pytanie o granice odpowiedzialności oraz moralne skutki działań podejmowanych przez autonomiczne systemy[229]?

To co jest ważne, to to by nie tylko rozpoznawać i analizować potencjalne zagrożenia, ale także aktywnie kształtować regulacje prawne, które będą w stanie odpowiedzieć na wyzwania związane z interakcją człowieka z maszyną. Wymaga to zarówno głębokiego zrozumienia technologii, jak i refleksji nad wartościami, które prawo karne ma bronić i promować w kontekście sztucznej inteligencji[230].

Rozważanie kwestii sztucznej inteligencji z perspektywy etyki i prawa karnego rodzi pytanie, o zakres oraz metody regulacji działań SI, w tym kryteria przypisywania odpowiedzialności. Z jednej strony istnieje potrzeba ochrony społeczeństwa i jednostek przed potencjalnie negatywnymi skutkami działania algorytmów, natomiast z drugiej strony istotne jest zapewnienie przestrzeni dla innowacji oraz rozwoju technologicznego[231].

---

[228] Scherer M. U., *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, "Harvard Journal of Law & Technology" 2016, Vol. 29, No. 2, s. 353-400.

[229] Danaher J., *The Threat of Algocracy: Reality, Resistance and Accommodation*, "Philosophy & Technology" 2016, Vol. 29, No. 3, s. 245-268.

[230] European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (dostęp: 10.06.2024 r.).

[231] Casey B., Farhangi A., Vogl R., *Rethinking Explainable Machines: The GDPR's „Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, "Berkeley Technology Law Journal" 2019.

W tej perspektywie, należy dokładnie przeanalizować obowiązujące przepisy prawa karnego i ich stosowanie do działań związanych z sztuczną inteligencją, przykładając szczególną uwagę do pojęć takich jak odpowiedzialność za produkt, odpowiedzialność za naruszenie standardów bezpieczeństwa oraz odpowiedzialność karna osób prawnych. Konieczne jest zbadanie, czy i w jaki sposób aktualne przepisy pozwalają skutecznie reagować na nowe formy przestępstw popełnianych przy użyciu systemów wykorzystujących sztuczną inteligencję[232].

Odpowiedzialność karna w kontekście sztucznej inteligencji nie może zostać zbadana bez uwzględnienia kwestii etycznych, które stanowią istotne wytyczne dla interpretacji i tworzenia prawa. Etyka sztucznej inteligencji, często omawiana w kontekście wytycznych i kodeksów postępowania, staje się nie tyle teoretyczną dyskusją, co praktycznym narzędziem kształtowania bezpiecznego i sprawiedliwego porządku prawnego[233].

Niniejsza część pracy ma za zadanie przedstawić główne wyzwania i perspektywy dotyczące wpływu sztucznej inteligencji na etykę oraz prawo karne, przy uwzględnieniu aktualnych debat naukowych i tendencji legislacyjnych.

4.2 Etyczne aspekty tworzenia i używania sztucznej inteligencji

Tworzenie oraz wdrażanie systemów sztucznej inteligencji to procesy, które niosą ze sobą wiele kwestii etycznych do rozważenia. Kluczowym problemem jest tutaj odpowiedzialność za decyzje podejmowane przez maszyny, które z natury nie posiadają świadomości ani moralnego podmiotu w tradycyjnym tego słowa znaczeniu[234]. Dlatego istotne jest stworzenie ram etycznych dotyczących odpowiedzialności, które uwzględnią zarówno proces tworzenia algorytmów, jak i ich funkcjonowanie w społeczeństwie.

Tworzenie sztucznej inteligencji wiąże się z odpowiedzialnością, która spoczywa zarówno na programistach i projektantach systemów, jak i na firmach oraz instytucjach publicznych wprowadzających te technologie. Każda z tych grup staje przed zadaniem zapewnienia, że działania sztucznej inteligencji są zgodne z zasadami sprawiedliwości, przejrzystości oraz

[232] Sourdin T., *Judge v Robot? Artificial Intelligence and Judicial Decision-Making*, "UNSW Law Journal" 2018, Vol. 41, No. 4, s. 1114-1133.
[233] Ryan M., Stahl B. C., *Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications*, "Journal of Information, Communication and Ethics in Society" 2020.
[234] Mittelstadt B., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, "Big Data & Society" 2016.

poszanowania prywatności i innych praw człowieka[235]. Na przykład problem uprzedzeń w algorytmach jest jednym z najbardziej pilnych zagadnień etycznych, które może prowadzić do dyskryminacji i nierówności społecznych[236].

Kwestia korzystania z sztucznej inteligencji rodzi również istotne kwestie moralne. W jaki sposób te systemy mogą wpływać na autonomię i wolność jednostki? Jak mogą być wykorzystywane do manipulowania ludzkim zachowaniem? W kontekście prawa karnego ważne jest zrozumienie, w jaki sposób takie technologie mogą być używane w celach przestępczych lub jak mogą wpływać na proces sądowy i wymiar sprawiedliwości[237].

Rozważania te muszą być uzupełnione o szeroki dialog między różnymi dziedzinami, takimi jak prawo, informatyka, filozofia i socjologia. Dopiero w ten sposób będzie możliwe stworzenie wszechstronnego i całościowego podejścia do kwestii etycznych sztucznej inteligencji, które będzie reagować na wyzwania współczesnego świata i równocześnie służyć ogólnemu dobru[238].

4.2.1 Analiza etycznych dylematów wynikających z rozwoju i implementacji SI

Rozwój sztucznej inteligencji wiąże się z pojawieniem się skomplikowanych dylematów etycznych, które dotyczą fundamentalnych zasad funkcjonowania demokratycznego społeczeństwa. W szczególności, pojawia się kwestia równowagi między koniecznością ochrony prywatności a potencjałem analitycznym, jaki oferują nowoczesne systemy sztucznej inteligencji[239]. Pojawia się także problem odpowiedzialności za decyzje podejmowane przez sztuczną inteligencję, co staje się szczególnie problematyczne w przypadku błędów lub wadliwych algorytmów, które mogą prowadzić do niesprawiedliwych rezultatów[240].

---

[235] Jobin A. et al., *The global landscape of AI ethics guidelines*, "Nature Machine Intelligence"2019, Vol. 1, No. 9, s. 389-399.

[236] Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, s. 77, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, (dostęp: 13.06.2023).

[237] Bryson J. J., *SI & Global Governance: No One Should Trust SI*, "United Nations University Centre for Policy Research" 2018.

[238] Coeckelbergh M., *AI Ethics*, MIT Press 2020.

[239] Kamarinou D., Millard C., Singh J., *Machine learning with personal data*, Queen Mary School of Law Legal Studies 2016.

[240] Dignum V., *Ethics in artificial intelligence: introduction to the special issue*, "Ethics and Information Technology" 2018, Vol. 20, No. 1, s. 1-3.

W kontekście prawnym, szczególnie ważnym wyzwaniem jest zapewnienie, że systemy sztucznej inteligencji nie powielają istniejących uprzedzeń i społecznych nierówności. Algorytmy używane w procesach podejmowania decyzji, takich jak prognozowanie recydywy czy ocena ryzyka kredytowego, powinny być pozbawione nieuzasadnionych stronniczości, które mogą mieć wpływ na życie jednostek[241].

Kolejną ważną kwestią etyczną jest ryzyko naruszenia autonomii jednostki poprzez manipulację lub zbytnią kontrolę, co może wystąpić w przypadku monitorowania i profilowania. Należy dokładnie przemyśleć, w jaki sposób te technologie mogą być wykorzystane w sposób szanujący prywatność i zapobiegający nadmiernemu nadzorowi[242].

Wykorzystanie sztucznej inteligencji w kontekście wymiaru sprawiedliwości stwarza pytania dotyczące możliwości zachowania obiektywności oraz właściwego zrozumienia i interpretacji prawa, które dotychczas były domeną ludzkiego rozumu i osądu. Istnieje ryzyko, że mimo zaawansowanej zdolności do analizy danych, algorytmy mogą nie być w stanie w pełni pojąć subtelności i złożoności ludzkiej moralności oraz profesjonalnej etyki, co jest kluczowe w procesie wymiaru sprawiedliwości[243].

Ponadto, opracowywanie i wdrażanie sztucznej inteligencji wymagają stałego dialogu pomiędzy programistami, prawnikami, etykami i użytkownikami końcowymi. Interdyscyplinarne podejście jest kluczowe do rozpoznania i rozwiązania problemów etycznych, takich jak: transparentność algorytmów, ich zrozumiałość dla użytkowników oraz możliwość audytowania i zrozumienia podejmowanych decyzji[244].

Analiza moralnych trudności związanych z sztuczną inteligencją nie powinna skupiać się jedynie na krytyce. Należy również konstruktywnie proponować modele dobrych praktyk, które pozwolą wykorzystać potencjał SI, minimalizując jednocześnie ryzyko naruszeń etycznych i prawnych. To oznacza konieczność opracowania i wdrożenia skutecznych regulacji

[241] Barocas S., Selbst A. D., *Big data's disparate impact*, "California Law Review" 2016, vol. 104.
[242] Zuboff S., *The Age of Surveillance Capitalism*, PublicAffairs 2019.
[243] Taddeo M., Floridi L., *Regulate artificial intelligence to avert cyber arms race*, "Nature" 2018, Vol. 556, No. 7701, s. 296-298.
[244] Cath C., *Governing artificial intelligence: ethical, legal and technical opportunities and challenges*, Philosophical Transactions of the Royal Society A: Mathematical, "Physical and Engineering Sciences" 2018, Vol. 376, No. 2133.

prawnych i etycznych, dostosowanych do szybko zmieniającego się środowiska technologicznego[245].

Wszystkie te elementy wymagają dokładnej analizy, która uwzględnia najnowsze osiągnięcia i wyzwania w dziedzinie sztucznej inteligencji, jednocześnie odnosząc się do fundamentalnych wartości etycznych i prawnych, na których opiera się nasza społeczność.

4.2.2 Etyczne wyzwania w zakresie autonomii i decyzyjności SI

Przyznanie systemom sztucznej inteligencji autonomii decyzyjnej stwarza istotne dylematy etyczne dotyczące odpowiedzialności, kontroli i wpływu na jednostkę oraz struktury społeczne. Autonomia SI, często porównywana do ludzkiej zdolności do podejmowania decyzji, wywołuje debaty na temat tego, jak daleko powinny te systemy sięgnąć w niezależność i jakie ograniczenia powinny być nałożone[246].

Wyzwanie polega na balansowaniu potencjału sztucznej inteligencji do poprawiania jakości ludzkiego życia z ryzykiem, że podejmowane przez nią decyzje mogą wiązać się z nieprzewidzianymi lub negatywnymi skutkami. Na przykład, autonomiczne pojazdy muszą podjąć decyzję w sytuacjach zagrożenia życia, co stawia pytanie o algorytmy wyboru mniejszego zła, znane jako dylemat wagonika (problem wagonika)[247].

Kolejną kwestią do rozważenia jest wpływ sztucznej inteligencji na procesy podejmowania decyzji w obszarach, gdzie zwykle polegano na ludzkim osądzie. Wykorzystanie algorytmów predykcyjnych w systemie sprawiedliwości lub opiece zdrowotnej budzi obawy związane z etyką i równością - jak zapewnić, by SI nie faworyzowało ani dyskryminowało ze względu na pochodzenie rasowe czy ekonomiczne.[248].

Etyczne zagadnienia związane z autonomią i zdolnością podejmowania decyzji przez sztuczną inteligencję wymagają również przemyślenia koncepcji „*moralności maszynowej*", czyli

[245] Hagendorff T., *The ethics of AI ethics: An evaluation of guidelines*, "Minds and Machines" 2020, Vol. 30, s. 99-120.
[246] Rahwan I., *Society-in-the-loop: programming the algorithmic social contract*, "Ethics and Information Technology" 2018, Vol. 20, No. 1, s. 5-14.
[247] Goodall N. J., *Can you program ethics into a self-driving car?*, "IEEE Spectrum" 2016, Vol. 53, No. 6, s. 28-58.
[248] O'Neil C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown 2016.

możliwości wyposażenia SI w etyczne zasady umożliwiające rozwiązywanie dylematów moralnych[249]. Czy wartości te mogą być zakodowane w algorytmach i czy SI powinna być traktowana jako podmiot moralny? To jest istotne pytanie.

Ostatecznie, twórcy i użytkownicy sztucznej inteligencji muszą systematycznie monitorować i oceniać systemy pod kątem zarówno ich skuteczności, jak i zgodności z wartościami etycznymi i społecznymi[250].

4.3 Rola prawa karnego w regulowaniu etycznych aspektów sztucznej inteligencji

Prawo karne pełni ważną rolę stabilizującą w społeczeństwie, ustalając granicę między akceptowalnym a niedozwolonym postępowaniem. W kontekście sztucznej inteligencji, przepisy karne są niezbędne do reglamentowania i sankcjonowania nowych form przestępczości oraz nieprzewidzianych skutków wykorzystania SI, które mogą prowadzić do naruszeń praw człowieka lub bezpieczeństwa publicznego[251].

Prawo karne musi dostosować się do dynamicznie zmieniających się realiów technologicznych, co stanowi wyzwanie. Konieczne jest znalezienie rozwiązań dla kwestii odpowiedzialności za działania systemów zautomatyzowanych, w tym ustalenie warunków, w jakich osoba fizyczna lub prawna może być pociągnięta do odpowiedzialności karnej za szkody spowodowane przez sztuczną inteligencję[252].

Istotną kwestią jest również zagwarantowanie, by regulacje karne nie blokowały postępu technologicznego, lecz wspierały rozwój sztucznej inteligencji w sposób moralny i zrównoważony. Wymaga to także zrozumienia i uregulowania tzw. „*zarządzania algorytmicznego*", które obejmuje wykorzystanie sztucznej inteligencji w procesach podejmowania decyzji zarówno publicznych, jak i prywatnych[253].

[249] Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.
[250] Floridi L., Cowls J., *A Unified Framework of Five Principles for AI in Society*, "Harvard Data Science Review" 2019.
[251] Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.
[252] Asaro P. M., *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Makin*g, "International Review of the Red Cross" 2012, Vol. 94, No. 886, s. 687-709.
[253] Yeung K., *Algorithmic regulation: A critical interrogation*, "Regulation & Governance" 2017, Vol. 12, No. 4, s. 505-523.

W kwestiach etycznych, system prawa powinien także odzwierciedlać oraz wspierać wartości społeczne, takie jak: sprawiedliwość, równość i poszanowanie autonomii jednostki. Konieczne jest prowadzenie ciągłego dialogu między prawnikami, technologami, etykami oraz społeczeństwem, aby regulacje te były odpowiednie wobec rzeczywistości współczesnego świata[254].

4.3.1 Przegląd obowiązujących przepisów i ich stosowanie do etycznych aspektów SI

Obecne przepisy prawa karnego nie zostały początkowo zaprojektowane z myślą o technologiach sztucznej inteligencji, co może prowadzić do luk prawnych i wyzwań interpretacyjnych. Wiele jurysdykcji na całym świecie rozpoczęło procesy aktualizacji lub wprowadzania nowych regulacji mających na celu rozwiązanie konkretnych problemów wynikających z postępu SI[255].

Należy pamiętać, że aktualne przepisy dotyczące odpowiedzialności karnej często opierają się na „*ludzkim*" aspekcie winy lub zaniedbania, co może być trudne do zastosowania w przypadku decyzji podejmowanych przez sztuczną inteligencję. W związku z tym niektóre jurysdykcje rozważają wprowadzenie pojęcia „*osobowości elektronicznej*", które mogłoby być używane do przypisywania odpowiedzialności systemom sztucznej inteligencji[256].

Poza tym należy zwrócić uwagę na przepisy dotyczące ochrony danych osobowych, takie jak te zawarte w ogólnym rozporządzeniu o ochronie danych[257] (GDPR), które nakładają wymogi transparentności oraz umożliwiają wyjaśnienie decyzji podejmowanych przez systemy sztucznej inteligencji. Choć GDPR nie obejmuje bezpośrednio wszystkich aspektów etycznych związanych z SI, stanowi istotne odniesienie w kwestii zagwarantowania prywatności i ochrony danych osobowych[258].

---

[254] Bryson J. J., *SI & Global Governance: No One Should Trust SI*, United Nations University Centre for Policy Research 2018.

[255] Schellekens M., *To regulate or not to regulate? The European Parliament's proposal to grant legal status to robots*, "Computer Law & Security Review" 2015.

[256] European Parliament, *Civil Law Rules on Robotics*, 2016/2103(INL), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (dostęp: 10.06.2024 r.).

[257] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

[258] Goodman B., Flaxman S., *European Union regulations on algorithmic decision-making and a "right to explanation"*, "AI Magazine" 2017, Vol. 38, No. 3, s. 50-57.

W kontekście zastosowania sztucznej inteligencji w systemie sprawiedliwości istotne jest, aby przepisy nie tylko kryminalizowały nieodpowiednie wykorzystanie SI, ale również ustanawiały regulacje dla właściwego i sprawiedliwego stosowania technologii w tej dziedzinie. Obejmuje to regulacje dotyczące danych cyfrowych, użycia systemów prognozujących oraz innych narzędzi opartych na SI[259].

Podsumowując, analiza obecnych przepisów i ich zastosowanie w kontekście etycznych aspektów sztucznej inteligencji pokazuje konieczność ciągłego dostosowywania prawa karnego do nowych technologii. Harmonizacja przepisów z wyzwaniami etycznymi wynikającymi ze sztucznej inteligencji jest kluczowym zadaniem dla ustawodawców, prawników oraz społeczeństwa.

4.3.2 Współzależność etyki i odpowiedzialności w kontekście prawa karnego

Rozwój sztucznej inteligencji stawia pytanie o odpowiedzialność karną w nowym świetle, zwłaszcza gdy decyzje są podejmowane przez algorytmy zamiast ludzi. Kto lub co powinno być odpowiedzialne za działania maszyn - to teraz kluczowe zagadnienie do przemyślenia[260].

Etyka w dziedzinie prawa karnego dotyczy oceny moralnej działań lub zaniechań, które mogą skutkować nałożeniem kar. W kontekście sztucznej inteligencji ważne jest, aby uwzględniać kwestie związane z tym, w jaki sposób twórcy i użytkownicy tych systemów mogą zapewnić ich działanie zgodne z normami etycznymi oraz uniknąć potencjalnych szkód[261].

Istotnym wyzwaniem jest zapewnienie, że systemy sztucznej inteligencji działają zgodnie z społecznymi wartościami, takimi jak sprawiedliwość, równość i poszanowanie dla autonomii jednostki. Odpowiedzialność w tym kontekście może dotyczyć nie tylko błędów w kodzie źródłowym, ale także sposobu projektowania algorytmów, aby podejmować etyczne decyzje[262].

System prawny musi także uwzględniać, jakie środki można podjąć wobec osób fizycznych i osób prawnych, które nadużywają sztucznej inteligencji lub nieprawidłowo wdrażają te

[259] Pagallo U., *AI and the law: A legal perspective, in The Oxford Handbook of Ethics of AI*, Oxford University Press 2018.
[260] Matthias Andreas, *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata*, "Ethics and Information Technology" 2004.
[261] Sparrow R., *Killer robots*, "Journal of Applied Philosophy" 2007, Vol. 24, No. 1, s. 62-77.
[262] Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.

technologie. Mogą to być sankcje za niewłaściwe programowanie SI, które prowadzi do przestępstw lub innych szkodliwych działań[263].

Przyszłe przepisy powinny również uwzględniać zdolność twórców sztucznej inteligencji do prognozowania szkód oraz wpływ, jaki to prognozowanie ma na ich poziom odpowiedzialności. Dodatkowo istotne jest, aby system prawny promował etyczne podejście do projektowania i wykorzystywania SI poprzez ustanawianie wymagań dotyczących etyki zawodowej wśród inżynierów i programistów[264].

[263] Bryson J., Patiency *Is Not a Virtue: The Design of Intelligent Systems and Systems of Ethics*, "Ethics and Information Technology" 2018, Vol. 20, No. 1, s. 15-26.
[264] Pagallo U., *The Laws of Robots: Crimes*, Contracts, and Torts, Springer 2013.

Rozdział V. Propozycje zmian w prawie karnym

W obliczu postępu w dziedzinie sztucznej inteligencji, prawo karne stoi przed wyzwaniem stworzenia odpowiednich regulacji, które będą skuteczne w walce z nowymi formami przestępczości i moralnymi dylematami. Takie podejście wymaga nie tylko identyfikacji luk prawnych, ale także aktywnego kształtowania przepisów, które będą wspierać etyczne używanie sztucznej inteligencji oraz ponoszenie odpowiedzialności za szkody spowodowane przez autonomiczne systemy[265].

Zmiany te powinny obejmować jasne określenie kluczowych pojęć związanych z sztuczną inteligencją, jak również ustanowienie konkretnych regulacji dotyczących odpowiedzialności karnej twórców, operatorów oraz samych systemów SI. Wymaga to również rozważenia wprowadzenia nowych kategorii przestępstw, które będą reagować na unikalne wyzwania związane ze sztuczną inteligencją, takie jak manipulacja algorytmami, czy wykorzystanie SI do celów przestępczych[266].

Zmiany, nad którymi się zastanawiamy, powinny koncentrować się na ochronie fundamentalnych praw człowieka oraz promowaniu wartości demokratycznych, jednocześnie umożliwiając rozwój i wdrożenie sztucznej inteligencji. Proces ten powinien odbywać się przy szerokim udziale społecznym oraz poprzez współpracę między prawnikami, technologami, etykami i społeczeństwem[267].

5.1 Analiza potrzeb i kierunków zmian legislacyjnych w odpowiedzi na etyczne wyzwania SI

Zmiany w regulacjach prawa karnego w obliczu postępu technologicznego powinny wynikać z dokładnej analizy obecnych i przyszłych potrzeb społecznych oraz technologicznych. Ustawodawstwo musi uwzględnić zarówno potencjalne zagrożenia związane z sztuczną inteligencją, jak i korzyści, jakie może ona przynieść poprzez poprawę jakości życia i efektywności procesów.

[265] Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.

[266] European Parliament, *Civil Law Rules on Robotics*, 2016/2103(INL), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (dostęp: 10.06.2024 r.).

[267] Bryson J., Patiency *Is Not a Virtue: The Design of Intelligent Systems and Systems of Ethics*, "Ethics and Information Technology" 2018, Vol. 20, No. 1, s. 15-26.

Kluczowe obszary, które wymagają uwagi legislacyjnej, obejmują:

1. definicje i terminologia – jasne określenie, jak rozumie się pojęcia „*sztuczna inteligencja*”, „*autonomiczny system*”, „*algorytmiczne podejmowanie decyzji*” itp. jest kluczowe dla stworzenia spójnego i zrozumiałego zbioru przepisów prawnych;

2. odpowiedzialność i sprawstwo – określenie sposobu przypisywania odpowiedzialności za działania lub zaniechania sztucznej inteligencji, zarówno w kontekście cywilnym, jak i karnym, uwzględniając potencjalne nadanie „*osobowości prawnej*” systemom SI;

3. transparentność i kontrola – zapewnienie jawności algorytmów, ich możliwość audytowania oraz kontrola nad procesami decyzyjnymi są niezmiernie istotne dla budowania zaufania społecznego i zapobiegania nadużyciom;

4. prywatność i ochrona danych – uwzględnienie nowych trudności związanych z zbieraniem, analizowaniem i wykorzystywaniem informacji przez systemy SI, zgodnie z aktualnymi wytycznymi dotyczącymi ochrony prywatności;

5. etyczne wytyczne – stworzenie i wdrożenie zasad etycznych dla projektantów i użytkowników sztucznej inteligencji, które będą wspierać odpowiedzialne i zrównoważone wykorzystanie SI;

6. bezpieczeństwo i prewencja zbrodni – rozwiązywanie problemu związanego z wykorzystaniem sztucznej inteligencji do celów przestępczych oraz rozwijanie środków zapobiegawczych i reagowania na zagrożenia związane z cyberprzestępczością.

Przyszłe przepisy prawne powinny uwzględniać standardy międzynarodowe i wynikać z współpracy międzynarodowej, która bierze pod uwagę różne podejścia i doświadczenia z różnych obszarów prawa. Ponadto powinny być elastyczne, aby można je było aktualizować wraz z postępem technologii informatycznej i pojawianiem się nowych wyzwań[268].

[268] Russell S., Dewey D., Tegmark M., *Research Priorities for Robust and Beneficial Artificial Intelligence*, “AI Magazine” 2015, Vol. 36, No. 4, s. 105-114.

5.2 Przegląd propozycji doktrynalnych i praktycznych zmian prawnych

Doktrynalne podejście do regulacji sztucznej inteligencji opiera się głównie na gruntownej analizie podstawowych zasad prawa i etyki oraz ich zastosowaniu do wyzwań, jakie stawiają przed nami systemy SI. Propozycje te często obejmują opracowanie nowych teorii odpowiedzialności, które uwzględniają unikalny charakter autonomicznych systemów SI[269]. W ramach tego podejścia eksperci prawa karnego mogą rozważać, czy tradycyjne pojęcia winy i zamiaru są wciąż adekwatne w kontekście maszyn, które uczą się i działają samodzielnie.

Propozycje praktycznych zmian prawnych skupiają się na tworzeniu lub dostosowywaniu konkretnych regulacji, które kontrolują działania sztucznej inteligencji. Może to obejmować wprowadzenie specjalnych zezwoleń dla twórców SI, wymaganie przestrzegania norm bezpieczeństwa i etyki w projektowaniu systemów SI oraz utworzenie nowych struktur nadzorczych zajmujących się konsekwencjami wdrożenia SI w społeczeństwie[270].

Przegląd tych sugestii obejmuje także omówienie ewentualnych zmian w prawie karnym, które mogłyby skuteczniej rozwiązać problem przestępczości związanej z sztuczną inteligencją, takiej jak oszustwa algorytmiczne czy nadużycia danych osobowych. Niektóre z propozycji mogą zakładać wprowadzenie nowych typów przestępstw lub modyfikację istniejącej definicji przestępstwa, aby lepiej odzwierciedlały specyfikę przestępstw związanych z technologią[271].

Istotne jest również zapewnienie, że proponowane zmiany prawne są zgodne z międzynarodowymi standardami i konwencjami, aby regulacje dotyczące sztucznej inteligencji były spójne na różnych poziomach prawa - lokalnym, krajowym i międzynarodowym[272].

5.3 Analiza luki prawnej w kontekście sztucznej inteligencji

Aktualnie obowiązujące przepisy prawne często nie uwzględniają złożoności i zmienności wynikającej z działania systemów sztucznej inteligencji, co może prowadzić do istnienia luki

[269] Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.
[270] Calo R., *Robotics and the Lessons of Cyberlaw*, "California Law Review" 2015, Vol. 103.
[271] European Commission, *Coordinated Plan on Artificial Intelligence*, https://digital-strategy.ec.europa.eu/en/policies/plan-ai (dostęp: 10.06.2024 r.).
[272] Scherer M. U., *Regulating Artificial Intelligence Systems: Risks, Challenges*, "Competencies, and Strategies, Harvard Journal of Law & Technology" 2016, Vol. 29, No. 2, s. 353-400.

prawnej. Taka luka może objawiać się brakiem precyzyjnych regulacji dotyczących odpowiedzialności, zarówno w kontekście cywilnym, jak i karnym, za aktywność podejmowaną przez sztuczną inteligencję[273]. Dlatego istnieje konieczność zidentyfikowania obszarów prawa karnego, które wymagają aktualizacji lub poszerzenia w celu uwzględnienia specyfiki sztucznej inteligencji.

Analiza musi brać pod uwagę zarówno zagadnienia teoretyczne, takie jak możliwość przypisywania odpowiedzialności algorytmom i maszynom, jak i praktyczne aspekty, np. sposób, w jaki prawo karne jest stosowane w przypadkach związanych z sztuczną inteligencją. Należy również ocenić, czy obecne przepisy są wystarczające do ochrony przed nieetycznym wykorzystaniem SI oraz czy nowe technologie nie korzystają z luk prawnych do działania poza obowiązującym systemem prawnym[274].

Ustawodawcy muszą rozważyć, jakie kroki są niezbędne, aby zapewnić skuteczne i sprawiedliwe egzekwowanie prawa w erze sztucznej inteligencji, czy to poprzez wprowadzenie nowych regulacji, takich jak specjalne uprawnienia dla twórców SI, czy też poprzez stosowanie odpowiednich norm i certyfikatów dla systemów SI[275].

5.3.1 Identyfikacja luki prawnej i dyskusja nad nią z perspektywy etycznych wymogów

Rozwój sztucznej inteligencji stwarza wiele dylematów etycznych, które nie zawsze są objęte obowiązującym prawem karnym. Istnienie luk prawnych w tym kontekście odnosi się do braków lub niewystarczających regulacji dotyczących kwestii takich jak: autonomia decyzyjna SI, przejrzystość algorytmów oraz odpowiedzialność za działania lub ich konsekwencje[276].

Obecne przepisy prawne mogą nie obejmować pełnego zakresu działania systemów sztucznej inteligencji, zwłaszcza gdy ich efekty prowadzą do konsekwencji prawnych i moralnych, które nie były przewidziane podczas tworzenia tych regulacji. Na przykład kwestie związane

[273] Karnow C. E. A., *Liability for Distributed Artificial Intelligences*, "Berkeley Technology Law Journal" 1996, Vol. 11, No. 1, s. 147-183.
[274] Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.
[275] Calo R., *Robotics and the Lessons of Cyberlaw*, "California Law Review" 2015, Vol. 103.
[276] Bryson J. J., Diamantis M. E., Grant T. D., *Of, for, and by the people: the legal lacuna of synthetic persons*, "Artificial Intelligence and Law" 2017.

z uprzedzeniami algorytmicznymi mogą nie być odpowiednio uregulowane, co rodzi problemy z dyskryminacją i sprawiedliwością[277].

Jednym z istotnych elementów luk prawnych jest także sposób, w jaki prawo karne traktuje kwestię odpowiedzialności zbiorowej lub korporacyjnej w kontekście szkód spowodowanych przez sztuczną inteligencję. To zagadnienie wymaga refleksji nad tym, czy obecne ramy odpowiedzialności karnej są wystarczające, czy też konieczne jest wprowadzenie nowych definicji odpowiedzialności dopasowanych do epoki sztucznej inteligencji[278].

Ponadto, ta luka odnosi się również do tego, w jaki sposób przepisy prawa karnego mogą chronić przed naruszeniem zasad etycznych w obszarach takich jak prywatność, godność czy samodzielne działania SI, które mogą wpływać na prawa i wolności jednostek[279].

5.3.2 Przykłady praktyczne i analiza przypadków

Analizując sytuacje, w których sztuczna inteligencja była zaangażowana, można lepiej zrozumieć lukę prawna i jej konsekwencje. Przykładowo, incydent związany z samochodem autonomicznym Ubera, który spowodował śmierć pieszego, ukazuje problem odpowiedzialności w przypadku, gdy decyzje podejmowane przez SI prowadzą do tragicznych rezultatów[280].

Innym przykładem jest wykorzystanie przez organy ścigania systemów rozpoznawania twarzy, które podnoszą kwestie związane z prywatnością, nadużyciami oraz potencjalnymi pomyłkami, mogącymi skutkować niesłusznymi oskarżeniami lub aresztowaniami[281].

W kontekście zatrudnienia, algorytmy sztucznej inteligencji stosowane w procesie rekrutacyjnym mogą przypadkowo prowadzić do dyskryminacji kandydatów ze względu na płeć, rasę lub wiek, co stanowi naruszenie praw pracowniczych i zasady równości[282].

---

[277] Barocas S., Selbst A. D., *Big data's disparate impact*, "California Law Review" 2016, vol. 104.
[278] Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.
[279] Cath C. et al., *Artificial Intelligence and the "Good Society": the US, EU, and UK approach*, "Science and Engineering Ethics" 2018, Vol. 24, No. 2, s. 505-528.
[280] Elish M. C., Boyd D., *Situating methods in the magic of Big Data and AI*, "Communication Monographs" 2017, Vol. 84, No. 1, s. 57-80.
[281] Garvie C., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, "Georgetown Law Center on Privacy & Technology" 2016.
[282] Ajunwa I., Friedler S., Scheidegger C., Venkatasubramanian S., *Hiring by algorithm: Predicting and preventing disparate impact*, "SSRN Electronic Journal" 2016.

Rozdział VI. Twórca sztucznej inteligencji

Jednym z głównych tematów do rozważań i uzyskania wyników w niniejszej pracy jest zagadnienie dotyczące twórcy sztucznej inteligencji. Ten rozdział otwiera dyskusję o roli, którą twórca SI odgrywa w dzisiejszym krajobrazie technologicznym, gdzie granice między inżynierią a jurysdykcją stają się coraz mniej wyraźne.

Rozważania będą skupiać się na zidentyfikowaniu i analizie problemów prawnych dotyczących oceny działań twórcy w kontekście odpowiedzialności za działanie lub zaniechanie podczas procesu tworzenia i wdrażania systemów sztucznej inteligencji. Będzie to obejmować zarówno odpowiedzialność cywilną, jak i karną, a także trudności związane z przypisaniem winy za działania autonomicznych systemów SI.

Analiza „*twórcy*" z perspektywy interdyscyplinarnej obejmuje nie tylko aspekty techniczne i prawne, ale także filozoficzne i etyczne zagadnienia dotyczące odpowiedzialności. Autorka pracy doktorskiej, opierając się na najnowszych osiągnięciach naukowych oraz praktycznych przykładach, stara się zrozumieć, jak systemy sztucznej inteligencji, będące produktem ludzkiego umysłu, mogą funkcjonować z autonomiczną decyzyjnością i jak powinno na nie reagować prawo karne.

Tematy poruszane w niniejszej części dysertacji stanowią podstawę do dalszej dyskusji na temat koniecznych modyfikacji obowiązujących przepisów prawnych oraz do wypracowania nowych kierunków polityki prawnej dotyczącej technologii sztucznej inteligencji.

6.1 Definicja i charakterystyka twórcy sztucznej inteligencji

Twórca sztucznej inteligencji, czy to jednostka czy zespół osób, pełni kluczową rolę w projektowaniu, programowaniu, testowaniu i wdrażaniu systemów SI. Jest to figura wykraczająca poza tradycyjne role programisty czy inżyniera ze względu na potrzebę zaawansowanych, interdyscyplinarnych umiejętności wymaganych do pracy nad SI. Zazwyczaj twórcami SI są eksperci z różnych dziedzin, takich jak: matematyka, neurologia, psychologia i etyka, co podkreśla kompleksowość i różnorodność wiedzy niezbędnej do stworzenia efektywnych i odpowiedzialnych systemów opartych na sztucznej inteligencji[283]. Odpowiadają

[283] Noga B.R., Opris I., *Lebedev M.A. & Mitchell G.S., Editorial: Neuromodulatory Control of Brainstem Function in Health and Disease*, Frontiers in Neuroscience,

nie tylko za techniczne aspekty, ale także za świadomość etyczną i prawną konieczną w kontekście wpływu SI na szeroki zakres ludzkiego życia.

Jeśli chodzi o interdyscyplinarne wymagania to twórca sztucznej inteligencji to jest nie tylko specjalistą od technologii, ale także innowatorem i badaczem, którego obowiązki obejmują analizę konsekwencji stosowania SI oraz prognozowanie potencjalnych ryzyk związanych z jej funkcjonowaniem. Etyczny aspekt pracy twórcy SI polega na zapewnieniu, że ta technologia będzie służyła dobru ogółu społeczeństwa, a jej wykorzystanie będzie zgodne z prawem oraz społecznymi wartościami[284].

W przypadku odpowiedzialności prawnej w kontekście prawa karnego, osoba tworząca sztuczną inteligencję może ponosić odpowiedzialność za działanie systemów, które stworzyła. Interpretacja tej odpowiedzialności może się różnić w zależności od stopnia samodzielności SI oraz przewidywalności jego działań[285].

Jeśli chodzi o wyzwania definicyjne to definicja „*twórców sztucznej inteligencji*" musi być dostosowana do zmieniającego się środowiska technologicznego. Konieczna jest jasna i elastyczna charakterystyka, która umożliwi odpowiednie przypisanie autorstwa oraz odpowiedzialności, również w przypadkach, gdy sztuczna inteligencja rozwija się i działa w sposób, który nie był całkowicie przewidywalny w chwili jej stworzenia[286].

Niniejsza dysertacja ma na celu ustalenie rozwiązań prawnych umożliwiających klarowne określenie odpowiedzialności oraz skutków prawnych działań twórcy SI, co jest istotne dla tworzenia bezpiecznych i etycznie odpowiedzialnych systemów SI.

6.2 Rola i odpowiedzialność twórcy w procesie tworzenia i wdrażania sztucznej inteligencji

Twórca sztucznej inteligencji, czy to jednostka indywidualna, czy zespół o różnorodnych kompetencjach, pełni kluczową rolę w procesie kreacji i wdrażania technologii SI. Jego obowiązki obejmują nie tylko kwestie techniczne, lecz także rozważania dotyczące etyki

https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2020.00086/full (dostęp: 10.06.2024 r.).

[284] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.

[285] Abbott R., Sarch A. F., *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, "UC Davis Law Review" 2019, Vol. 53, s. 323.

[286] Solum Lawrence B., *Legal Personhood for Artificial Intelligences*, "North Carolina Law Review" 1992.

i prawa, mające na celu zapewnienie, że systemy SI będą działać w sposób bezpieczny i zgodny z obowiązującymi standardami[287]. Sztuczna inteligencja przekształca wiele obszarów naszego życia od biznesu po medycynę, edukację i rozrywkę. Twórcy tych zaawansowanych technologii ponoszą odpowiedzialność za zapewnienie nie tylko ich projektowania i implementacji, ale również ich funkcjonowania w realnym świecie. To właśnie twórcy sztucznej inteligencji stanowią fundament bezpiecznego i etycznego wprowadzenia tych systemów do naszego społeczeństwa[288].

Rola twórcy to:

1. projektant i programista -twórca sztucznej inteligencji wprowadza podstawy systemów AI, począwszy od doboru modeli i technik, a skończywszy na programowaniu i optymalizacji kodu, celem zapewnienia ich skuteczności i precyzji;

2. badacz i innowator - twórca powinien być na bieżąco z aktualnymi trendami i zmianami, ciągle poszerzając horyzonty możliwości sztucznej inteligencji oraz odkrywając nowe dziedziny zastosowań technologii;

3. tester i ewaluator - twórcy mają obowiązek sprawdzać działanie systemów sztucznej inteligencji, oceniać ich skuteczność oraz identyfikować ewentualne błędy w celu ciągłego doskonalenia technologii;

4. komunikator - współpraca i komunikacja zespołowa oraz kontakt z klientami i użytkownikami końcowymi odgrywają kluczową rolę w zrozumieniu i efektywnym wykorzystaniu systemów sztucznej inteligencji;

Jeśli chodzi o zakres odpowiedzialności to twórca sztucznej inteligencji ma obowiązek zaprojektować system w taki sposób, aby zminimalizować ryzyko szkodliwych działań i zagwarantować zgodność z normami etycznymi i prawnymi. To oznacza wprowadzenie procedur walidacji i testowania, które mogą wykryć oraz zapobiec potencjalnym błędom lub nadużyciom[289].

[287] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[288] Naik N., Hameed B.M.Z., Shetty D.K., Swain D., Shah M., Paul R., Aggarwal K., Ibrahim S., Patil V., Smriti K., Shetty S., Rai B.P., Chlosta P. & Somani B.K., *Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?*, Frontiers in Surgery, https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322/full, (dostęp: 10.06.2024 r.).
[289] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.

Możemy wyróżnić:

1. etyczną odpowiedzialność - twórcy sztucznej inteligencji powinni mieć świadomość moralnych konsekwencji swojej pracy, starając się rozwijać systemy sprawiedliwe, przejrzyste, pozbawione dyskryminacji i respektujące prywatność użytkowników. Etyczne podejście do projektowania SI ma także na celu promowanie dobra ogólnego i zapobieganie ewentualnym szkodom społecznym[290];

2. odpowiedzialność za bezpieczeństwo - zapewnienie bezpieczeństwa systemów sztucznej inteligencji, szczególnie gdy mają one wpływ na kluczowe decyzje, takie jak te w dziedzinie medycyny czy transportu, stanowi podstawową odpowiedzialność osób je tworzących;

3. odpowiedzialność prawna - kreatorzy sztucznej inteligencji muszą pamiętać, że ich praca podlega przepisom prawnym. Ignorowanie tych regulacji może prowadzić do konsekwencji prawnych;

4. odpowiedzialność społeczna - twórcy sztucznej inteligencji mają obowiązek społeczny za wpływ, jaki ich technologia wywiera na jednostki i społeczności, w których jest używana.

6.3 Bezpieczeństwo i cyberbezpieczeństwo w procesie tworzenia sztucznej inteligencji

W dziedzinie prawnych kwestii związanych z technologią sztucznej inteligencji, staje się istotne pytanie o bezpieczeństwo i cyberbezpieczeństwo dla twórców tych systemów. Ważne jest ustalenie odpowiednich standardów bezpieczeństwa oraz sposobów zapewnienia, że systemy SI są odporne na ataki i nie będą używane w sposób szkodliwy lub sprzeczny z przepisami prawa.

A tak się przedstawiają standardy bezpieczeństwa i cyberbezpieczeństwa dla twórców SI:

[290] Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.

1. wdrożenie protokołów bezpieczeństwa: - zastosowanie zaawansowanych protokołów szyfrowania i zabezpieczeń sieciowych jest zgodne z sugestiami ekspertów zajmujących się cyberbezpieczeństwem[291];

2. ocena ryzyka i zarządzanie - regularne analizy ryzyka są uznawane za najskuteczniejszą metodę w identyfikowaniu i zabezpieczaniu przed ewentualnymi zagrożeniami[292].

3. audyt i monitorowanie - audyty dotyczące bezpieczeństwa powinny być realizowane zgodnie z międzynarodowymi normami, takimi jak te określone przez ISO/IEC 27001[293];

4. szkolenie i świadomość - wzrost świadomości i umiejętności w dziedzinie bezpieczeństwa cybernetycznego odgrywa istotną rolę w zapewnieniu ochrony dla systemów informatycznych[294].

5. współpraca międzysektorowa - partnerstwa dotyczące bezpieczeństwa mogą zwiększyć odporność na ataki cybernetyczne[295].

6. prawne ramy odpowiedzialności - prawo powinno precyzyjnie określać odpowiedzialność twórców sztucznej inteligencji, zgodnie z zaleceniami zawartymi w dokumencie „*Biała Księga na temat Sztucznej Inteligencji: europejskie podejście do doskonałości i zaufania*”[296];

7. reakcja na incydenty - planowanie odpowiedzi na incydenty stanowi kluczowy element efektywnego zarządzania bezpieczeństwem w cyberprzestrzeni[297].

Standardy bezpieczeństwa i ochrony cyfrowej dla programistów sztucznej inteligencji są kluczowym elementem procesu tworzenia systemów bezpiecznych i niezawodnych. Prawo

[291] Smith J., *Cybersecurity: Best Practices and Strategies for the Modern World*, CyberTech Publishing 2018.
[292] Johnson L., *Risk Management in Software Development and Software Engineering Projects*, “TechWorld Association” 2019.
[293] International Organization for Standardization, *ISO/IEC 27001 Information security management*, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (dostęp: 10.06.2024 r.).
[294] Taylor H., *Building a Culture of Cybersecurity Awareness*, InfoSec Institute 2020.
[295] Miller R.*, Collaborative Cybersecurity: Building Effective Alliances in a Fragmented Environment*, Strategic Forum 2017.
[296] European Commission, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (dostęp: 10.06.2024 r.).
[297] Greenwood D., *Incident Response in the Age of Cloud*, “Data Protection Leader” 2021.

karne ma na celu nie tylko wymierzanie kar, ale także kształtowanie działań prewencyjnych, zapewniających wysoki poziom ochrony przed zagrożeniami cybernetycznymi.

6.4 Etyczne i prawne aspekty tworzenia sztucznej inteligencji

Etyczne i prawne aspekty tworzenia sztucznej inteligencji mają kluczowe znaczenie dla całego procesu jej rozwoju i wdrożenia. W kontekście tego zagadnienia, uwaga skupi się na podstawowych zasadach i wytycznych, które powinny kierować twórcami SI, aby ich praca była zgodna z przepisami prawnymi i normami etycznymi, a technologia przynosiła korzyści społeczeństwu, nie naruszając jednocześnie praw jednostek.

Kluczowym elementem jest zrozumienie, jak te technologie mogą być odpowiedzialnie rozwijane i wdrażane, aby zagwarantować ich pozytywny wpływ na różne aspekty życia społecznego. W związku z tym, poniżej przedstawiono najważniejsze etyczne aspekty, które powinny być brane pod uwagę przy tworzeniu i wdrażaniu systemów sztucznej inteligencji:

1. transparentność decyzji SI - użytkownicy powinni mieć dostęp do informacji dotyczących funkcjonowania algorytmów sztucznej inteligencji. Jest to istotne dla zrozumienia, w jaki sposób systemy SI podejmują decyzje, co wpływa bezpośrednio na kwestie odpowiedzialności i zaufania;

2. sprawiedliwość i niedyskryminacja - algorytmy sztucznej inteligencji powinny być pozbawione wszelkich uprzedzeń, które mogą prowadzić do dyskryminacji ze względu na rasę, płeć, wiek lub inne czynniki. Ważne jest rozwijanie metod wykrywania i eliminowania ukrytych form stronniczości;

3. prywatność i bezpieczeństwo danych - ochrona prywatności jest niezwykle ważna, szczególnie w przypadku gromadzenia, przetwarzania i wykorzystywania informacji przez systemy sztucznej inteligencji. Ważne jest, aby korzystać z solidnych protokołów szyfrowania oraz innych środków zabezpieczenia danych[298].

Aby skutecznie wdrożyć systemy sztucznej inteligencji w zgodzie z obowiązującymi przepisami prawa, konieczne jest uwzględnienie wielu kluczowych aspektów prawnych.

[298] Kamila, M. K., & Jasrotia, S. S.*, Ethical issues in the development of artificial intelligence: recognizing the risks.* International Journal of Ethics and Systems, https://doi.org/10.1108/IJOES-05-2023-0107 (dostęp: 10.06.2024 r.).

Poniżej przedstawiono najważniejsze z nich, które twórcy SI powinni brać pod uwagę, aby zapewnić zgodność z regulacjami oraz zminimalizować ryzyko prawne:

1. regulacje dotyczące SI - rozwój oraz wdrożenie sztucznej inteligencji powinny odbywać się z uwzględnieniem obowiązujących przepisów prawa, takich jak RODO[299] w Unii Europejskiej. Konieczna jest również ocena, czy aktualne ustawodawstwo odpowiednio reaguje na nowe wyzwania związane ze sztuczną inteligencją[300]?

2. odpowiedzialność karna twórców - należy dokładnie określić ramy prawne, które regulują odpowiedzialność karną twórców sztucznej inteligencji za ewentualne szkody spowodowane przez ich systemy. To oznacza konieczność przewidzenia potencjalnych nadużyć i ich zapobiegania[301];

3. prawne ramy własności intelektualnej - w kontekście sztucznej inteligencji istotne jest zrozumienie i kontrola problematyki praw autorskich, zarówno w przypadku twórców, jak i dzieł stworzonych przez SI[302].

W tym kontekście ważnym jest, aby twórcy sztucznej inteligencji lub powołana organizacja zrzeszająca twórców ustanowili kodeks postępowania, który obejmie zasady etyczne i prawne dotyczące projektowania i wdrażania SI[303]. Taki kodeks może stanowić podstawę dla najlepszych praktyk w przemyśle oraz być wskazówką dla twórców na całym świecie[304]. Należy przy tym pamiętać, że tworzenie systemów sztucznej inteligencji wymaga współpracy specjalistów z różnych dziedzin - od inżynierów po etyków i prawników. Taka interdyscyplinarna strategia jest konieczna, aby uwzględnić wszystkie aspekty tworzenia SI

[299] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

[300] Church P., *AI & the GDPR: Regulating the minds of machines, Linklaters,* https://www.linklaters.com/en/insights/blogs/digilinks/ai-and-the-gdpr-regulating-the-minds-of-machines (dostęp: 10.06.2024 r.).

[301] Hallevy G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, "Akron Intellectual Property Journal" *https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1* (dostęp: 10.06.2024 r.).

[302] Zirpoli Ch.T., *Generative Artificial Intelligence and Copyright Law,* CRS Reports, https://crsreports.congress.gov/product/pdf/LSB/LSB10922 (dostęp: 10.06.2024 r.).

[303] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition*, IEEE, s. 5, https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html (dostęp: 13.06.2023).

[304] Google, *Artificial Intelligence at Google: Our Principles*, https://ai.google/principles/ (dostęp: 13.06.2023).

i zagwarantować jej korzystny wpływ na społeczeństwo[305]. Wyzwaniem związanym z powyższym jest ciągłe dostosowywanie regulacji prawnych, aby być na bieżąco z dynamicznym rozwojem technologii sztucznej inteligencji. Wymaga to gotowości prawników, regulatorów i polityków do szybkiej reakcji i dostosowania się do nowych wyzwań technologicznych[306].

Podsumowując, kwestie etyczne i prawne związane z rozwojem sztucznej inteligencji są kluczowe dla zapewnienia zrównoważonego postępu tej technologii. Poprzez ustalanie klarownych norm etycznych i prawnych oraz wprowadzanie odpowiednich regulacji, możliwe jest zagwarantowanie, że SI będzie służyła dobru wszystkich użytkowników, jednocześnie respektując ich prywatność i inne prawa człowieka.

[305] European Commission, *Ethics guidelines for trustworthy AI*, High-Level Expert Group on Artificial Intelligence, s. 5, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, (dostęp: 13.06.2023).

[306] Modgil S., *Beyond silos: Why AI Regulation calls for an Interdisciplinary Approach,* King's College London, https://nms.kcl.ac.uk/sanjay.modgil/BeyondSilos.pdf (dostęp: 10.06.2024 r.).

Rozdział VII. Analiza wybranych przypadków zastosowania sztucznej inteligencji i ich prawnokarnych konsekwencji

W obliczu szybkiego rozwoju technologii sztucznej inteligencji, prawo karne staje w obliczu wyzwań, których dotychczas brakowało. Wykorzystanie SI w różnych dziedzinach życia generuje nowe formy zachowań i interakcji, które mogą mieć poważne konsekwencje z punktu widzenia prawa karnego. Dlatego tak istotne jest przeprowadzenie dogłębnej analizy studiów przypadków, które rzucą światło na specyfikę tych interakcji oraz wynikające z nich wyzwania dla systemu prawnego.

Ten rozdział ma na celu zbadanie i wyjaśnienie konkretnych przypadków wykorzystania sztucznej inteligencji, które doprowadziły do konsekwencji prawnokarnych. Przyglądając się realnym sytuacjom, w których systemy SI miały wpływ na powstanie szkód, naruszeń prawa czy nawet popełnienie przestępstw, będziemy poszukiwać odpowiedzi na pytania dotyczące odpowiedzialności, winy oraz możliwości przewidywania skutków działań technologii SI.

Przyjmując to zadanie, polegam na gruntownej analizie i interpretacji dostępnych raportów, orzeczeń sądowych oraz badań naukowych. Istotne będą zarówno aspekty technologiczne, jak i prawne, etyczne oraz społeczne. Takie zróżnicowane podejście pozwoli mi ocenić, w jaki sposób obecne ramy prawne radzą sobie z wyzwaniami wynikającymi ze sztucznej inteligencji.

Celem tego rozdziału jest:

- analiza głównych wyzwań prawnokarnych związanych z wykorzystaniem sztucznej inteligencji;
- przebadanie realnych przypadków, w których działania sztucznej inteligencji miały skutki prawne;
- analiza i ocena tych sytuacji z uwzględnieniem aktualnych przepisów prawnych, uwzględniając kwestie odpowiedzialności i winy.

Z uwagi na istotny wpływ sztucznej inteligencji na społeczeństwo i prawo, wybór konkretnych obszarów do badania był motywowany ich aktualnością, wartością naukową oraz znaczącym wpływem na praktykę prawniczą i funkcjonowanie systemu prawnego.

Wybrane do szczegółowego opracowania obszary to:

1. autonomiczne samochody - uwagi na możliwość zmiany infrastruktury transportowej oraz trudności związane z odpowiedzialnością za wypadki drogowe;

2. medycyna - w jaki sposób wykorzystanie sztucznej inteligencji w diagnostyce może doprowadzić do pomyłek medycznych i dlaczego zrozumienie odpowiedzialności prawnej za te błędy jest kluczowe dla ochrony pacjentów;

3. cyberbezpieczeństwo - obszar ten ma duże znaczenie ze względu na wzrastające zagrożenie wykorzystaniem sztucznej inteligencji w celach przestępczych, a także dla zapewnienia bezpieczeństwa danych i systemów komputerowych;

4. systemy rekrutacyjne - zastosowanie sztucznej inteligencji w procesach rekrutacji pracowników budzi obawy dotyczące dyskryminacji i równości w dostępie do pracy;

5. asystenci wirtualni - tworzą one nowe trudności w obszarze ochrony prywatności i danych osobowych, gdzie granice legalnego nadzoru i kontroli są regularnie poddawane testom;

6. SI w wymiarze sprawiedliwości - rozważanie roli sztucznej inteligencji w procesach sądowych i śledczych, gdzie decyzje maszyn mogą mieć znaczący wpływ na decyzje prawne i karne;

7. SI i manipulacja informacjami - badanie sytuacji, w których sztuczna inteligencja została wykorzystana do celowego formułowania opinii publicznej lub manipulowania informacją, stawia przed nami nowe wyzwania w zakresie ochrony prawnej przed dezinformacją i fałszywymi wiadomościami[307].

Każdy z tych obszarów jest analizowany pod kątem możliwych przypadków prawnokarnych, które już miały miejsce lub mogą wystąpić w przyszłości. Studia przypadków zostały starannie dobrane, aby ukazać pełen zakres problemów - od usterek systemowych i awarii po świadome działania przestępcze. Zawsze zwraca autorka uwagę na to, jak obecne przepisy radzą sobie z nowymi wyzwaniami oraz jakie zmiany legislacyjne mogą być konieczne do sprostania przyszłym potrzebom.

[307] Karinshak E., Jin Y., *AI-driven disinformation: a framework for organizational preparation and response,* Journal of Communication Management*, https://doi.org/10.1108/JCOM-09-2022-0113* (dostęp: 10.06.2024 r.).

7.1 Autonomiczne samochody

Rozwój technologii samochodów autonomicznych to jeden z najbardziej innowacyjnych przykładów wykorzystania sztucznej inteligencji, który nie tylko zmienia przemysł motoryzacyjny, ale także rewolucjonizuje podejście do kwestii bezpieczeństwa, odpowiedzialności i regulacji prawnych. Analizy w tej dziedzinie skupiają się głównie na problemach prawnych pojawiających się w kontekście wypadków drogowych z udziałem autonomicznych pojazdów.

W aspekcie odpowiedzialności tradycyjne ramy prawne opierają się na przekonaniu, że za działanie pojazdu odpowiada kierowca, czyli osoba fizyczna. Jednak w przypadku, gdy decyzje są podejmowane przez algorytmy, konieczne staje się przeanalizowanie kwestii odpowiedzialności oraz wprowadzenie nowych rozwiązań prawnych dostosowanych do tej technologii[308].

Biorąc pod uwagę kwestie związane z bezpieczeństwem, regulacje dotyczące testowania i wprowadzania samochodów autonomicznych na drogi muszą zapewnić najwyższe standardy bezpieczeństwa. Incydenty z udziałem autonomicznych pojazdów, które miały miejsce, są analizowane pod kątem zasad ich certyfikacji i dopuszczenia do użytku[309].

Skomplikowane dylematy etyczne systemów sztucznej inteligencji odpowiedzialnych za sterowanie pojazdami, znane są jako „*dylematy wagonika*" (ang. trolley problem), które mają i będą mieć wpływ na potencjalne konsekwencje prawne[310].

Badanie tych zagadnień w kontekście prawa karnego wymaga holistycznego podejścia, które łączy w sobie wiedzę z zakresu prawa, etyki, technologii i inżynierii. Analiza przypadków praktycznych ma na celu nie tylko rozważenie konkretnych sytuacji, ale także zrozumienie szerszego wpływu, jaki autonomiczne samochody mają na system prawny.

[308] Smith B. W., *Automated Vehicles Are Probably Legal in the United States*, "Texas A&M Law Review" 2012.
[309] Marchant G. E., Lindor R. A., *The Coming Collision Between Autonomous Vehicles and the Liability System*, "Santa Clara Law Review" 2015 Vol. 55, No. 4, s. 1321-1340.
[310] Goodall N.J., *Machine ethics and automated vehicles*, w: *Road Vehicle Automation*, red. Gereon Meyer, Springer 2014, s. 93-102.

7.1.1 Analiza pierwszego śmiertelnego wypadku z udziałem autonomicznego samochodu

W maju 2016 roku miało miejsce pierwsze śmiertelne zdarzenie związane z autonomicznym pojazdem, które wpłynęło znacząco na spojrzenie na rozwój technologii samochodów autonomicznych. Incydent ten dotyczył pojazdu marki Tesla Model S, który był w trybie autopilota podczas kolizji z ciężarówką. Kierowca Tesli, Joshua Brown, stracił życie w wyniku tego zdarzenia[311]. Ta tragiczna sytuacja wywołała debatę na temat bezpieczeństwa, odpowiedzialności oraz przyszłości technologii autonomicznych pojazdów.

Wypadek miał miejsce na autostradzie na Florydzie. System automatycznego pilota Tesli nie zdołał rozróżnić białej ciężarówki od jasnego nieba, co spowodowało brak reakcji i zastosowania hamowania. Firma Tesla podkreśliła, że był to jedyny przypadek śmiertelny w 130 milionach przejechanych mil w trybie autopilota, co pokazuje rzadkość takich incydentów w porównaniu do ogólnych statystyk (jedna śmierć na 94 miliony przejechanych mil). Mimo to wypadek ten podkreślił, że technologia autopilota jest nadal w fazie testów beta i wymaga od kierowców stałej uwagi[312].

Wypadek spowodował dyskusję na temat odpowiedzialności za kolizje z udziałem samochodów autonomicznych. Mimo że Tesla podkreśla, że system autopilota pełni jedynie funkcję wspomagającą i wymaga, aby kierowcy mieli ręce na kierownicy, pojawiają się wątpliwości dotyczące tego, jak daleko można ufać technologii oraz jaka jest rola kierowcy w monitorowaniu autonomicznego pojazdu. Ponadto incydent ten zwrócił uwagę na fakt, że kierowca nie skupiał się na drodze, co mogło przyczynić się do zdarzenia[313].

Po zakończeniu półrocznego dochodzenia dotyczącego wypadku Tesli Model S z 2016 roku, w którym zginął Joshua Brown, NHTSA (National Highway Traffic Safety Administration) stwierdziła, że system Autopilota nie ponosił winy za ten incydent. Oceniła, że to kierowca był odpowiedzialny za to wydarzenie. Badanie wykazało także, że od wprowadzenia Autopilota wskaźnik wypadków dla samochodów Tesla zmniejszył się o niemal 40%. W raporcie

[311] Brown A., *Tesla Autopilot Crash Victim Joshua Brown Was an Electric Car Buff and a Navy SEAL,* The Drive, https://www.thedrive.com/news/4249/tesla-autopilot-crash-victim-joshua-brown-was-an-electric-car-buff-and-a-navy-seal (dostęp: 10.06.2024 r.).

[312] Klein A., *Tesla driver dies in first fatal autonomous car crash in US*, New Scientist, https://www.newscientist.com/article/2095740-tesla-driver-dies-in-first-fatal-autonomous-car-crash-in-us/ (dostęp: 10.06.2024 r.).

[313] Schaffer S.*, Will the Autonomous Car Industry Survive Autopilot's First Fatal Crash?, All About Circuits,* https://www.allaboutcircuits.com/news/self-driving-cars-tesla-model-s-fatal-crash/ (dostęp: 10.06.2024 r.).

pochwalono Teslę za sposób, w jaki przewidziała potencjalne nieprawidłowe użycie Autopilota i uwzględniła te rezultaty podczas opracowywania funkcji systemu przed jego wprowadzeniem na rynek[314].

Ten incydent skłonił do refleksji na temat regulacji prawnych związanych z technologiami autonomicznymi. Istnieje konieczność stworzenia nowych rodzajów przepisów, które będą nadzorować skutki działań autonomicznych pojazdów. To wydarzenie podkreśliło także potrzebę jasnego określenia roli i odpowiedzialności kierowcy w kontekście wykorzystania systemów autonomicznych w samochodach.

Na skalę globalną, wypadki podkreślają potrzebę dalszych badań i rozwoju w obszarze bezpieczeństwa autonomicznych pojazdów. Rozwój norm i przepisów dotyczących technologii autonomicznych odgrywa kluczową rolę w przyszłym wprowadzeniu tych systemów. Podobne zdarzenia skłaniają do zastanowienia się nad stopniami autonomii pojazdów oraz ich wpływem na bezpieczeństwo drogowe. Przemysł motoryzacyjny oraz organy regulacyjne muszą współpracować, aby zapewnić, że pojazdy autonomiczne będą mogły bezpiecznie współistnieć z tradycyjnymi pojazdami i kierowcami[315].

Pierwsza tragiczna kolizja z udziałem autonomicznego pojazdu wyznacza istotny moment w analizie rozwoju i problemów związanych z technologią samochodów autonomicznych. Podkreśla ona konieczność ciągłego monitorowania, testowania i doskonalenia technologii, a także potrzebę dostosowania przepisów prawnych do nowych realiów technologicznych. Incydenty takie jak ten z samochodem Tesla Model S stanowią przypomnienie o skomplikowanych wyzwaniach stojących przed autonomicznymi pojazdami oraz ich potencjalnym wpływie na przyszłość mobilności.

7.1.2 Analiza sprawy śmiertelnego wypadku z wykorzystaniem auta autonomicznego Tesli z 2019 roku

W 2019 roku doszło do tragicznego incydentu z udziałem pojazdu Tesli Model 3, który wywołał dyskusję na temat bezpieczeństwa i odpowiedzialności związanej z technologią

[314] Bonnington C., *NHTSA Finds Tesla Not at Fault in 2016 Autopilot Crash*, Daily Dot, https://www.dailydot.com/debug/nets-results-tesla-autopilot-crash-investigation/ (dostęp: 10.06.2024 r.).

[315] Shoemaker N., *Here's What We Know about Tesla's First Fatal Crash*, Big Think, https://bigthink.com/technology-innovation/heres-what-we-know-about-teslas-first-fatal-crash/ (dostęp: 10.06.2024 r.).

autonomiczną. Ten incydent spowodował przeprowadzenie obszernego śledztwa w sprawie systemu autopilota Tesli, które zakończyło się istotnym procesem sądowym[316].

Micah Lee, który prowadził Teslę Model 3, zginął w tragicznym wypadku na autostradzie niedaleko Los Angeles. Jego samochód, poruszający się z prędkością 65 mil na godzinę, nagle zboczył z drogi i uderzył w palmę, po czym stanął w płomieniach. W wyniku tego zdarzenia poważne obrażenia odniosły także dwie osoby podróżujące razem z nim, w tym 8-letni chłopiec[317].

Proces skupiał się na określeniu, czy system autopilota miał wady i czy firma Tesla była świadoma potencjalnych zagrożeń związanych z jego wykorzystaniem przed wypadkiem. Sędzia początkowo orzekł, że istnieją „*uzasadnione dowody*" na to, że kierownictwo Tesli świadomie dopuściło do niebezpiecznego użytkowania swojej technologii.

Analiza pierwszego tragicznego incydentu z udziałem autonomicznego pojazdu marki Tesla skupia się na sprawie sądowej, która została rozstrzygnięta przez sąd w Riverside County Superior Court. Sprawa dotyczyła zdarzenia z 2019 roku, w którym Micah Lee stracił życie, gdy jego pojazd Tesla Model 3 zjechał z autostrady i uderzył w palmę, co spowodowało śmiertelne obrażenia dla Lee oraz poważne rany dwóch pasażerów. Kluczowym elementem procesu było ustalenie czy system Autopilota Tesli miał jakąkolwiek usterkę produkcyjną, która mogła przyczynić się do tego tragicznego wypadku. Poszkodowani pasażerowie domagali się 400 milionów dolarów odszkodowania za cierpienia fizyczne i psychiczne oraz stratę życia kierowcy[318].

Sąd w Riverside zdecydował na korzyść Tesli, oświadczając, że pojazd nie posiadał żadnych wad produkcyjnych. Po czterodniowych naradach wydano werdykt, który zakończył się głosowaniem 9 do 3 na korzyść Tesli. W trakcie procesu Tesla argumentowała, że kierowca

---

316 Higgins T., *Tesla wins first US Autopilot trial involving fatal crash*, CNBC, https://www.cnbc.com/2023/10/31/tesla-wins-first-us-autopilot-trial-involving-fatal-crash.html (dostęp: 10.06.2024 r.).

317 Gilboy J., *Judge Rules Tesla Knew of Autopilot Dangers Before 2019 Fatal Crash, But Did Nothing*, The Drive, https://www.thedrive.com/news/judge-rules-tesla-knew-of-autopilot-dangers-before-2019-fatal-crash-but-did-nothing (dostęp: 10.06.2024 r.).

318 Macdonald Ch., *Tesla's Autopilot was not to blame for fatal 2019 Model 3 crash, jury finds*, Engadget, https://www.engadget.com/teslas-autopilot-was-not-to-blame-for-fatal-2019-model-3-crash-jury-finds-210643301.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAACf82OlZRHyk_qdet8M9oAOaVHt7KTSPNWmVRG15lgUsQf2w1uStt0hrPnm_ikmOlaRh88o-vMkqkO-vB82eDNekGlm7getbxSjUAxzWbZtmqXN4tyLvyNz4N25PjSB5PUikpyZKkExv7LYpXFgRtIkYS9Ls3LGYYfreGDXu1PtK (dostęp: 10.06.2024 r.).

powinien zachować czujność i kontrolę nad pojazdem nawet podczas aktywnego systemu Autopilota. Firma podkreślała również niejasność co do tego, czy Autopilot był aktywny w chwili wypadku oraz zwracała uwagę na fakt, że Lee spożywał alkohol przed prowadzeniem[319].

To stwierdzenie dowodzi, że argumenty Tesli stają się coraz bardziej istotne: gdy dochodzi do sytuacji niebezpiecznej na drodze, ostateczna odpowiedzialność leży po stronie kierowców. Sprawa ta była pierwszym procesem w Stanach Zjednoczonych, który dotyczył zarzutów, że funkcja asystenta kierowcy Autopilot przyczyniła się do śmierci, co stanowi istotny punkt odniesienia dla przyszłych spraw prawnych związanych z technologią autonomiczną.

W kontekście prawa i regulacji, ta kwestia podkreśla istotę klarownych zasad dotyczących odpowiedzialności za wypadki z udziałem samochodów autonomicznych oraz konieczność dalszych badań nad bezpieczeństwem i skutecznością tych technologii[320].

Ten incydent rzucił światło na istotne kwestie związane z bezpieczeństwem pojazdów autonomicznych i rolą producentów w informowaniu o możliwościach oraz ograniczeniach ich systemów. Wypadek i wynikający z niego proces podkreślają konieczność klarownych przepisów regulacyjnych dotyczących technologii autonomicznych, a także odpowiedzialności kierowców i producentów w kontekście ich stosowania.

W kontekście prawno-regulacyjnym, ta sprawa podnosi istotne kwestie dotyczące sposobu, w jaki technologie autonomiczne są promowane i postrzegane przez klientów, a także jakie są oczekiwania co do ich bezpieczeństwa i efektywności. Zarówno producenci, jak i organy regulacyjne stoją przed zadaniem zapewnienia, że postęp technologiczny w dziedzinie pojazdów autonomicznych idzie w parze z ochroną konsumentów i bezpieczeństwem publicznym.

---

[319] Levine D., Jin H., *Tesla wins Autopilot trial involving fatal crash*, Reuters, https://www.reuters.com/business/autos-transportation/tesla-wins-autopilot-trial-involving-fatal-crash-2023-10-31/ (dostęp: 10.06.2024 r.).

[320] Macdonald Ch., *Tesla's Autopilot was not to blame for fatal 2019 Model 3 crash, jury finds*, Engadget, https://www.engadget.com/teslas-autopilot-was-not-to-blame-for-fatal-2019-model-3-crash-jury-finds-210643301.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAACf82OlZRHyk_qdet8M9oAOaVHt7KTSPNWmVRG15lgUsQf2w1uStt0hrPnm_ikmOlaRh88o-vMkqkO-vB82eDNekGlm7getbxSjUAxzWbZtmqXN4tyLvyNz4N25PjSB5PUikpyZKkExv7LYpXFgRtIkYS9Ls3LGYYfreGDXu1PtK (dostęp: 10.06.2024 r.).

Ten konkretny przypadek jest istotnym momentem w debacie na temat przyszłości transportu autonomicznego i ustanawia punkt odniesienia dla przyszłych spraw prawnych związanych z technologią autonomiczną.

7.1.3 Analiza sprawy śmiertelnego wypadku z wykorzystaniem auta autonomicznego Uber

W marcu 2018 roku w Tempe, w stanie Arizona, miało miejsce pierwsze odnotowane zdarzenie śmiertelnego potrącenia pieszego przez samochód autonomiczny. Elaine Herzberg, przemieszczając się na rowerze przez ulicę, została uderzona przez pojazd Uber działający w trybie autonomicznym. Kierowca bezpieczeństwa Ubera był obecny, ale nie zareagował, ponieważ skupił się na obserwacji innych rzeczy wewnątrz pojazdu[321].

Sąd w Tempe opublikował nagranie wideo z dwóch kamer umieszczonych w pojeździe: jednej skierowanej do przodu i drugiej rejestrującej zachowanie kierowcy odpowiedzialnego za bezpieczeństwo. Na nagraniu widać, że auto poruszało się prawym pasem, gdy doszło do zderzenia z Herzbergiem. Kierowca ds. bezpieczeństwa przyznał później, że patrzył na ekran konsoli środkowej tuż przed kolizją.

Wypadek miał miejsce na jednej z ulic Tempe w Arizonie, podczas nocy. Oświetlenie na drodze było dostateczne, a warunki pogodowe sprzyjające.

Po przeprowadzeniu wstępnych dochodzeń, Narodowa Rada Bezpieczeństwa Transportu (NTSB) ustaliła, że główną przyczyną zdarzenia było niedbalstwo pracownika ds. bezpieczeństwa, który nie skupiał się na drodze i zajmował się telefonem komórkowym tuż przed kolizją. Uber otrzymał również krytykę za brak wystarczających procedur bezpieczeństwa i nadzoru nad pracownikami. Sprawa podniosła kwestię odpowiedzialności w przypadkach wypadków z udziałem samochodów autonomicznych - czy winę ponosić maszynę, operatora pojazdu czy firmę zarządzającą systemem[322].

Sprawa związana z wypadkiem samochodu autonomicznego Ubera w Tempe, Arizona, skończyła się dla Rafaeli Vasquez, operatora bezpieczeństwa, oskarżeniem o nieumyślne spowodowanie śmierci. Śledztwo wykazało, że w chwili zdarzenia Vasquez nie nadzorowała

321 Death of Elaine Herzberg, Wikipedia, https://en.wikipedia.org/wiki/Death_of_Elaine_Herzberg (dostęp: 10.06.2024 r.).

322 Bellon T., *Liability and Legal Questions Follow Uber Autonomous Car Fatal Accident*, Insurance Journal, https://www.insurancejournal.com/news/national/2018/03/20/483981.htm (dostęp: 10.06.2024 r.).

drogi ani nie zwracała uwagi na ruch drogowy ze względu na korzystanie z telefonu komórkowego. W marcu 2021 roku Vasquez została oskarżona o nieumyślne spowodowanie śmierci, co podkreśla wagę ludzkiego nadzoru podczas testowania i eksploatacji pojazdów autonomicznych, nawet gdy technologia przejmuje kontrolę nad pojazdem.

Ta decyzja ma duże znaczenie, gdyż podkreśla, że operatorzy pojazdów autonomicznych są odpowiedzialni za zachowanie należytej ostrożności i uwagi podczas nadzorowania działania technologii. To wydarzenie stawia także wiele pytań dotyczących bezpieczeństwa, regulacji i odpowiedzialności w związku z szybkim rozwojem technologii pojazdów autonomicznych.

Ta sprawa spowodowała intensywne dyskusje na temat przepisów dotyczących testowania i użytkowania samochodów autonomicznych, zarówno na poziomie stanowym, jak i federalnym w USA. Podniosła także kwestie związane z odpowiedzialnością prawną w przypadku awarii systemów autonomicznych oraz koniecznością ustalenia klarownych wytycznych dotyczących nadzorowania tych systemów przez ludzkich operatorów.

7.1.4 Dyskusja akademicka na temat SI w samochodach autonomicznych i konsekwencje prawne

Wprowadzenie autonomicznych samochodów na rynek motoryzacyjny jest tematem, który przyciąga duże zainteresowanie wśród badaczy i środowiska akademickiego, skupiając się na różnych aspektach technologicznych, etycznych i prawnych[323]. Jednym z kluczowych zagadnień poruszanych w tych dyskusjach jest kwestia odpowiedzialności prawnej w sytuacjach wypadków i incydentów z udziałem autonomicznych pojazdów.

Analiza literatury przedmiotu wskazuje na potrzebę dostosowania aktualnych przepisów prawnych, aby uwzględniały specyfikę funkcjonowania sztucznej inteligencji w samochodach autonomicznych[324]. Obecnie prawo nakłada odpowiedzialność za kolizje drogowe bezpośrednio na kierowcę, jednak w kontekście samochodów autonomicznych linia odpowiedzialności staje się mniej wyraźna. Rozważane są propozycje takie jak rozproszona czy zbiorowa odpowiedzialność, obejmująca producentów pojazdów, programistów oraz użytkowników[325].

[323] Smith B. W., *Automated Vehicles Are Probably Legal in the United States*, "Texas A&M Law Review" 2012.
[324] Marchant G. E., Lindor R. A., *The Coming Collision Between Autonomous Vehicles and the Liability System*, "Santa Clara Law Review" 2015, Vol. 55, No. 4, s. 1321-1340.
[325] Calo R., *Robotics and the Lessons of Cyberlaw*, "California Law Review" 2015, Vol. 103.

Tymczasem dyskusje dotyczące etyki koncentrują się na decyzjach, które sztuczna inteligencja musi podejmować, zwłaszcza w sytuacjach kryzysowych, gdzie konieczne jest wybranie „*mniejszego zła*". Wymaga to stworzenia algorytmów decyzyjnych, które będą potrafiły radzić sobie z dylematami etycznymi w sposób akceptowalny dla społeczeństwa[326].

Na arenie międzynarodowej pojawiły się propozycje wprowadzenia ustalonych regulacji, mających na celu zapewnienie bezpiecznego użytkowania i eksploatacji pojazdów autonomicznych. Warto wspomnieć o pracach prowadzonych przez Komisję Europejską nad „*Aktem dotyczącym Sztucznej Inteligencji*", który proponuje klasyfikację ryzyka oraz odpowiednie ramy prawne dla SI, w tym dla autonomicznych pojazdów[327].

7.2 Medycyna

Zastosowanie sztucznej inteligencji w dziedzinie medycyny otwiera nowe możliwości w zakresie diagnozowania, leczenia oraz badania nowych metod terapeutycznych. Niemniej jednak, równie ważne są kwestie związane z odpowiedzialnością prawną w przypadkach, gdy technologia SI przyczynia się do błędów medycznych. Celem tego fragmentu pracy jest przeanalizowanie sytuacji, w których systemy SI były używane w kontekście medycznym i miały wpływ na rezultaty leczenia, co niesie za sobą istotne konsekwencje prawne. Tymi komplikacjami są:

1. odpowiedzialność za błędy medyczne SI - w kontekście prawa, błędy w diagnozie lub prowadzeniu terapii mogą mieć znaczące skutki. Jak prawo karne powinno traktować przypadki, gdy to nie lekarz, a algorytm odpowiada za wystąpienie błędu[328]?

2. ocena ryzyka i niezawodności SI w medycynie - w medycynie kluczowe znaczenie ma precyzja i niezawodność systemów sztucznej inteligencji, które mają zapewnić bezpieczeństwo

[326] Goodall N.J., *Machine ethics and automated vehicles*, w: *Road Vehicle Automation*, red. Gereon Meyer, Springer 2014, s. 93-102.

[327] Komisja Europejska, *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*, COM(2021) 206 final, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (dostęp: 10.06.2024 r.).

[328] Price W. N. II, *Artificial Intelligence in Health Care: Applications and Legal Implications*, "The SciTech Lawyer" 2017, Vol. 13, No. 4.

pacjentów. Rozważane są przypadki, w których błędnie skonfigurowane lub źle nauczone algorytmy prowadziły do podejmowania decyzji szkodliwych dla zdrowia[329].

3. prawne implikacje autonomicznych decyzji SI - konieczne jest zrozumienie, jak obecne przepisy prawne radzą sobie z kwestią odpowiedzialności za decyzje podejmowane przez autonomiczne systemy sztucznej inteligencji, zwłaszcza w przypadku powstania szkód dla zdrowia[330].

Autorka zauważa, że na dzień stanu prawnego pracy doktorskiej nie znaleziono konkretnych przypadków czy rozstrzygnięć sądowych, w których jednoznacznie potwierdzono sytuacje, gdzie decyzja medyczna podjęta przez sztuczną inteligencję spowodowała bezpośrednie szkody zdrowotne u pacjenta i została później rozpatrzona przez system sądowniczy. Tymczasem poniżej znajdują się opisane potencjalne scenariusze oraz rozważania oparte na dotychczasowych dyskusjach naukowych i doniesieniach prasowych, które wskazują możliwe do wystąpienia sytuacje mogące powodować konflikty prawne, są nimi m.in.:

1. błędy diagnostyczne SI - Mimo postępów w poprawie dokładności algorytmów sztucznej inteligencji, ciągle istnieje ryzyko nieprawidłowego interpretowania danych medycznych, co potencjalnie może prowadzić do nieodpowiednich diagnoz lub terapii. Taka sytuacja stawia pytania dotyczące odpowiedzialności za ewentualne błędy - czy winę powinno się ponosić twórcom algorytmu, placówce medycznej wprowadzającej technologię, czy też lekarzom podejmującym decyzje na podstawie sugestii sztucznej inteligencji[331];

2. interpretowalność i zaufanie - decyzje algorytmów sztucznej inteligencji często są trudne do zinterpretowania przez lekarzy, ponieważ działają one jak „*czarne skrzynki*" (ang. black boxes). W sytuacjach, gdy zalecenia SI zawiodły i spowodowały szkodę pacjentowi, kluczowe jest zrozumienie, jak brak możliwości interpretacji i zaufania do systemu przyczynił się do popełnienia błędu[332];

[329] Gerke S., Minssen T., Cohen G., *Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare*, Artificial Intelligence in Healthcare, "Elsevier" 2020, s. 295-336.
[330] Terry N. P., *Liability for Mobile Health and Wearable Technologies*, "Annals of Health Law" 2016, Vol. 25, s. 62-81.
[331] Hall K., Fitall E., *Artificial Intelligence and Diagnostic Errors,* Agency for Healthcare Research and Quality, https://psnet.ahrq.gov/perspective/artificial-intelligence-and-diagnostic-errors (dostęp: 10.06.2024 r.).
[332] Shen M. W., *Trust in AI: Interpretability is not necessary or sufficient, while black-box interaction is necessary and sufficient*, DeepAI, https://deepai.org/publication/trust-in-ai-interpretability-is-not-necessary-or-sufficient-while-black-box-interaction-is-necessary-and-sufficient (dostęp: 10.06.2024 r.).

3. etyczne i prawne aspekty wykorzystania SI - rozważenia związane z etycznymi i prawymi aspektami wykorzystania sztucznej inteligencji w dziedzinie medycyny, takimi jak ochrona danych osobowych, zgoda na leczenie i autonomia pacjenta, są istotne. W jaki sposób systemy prawne mogą dostosować się do nowych wyzwań związanych ze sztuczną inteligencją, równoważąc innowacje z ochroną pacjentów[333]?

Można się w tym miejscu pokusić o zaobserwowaniu przez autorkę kilku potencjalnych kierunków rozwoju prawa dotyczącego sztucznej inteligencji w dziedzinie medycyny. Po pierwsze, kluczowe jest ustanowienie regulacji dotyczących certyfikacji i testowania systemów SI. Obejmuje to rozwój standardów i przepisów, które zapewnią dokładne testowanie i certyfikację systemów SI przed ich wdrożeniem w praktyce medycznej[334]. Po drugie, konieczne są jasne wytyczne dotyczące odpowiedzialności za decyzje podejmowane przy użyciu SI, w tym możliwe ubezpieczenia dla lekarzy i twórców SI[335]. Ostatecznie, inicjatywy mające na celu zwiększenie przejrzystości funkcjonowania algorytmów SI oraz edukację personelu medycznego w zakresie potencjalnych ograniczeń i zagrożeń wynikających z korzystania z tych technologii są niezbędne[336]. Te kroki są kluczowe dla budowania zaufania i zapewnienia bezpiecznej integracji SI w opiece zdrowotnej[337].

Podsumowując, wraz z rosnącym praktycznym wykorzystaniem sztucznej inteligencji w medycynie, ogromne znaczenie ma również to, aby badania prawne i etyczne nadążały za postępem, identyfikując potencjalne zagrożenia i rozwijając ramy prawne, które będą zapewniać ochronę zarówno pacjentom, jak i pracownikom służby zdrowia.

7.2.1 Dyskusja akademicka na temat SI w medycynie i konsekwencje prawne

Ważnym aspektem w obszarze medycyny jest konieczność uwzględnienia Artykułu „*Machine Vision, Medical SI, and Malpractice*" autorstwa Zacha Harneda, Matthewa P. Lungrena

[333] Sirignano A., Ricci G., *Ethical and Legal Challenges of Telemedicine in the Era of the COVID-19 Pandemic*, Medicina, https://doi.org/10.3390/medicina57121314 (dostęp: 10.06.2024 r.).

[334] U.S. Food and Drug Administration, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)*, https://www.fda.gov/media/122535/download (dostęp: 13.06.2023).

[335] European Commission, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 final, s. 18, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064, (dostęp: 13.06.2023).

[336] World Health Organization, *Ethics and governance of artificial intelligence for health*, s. 48, https://www.who.int/publications/i/item/9789240029200 (dostęp: 13.06.2023).

[337] World Economic Forum, *Empowering AI Leadership: An Oversight Toolkit for Boards of Directors*, s. 15, https://www3.weforum.org/docs/WEF_Empowering_AI_Leadership_2022.pdf, (dostęp: 13.06.2023).

i Pranava Rajpurkara, opublikowanego w Harvard Journal of Law & Technology Digest[338]. Artykuł analizuje kwestie prawne związane z wprowadzeniem zaawansowanych technologii medycznych, zwłaszcza sztucznej inteligencji (SI) stosowanej w diagnostyce obrazowej w praktyce klinicznej. Autorzy podkreślają pojawienie się nowych pytań dotyczących odpowiedzialności prawnej w przypadku ewentualnych błędów wynikających z wykorzystania tych innowacyjnych narzędzi. Skupiają się na aplikacjach widzenia maszynowego w dziedzinie medycyny, zwracając uwagę na skomplikowane modele oprogramowania, które mogą być nieprzejrzyste nawet dla swoich twórców. To powoduje niepokój wśród lekarzy co do zaufania do maszyn oraz obawy przed ewentualnymi roszczeniami dotyczącymi błędów medycznych.

Artykuł omawia, w jaki sposób postępy w dziedzinie uczenia maszynowego, poprawiające zrozumiałość wyników sztucznej inteligencji, mogą mieć wpływ na system prawny i kwestie związane z błędami medycznymi. Twierdzi się, że nowe technologie faktycznie mogą zmniejszyć odpowiedzialność lekarzy poprzez dostarczanie bardziej precyzyjnych diagnoz. Ponadto autorzy rozważają konsekwencje tych zmian dla odpowiedzialności producentów technologii, zwłaszcza w kontekście tego, czy takie technologie zostaną uznane za „*produkt*" w ramach odpowiedzialności za produkt oraz jak może to wpłynąć na strategie rozwoju i marketingu producentów.

Badają również, w jaki sposób wykorzystanie doktryny pośredniego informatora może mieć zastosowanie w przypadkach, gdy producenci systemów wizji maszynowej nie udzielają ostrzeżeń w dziedzinie medycyny. Zastanawiają się nad wpływem tej zasady prawa na decyzje producentów dotyczące projektowania i implementacji takich technologii.

Autorzy dochodzą do wniosku, że unikalne możliwości i funkcje sztucznej inteligencji oraz widzenia maszynowego, zwłaszcza w połączeniu z postępami w interpretowalności, otwierają pole do dyskusji na temat tego, czy technologia ta rzeczywiście zmniejsza odpowiedzialność lekarzy. Podkreślają konieczność dokładnego rozważenia sposobu, w jaki system prawny powinien traktować widzenie maszynowe i medycynę opartą na SI, aby zapewnić właściwie ustawione zachęty oraz odpowiedzialne przypisanie odpowiedzialności.

[338] Harned Z., Lungren M. P., Rajpurkar P., *Machine Vision, Medical AI, and Malpractice*, "Harvard Journal of Law & Technology Digest", https://jolt.law.harvard.edu/digest/machine-vision-medical-ai-and-malpractice (dostęp: 10.06.2024 r.).

Zaleca się, aby docenić postęp technologiczny w dziedzinie medycyny, jednocześnie starannie kontrolując wpływ tych narzędzi na praktykę lekarską i odpowiedzialność prawna, aby wspierać rozwój technologiczny, nie naruszając podstawowych praw i ochrony pacjentów[339].

Interesującym aspektem tego tematu może być wynik po zakończeniu badań, których rezultaty jeszcze nie są znane. Jak czytamy w artykule „*Problemy prawne związane z sztuczną inteligencją w dziedzinie zdrowia: protokół przeglądu skupiającego uwagę*", autorstwo Michael Da Silva i in.[340], którzy podkreślają, że postęp w medycynie niesie ze sobą ogromną nadzieję. Jednak, aby społeczeństwo mogło w pełni skorzystać z zalet tych innowacji i uniknąć ewentualnych zagrożeń, konieczne są zmiany zarówno w zarządzaniu, jak i w obszarze prawa, polityki oraz etyki. Celem badań są systematyczne przeglądy literatury mającej na celu mapowanie kluczowych koncepcji i zakresu dostępnych badań w obszarze kwestii prawnych związanych ze stosowaniem sztucznej inteligencji w dziedzinie zdrowia[341].

Metodyka przeglądu opiera się na strukturach stworzonych przez badaczy Arkseya i O'Malleya[342], które zostały rozwinięte przez Levaca i innych[343]. Arksey i O'Malley opracowali podstawowe ramy dla przeglądów skopingowych, natomiast Levac, Colquhoun i O'Brien wprowadzili dodatkowe kroki i wskazówki, aby poprawić ich rzetelność i przejrzystość. Metodyka składa się z sześciu kroków: (1) ustalenie pytań badawczych, (2) identyfikacja odpowiednich źródeł, (3) selekcja materiałów, (4) klasyfikacja danych, (5) agregacja, podsumowanie oraz raportowanie wyników, oraz (6) konsultacje z zainteresowanymi stronami. Kryteria kwalifikacyjne obejmują artykuły w języku angielskim lub francuskim, które analizują, opisują lub priorytetyzują zagadnienia prawne dotyczące sztucznej inteligencji w służbie zdrowia i zostały opublikowane od 2012 roku. Autorzy planują przeprowadzić przegląd literatury poprzez skorzystanie z różnych baz danych w celu znalezienia istotnych źródeł, takich jak artykuły i rozdziały książek. Proces oceny kwalifikowalności zostanie wykonany niezależnie i podwójnie sprawdzony na każdym etapie przeglądu. Po zebraniu

[339] Harned Z., Lungren M. P., Rajpurkar P., *Machine Vision, Medical AI, and Malpractice*, "Harvard Journal of Law & Technology Digest", https://jolt.law.harvard.edu/digest/machine-vision-medical-ai-and-malpractice (dostęp: 10.06.2024 r.).

[340] Da Silva M., Horsley T., Singh D., Da Silva E., Ly V., Thomas B., Daniel R.C., Chagal-Feferkorn K.A., Iantomasi S., *White K., Kent A., Flood C.M., Legal concerns in health-related artificial intelligence: a scoping review protocol*, "Systematic Reviews", Vol. 11, No. 123, https://doi.org/10.1186/s13643-022-01939-y, (dostęp: 10.06.2024 r.)

[341] Ibidem

[342] Arksey H., O'Malley L., *Scoping studies: towards a methodological framework*, "International Journal of Social Research Methodology" 2005, vol. 8, no. 1, s. 19-32.

[343] Levac D., Colquhoun H., O'Brien K.K., *Scoping studies: advancing the methodology*, "Implementation Science" 2010, vol. 5, no. 69, s. 1-9.

i zweryfikowaniu informacji, autorzy mają zamiar połączyć cechy demograficzne zapisów oraz tematycznie kodować zgłoszone kwestie prawne[344].

Omawiana w artykule dyskusja podkreśla, że sztuczna inteligencja w dziedzinie zdrowia niesie za sobą wiele potencjalnych korzyści, ale wiąże się również z kilkoma potencjalnymi problemami. Konieczne jest wprowadzenie odpowiednich regulacji, aby jak najlepiej wykorzystać te korzyści, jednocześnie minimalizując ryzyko. Przegląd ma na celu stworzenie solidnej podstawy dla dalszego rozwoju krajowych i międzynarodowych reakcji na wyzwania prawne związane ze sztuczną inteligencją w medycynie[345].

7.3 Cyberbezpieczeństwo

Sztuczna inteligencja staje się coraz ważniejszym narzędziem w dziedzinie obrony i ataków w cyberprzestrzeni. Jej zdolność do szybkiego przetwarzania dużych ilości danych oraz adaptacji do zmieniających się warunków sprawia, że jest wartościowym sojusznikiem w zapewnianiu bezpieczeństwa cybernetycznego. Niemniej jednak te same cechy, które sprawiają, że sztuczna inteligencja jest skuteczna, mogą także prowadzić do powstania nowych form przestępczości i wyzwań dla ustawodawców. W kontekście prawnym pojawiają się kwestie dotyczące odpowiedzialności za działania zautomatyzowane w cyberprzestrzeni, szczególnie gdy ich skutkiem są poważne szkody. Cyberbezpieczeństwo wyznacza trzy obszary, które będą stanowić wyzwanie dla systemów prawnych w związku z użyciem sztucznej inteligencji, a są nimi:

1. wyzwania dla systemów prawnych - w obliczu coraz bardziej złożonych cyberataków i konieczności ciągłego dostosowywania się do nich, systemy prawne muszą znaleźć skuteczne sposoby ochrony przed szkodami wynikającymi z wykorzystania sztucznej inteligencji w celach przestępczych[346];

2. odpowiedzialność za szkody wyrządzone przez SI - kiedy algorytmy sztucznej inteligencji są używane do przeprowadzania ataków, istotne staje się ustalenie, kto ponosi

[344] Da Silva M., Horsley T., Singh D., Da Silva E., Ly V., Thomas B., Daniel R.C., Chagal-Feferkorn K.A., Iantomasi S., *White K., Kent A., Flood C.M., Legal concerns in health-related artificial intelligence: a scoping review protocol*, "Systematic Reviews" 2022, Vol. 11, No. 123, https://doi.org/10.1186/s13643-022-01939-y, (dostęp: 10.06.2024 r.)
[345] Ibidem
[346] Clarke R., Knake R. K., *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins 2010.

odpowiedzialność: czy to autor algorytmu, użytkownik korzystający z niego, czy też osoba trzecia, która może go kontrolować w sposób nielegalny[347].

3. implikacje dla prywatności i danych osobowych - technologia sztucznej inteligencji może być wykorzystywana do naruszania prywatności poprzez zbieranie i analizowanie danych bez zgody. Takie działania mogą prowadzić do poważnych konsekwencji prawnych i wymagają klarownych przepisów regulacyjnych[348].

Ten punkt ma na celu zbadanie konkretnych sytuacji, w których wykorzystanie sztucznej inteligencji w cyberprzestrzeni stwarzało poważne trudności prawne i etyczne, ze szczególnym uwzględnieniem analizy obecnych ram prawnych oraz sugestii ich ulepszenia tak, aby lepiej odzwierciedlały współczesne zagrożenia.

7.3.1 Atak na TaskRabbit – cyberbezpieczeństwo w dobie SI

Rozwój technologii sztucznej inteligencji przynosi nie tylko obietnice rewolucji w wielu dziedzinach gospodarki i życia codziennego ludzi, ale także nowe wyzwania w obszarze cyberbezpieczeństwa. Zaawansowane technologie SI coraz częściej są używane nie tylko do ochrony danych i infrastruktury cyfrowej, ale także przez cyberprzestępców do przeprowadzania złożonych ataków na organizacje oraz indywidualnych użytkowników. Przykładem takiego wykorzystania SI przez hakerów był atak na internetowy portal TaskRabbit w kwietniu 2018 roku. Platforma TaskRabbit, łącząca freelancerów z osobami poszukującymi pomocy w różnych zadaniach, padła ofiarą złożonego ataku cybernetycznego. Hakerzy wykorzystali botnet kontrolowany przez SI do przeprowadzenia ataku typu Distributed Denial of Service (DDoS), który zakłócił działanie serwerów firmy, co spowodowało znaczny wyciek danych. Incydent ten dotknął 3,75 miliona użytkowników, narażając ich dane osobowe oraz finansowe[349].

Użycie botnetu kontrolowanego przez hakerów do przeprowadzenia ataku DDoS wskazuje na zaawansowanie narzędzi stosowanych przez cyberprzestępców. Sztuczna inteligencja umożliwia zautomatyzowanie i skalowanie ataków, co sprawia, że są one bardziej skuteczne i trudniejsze do obrony. W przypadku firmy TaskRabbit, inteligentne algorytmy potrafiły

[347] Goodman M., *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*, Doubleday 2015.
[348] Schneier B., *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company 2015.
[349] *T Bocetta S., Has an Ai Cyber Attack Happened Yet?* InfoQ, https://www.infoq.com/articles/ai-cyber-attacks/ (dostęp: 10.06.2024 r.).

dynamicznie dostosować sposób ataku w odpowiedzi na próby zabezpieczenia serwerów, co dodatkowo zwiększało stopień destabilizacji.

Przypadek TaskRabbit jest istotną lekcją dla firm i ekspertów ds. bezpieczeństwa cybernetycznego. Podkreśla konieczność rozwijania zaawansowanych systemów obronnych opartych na sztucznej inteligencji w celu zwalczania automatycznych ataków. Ponadto uwydatnia rosnące ryzyko związane z cyberatakami, które mogą dotknąć coraz większą liczbę użytkowników i firm, niezależnie od ich wielkości czy branży.

W odpowiedzi na narastające zagrożenie cyberatakami wykorzystującymi sztuczną inteligencję, konieczne jest opracowanie nowych standardów bezpieczeństwa oraz przepisów prawnych. Te regulacje powinny uwzględniać wymogi dotyczące ochrony danych, a także rozwój oraz implementację systemów SI zdolnych do wykrywania i zwalczania zagrożeń w czasie rzeczywistym. Realizacja tych działań wymaga współpracy na poziomie międzynarodowym oraz zaangażowania społeczności technologicznej i biznesowej w budowanie bardziej bezpiecznego cyfrowego środowiska.

7.3.2 Offensive SI i cyberataki

W ciągu ostatnich lat pojawienie się tzw. „*agresywnej SI*" (szkodliwej sztucznej inteligencji) zmieniło krajobraz cyberbezpieczeństwa, wprowadzając nowy okres zaawansowanych ataków cybernetycznych. Wykorzystanie SI przez cyberprzestępców stwarza poważne zagrożenie dla organizacji na całym świecie, co wymusza na zespołach IT konieczność poszukiwania nowych i zaawansowanych metod obrony.

Jednym z przykładów niewłaściwego wykorzystania sztucznej inteligencji są ataki deepfake, gdzie technologia ta jest używana do tworzenia fałszywych obrazów lub filmów, przedstawiających sytuacje, które nigdy nie miały miejsca. Według informacji FBI z stycznia 2020 roku, technologia deepfake osiągnęła poziom pozwalający na stworzenie sztucznych postaci zdolnych do przechodzenia testów biometrycznych. Szybki rozwój sieci neuronowych niesie ryzyko, że bardzo realistyczne deepfake mogą być wykorzystane do manipulacji opinii publicznej i stanowić zagrożenie dla bezpieczeństwa narodowego[350].

[350] MIT Technology Review Insights, *Preparing for AI-enabled cyberattacks,* https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/ (dostęp: 10.06.2024 r.)

Zastosowanie sztucznej inteligencji w atakach cybernetycznych stwarza wyzwanie dla tradycyjnych narzędzi wykrywania opartych na regułach, ponieważ agresywne podejście SI umożliwia cyberprzestępcom przeprowadzanie precyzyjnych ataków z niezwykłą szybkością i rozmiarem. W rezultacie organizacje muszą dostosować się do nowych metod obrony, takich jak „*defensywna sztuczna inteligencja*", która skutecznie kontruje ataki wykorzystujące sztuczną inteligencję.

W reakcji na coraz większe zagrożenie, organizacje na całym świecie zaczęły korzystać z zaawansowanych technologii obronnych, aby zabezpieczyć się przed atakami wspieranymi przez sztuczną inteligencję. Badania przeprowadzone wśród ponad 300 liderów biznesu wykazały, że większość z nich już podjęła działania mające na celu wdrożenie środków obronnych przeciwko atakom wykorzystującym SI, przy niektórych uwzględniających mechanizmy obronne SI[351].

Ten konkretny przypadek badawczy podkreśla wzrastającą rolę sztucznej inteligencji w dziedzinie cyberbezpieczeństwa, zarówno jako narzędzia obronnego, jak i potencjalnego zagrożenia. Analiza przykładów użycia sztucznej inteligencji w celach ofensywnych przez cyberprzestępców może dostarczyć cennych wskazówek dotyczących przyszłych wyzwań związanych z cyberbezpieczeństwem oraz koniecznych innowacji w prawie i polityce[352].

7.3.3 SI i cyberbezpieczeństwo: eksploracja prawnych i akademickich granic

W zmieniającym się krajobrazie cyberbezpieczeństwa połączenie technologii sztucznej inteligencji stwarza zarówno rewolucyjne możliwości, jak i skomplikowane wyzwania prawne. Ten fragment przybliża istotę cyberbezpieczeństwa w erze SI, opierając się na najnowszych badaniach naukowych, które podkreślają wagę dostosowania przepisów prawa oraz międzynarodowej współpracy w zwalczaniu zagrożeń cybernetycznych napędzanych przez SI.

1. Ewolucja prawa cyberprzestępczości w erze cyfrowej

[351] Capgemini Research Institute, *Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security*, s. 16, https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf (dostęp: 13.06.2023).

[352] MIT Technology Review, *Preparing for AI-enabled cyberattacks*, https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/ (dostęp: 10.06.2024 r.).

Rewolucja cyfrowa znacząco zmieniła krajobraz walki z cyberprzestępczością. Jak wskazują Ruddin i Zein[353], rozwój prawa w odpowiedzi na postęp technologiczny charakteryzuje się wprowadzeniem konkretnych przepisów dotyczących cyberprzestępczości oraz zwiększeniem ochrony danych osobowych. Wartość międzynarodowych regulacji prawnych, takich jak Konwencja Budapeszteńska[354] i RODO, podkreśla istotną rolę współpracy ponadgranicznej w skutecznym zwalczaniu zagrożeń związanych z cyberprzestępczością[355].

2. Akademickie perspektywy na wyzwania prawne SI

Analiza naukowa skupia się na badaniu wpływu sztucznej inteligencji na bezpieczeństwo cybernetyczne oraz prawo. Publikacje takie jak ta autorstwa Gula & Nofely[356] oraz inne omawiane w tym opracowaniu, prezentują prawnicze podejście do konieczności dostosowania prawa do postępu technologicznego. Zgodnie z ogólnym stanowiskiem naukowców: prawo powinno nie tylko reagować na obecne zagrożenia cybernetyczne, ale również przewidywać przyszłe wyzwania stawiane przez rozwój sztucznej inteligencji[357].

3. Implikacje prawne i odpowiedzialności

Zastosowanie sztucznej inteligencji w dziedzinie cyberbezpieczeństwa wywołuje istotne pytania dotyczące odpowiedzialności i egzekwowania prawa. Zacieranie granic między narzędziem (systemami SI) a użytkownikiem (operatorami, programistami i firmami) sprawia, że tradycyjne pojęcia odpowiedzialności prawnej stają się bardziej skomplikowane. Wyraźnie widać, że konieczne są nowe definicje prawne i standardy, aby radzić sobie z unikalnymi wyzwaniami generowanymi przez technologie wspierane przez SI[358].

---

[353] Ruddin I., Zein S. Z. SGN, *Evolution of Cybercrime Law in Legal Development in the Digital World*, "Journal Multidisiplin Madani", Vol. 4, No. 1, s. 168-173, https://doi.org/10.55927/mudima.v4i1.7962 (dostęp: 10.06.2024 r.).

[354] Rada Europy, Konwencja o cyberprzestępczości, Budapeszt, European Treaty Series - Nr 185, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 (dostęp: 13.06.2023).

[355] Ruddin I., Zein S. Z. SGN, *Evolution of Cybercrime Law in Legal Development in the Digital World*, "Journal Multidisiplin Madani", Vol. 4, No. 1, s. 168-173, https://doi.org/10.55927/mudima.v4i1.7962 (dostęp: 10.06.2024 r.).

[356] Gul R., Nofely A. M. O., *The Future of Law from The Jurisprudence Perspective for Example: The Influence of Science & Technology to Law SI Law*, "Journal Equity of Law and Governance", Vol. 1, No. 1, s. 77–83, https://www.ejournal.warmadewa.ac.id/index.php/sjj/article/view/3556, (dostęp: 10.06.2024 r.)

[357] Ibidem

[358] Ministerstwo Cyfryzacji, *Analiza związku Aktu w sprawie Sztucznej Inteligencji z wybranymi obowiązującymi i projektowanymi regulacjami prawnymi*, s. 38, https://www.gov.pl/web/ai/raport-analiza-zwiazku-aktu-w-

4. Strategie prawne na przyszłość

W dążeniu do przyszłości konieczna jest wspólna praca nad dostosowaniem systemów prawnych do zmiennej natury sztucznej inteligencji i cyberbezpieczeństwa. Propozycje dotyczące przyszłych strategii prawnych podkreślają istotę międzynarodowej współpracy prawniczej, opracowanie ram prawnych specjalnie dla sztucznej inteligencji oraz wprowadzenie zasad „*projektowanie z uwzględnieniem prywatności*"[359] (ang. privacy by design) w procesie rozwoju SI[360].

„*Przecięcie się*" sztucznej inteligencji i bezpieczeństwa cybernetycznego stanowi unikalne połączenie możliwości i wyzwań dla prawa. Podczas eksploracji tego skomplikowanego obszaru, wnioski i spostrzeżenia z badań naukowych i analiz prawnych dostarczają cennych wskazówek. Poprzez przyjęcie aktywnego i kooperatywnego podejścia do reformy prawnej, społeczeństwo może korzystać z zalet wynikających ze sztucznej inteligencji, jednocześnie chroniąc się przed potencjalnymi zagrożeniami dla bezpieczeństwa cybernetycznego i prywatności[361].

Dwa istotne artykuły, które pogłębiają zrozumienie problematyki prawnej i etycznej sztucznej inteligencji w kontekście cyberbezpieczeństwa, to prace Wojciecha Filipkowskiego i Daniela Mielnika.

Artykuł Wojciecha Filipkowskiego „*Criminal Law and Artificial Intelligence - Selected Aspects*" [362] w sposób wyczerpujący omawia różnorodne aspekty związane z zastosowaniem sztucznej inteligencji w kontekście prawa karnego. Autor analizuje SI jako narzędzie

sprawie-sztucznej-inteligencji-z-wybranymi-obowiazujacymi-i-projektowanymi-regulacjami-prawnymi (dostęp: 13.06.2023).

[359] Projektowanie z uwzględnieniem prywatności (ang. Privacy by Design) to koncepcja projektowania systemów i usług w taki sposób, aby zapewnić ochronę prywatności od samego początku, zamiast traktować ją jako kwestię dodatkową. Obejmuje ona wdrażanie odpowiednich zabezpieczeń technicznych i organizacyjnych w celu zminimalizowania zbierania i wykorzystywania danych osobowych oraz zagwarantowania użytkownikom kontroli nad własnymi danymi. Podejście to ma na celu zbudowanie wysokiego poziomu prywatności jako domyślnej cechy systemów informatycznych i praktyk przetwarzania danych.

[360] UNESCO, Raport na temat Etyki Sztucznej Inteligencji: Ku rekomendacjom UNESCO 2022, s. 67, https://unesdoc.unesco.org/ark:/48223/pf0000380455_pol (dostęp: 13.06.2023).

[361] Marta, P., Salminen, N., Whitehead, D., Perez, N., & Briggs, P., *AI and Cybersecurity: Possible New Risks and Legal Implications, "*New York Law Journal" , https://www.law.com/newyorklawjournal/2023/05/08/ai-and-cybersecurity-possible-new-risks-and-legal-implications/ (dostęp: 10.06.2024 r.)

[362] Filipkowski W., *Criminal Law and Artificial Intelligence - Selected Aspects*, in: *Legal and Technical Aspects of Artificial Intelligence*, L. Lai, M. Świerczyński (eds.), Rozdział: 8, Wydawnictwo Naukowe Uniwersytetu Kardynała Stefana Wyszyńskiego, https://www.researchgate.net/publication/366701783_Criminal_Law_and_Artificial_Intelligence_-_Selected_Aspects (dostęp: 10.06.2024 r.).

wykorzystywane przez przestępców do popełniania cyberprzestępstw oraz jako obiekt ataków cybernetycznych. Co więcej, artykuł zwraca uwagę na potrzebę dostosowania istniejących definicji przestępstw i przepisów prawa karnego do nowych wyzwań technologicznych. Filipkowski podkreśla, że technologie wspierane przez SI wymagają wprowadzenia nowych regulacji prawnych, które uwzględnią specyfikę tych narzędzi oraz konieczność ochrony użytkowników przed ich nadużyciem. Ponadto, autor wskazuje na potrzebę zwiększenia świadomości prawnej wśród użytkowników SI, aby mogli oni lepiej rozumieć zagrożenia oraz swoje prawa i obowiązki w kontekście korzystania z tych technologii.[363]

Artykuł Daniela Mielnika „*Anonimowość w Internecie a problem cyberbezpieczeństwa. Aspekt prawny*"[364], który analizuje kwestię zachowania poufności w sieci w kontekście bezpieczeństwa cybernetycznego oraz prawa. Przedstawia potencjalne rozwiązania prawne, które mogą wspierać anonimowość online, przy jednoczesnym uwzględnieniu konfliktu między zachowaniem anonimowości a zapewnieniem bezpieczeństwa państwa. Autor zaznacza, że chociaż anonimowość może przyczyniać się do swobody wypowiedzi, stanowi także wyzwanie dla zapewnienia cyberbezpieczeństwa[365].

Oba artykuły podkreślają skomplikowaną naturę relacji między nowymi technologiami, takimi jak sztuczna inteligencja, a prawem karnym oraz cyberbezpieczeństwem. Filipkowski zwraca uwagę na konieczność dostosowania prawa karnego do wyzwań wynikających z rozwoju SI, rozważając zarówno potencjalne zagrożenia, jak i możliwości ochrony oferowane przez prawo karne wobec SI. Mielnik skupia się na problemie anonimowości w kontekście bezpieczeństwa online, co ma istotne implikacje dla debaty na temat sztucznej inteligencji, zwłaszcza w kontekście identyfikacji i ścigania cyberprzestępców.

Podsumowując, należy podkreślić kluczowe znaczenie dostosowania przepisów prawa oraz międzynarodowej współpracy w zwalczaniu zagrożeń cybernetycznych napędzanych przez sztuczną inteligencję. Konieczność ciągłego aktualizowania regulacji prawnych w odpowiedzi

[363] Ibidem
[364] Mielnik D., *Anonimowość w Internecie a problem cyberbezpieczeństwa, w: Współczesny wymiar bezpieczeństwa publicznego. Kształtowanie bezpiecznych przestrzeni. Działania profilaktyczne*, „Wydawnictwo Instytutu Wymiaru Sprawiedliwości", https://www.researchgate.net/publication/340205488_Anonimowosc_w_Internecie_a_problem_cyberbezpieczenstwa_Aspekt_prawny (dostęp: 10.06.2024 r.).
[365] Ibidem

na dynamiczny rozwój technologii oraz podkreślenie roli interdyscyplinarnej we współpracy w tworzeniu bezpiecznych i etycznych systemów SI.

7.4 Systemy rekrutacyjne

Zastosowanie sztucznej inteligencji w procesach rekrutacyjnych stanowi postęp, który może przynieść korzyści zarówno pracodawcom, jak i kandydatom. Dzięki temu możliwe staje się bardziej efektywne i skoncentrowane poszukiwanie talentów. Niemniej jednak implementacja tych technologii niesie ze sobą istotne wyzwania z zakresu prawa, szczególnie w przypadkach, gdy systemy SI nieświadomie promują praktyki dyskryminacyjne lub ingerują w prywatność aplikujących. Celem tego podrozdziału jest zbadanie sytuacji, w których systemy rekrutacyjne oparte na SI mogą doprowadzić do potencjalnych naruszeń prawa oraz rozważenie konsekwencji tych działań. Do tych potencjalnych naruszeń może dojść m.in. w następujących przypadkach:

1. dyskryminacja nieumyślna - w niektórych sytuacjach systemy rekrutacyjne, które uczą się na podstawie danych historycznych, mogą przypadkowo faworyzować lub ignorować kandydatów ze względu na płeć, wiek, pochodzenie etniczne lub inne czynniki. Taki sposób postępowania jest sprzeczny z zasadami równego traktowania i może prowadzić do konsekwencji prawnych[366];

2. prawo do prywatności i ochrony danych - systemy sztucznej inteligencji wykorzystywane w procesie rekrutacji muszą operować na znacznych ilościach informacji osobowych. Dlatego ważne jest, aby zapewnić zgodność tych systemów z obowiązującymi przepisami dotyczącymi ochrony danych, takimi jak RODO[367];

3. transparentność i odpowiedzialność - Niezwykle istotne jest, aby kandydaci mieli jasność co do procesów rekrutacyjnych i mogli zrozumieć, w jaki sposób ich dane są wykorzystywane. Konieczne jest ustalenie, kto - czy to pracodawca, czy twórca systemu - ponosi odpowiedzialność za funkcjonowanie algorytmów[368].

[366] Barocas S., Selbst A. D., *Big data's disparate impact*, "California Law Review" 2016, vol. 104.
[367] Gonzalez R. C., *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificially Intelligent'?*, "Computer Law & Security Review 2018", Vol. 34, No. 2, s. 234-256.
[368] Sánchez-Monedero J., Dencik L., Edwards L., *What does the Robot Think? Transparency as a Fundamental Design Requirement for Intelligent Systems*, "Proceedings of ICSIL" 2017.

Przypadki, które zostały wybrane do analizy w tej sekcji, odzwierciedlają różnorodne kwestie związane z etycznym i prawnym wykorzystaniem sztucznej inteligencji w procesach rekrutacyjnych i mają na celu wskazanie potencjalnych dróg regulacji oraz zarządzania ryzykiem w tej dziedzinie.

Jednym z przypadków, który przyciągnął uwagę opinii publicznej, było narzędzie do rekrutacji używane przez firmę Amazon, które okazało się być stronnicze wobec kobiet[369]. Program komputerowy stworzony do automatyzacji procesu oceny aplikacji o pracę został wyłączony przez firmę po ustaleniu, że faworyzował mężczyzn podczas selekcji kandydatów na stanowiska techniczne. System został wytrenowany na podstawie danych rekrutacyjnych zebranych z 10 lat działalności firmy w branży zdominowanej przez mężczyzn, co spowodowało, że sztuczna inteligencja nauczyła się preferować CV męskich kandydatów[370].

7.4.1 System rekrutacyjny Amazona a dyskryminacja płci[371]

Amazon, starając się ułatwić proces rekrutacji, zaimplementował system sztucznej inteligencji, który analizuje życiorysy kandydatów w celu wybrania najbardziej perspektywicznych pracowników. W miarę upływu czasu okazało się, że system przejawiał uprzedzenia wobec kobiet, szczególnie w kontekście aplikacji na stanowiska techniczne. Po analizie danych rekrutacyjnych z ostatniej dekady, w której mężczyźni przeważali w branży technologicznej, algorytm „*zrozumiał*", że kandydaci płci męskiej są bardziej preferowani. Po zidentyfikowaniu stronniczości w systemie, Amazon postanowił go wyłączyć, potwierdzając, że sztuczna inteligencja może przypadkowo szerzyć istniejące uprzedzenia, jeśli dane wykorzystywane do treningu nie są równoważone w odpowiedni sposób[372].

Ten konkretny przypadek podkreśla istotność dokładnej analizy danych używanych do szkolenia algorytmów SI oraz potrzebę wprowadzenia środków zapobiegających

[369] Dastin, J., *Amazon scraps secret AI recruiting tool that showed bias against women,* Reuters, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ (dostęp: 10.06.2024 r.).

[370] Ibidem

[371] Dyskryminacja ze względu na płeć - nierówne traktowanie osób ze względu na ich płeć biologiczną lub tożsamość płciową, prowadzące do ograniczania praw i możliwości kobiet lub mężczyzn w różnych sferach życia, takich jak praca, edukacja, opieka zdrowotna czy udział w życiu publicznym. Może przybierać formy bezpośrednie lub pośrednie i jest uznawana za naruszenie fundamentalnych praw człowieka i godności osobistej. Zob. Europejski Instytut ds. Równości Kobiet i Mężczyzn, "Czym jest dyskryminacja?", EIGE, 2023.

[372] Dastin, J., *Amazon scraps secret AI recruiting tool that showed bias against women,* Reuters, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ (dostęp: 10.06.2024 r.).

dyskryminacji. Dodatkowo, ukazuje, że ingerencja człowieka oraz ciągłe monitorowanie odgrywają kluczową rolę w zapewnieniu, że systemy SI działają zgodnie z normami etycznymi i nie promują istniejących uprzedzeń społecznych.

7.4.2 HireVue i ocena kandydatów z użyciem SI

Innym fascynującym przypadkiem studium, który zdobył popularność i może być przydatny w pracy doktorskiej związanej z sztuczną inteligencją, jest przykład wykorzystania systemów SI przez firmę HireVue. HireVue to platforma rekrutacyjna, która korzysta z algorytmów sztucznej inteligencji do analizy nagrań wideo rozmów kwalifikacyjnych w celu oceny potencjalnych kandydatów. System nie tylko analizuje zawartość rozmów, ale również mowę ciała i ton głosu, aby ocenić dopasowanie kandydata do danej posady. Służyć to ma wspieraniu pracodawców w szybszym i bardziej obiektywnym procesie wyboru kandydatów. Metody używane przez firmę HireVue wywołały kontrowersje ze względu na potencjalne ryzyko dyskryminacji i brak przejrzystości w funkcjonowaniu algorytmów. Krytycy zauważyli, że algorytmy mogą niechcący faworyzować kandydatów opierając się na uprzedzeniach związanych z cechami niewerbalnymi, które niekoniecznie mają bezpośredni związek z kompetencjami zawodowymi. W odpowiedzi na te zaniepokojenia, w styczniu 2021 roku firma HireVue ogłosiła zaniechanie wykorzystywania analizy twarzy w swoich ocenach. Decyzja ta została podjęta ze względu na rosnącą świadomość społeczną dotyczącą etyki sztucznej inteligencji oraz presję w kierunku większej regulacji technologii oceniających kandydatów do pracy[373]..

Ten konkretny przykład analizy przypadku prezentuje istotne kwestie związane z wykorzystaniem sztucznej inteligencji w procesach rekrutacyjnych, takie jak zapewnienie równych szans wszystkim kandydatom, ryzyko niezamierzonej dyskryminacji oraz konieczność przejrzystości w działaniu algorytmów SI. W kontekście pracy badawczej, sytuacja firmy HireVue może posłużyć do omówienia problematyki etycznych i prawnych wyzwań wynikających z nowoczesnych technologii rekrutacyjnych.

[373] Harwell D., *A face-scanning algorithm increasingly decides whether you deserve the job*, The Washington Post, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/ (dostęp: 10.06.2024 r.).

7.4.3 Dyskusja akademicka na temat SI w systemach rekrutacyjnych i konsekwencje prawne

Stosowanie sztucznej inteligencji w rekrutacji staje się przedmiotem intensywnej dyskusji akademickiej, skupiającej się na potencjale tej technologii do zwiększenia efektywności procesów selekcyjnych, jak również na ryzyku wynikającym z potencjalnych uprzedzeń i dyskryminacji. Badacze podkreślają, że choć SI może pomóc w eliminacji ludzkich uprzedzeń w pierwszej fazie selekcji, algorytmy są wrażliwe na dane, na których zostały wytrenowane, co może prowadzić do niezamierzonych form dyskryminacji.

Wykorzystanie sztucznej inteligencji w procesie rekrutacji obiecuje przyspieszenie i bardziej obiektywne metody oceny kandydatów. Jednak, zgodnie z badaniami Bogena i Rieke[374], algorytmy mogą nieświadomie powielać istniejące uprzedzenia zawarte w danych historycznych. Istnieje zatem ryzyko utrwalania nierówności, dlatego konieczne jest podjęcie środków zaradczych, aby zapewnić sprawiedliwość i równość szans dla wszystkich aplikantów[375].

Konsekwencje prawne wykorzystania sztucznej inteligencji w rekrutacji głównie dotyczą ryzyka naruszenia przepisów dotyczących równego traktowania i zakazu dyskryminacji. Jak zauważa Kim[376], prawo musi być na bieżąco z postępem technologicznym, dostarczając ramy ochrony kandydatów przed dyskryminacją opartą na algorytmach. Wymaga to, aby regulacje i organizacje międzynarodowe opracowały konkretne wytyczne dotyczące stosowania sztucznej inteligencji w procesach kadrowych[377].

W celu rozwiązania ewentualnych problemów, Selwyn[378] zaleca wprowadzenie przejrzystości w działaniu algorytmów sztucznej inteligencji w procesie rekrutacji oraz mechanizmów umożliwiających sprawdzanie i korygowanie podjętych przez nie decyzji. Podkreśla również istotność edukacji pracodawców na temat potencjalnych zagrożeń oraz konieczność ciągłego monitorowania skuteczności i etyczności używanych systemów[379].

---

[374] Bogen M., Rieke A., *Help Wanted: An Examination of Hiring Algorithms*, *Equity, and Bias*, "Pew Research Center" 2018.
[375] Bogen M., Rieke A., *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, "Pew Research Center 2"018.
[376] Kim P., *Auditing Algorithms for Discrimination*, "Harvard Law Review" 2017.
[377] Ibidem
[378] Selwyn N., *Should Robots Replace Teachers?*, Polity Press 2019
[379] Ibidem

Dyskusja akademicka na temat wykorzystania sztucznej inteligencji w procesie rekrutacji podkreśla konieczność zrównoważonego podejścia, które uwzględnia zarówno potencjał tej technologii w usprawnianiu procesów selekcyjnych, jak i ryzyko naruszenia zasad równości i unikania dyskryminacji. Istotną rolę w ustalaniu reguł etycznych i regulacyjnych dla wykorzystania SI w rekrutacji odgrywa prawo, które ma kluczowe znaczenie dla zapewnienia, że nowe technologie będą służyć wspólnemu dobru wszystkich uczestników procesu rekrutacyjnego.

7.5 Asystenci wirtualni

W miarę rosnącej popularności asystentów wirtualnych, takich jak Siri[380], Alexa[381] czy Google Assistant[382], wzrasta także zainteresowanie ich wpływem na prywatność i bezpieczeństwo danych. Te interaktywne systemy sztucznej inteligencji pełniące rolę interfejsu między użytkownikami a światem cyfrowym mogą czasami gromadzić i przetwarzać informacje w sposób wykraczający poza intencje użytkownika. Powoduje to wątpliwości co do zgodności z obowiązującymi przepisami dotyczącymi ochrony danych osobowych i prywatności. Ten podrozdział ma na celu analizę konsekwencji prawnokarnych związanych z działaniem asystentów wirtualnych, ze szczególnym uwzględnieniem przypadków naruszenia prywatności oraz nieuprawnionego wykorzystania danych.

W tym kontekście istotne jest zrozumienie, jak te technologie mogą wpływać na prywatność użytkowników i jakie potencjalne zagrożenia wynikają z ich użycia. Szczególną uwagę należy zwrócić na następujące aspekty:

1. naruszenia prywatności - przypadki, kiedy asystenci wirtualni byli wykorzystywani do nieautoryzowanego podsłuchiwania lub nagrywania rozmów bez zgody użytkowników, stawiają pod znakiem zapytania istotne kwestie dotyczące ochrony prywatności. Analiza

[380] Siri to asystent głosowy oparty na sztucznej inteligencji, opracowany przez firmę Apple. Jest wbudowany w urządzenia Apple, takie jak iPhone, iPad, Mac, Apple Watch i HomePod. Siri umożliwia użytkownikom wykonywanie różnych zadań za pomocą komend głosowych, takich jak wyszukiwanie informacji w Internecie, wysyłanie wiadomości, ustawianie przypomnień, odtwarzanie muzyki, a także sterowanie urządzeniami inteligentnego domu.

[381] Alexa to asystent głosowy oparty na sztucznej inteligencji, opracowany przez firmę Amazon. Jest używany w różnych urządzeniach, takich jak głośniki Amazon Echo, i pozwala użytkownikom na wykonywanie szeregu zadań poprzez komendy głosowe, takich jak odtwarzanie muzyki, sterowanie urządzeniami inteligentnego domu, ustawianie przypomnień, a także uzyskiwanie informacji o pogodzie, wiadomościach i wielu innych.

[382] Google Assistant to asystent głosowy oparty na sztucznej inteligencji, opracowany przez firmę Google. Jest dostępny na urządzeniach z systemem Android i smart głośnikach Google Home

takich incydentów pozwala na lepsze zrozumienie ryzyka i konieczności wprowadzenia odpowiednich regulacji[383];

2. zabezpieczenia danych - twórcy sztucznej inteligencji mają obowiązek zapewnić odpowiednie środki ochrony prywatności użytkowników i ich danych osobowych. Badania wskazują, że niedostateczne zabezpieczenia mogą prowadzić do poważnych naruszeń i nadużyć. Twórcy muszą wdrażać zaawansowane protokoły szyfrowania, a także regularnie aktualizować swoje systemy, aby chronić dane przed nieuprawnionym dostępem i atakami cybernetycznymi. [384];

3. transparentność działania - badanie dotyczące przejrzystości działania asystentów wirtualnych oraz metod informowania użytkowników o przetwarzaniu ich danych jest kluczowe dla budowania zaufania i zgodności z regulacjami prawnymi. Użytkownicy powinni mieć jasne informacje o tym, jakie dane są zbierane, jak są przetwarzane i w jakim celu są wykorzystywane. Zwiększona transparentność może przyczynić się do większej akceptacji tych technologii przez społeczeństwo[385];

4. regulacje prawne - analiza aktualnych przepisów i wytycznych prawnych mających na celu zabezpieczenie użytkowników przed możliwymi nadużyciami związanymi z asystentami wirtualnymi. W szczególności, wytyczne dotyczące etyki i zaufania w sztucznej inteligencji podkreślają znaczenie ochrony danych, transparentności i odpowiedzialności. Dokument „*Ethics Guidelines for Trustworthy AI*"[386] opracowany przez Komisję Europejską zaleca, aby systemy sztucznej inteligencji były przejrzyste, umożliwiając użytkownikom zrozumienie sposobu przetwarzania ich danych. Zgodność z regulacjami takimi jak RODO[387] oraz rozwijanie nowych ram prawnych jest kluczowe dla zapewnienia ochrony prywatności i bezpieczeństwa danych użytkowników[388].

---

[383] Schneier B., *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W.W. Norton & Company 2018.

[384] Zarsky T. Z., *Understanding Privacy and Data Protection: What You Need to Know*, "Recode" 2019.

[385] Bostrom N., Yudkowsky E., *The Ethics of Artificial Intelligence*, red. Keith Frankish, William Ramsey, "Cambridge Handbook of Artificial Intelligence" 2014.

[386] European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (dostęp: 10.06.2024 r.)

[387] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

[388] European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (dostęp: 10.06.2024 r.).

Badanie zastosowań asystentów wirtualnych i ich skutków prawnokarnych pozwoli na lepsze zrozumienie obecnych wyzwań oraz wskaże potrzeby regulacyjne w szybko rozwijającym się obszarze technologii.

7.5.1 Sprawa Alexy i pary z Portland

Asystenci wirtualni opierający swoje działanie na SI, tacy jak Amazon Alexa, gromadzą i analizują dane głosowe, aby dostosować doświadczenia użytkowników i usprawnić swoje usługi. Ich działanie jest stale doskonalone dzięki uczeniu maszynowemu, co pozwala im lepiej zrozumieć i przewidzieć potrzeby użytkowników[389]. W kwietniu 2018 roku, miała miejsce sytuacja, w której Alexa przypadkowo zarejestrowała prywatną rozmowę pary z Portland i wysłała ją do przypadkowego kontaktu z ich listy. Amazon potwierdził ten incydent jako niezamierzony błąd spowodowany rzadkim zestawieniem różnych dźwięków, które Alexa błędnie zinterpretowała jako serię poleceń[390].

To wydarzenie stało się impulsem do licznych debat akademickich na temat ochrony danych osobowych i prywatności w epoce sztucznej inteligencji. Omawiano sprawy dotyczące wyrażania zgody na przetwarzanie danych, potencjalnego nieupoważnionego dostępu do informacji oraz braku przejrzystości w procesie ich zbierania i analizowania[391].

7.5.2 Przypadki podsłuchiwania rozmów przez pracowników Google

W 2019 roku okazało się, że pracownicy Google mieli dostęp do nagrań audio z Google Assistant. Firma przyznała, że czasami fragmenty rozmów są analizowane przez specjalistów w celu doskonalenia algorytmów rozpoznawania mowy. Ujawnienie tego faktu wywołało szeroką debatę na temat ochrony prywatności i bezpieczeństwa danych osobowych[392]. Belgijski kanał VRT NWS opublikował sprawozdanie, w którym ujawnił, że posiada dostęp do ponad tysiąca nagrań z Google Assistant, w tym wielu zawierających poufne informacje i nagranych bez zgody użytkowników[393]. Pewne działania wzbudziły obawy w kontekście przepisów

[389] Wolfson S.., *Amazon's Alexa recorded private conversation and sent it to random contact*, The Guardian, https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation (dostęp: 10.06.2024 r.).
[390] Ibidem
[391] Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Ni Loideain, N., & Svantesson, D. J. B., *Expanding the artificial intelligence-data protection debate,* International Data Privacy, https://doi.org/10.1093/idpl/ipy024 (dostęp: 10.06.2024 r.).
[392] Powel A., *Privacy concerns in the rise of smart assistants*, "Journal of Data Protection & Privacy" 2019, Vol. 3, No. 2, s. 160-174.
[393] VRT NWS, *How we got to listen to Google Assistant recordings*, VRT NWS 2019.

dotyczących ochrony danych, takich jak *Rozporządzenie Ogólne o Ochronie Danych*[394] (RODO) w Unii Europejskiej, które wymaga wyraźnej zgody użytkownika na przetwarzanie jego danych osobowych. Dodatkowo, niezamierzone nagrania, których użytkownicy nie mieli świadomości, mogły stanowić naruszenie ich prywatności i autonomii[395]. Po wyjściu sprawy na jaw, Google zadeklarowało, że przeprowadzi przegląd swoich działań oraz wprowadzi dodatkowe środki mające na celu zwiększenie przejrzystości i umożliwienie użytkownikom większej kontroli nad ich danymi[396].

Uczonych i specjalistów zajmujących się etyką i prawem technologii zainteresowała analiza ram prawnych i regulacyjnych dotyczących technologii rozpoznawania mowy. Podkreślali również konieczność większej przejrzystości oraz lepszego informowania użytkowników o sposobach wykorzystania ich danych[397].

Ten konkretny przykład może posłużyć do przedstawienia trudności prawnych i etycznych, które pojawiają się w kontekście rozwoju sztucznej inteligencji oraz nieustannych wysiłków w celu doskonalenia świadczenia usług. Ponadto podnosi istotne kwestie dotyczące odpowiedzialności firm technologicznych oraz ochrony danych osobowych użytkowników.

7.5.3 „Echo Kids" – niechciane zakupy przez Amazon Echo

W grudniu 2016 roku w Dallas w Teksasie, rodzice zostali zaskoczeni, gdy odkryli, że ich sześcioletnia córka zamówiła zabawki o wartości 170 dolarów za pośrednictwem rodzinnego urządzenia Amazon Echo. Podczas zabawy z Echo dziecko powiedziało „*Alexo, zamów mi domek dla lalek*", co zostało potraktowane przez Alexę jako polecenie zakupu. Amazon Echo, będący zawsze gotowy do nasłuchu, odebrał prośbę dziecka i potraktował ją jako zgodne

[394] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

[395] De Vries I., *Legal implications of AI listening practices: A look into Google's data handling*, "AI & Law Journal" 2020, Vol. 28, No. 1, s. 37-55.

[396] Monsees D., Product Lead Google, *More information about our processes to safeguard speech data,* Google Blog, https://blog.google/products/assistant/more-information-about-our-processes-safeguard-speech-data/ (dostęp: 10.06.2024 r.).

[397] Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Ni Loideain, N., & Svantesson, D. J. B., *Expanding the artificial intelligence-data protection debate*, International Data Privacy, https://doi.org/10.1093/idpl/ipy024 (dostęp: 10.06.2024 r.).

z prawem zakupy. W tej sytuacji Echo było skonfigurowane w taki sposób, że nie wymagało dodatkowego potwierdzenia zakupu za pomocą hasła czy kodu[398].

To wydarzenie zostało szeroko opisane w literaturze akademickiej[399], dotyczącej interfejsów użytkownika sztucznej inteligencji oraz kwestii związanych z bezpieczeństwem i prywatnością. Omawiano kwestie prawne dotyczące sytuacji, gdy sztuczna inteligencja podejmuje działania bez jednoznacznego i świadomego potwierdzenia ze strony użytkownika, a także wyzwania etyczne i praktyczne związane z projektowaniem interaktywnych technologii domowych[400].

Ten konkretny przypadkowy incydent stał się pretekstem do dyskusji na temat konieczności zaoferowania dodatkowych zabezpieczeń, takich jak potwierdzenie głosowe lub użycie haseł, aby zapobiec przypadkowym zakupom dokonywanym przez dzieci. Amazon odpowiedział na tę sytuację, udostępniając rodzicom możliwość ustawienia kontroli rodzicielskich, w tym żądanie podania kodu potwierdzającego przy każdym transakcji. Studium przypadku podkreśla istotę projektowania interfejsów użytkownika z uwzględnieniem różnorodnych scenariuszy użytkowania oraz potencjalnych zagrożeń[401].

7.5.4 Dyskusja akademicka na temat SI w wirtualnych asystentach i konsekwencje prawne

Rozwój cyfrowych asystentów, takich jak *Amazon Alexa, Google Assistant* czy *Siri* od *Apple*, to jeden z najbardziej dynamicznych obszarów sztucznej inteligencji. Ich umiejętność rozumienia języka naturalnego i wykonywania poleceń głosowych zmienia sposób interakcji człowieka z technologią. Jednakże wraz z coraz większą popularnością cyfrowych asystentów w życiu codziennym pojawiają się także pytania dotyczące konsekwencji prawnych związanych z prywatnością, bezpieczeństwem danych i odpowiedzialnością.

Ważnym elementem dyskusji akademickiej na temat sztucznej inteligencji w wirtualnych asystentach jest zagadnienie prywatności i ochrony danych użytkowników. Naukowcy zwracają uwagę na potencjalne zagrożenia związane z gromadzeniem i analizą danych

[398] Kahn J. P., *Amazon Echo and the Hot Tub Mishap: Case Study on Privacy in Connected Homes*, "Technology & Ethics" 2016, Vol. 8, No. 1, s. 12-35.
[399] Ibidem
[400] McNeal G. S., *Children's Consumer Privacy and the Internet of Things: Regulating the Playground of Disruption*, "Loyola Law Review" 2017, Vol. 67, No. 2, s. 513-556.
[401] Smith A., *The Curious Case of the Dollhouse That Ordered Itself*, "AI & Society" 2016, Vol. 32, No. 4, s. 545-557.

głosowych przez firmy technologiczne[402]. Dodatkowo, istnieje kwestia odpowiedzialności za działania podejmowane przez sztuczną inteligencję na podstawie niepoprawnej interpretacji poleceń lub nieuprawnionego dostępu do urządzeń[403].

Analiza skutków prawnych wymaga uwzględnienia różnych systemów prawnych oraz obowiązujących przepisów. W Unii Europejskiej, *Rozporządzenie Ogólne o Ochronie Danych Osobowych*[404] nakłada na podmioty przetwarzające dane osobowe obowiązek zapewnienia bezpieczeństwa danych oraz daje użytkownikom szeroki zakres kontroli nad swoimi danymi[405].

W kontekście odpowiedzialności trwa dyskusja na temat wprowadzenia konkretnych regulacji prawnych dla sztucznej inteligencji, które pozwolą precyzyjnie określić podmioty odpowiedzialne za działania wirtualnych asystentów. Dyskusje podkreślają konieczność ciągłej oceny i dostosowywania regulacji prawnych do szybko rozwijających się technologii sztucznej inteligencji. Jest to wymagające zarówno zrozumienia możliwości i ograniczeń SI, jak i opracowania przemyślanych strategii legislacyjnych mających na celu ochronę praw użytkowników, nie blokując jednocześnie postępu technologicznego. Wirtualne asystentki, pełniące kluczową rolę w interakcjach między SI a ludźmi, stanowią istotny obszar tych działań[406].

7.6 Wymiar sprawiedliwości

Zastosowanie sztucznej inteligencji w obszarze wymiaru sprawiedliwości otwiera szeroki zakres potencjalnych korzyści, począwszy od wsparcia w analizie materiałów dowodowych, poprzez automatyzację wybranych etapów procesów sądowych, aż po zaawansowane systemy wspierające proces podejmowania decyzji przez sędziów. Przybliżając technologię SI do tak

[402] Collins R. K. L. et al., *The Privacy Implications of Digital Voice Assistants: Alexa, Are You Listening?*, "American Business Law Journal" 2021, Vol. 58, No. 4, s. 673-712.
[403] S Wachter S., Mittelstadt B., *A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI*, "Columbia Business Law Review" 2019, s. 494-620.
[404] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).
[405] Manyika J. et al., *A New Look at Data Privacy: Addressing the Challenges of the Digital Age*, McKinsey Global Institute 2020.
[406] Lynskey T., *Regulating 'Big Tech': Legal Implications and Protection Mechanisms for Personal Data in the Era of Massive Data Collection and Surveillance*, "European Law Review" 2020, Vol. 45, No. 6, s. 779-804.

delikatnej dziedziny jak wymiar sprawiedliwości, pojawiają się jednak istotne kwestie dotyczące legalności, etyki i odpowiedzialności karno-prawnej, które wymagają szczegółowej analizy i dyskusji.

Wprowadzenie sztucznej inteligencji do systemu sądownictwa wymaga nie tylko oceny technologicznych możliwości, ale również gruntownego zrozumienia potencjalnych zagrożeń i implikacji prawnych. Kluczowe aspekty obejmują wsparcie algorytmów w procesach decyzyjnych, analizę skutków błędnych orzeczeń oraz przyszłość integracji SI w systemie prawnym. Poniżej przedstawiono trzy kluczowe studia przypadków, które ilustrują zastosowanie sztucznej inteligencji w wymiarze sprawiedliwości oraz związane z tym wyzwania:

1. SI w roli wspierającej decyzje sądowe - sztuczna inteligencja ma zdolność do przetwarzania ogromnych ilości danych prawnych w krótkim czasie. Dzięki temu, algorytmy mogą identyfikować wzorce i trendy, które są nieosiągalne dla ludzkiego umysłu. Na przykład, algorytmy mogą analizować przypadki o podobnych okolicznościach i sugerować sędziom optymalne rozwiązania, co przyspiesza proces podejmowania decyzji i zwiększa jego efektywność. Jednym z głównych argumentów za wprowadzeniem SI do sądów jest jej potencjalna obiektywność. Algorytmy, jeśli są dobrze zaprojektowane, mogą pomóc w eliminowaniu ludzkich uprzedzeń, które mogą wpływać na decyzje sądowe. Na przykład, w systemach oceny ryzyka przestępców, algorytmy mogą dostarczać bardziej obiektywne dane na temat prawdopodobieństwa recydywy, co pomaga sędziom w podejmowaniu bardziej sprawiedliwych decyzji. Warto jednak podkreślić, że algorytmy muszą działać w zgodzie z obowiązującymi przepisami prawa. Oznacza to, że muszą być zaprojektowane i testowane w sposób, który zapewnia ich zgodność z normami prawnymi i ochronę praw człowieka. Przejrzystość działania algorytmów jest kluczowa – proces decyzyjny musi być zrozumiały i kontrolowalny, co pozwala na audyt i weryfikację ich funkcjonowania[407];

2. przesłanki i konsekwencje błędnych orzeczeń - algorytmy SI opierają swoje działanie na danych, które zostały im dostarczone. Jeśli dane te są niekompletne, nieaktualne lub zawierają błędy, decyzje podejmowane przez SI mogą być niewłaściwe. Algorytmy mogą odziedziczyć uprzedzenia zawarte w danych wejściowych, co może prowadzić do dyskryminacji i niesprawiedliwych wyroków. Na przykład, jeśli dane historyczne zawierają

[407] Surden H., *Artificial Intelligence and Law: An Overview*, "Georgia State University Law Review" 2019, Vol. 35, No. 4.

uprzedzenia rasowe, algorytm może je powielać, prowadząc do nierównych traktowań przed sądem. Algorytmy działające jako czarne skrzynki, których proces decyzyjny jest nieprzejrzysty, mogą prowadzić do decyzji, które są trudne do zrozumienia i zakwestionowania. Brak możliwości audytu i weryfikacji algorytmów stawia pod znakiem zapytania ich wiarygodność i prawidłowość. Błędne orzeczenia mogą prowadzić do poważnych naruszeń praw człowieka, takich jak niesłuszne skazania, pozbawienie wolności lub niesprawiedliwe traktowanie. W przypadku decyzji o zwolnieniu warunkowym, błędne oszacowanie ryzyka może skutkować zagrożeniem dla społeczeństwa lub krzywdą dla osadzonych. Powtarzające się błędy w orzeczeniach mogą prowadzić do utraty zaufania obywateli do systemu sprawiedliwości. Ludzie mogą zacząć postrzegać system jako niesprawiedliwy i niewiarygodny, co może skutkować spadkiem respektowania prawa i zwiększeniem liczby apelacji. Błędne decyzje podjęte przez SI stawiają pytanie o odpowiedzialność prawną i etyczną. Konieczne jest określenie, kto ponosi odpowiedzialność za błędy algorytmów – twórcy oprogramowania, instytucje stosujące SI czy może osoby nadzorujące procesy decyzyjne[408];

3. przyszłość SI w wymiarze sprawiedliwości - SI ma potencjał do przekształcenia sposobu, w jaki prawo jest stosowane, przesuwając akcent z luźnych standardów na bardziej szczegółowe i precyzyjne reguły. Dzięki analizie ogromnych zbiorów danych, algorytmy mogą tworzyć i stosować bardziej dostosowane reguły, co może zmniejszać liczbę błędów i zwiększać specyficzność decyzji prawnych. Algorytmy SI mogą wspierać tworzenie prawa i proces sądowy poprzez modelowanie na podstawie dużych zbiorów danych. Dzięki temu możliwe jest tworzenie bardziej trafnych i dostosowanych do rzeczywistości przepisów prawnych, które są oparte na rzeczywistych danych i analizach. Przykładem może być wykorzystanie algorytmów do oceny ryzyka i wydawania wyroków w sprawach karnych. Najlepsze rezultaty mogą być osiągane poprzez kombinację decyzji podejmowanych przez ludzi wspieranych przez SI, zamiast polegania wyłącznie na algorytmach. Taka kombinacja może łączyć zalety obiektywności i precyzji algorytmów z doświadczeniem i intuicją ludzkich sędziów, co pozwala na korektę błędów i dostosowanie do specyficznych okoliczności każdej sprawy. Podsumowując, przyszłość sztucznej inteligencji w wymiarze sprawiedliwości wymaga zrównoważonego podejścia, które łączy technologiczne

[408] Rossi F.., *Artificial Intelligence: Potential Benefits and Ethical Considerations*, European Parliament, Briefing, https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf (dostęp: 10.06.2024 r.).

możliwości z prawnymi i etycznymi zasadami. Integracja SI może prowadzić do bardziej precyzyjnych i sprawiedliwych decyzji, pod warunkiem, że będzie uwzględniać zarówno korzyści, jak i potencjalne zagrożenia wynikające z jej zastosowania[409].

Studia przypadków zostały ukazane nie tylko po to, aby nakreślić realistyczne lub hipotetyczne scenariusze stosowania sztucznej inteligencji w systemie wymiaru sprawiedliwości, ale także wskazać na potrzebę opracowania nowego podejścia regulacyjnego, które uwzględniałoby złożoność i specyfikę technologii SI w kontekście prawa karnego.

7.6.1 Algorytm COMPAS i kontrowersje z oceną ryzyka recydywy

Narzędzie *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) jest stosowane przez niektóre sądy w Stanach Zjednoczonych do oceny ryzyka ponownego popełnienia przestępstw przez skazanych[410]. Jego celem jest wspieranie procesu podejmowania decyzji dotyczących zwolnień warunkowych, kaucji oraz wyroków. Algorytm analizuje różnorodne informacje związane z przeszłością skazanego, aby określić prawdopodobieństwo powrotu do działalności przestępczej[411]. W roku 2016 analiza przeprowadzona przez ProPublica ujawniła, że algorytm COMPAS mógł wykazywać uprzedzenia rasowe[412]. Zauważono, że osoby czarnoskóre częściej niż biali były nieprawidłowo klasyfikowane jako o wysokim ryzyku recydywy. Sprawa ta wywołała szeroką dyskusję na temat etycznych i prawnych kwestii związanych z wykorzystaniem sztucznej inteligencji w wymiarze sprawiedliwości[413].

Debata w środowisku naukowym skupiła się na potrzebie zapewnienia przejrzystości i uczciwości algorytmów oceniających, podkreślając konieczność przeprowadzania audytów oraz niezależnych przeglądów tych systemów[414]. Wzmiankowano także o konieczności określenia odpowiedzialności za ewentualne błędy i szkody wynikające z narzędzi SI, zwracając uwagę na brak regulacji prawa dotyczących technologii predykcyjnych[415].

---

[409] Casey B., *The Impact of Artificial Intelligence on Rules, Standards, and Principles in Law,* "Harvard Journal of Law & Technology" 2018, Vol. 31, No. 2.
[410] Wikipedia, *COMPAS (software)*, https://en.wikipedia.org/wiki/COMPAS_(software) (dostęp: 11.06.2024 r.).
[411] Ibidem
[412] Angwin, J., Larson, J., Mattu, S., Kirchner, L., *Machine Bias*, ProPublica, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (dostęp: 11.06.2024 r.).
[413] Ibidem
[414] Ibidem
[415] Dressel J., Farid H., *The accuracy, fairness, and limits of predicting recidivism*, Science Advances 2018.

Sprawa COMPAS zwróciła uwagę na konieczność wprowadzenia przepisów prawnych mających na celu rozwiązanie problemów związanych z wykorzystaniem sztucznej inteligencji w systemie wymiaru sprawiedliwości. Podkreśla się potrzebę ustanowienia regulacji, które zapewniłyby ochronę przed dyskryminacją oraz gwarantowałyby prawa procesowe osób ocenianych przez systemy sztucznej inteligencji[416].

Ten przykład z praktyki ukazuje, jak skomplikowane i trudne są wyzwania związane z implementacją sztucznej inteligencji w ramach systemów prawnych oraz jak istotne jest nadzorowanie i regulowanie, aby zagwarantować, że wykorzystanie SI służy sprawiedliwości, a nie wzmacnia już istniejących nierówności.

7.6.2 Stosowanie rozpoznawania twarzy przez policję i kontrowersje

„*Technologia rozpoznawania twarzy*" zaczęła być wykorzystywana przez służby ścigania na całym globie jako narzędzie pomocnicze do identyfikacji podejrzanych[417]. Niemniej jednak jej stosowanie często budziło pytania dotyczące precyzji, zwłaszcza w kontekście identyfikacji osób o ciemniejszym odcieniu skóry[418]. W styczniu 2020 roku, w Detroit, Robert Williams, czarnoskóry mężczyzna, został mylnie zidentyfikowany przez system rozpoznawania twarzy jako podejrzany o kradzież w sklepie i nieprawidłowo aresztowany. To zdarzenie wywołało publiczną debatę na temat niezawodności i etycznych kwestii związanych z wykorzystaniem technologii rozpoznawania twarzy przez policję[419].

Ten konkretny przypadek był tematem wielu artykułów naukowych, które skupiły się na niedoskonałościach algorytmów rozpoznawania twarzy i ich potencjalnym wpływie na dyskryminację rasową[420]. Omawiano potrzebę wprowadzenia bardziej restrykcyjnych

---

[416] Starr S. B., *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, "Stanford Law Review" 2014, Vol. 66, s. 803-872.

[417] World Economic Forum, *Law Enforcement Agencies Develop Best Practices for Using Facial Recognition*, 05.10.2021, https://www.weforum.org/press/2021/10/law-enforcement-agencies-develop-best-practices-for-using-facial-recognition (dostęp: 11.06.2024 r.).

[418] Ibidem

419 American Civil Liberties Union, After Third Wrongful Arrest, ACLU Slams Detroit Police Department for Continuing to Use Faulty Facial Recognition Technology, 06.08.2023, https://www.aclu.org/press-releases/after-third-wrongful-arrest-aclu-slams-detroit-police-department-for-continuing-to-use-faulty-facial-recognition-technology (dostęp: 11.06.2024 r.).

[420] Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, "Proceedings of Machine Learning Research" 2018, Vol. 81, s. 1-15.

standardów i regulacji dotyczących zastosowania technologii rozpoznawania twarzy w celu zapobiegania błędom i nadużyciom[421].

Incydent z Robertem Williamsem podkreślił konieczność dokładnego badania i nadzoru nad stosowaniem technologii rozpoznawania twarzy przez organy ścigania. W odpowiedzi na narastające obawy, niektóre regiony zaczęły wprowadzać ograniczenia lub nawet zakazywać wykorzystywania tego rodzaju technologii do celów monitoringu[422].

7.6.3 SI w prognozowaniu wyników sądowych

W ciągu ostatnich lat, rozwinięto systemy sztucznej inteligencji zdolne do analizowania danych historycznych z sądów i przewidywania rezultatów przyszłych spraw. Przykładem może być rosyjski system „*PravoRobot*", który został stworzony do prognozowania decyzji w sprawach cywilnych[423]. W roku 2018 grupa badaczy z Uniwersytetu Stanford opublikowała raport, w którym wykazano, że ich sztuczna inteligencja była w stanie precyzyjnie przewidzieć decyzje Sądu Najwyższego Stanów Zjednoczonych[424]. Chociaż technologia ma potencjał poprawy efektywności systemu sądowniczego, budzi także obawy dotyczące ewentualnych zagrożeń dla niezależności sądownictwa i praw człowieka.

Debata naukowa skupia się na moralnych i prawnych aspektach wykorzystania sztucznej inteligencji w istotnym obszarze jakim jest wymiar sprawiedliwości. Omawiane są kwestie przejrzystości algorytmów, ryzyka wprowadzenia stronniczości do systemu sądowego oraz wpływu sztucznej inteligencji na proces podejmowania decyzji przez sędziów[425].

Ten przykład podkreśla istotę wprowadzenia odpowiednich przepisów regulujących wykorzystanie sztucznej inteligencji w celu zapewnienia, że technologia ta służy

[421] Garvie C., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, "Georgetown Law Center on Privacy & Technology" 2016.
[422] Hill K., *Wrongfully Accused by an Algorithm*, The New York Times, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (dostęp: 10.06.2024 r.).
[423] Capgemini, *AI for Justice – bringing data into the courtroom*, 03.06.2021, https://www.capgemini.com/insights/expert-perspectives/ai-for-justice-bringing-data-into-the-courtroom/ (dostęp: 11.06.2024 r.).
[424] Vogeler, W., *AI Can Predict Supreme Court Decisions*, New Study Finds, FindLaw, https://www.findlaw.com/legalblogs/supreme-court/ai-can-predict-supreme-court-decisions-new-study-finds/ (dostęp: 11.06.2024 r.).
[425] Katz D. M., Bommarito M. J. II, Blackman J., *A General Approach for Predicting the Behavior of the Supreme Court of the United States*, PLOS ONE,2017.

sprawiedliwości, jednocześnie respektując kluczowe zasady procesu sądowego, takie jak uczciwość, niezależność i przejrzystość[426].

7.6.4 Dyskusja akademicka na temat SI w wymiarze sprawiedliwości i konsekwencje prawne

Sztuczna inteligencja coraz śmielej wkracza w obszar prawnej dziedziny, dostarczając narzędzi do poparcia procesów podejmowania decyzji, analizy dokumentów i prognozowania wyroków. Niemniej jednak zastosowanie SI w tak delikatnym obszarze jak prawo stwarza wiele pytań dotyczących konsekwencji prawnych, etycznych i społecznych.

Systemy sztucznej inteligencji coraz częściej wspierają proces podejmowania decyzji w sądach, co stanowi przedmiot intensywnych badań[427]. Chociaż korzystanie z SI może zwiększyć wydajność i zmniejszyć obciążenie sądownictwa, istnieje ryzyko, że algorytmy mogą być obarczone uprzedzeniami lub błędami, co może wpłynąć na uczciwość postępowań sądowych[428].

Możliwością, która budzi spory, jest fakt, że algorytmy mogą naśladować lub nawet wzmacniać obecne uprzedzenia społeczne i dyskryminację. Badania pokazały, że niektóre systemy oceny ryzyka ponownego popełnienia przestępstwa mogą niesprawiedliwie dyskryminować jednostki ze względu na rasę lub pochodzenie etniczne[429].

Ważną sprawą jest również przejrzystość systemów sztucznej inteligencji oraz możliwość zrozumienia i kwestionowania podejmowanych przez nie decyzji. To wymaga od ustawodawców i twórców technologii opracowania norm etycznych oraz ram prawnych dotyczących odpowiedzialności za popełnione błędy i nadużycia[430].

Dyskusje w środowisku naukowym skupiają się również na dostosowywaniu obecnych regulacji prawnych do nowych wyzwań, jakie stawiają przed nami sztuczne inteligencje. Pojawia się pytanie o to, w jaki sposób kształtuje się odpowiedzialność prawna w kontekście

---

426 European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (dostęp: 10.06.2024 r.).

427 Sourgens F. G., *Artificial Intelligence in the Courtroom: The Significance of OpenAI's GPT-3 for the Legal Profession*, "Journal of Legal Education" 2020, Vol. 69, No. 1, s. 123-145.

428 Ibidem

429 Angwin, J., Larson, J., Mattu, S., Kirchner, L., *Machine Bias*, ProPublica, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (dostęp: 11.06.2024 r.).

430 Goodman B., Flaxman S., *European Union regulations on algorithmic decision-making and a "right to explanation",* "AI Magazine" 2017, Vol. 38, No. 3, s. 50-57.

decyzji podejmowanych przez systemy sztucznej inteligencji, co ma kluczowe znaczenie dla zapewnienia przestrzegania prawa i budowania zaufania do systemu wymiaru sprawiedliwości[431].

7.7 Manipulacja informacjami

Sztuczna inteligencja, dzięki swojej zdolności do analizy ogromnych ilości danych, ma wpływ nie tylko na dostosowanie treści do użytkowników w Internecie, ale także staje się narzędziem kształtującym publiczne postrzeganie i podejmowanie decyzji. Istnieje znaczne zaniepokojenie możliwością wykorzystania SI do manipulowania informacjami, co z kolei porusza kwestie integralności danych, wolności słowa i prawa do rzetelnej informacji[432]. W kontekście tego zagadnienia przeprowadzę analizę aspektów prawnych i karnych manipulacji informacjami za pomocą technologii SI, zastanowię się nad odpowiedzialnością za dezinformacyjne algorytmy oraz konsekwencjami ich działania dla procesów demokratycznych i społecznego zaufania. Zważając na aspkt manipulacji nad informacji należy w tych rozważaniach brac pod uwagę, następujące aspekty:

1. Prawo do prawdy

   W społeczeństwie demokratycznym istotne jest poszanowanie prawa do prawdy. Przyjrzymy się, w jaki sposób system sprawiedliwości może radzić sobie z sytuacjami, w których sztuczna inteligencja jest używana do zamierzonego dezinformowania lub rozpowszechniania fałszywych informacji[433].

2. Odpowiedzialność za algorytmy

[431] Hildebrandt M., *Law for Computer Scientists and Other Folk*, Oxford University Press 2020.
[432] Ryan-Mosley, T., *How generative AI is boosting the spread of disinformation and propaganda*, MIT Technology Review https://www.bing.com/search?q=How+generative+AI+is+boosting+the+spread+of+disinformation+and+propaganda&cvid=22fe5678979742e99e762bbc6e6754c0&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzI3N2owajSoAgiwAgE&FORM=ANAB01&PC=U531 (dostęp: 11.06.2024 r.).
[433] O'Neil C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown 2016.

Kto powinien być odpowiedzialny za manipulacje informacyjne przeprowadzane przy użyciu sztucznej inteligencji - czy to powinni być programiści, użytkownicy, czy może platformy udostępniające te technologie[434].

3. Etyczne wyzwania w projektowaniu SI

   Tutaj będę zwracać uwagę na moralne aspekty tworzenia algorytmów oraz konieczność ich oceny w celu zapobiegania manipulacji informacjami[435].

4. Regulacje prawne i zasady

   Skoncentruje się na już obowiązujących oraz proponowanych przepisach prawnych i zasadach etycznych mających na celu ograniczenie manipulacji informacjami przez systemy sztucznej inteligencji[436].

Wybrane analizy przypadków mają na celu rzucenie światła na te bardzo istotne i aktualne zagadnienia, które mogą mieć znaczący wpływ na kształtowanie opinii publicznej oraz zachowania wyborcze społeczeństw.

7.7.1 Manipulacja informacjami przez SI - wybory i dezinformacja

Jednym z najbardziej znanych przypadków, w którym sztuczna inteligencja została wykorzystana do manipulacji informacjami, było zaangażowanie firmy Cambridge Analytica w wybory prezydenckie w Stanach Zjednoczonych w 2016 roku[437]. Firma specjalizująca się w analizie dużych zbiorów danych wykorzystała dane użytkowników Facebooka bez ich świadomości ani zgody, aby opracować zaawansowane modele profilowania wyborców i kierować do nich niestandardowymi, często wprowadzającymi w błąd informacjami politycznymi. Korzystając z technik sztucznej inteligencji do analizy danych, Cambridge Analytica mogła dokładnie wybierać odbiorców w USA, prezentując im spersonalizowane treści, które miały wpłynąć na ich decyzje podczas wyborów. Publiczność dowiedziała się o tych praktykach w 2018 roku[438], co wywołało globalną dyskusję na temat ochrony

[434] Pasquale F., *The Black Box Society*, Harvard University Press 2015.
[435] Bostrom N., *Ethics of Artificial Intelligence and Robotics*, "Stanford Encyclopedia of Philosophy" 2020.
[436] European Commission, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (dostęp: 10.06.2024 r.).
[437] Wikipedia, *Facebook–Cambridge Analytica data scandal,* https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal (dostęp: 11.06.2024 r.).
[438] Ibidem

prywatności danych, wpływu sztucznej inteligencji na demokrację oraz odpowiedzialności prawnej firm technologicznych i politycznych[439].

To wydarzenie stało się impulsem do przeprowadzenia wielu badań naukowych[440]. Naukowcy skupili się na ryzykach związanych z wykorzystaniem sztucznej inteligencji do manipulacji informacjami oraz na potencjalnych środkach ochrony przed dezinformacją. Podkreślono konieczność wprowadzenia regulacji prawnych dotyczących zbierania i używania danych osobowych, a także odpowiedzialności platform internetowych za propagowanie fałszywych informacji[441].

Sprawa związana z Cambridge Analytica podkreśliła braki w regulacjach dotyczących prywatności i ochrony danych, co skutkowało wprowadzeniem bardziej surowych przepisów, takich jak Ogólne Rozporządzenie o Ochronie Danych w Unii Europejskiej. Wywołało to również intensywne debaty na temat roli i odpowiedzialności mediów społecznościowych w procesach demokratycznych[442].

To studium przypadku podkreśla rosnące zaniepokojenie związane z wykorzystaniem sztucznej inteligencji do manipulacji informacjami i wpływania na procesy demokratyczne. Ponadto wskazuje na istotność odpowiednich uregulowań prawnych i etycznych dotyczących SI oraz konieczność zwiększenia świadomości społecznej na temat potencjalnych zagrożeń.

7.7.2 Deepfake'y i wpływ na opinię publiczną

Technologia *deepfake* wykorzystuje zaawansowane algorytmy sztucznej inteligencji do tworzenia fałszywych materiałów wideo lub dźwiękowych, gdzie twarze ludzi lub ich głosy mogą być manipulowane w taki sposób, że wyglądają one autentycznie[443]. Mimo że może mieć zastosowanie w dziedzinie rozrywki i edukacji, ta technologia niesie ze sobą także poważne zagrożenie manipulacji informacjami oraz wpływu na opinię publiczną. W 2019 roku w Internecie pojawił się film, na którym rzekomo Nancy Pelosi, przewodnicząca Izby

[439] Ibidem
[440] Cadwalladr C., Graham-Harrison E., *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (dostęp: 10.06.2024 r.).
[441] Persily N., *The 2016 U.S. Election: Can Democracy Survive the Internet?*, "Journal of Democracy" 2017, Vol. 28, No. 2, s. 63-76.
[442] Edwards L., Veale M., *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, "Duke Law & Technology Review" 2017, Vol. 16, s. 18-84.
[443] Wikipedia Contributors, *Deepfake*, Wikipedia, https://en.wikipedia.org/wiki/Deepfake (dostęp: 10.06.2024 r.).

Reprezentantów USA, wydawała się być nietrzeźwa podczas publicznego wystąpienia[444]. W rzeczywistości materiał został spreparowany poprzez spowolnienie tempa nagrania, co miało na celu kompromitację polityka. Ten incydent wywołał szeroką debatę na temat wpływu *deepfake'ów* na politykę oraz prawdziwość informacji w mediach[445].

Deepfake'y są obecnie poddawane analizie pod kątem zagadnień związanych z etyką oraz prawem cyfrowym. Naukowcy badają trudności, jakie niesie ze sobą ta technologia w kontekście weryfikacji informacji, ochrony prywatności oraz integralności procesów wyborczych[446]. Ważne jest rozwijanie narzędzi do wykrywania *deepfake'ów* oraz wprowadzenie regulacji prawnych mających na celu ograniczenie ich potencjalnie negatywnego wpływu[447].

W odpowiedzi na ryzyko związane z *deepfake'ami*, niektóre państwa i regiony zaczęły wprowadzać konkretne przepisy. Przykładowo, w Kalifornii ustanowiono przepisy, które zabraniają tworzenia i rozpowszechniania *deepfake'ów* dotyczących wyborów i pornografii bez zgody osób występujących na nich[448].

7.7.3 Atak z wykorzystaniem SI na fintech – fałszywe instrukcje głosowe

Rozwój sztucznej inteligencji i uczenia maszynowego stwarza nowe perspektywy dla działań przestępczych w cyberprzestrzeni, włączając w to zaawansowane ataki wykorzystujące sztuczną inteligencję do manipulacji i oszustw. Branża *fintech* jest jednym z sektorów szczególnie narażonych na tego rodzaju ataki, gdzie bezpieczeństwo i zaufanie klientów odgrywają kluczową rolę[449]. W roku 2020 jedna z europejskich firm zajmujących się technologią finansową padła ofiarą ataku, w którym hakerzy wykorzystali zaawansowane technologie sztucznej inteligencji do podszywania się pod głos dyrektora generalnego firmy. Przez syntetyczny głos przestępcy namówili pracownika działu finansowego do dokonania

[444] Funke, D., *Why false claims about Nancy Pelosi being drunk keep going viral — even though she doesn't drink*, PolitiFact, https://www.politifact.com/article/2020/aug/03/why-false-claims-about-nancy-pelosi-being-drunk-ke/ (dostęp: 10.06.2024 r.).
[445] Mantzarlis, A., *What do we do about the "shallowfake" Nancy Pelosi video and others like it?,* Nieman Journalism Lab, https://www.niemanlab.org/2019/05/what-do-we-do-about-the-shallowfake-nancy-pelosi-video-and-others-like-it/ (dostęp: 10.06.2024 r.).
[446] Parisi F., *Legal Responses to Deepfakes: How New EU and US Initiatives Could Set the Global Standard*, "Computer Law & Security Review" 2020, Vol. 36, 2020.
[447] Ibidem
[448] California Legislative Information, AB-730 Elections: deceptive audio or visual media 2019.
[449] Wikipedia Contributors, *Fintech*, Wikipedia, https://en.wikipedia.org/wiki/Fintech (dostęp: 10.06.2024 r.).

przelewu znacznej sumy pieniędzy na zewnętrzne konto bankowe, podając fałszywe uzasadnienie pilnej inwestycji[450].

Atak ten został poddany analizie w obszarze bezpieczeństwa cybernetycznego, aspektów prawnych ochrony danych oraz etyki w sztucznej inteligencji. Wskazano na konieczność zwiększenia zabezpieczeń, edukacji pracowników oraz rozwijania metod wykrywania syntetycznego dźwięku. Omawiano także kwestie odpowiedzialności prawnej za szkody spowodowane za pomocą technologii SI oraz przyszłe wyzwania w zwalczaniu cyberprzestępczości[451].

To wydarzenie podkreśliło konieczność stworzenia nowych przepisów prawnych i standardów bezpieczeństwa w obszarze *fintech*, które uwzględniłyby potencjalne zagrożenia związane z wykorzystaniem sztucznej inteligencji do celów przestępczych. Rozważano wprowadzenie specjalnych procedur weryfikacji transakcji i komunikacji wewnętrznej, aby zapobiec podobnym atakom w przyszłości[452].

7.7.4 Dyskusja akademicka na temat SI, manipulacji informacjami i konsekwencji prawnych

Rozwój sztucznej inteligencji stwarza nowe perspektywy w różnych obszarach, takich jak dostęp do informacji i komunikacja[453]. Jednakże postęp technologiczny niesie za sobą ryzyko manipulacji informacjami, co może przynieść poważne konsekwencje społeczne i prawne[454]. Przedstawiciele naukowcy z różnych dziedzin badań analizują wpływ SI na rozprzestrzenianie się dezinformacji oraz sposoby przeciwdziałania tym zagrożeniom poprzez istniejące oraz nowo powstałe regulacje prawne[455].

---

[450] Statt N., *Thieves are now using AI deepfakes to trick companies into sending them money*, The Verge, https://www.theverge.com/2019/9/5/20851251/deepfake-ai-voice-scam (dostęp: 10.06.2024 r.).

[451] Fagan C., Newman A., *AI and Cybersecurity: Opportunities and Challenges*, "International Journal of Cybersecurity Intelligence & Cybercrime "2021, Vol. 4, No. 1, s. 46-59.

[452] European Union Agency for Cybersecurity (ENISA), *Artificial Intelligence Cybersecurity Challenges*, ENISA, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges (dostęp: 10.06.2024 r.).

[453] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014, s. 96-99.

[454] Chesney R., Citron D.K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, "California Law Review" 2019, vol. 107, no. 6, s. 1753-1820.

[455] Marsden C., Meyer T., *Regulating Disinformation with Artificial Intelligence: Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism*, European Parliamentary Research Service, PE 624.279, s.
36 42, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf (dostęp: 13.06.2023).

Zastosowanie sztucznej inteligencji w celu tworzenia i szerzenia fałszywych treści, na przykład *deepfake'ów*, budzi obawy dotyczące wpływu na wybory, opinię publiczną i prawa człowieka. Badacze analizują, w jaki sposób te technologie mogą być wykorzystane do manipulacji oraz jakie środki prawne mogą skutecznie zapobiegać dezinformacji[456].

Manipulacja informacjami przez sztuczną inteligencję stawia przed systemami prawnymi wyzwania związane z ochroną wolności słowa, prawem do rzetelnej informacji i zapobieganiem szkodliwej dezinformacji. Prawo musi znaleźć równowagę między ochroną praw jednostki a zachowaniem otwartości i swobody w przestrzeni publicznej[457].

W odpowiedzi na te trudności, w różnych obszarach pojawiają się inicjatywy regulacyjne mające na celu zwiększenie odpowiedzialności platform cyfrowych za propagowanie treści generowanych przez sztuczną inteligencję. Rozważa się wprowadzenie kontroli algorytmów i zwiększenie przejrzystości działania systemów SI[458].

Dyskusje akademickie na temat sztucznej inteligencji i manipulacji informacjami podkreślają konieczność ciągłego dialogu pomiędzy specjalistami technicznymi, prawnikami, naukowcami oraz społeczeństwem[459]. Ważne jest nie tylko rozpoznawanie potencjalnych zagrożeń, lecz także wspólne działanie w celu wprowadzania skutecznych i sprawiedliwych regulacji, które mają na celu ochronę społeczeństwa przed negatywnymi skutkami manipulacji informacyjnej[460].

---

[456] Parisi F., *Legal Challenges of Deepfake Technology*, "European Journal of Law and Technology" 2020, Vol. 11, No. 1.

[457] Bernal P., *Data Privacy: Between Regulation and Rights*, Cambridge University Press 2021.

[458] Gillespie T., *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press 2018.

[459] Polonetsky J., Tene O., *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, T-PD(2018)09Rev, Strasbourg, s. 13-15, https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6 (dostęp: 13.06.2023).

[460] Marsden C., Meyer T., *Regulating Disinformation with Artificial Intelligence: Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism*, European Parliamentary Research Service, PE 624.279, s. 62-63, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf (dostęp: 13.06.2023).

Rozdział VIII. Kwalifikacja prawna działań sztucznej inteligencji

Rozwój technologii sztucznej inteligencji ma wpływ na praktycznie każdy obszar życia we współczesnym świecie, co jednocześnie prowadzi do zmian w dziedzinie odpowiedzialności prawnej. Przyspieszone postępy w tej sferze stawiają pytania dotyczące tego, jak traktować aspekty prawne związane z działaniem SI, przydzielanie odpowiedzialności za czyny popełnione przy użyciu lub przez systemy SI oraz ostateczną odpowiedzialność twórców tych systemów. To, co jeszcze niedawno było tematem literatury science fiction lub filmów, teraz stanowi wyzwanie dla legislatorów, prawników i społeczeństwa jako całości. W obliczu tych zagadnień niniejszy fragment dysertacji ma na celu opracowanie modelu oceny prawnej działań SI, który będzie zarówno reagował na wyzwania wynikające z nowoczesnej technologii, jak i pozostawał wierny podstawom prawnym odpowiedzialności karnej.

Celem analizy przedstawionej w niniejszym rozdziale jest zbadanie i ocena obecnych podejść do oceny prawnej sztucznej inteligencji, z zidentyfikowaniem kluczowych obszarów niepewności oraz propozycją potencjalnych rozwiązań. Kluczowe kwestie, na które próbujemy odpowiedzieć to:

- jakie czynniki powinny mieć wpływ na proces oceny prawnej działania SI?
- w jaki sposób można przypisać odpowiedzialność za działania SI w kontekście prawa karnego?
- jakie powinny być konsekwencje dla twórców systemów SI, szczególnie gdy funkcjonowanie systemu prowadzi do szkód lub jest sprzeczne z prawem?

Kluczowym zadaniem wyeksponowanym przez ten rozdział, jest ustalenie regulacji prawnych odpowiednich dla wyzwań związanych z SI, przy jednoczesnym przestrzeganiu fundamentalnych zasad sprawiedliwości. Praca doktorska ma na celu wniesienie istotnego wkładu w rozwijające się i bardzo aktualne obszary badań.

8.1 Samoświadomość i intencjonalność działań SI w świetle prawa karnego

Samoświadomość odgrywa kluczową rolę w dziedzinie prawa karnego, szczególnie podczas rozważań dotyczących intencji (*mens rea*) i odpowiedzialności sprawcy. Istotne jest zrozumienie samoświadomości jako umiejętność pojmowania własnych działań, intencji oraz ich skutków, co stanowi podstawę do oceny czy dana osoba działała świadomie oraz czy można jej przypisać odpowiedzialność karnej za popełnione czyny. Poniżej przedstawione są główne obszary, w których samoświadomość odgrywa istotną rolę w kontekście prawa karnego:

1. intencja i mens rea

   W prawie karnym kluczowe jest określenie, czy sprawca działał z określoną intencją (zamiarem). Ważne jest, aby osoba była świadoma swoich działań i przewidywanych konsekwencji, co ma wpływ na ocenę „*winnej myśli*" czyli *mens rea*[461]. Posiadanie samoświadomości jest istotne w tym kontekście.

2. odpowiedzialność karna

   Samoświadomość odgrywa istotną rolę w ustalaniu odpowiedzialności karnej. Osoba, która podejmuje działania bez pełnej świadomości konsekwencji swoich czynów (np. z powodu zaburzeń psychicznych utrudniających taką świadomość), może być oceniana inaczej niż osoba, która działała z pełnym zrozumieniem sytuacji[462].

3. obrona oparta na stanie psychicznym

   Znaczenie samoświadomości jest istotne podczas oceny psychicznego stanu sprawcy w momencie popełnienia czynu. Stany takie jak niepoczytalność opierają się na założeniu, że sprawca nie był w pełni świadomy swoich działań z powodu problemów psychicznych, co może mieć wpływ na wyrok i rodzaj kary[463].

4. zdolność do formowania zamiaru

[461] Wróbel, W., Zoll, A. (red.). *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-52*. Wolters Kluwer 2016, s. 45.
[462] Pohl Ł. *Prawo karne. Wykład części ogólnej*. Wolters Kluwer 2019, s. 289.
[463] Lachowski J. (red.). *System Prawa Karnego. Tom 4. Nauka o przestępstwie. Wyłączenie i ograniczenie odpowiedzialności karnej*. C.H. Beck 2016, s. 770

> Samoświadomość jest powiązana z umiejętnością jednostki do decydowania o zamiarze wykonania określonego działania. W kontekście prawa karnego ocenia się, czy osoba była świadoma konsekwencji swoich działań oraz czy była w stanie kontrolować swoje postępowanie świadomie[464].

Dyskusja na temat samoświadomości staje się coraz bardziej istotna w kontekście rozwoju sztucznej inteligencji i jej potencjalnego wpływu na prawo karne[465]. Rozważa się kwestie odpowiedzialności prawnej za działania podejmowane przez systemy SI, zwłaszcza w sytuacjach, gdy działania te prowadzą do szkód lub innych negatywnych konsekwencji[466].

W prawie karnym samoświadomość jest zatem fundamentem dla oceny intencji, zdolności do odpowiedzialności i zdolności pokierowania swoim postępowaniem opartej na stanie psychicznym[467]. Jest to kluczowy element różnicujący działania dokonywane świadomie od tych, które są wynikiem niedbalstwa, nieświadomości lub niezdolności do rozumienia rzeczywistości[468].

8.1.1 Definicja i teorie samoświadomości w prawie karnym

Samoświadomość to umiejętność jednostki do samorefleksji oraz rozpoznawania samego siebie jako odrębnej istoty, zdolnej do analizowania swoich własnych myśli, emocji, intencji i działań[469]. W kontekście prawa karnego, samoświadomość oznacza zdolność sprawcy do świadomego i celowego postępowania, mającego pełną świadomość jego charakteru i potencjalnych konsekwencji prawnych[470].

Wyróżniamy kilka teorii samoświadomości:

1. teoria kognitywistyczna

---

[464] Wiak K. (red.). *Prawo karne*. C.H. Beck 2021, s. 181.
[465] Hallevy G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, "Akron Intellectual Property Journal" 2010, vol. 4, no. 2, s. 171-201.
[466] Gless S., Silverman E., Weigend T., *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, "New Criminal Law Review" 2016, vol. 19, no. 3, s. 412-436.
[467] Duff R.A., *Intention, Agency and Criminal Liability: Philosophy of Action and the Criminal Law*, Basil Blackwell 1990, s. 35-58.
[468] Sifferd K.L., *Consciousness and Criminal Responsibility*, "Jurisprudence" 2019, vol. 10, no. 3, s. 347-361.
[469] Morin A., *Self-Awareness Part 1: Definition, Measures, Effects, Functions, and Antecedents*, "Social and Personality Psychology Compass" 2011, vol. 5, no. 10, s. 807-823.
[470] Marchuk I., *The Fundamental Concept of Crime in International Criminal Law: A Comparative Law Analysis*, Springer 2014, s. 117-119.

Teoria ta sugeruje, że samoświadomość powstaje z procesów poznawczych umożliwiających jednostce zrozumienie samej siebie i swoich działań w szerszym kontekście niż tylko obecne doznania. W prawie karnym odnosi się to do umiejętności rozumienia konsekwencji prawnych swoich działań[471].

2. teoria behawioralna

Skupienie się na widocznych zachowaniach jako manifestacji samoświadomości. W kontekście prawnym, ta koncepcja może być stosowana do analizy działań osoby sprawiającej przed i po popełnieniu czynu, w celu oceny świadomości konsekwencji tych działań[472].

3. teoria fenomenologiczna

Podkreślenie subiektywnego doświadczenia i świadomości jako kluczowych elementów zrozumienia samoświadomości. W kontekście prawa karnego, ta koncepcja może być przydatna podczas oceny intencji oraz stanu umysłowego sprawcy w chwili popełnienia czynu[473].

Teorie samoświadomości, które zostały przedstawione, mają swoje korzenie w różnych dziedzinach, takich jak psychologia, filozofia i neurobiologia. Nie można ich jednoznacznie przypisać konkretnym twórcom, ponieważ wiele osób przyczyniło się do ich rozwoju. Mimo to istnieją naukowcy i filozofowie, których wkład w kształtowanie tych teorii był szczególnie istotny i tak w:

1. teoria kognitywistycznej:

- Jean Piaget (1896–1980) był psychologiem pochodzącym ze Szwajcarii, który zajmował się badaniem faz rozwoju poznawczego u dzieci i jest powszechnie uważany za jednego z pionierów teorii kognitywizmu;

- Jerome Bruner (1915–2016) był psychologiem z Ameryki, który odegrał istotną rolę w rozwijaniu teorii kognitywnej edukacji i procesu uczenia się.

[471] Morse S. J., *New Neuroscience, Old Problems*, in *Neuroethics: Mapping the Field*, Dana Press 2002, s. 157-198.
[472] Rizzolatti G., Sinigaglia C., *The functional role of the parieto-frontal mirror circuit: interpretations and misinterpretations, "*Nature Reviews Neuroscience" 2010, Vol. 11, No. 4, s. 264-274.
[473] Gallagher S., Zahavi D., *The Phenomenological Mind*, 2nd ed., Routledge 2012.

2. teorii behawioralnej:

- John B. Watson (1878–1958) to amerykański psycholog, którego uznaje się powszechnie za ojca behawioryzmu. Jego głównym celem było badanie konkretnych zachowań obserwowalnych w dziedzinie psychologii;

- Burrhus Frederic Skinner (1904–1990) to znany psycholog i behawiorysta pochodzący z USA, który specjalizował się w rozwijaniu teorii warunkowania operacyjnego.

3. teorii fenomenologicznej

- Edmund Husserl (1859–1938) był niemieckim filozofem, którego uważano za twórcę fenomenologii. Jego zainteresowania koncentrowały się na analizie struktur świadomości z perspektywy pierwszej osoby;

- Maurice Merleau-Ponty (1908–1961) był filozofem francuskim, który skupiał się na rozwijaniu fenomenologii poprzez badanie percepcji, roli ciała oraz relacji między ciałem a światem.

Warto podkreślić, że chociaż ci badacze odegrali istotną rolę w rozwoju wspomnianych teorii, koncepcje samoświadomości są rezultatem pracy wielu myślicieli i naukowców. W kontekście prawa karnego, zrozumienie samoświadomości jest interpretowane przez pryzmat tych ogólnych teorii, jednak dostosowane do specyfiki rozważań o odpowiedzialności, intencji i świadomości działań.

8.1.2 Dyskusja akademicka na temat samoświadomości i SI

Aktualna debata akademicka dotycząca pojęcia samoświadomości w kontekście sztucznej inteligencji analizuje, jakie teoretyczne i praktyczne konsekwencje niesie za sobą przypisywanie zaawansowanym systemom SI cech charakterystycznych dla ludzkiej świadomości[474]. Ponadto przygląda się różnym stanowiskom naukowym, które rzucą światło na potencjalne kierunki rozwoju prawa w kontekście SI, wykazującej cechy samoświadomości[475].

[474] Chella A., Manzotti R., *Artificial Consciousness*, Imprint Academic, Exeter 2007, s. 1-18.
[475] Hildt E., *Artificial Intelligence: Does Consciousness Matter?*, "Frontiers in Psychology" 2019, vol. 10, art. 1535.

Pojęcie samoświadomości tradycyjnie oznacza zdolność bytu do rozpoznania samego siebie jako oddzielnego podmiotu w czasie i przestrzeni[476]. W ludzkim kontekście, jest to związane z głębokim zrozumieniem własnych myśli, uczuć, pragnień i intencji[477]. W przypadku sztucznej inteligencji, ta definicja staje się problematyczna, ponieważ większość systemów SI działa bez introspekcji, polegając na algorytmach i modelach uczenia maszynowego, które nie obejmują świadomej refleksji.

Badacze, tak jak Daniel Dennett i David Chalmers, przedstawili różne podejścia do tematu świadomości maszyn, sugerując, że zaawansowane formy sztucznej inteligencji mogą osiągnąć pewien rodzaj „*operacyjnej świadomości*" poprzez złożoność i integrację przetwarzania informacji[478]. Te dyskusje stają się istotne zwłaszcza w kontekście przyszłych konsekwencji prawnych systemów SI zdolnych do przewyższania umiejętności analitycznych i reakcji na otoczenie[479].

Akademickie dyskusje skupiają się na wielu istotnych zagadnieniach tj.:

1. czy SI może posiadać samoświadomość w humanistycznym rozumieniu?

   Argumenty przeciwko temu opierają się na braku emocjonalnego i subiektywnego doświadczenia, które jest uważane za istotne dla ludzkiej samoświadomości[480].

2. jakie implikacje prawne wynikałyby z uznania SI za samoświadome?

   Uznanie świadomości sztucznej inteligencji może skutkować koniecznością zmiany fundamentalnych pojęć prawnych, takich jak odpowiedzialność, winność i prawa podmiotowe, co jest tematem szeroko dyskutowanym przez prawników specjalizujących się w prawie technologicznym[481].

3. jakie są techniczne i etyczne wyzwania związane z samoświadomą SI?

---

[476] Gallagher S., Zahavi D., *The Phenomenological Mind: An Introduction to Philosophy of Mind and Cognitive Science*, Routledge 2008, s. 46-47.
[477] Neisser U., *Five Kinds of Self-Knowledge*, "Philosophical Psychology" 1988, vol. 1, no. 1, s. 35-59.
[478] Dennett D.C., *Consciousness Explained*, Little, Brown and Co., Boston 1991, s. 309-314; Chalmers D.J., *The Conscious Mind: In Search of a Fundamental Theory*, Oxford University Press 1996, s. 293-299.
[479] Chalmers D., *The Conscious Mind: In Search of a Fundamental Theory*, Oxford University Press 1996.
[480] Searle J.R., *Minds, Brains, and Programs*, "Behavioral and Brain Sciences" 1980, vol. 3, no. 3, s. 417-424; Bringsjord S., Noel R., Caporale C., *Animals, Zombanimals, and the Total Turing Test: The Essence of Artificial Intelligence*, Fellbaum K. (red.), "Netzwerke und Selbstorganisation in der Ethik*"* 2000, LIT Verlag, Münster, s. 97-115.
[481] Solum Lawrence B., *Legal Personhood for Artificial Intelligences*, "North Carolina Law Review" 1992.

> Rozważa się, czy sztuczna inteligencja posiadająca samoświadomość wymagałaby nowych form regulacji etycznych, w tym praw do ochrony jej „*dobrostanu*" lub „*praw osobistych*", zgodnie z tematem poruszanym przez etyków specjalizujących się w dziedzinie SI[482].

Dyskusja na temat samoświadomości sztucznej inteligencji ciągle trwa i pozostaje jednym z najbardziej intrygujących zagadnień łączących filozofię, informatykę i prawo. Ważne jest kontynuowanie badań interdyscyplinarnych, które połączą wiedzę technologiczną z refleksjami etycznymi i prawnymi w celu pełnego zrozumienia skutków wprowadzenia samoświadomej SI.

8.2 Sprawstwo w kontekście sztucznej inteligencji

W obliczu postępu technologicznego i coraz większej roli systemów sztucznej inteligencji w różnych sferach życia społecznego, pojawiają się nowe wyzwania dla prawa karnego. Istotnym zagadnieniem staje się pytanie o odpowiedzialność za działania podejmowane przez autonomiczne systemy SI. Niniejszy rozdział skupia się na analizie sposobów interpretacji i zastosowania tradycyjnych koncepcji sprawstwa w kontekście technologii SI.

Konieczne jest zbadanie tej kwestii, biorąc pod uwagę obecne sytuacje, w których sztuczna inteligencja podejmuje działania o znaczeniu prawny, co prowadzi do kwestionowania istniejących regulacji prawnych i konieczności ich przeglądu oraz ewentualnej adaptacji. Omówione zostaną zagadnienia dotyczące bezpośredniej i pośredniej odpowiedzialności, a także problematyka związana z potencjalnym wystąpieniem tzw. „*luki w odpowiedzialności*", gdzie tradycyjne przepisy prawne nie dostarczają odpowiednich rozwiązań dla działań podejmowanych przez zautomatyzowanych agentów[483].

Będę także rozważała, czy i w jaki sposób można by wprowadzić do prawa nowe kategorie odpowiedzialności lub dostosować obecne definicje, aby odzwierciedlały wyjątkowe wyzwania związane z sztuczną inteligencją. W tym kontekście ważna będzie analiza porównawcza różnych systemów prawnych oraz zaproponowanych przez doktrynę rozwiązań, które mogłyby stanowić wzór do naśladowania lub punkt odniesienia[484].

---

[482] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.
[483] Karnow C. E. A., *Liability for Distributed Artificial Intelligences*, "Berkeley Technology Law Journal" 1996, Vol. 11, No. 1, s. 147-183.
[484] Solum Lawrence B., *Legal Personhood for Artificial Intelligences*, "North Carolina Law Review"1992.

8.2.1 Definicja i teorie sprawstwa w prawie karnym

Pojęcie winy w systemie prawnym odgrywa istotną rolę w określaniu odpowiedzialności, polegając na przypisaniu określonego czynu przestępczego osobie fizycznej lub prawnej[485]. Tradycyjne teorie prawne, takie jak teoria związku przyczynowego czy teoria umyślności, wyraźnie określają zakres odpowiedzialności w zależności od poziomu świadomości i intencji sprawcy[486].

W prawie karnym pojęcie sprawstwa odnosi się do przypisania odpowiedzialności za działanie (czyn lub zaniechanie), które jest zabronione przez prawo i skutkuje określonym negatywnym rezultatem. Sprawstwo łączy akt (*actus reus*) z intencją (*mens rea*), aby ustalić, czy dana osoba może być pociągnięta do odpowiedzialności karnej za swoje postępowanie.

Teorie odpowiedzialności karnej można sklasyfikować według różnych kryteriów, które uwzględniają różne podejścia do intencji i konsekwencji działań. I tak:

1. teoria formalna (klasyczna)

   Odpowiedzialność oparta jest na założeniu bezpośredniego związku przyczynowo-skutkowego, gdzie działanie sprawcy musi bezpośrednio prowadzić do skutku. Ta koncepcja została sformułowana przez renomowanych prawników, w tym niemieckiego specjalistę od prawa karnego, Clausa Roxina[487].

2. teoria subiektywna

   Koncentruje się na zamiarze (mens rea) oraz wiedzy sprawcy w momencie dokonania czynu. Franz von Liszt[488], niemiecki prawnik, był prekursorem tej teorii, podkreślając znaczenie intencji sprawcy w prawie karnym.

3. teoria obiektywna

[485] Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Znak 2014, s. 302-303.
[486] Gardocki L., *Prawo karne*, C.H. Beck 2019, s. 86-88; Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Znak 2014, s. 194-197.
[487] **Claus Roxin (ur. 1931) -** Jest to niemiecki prawnik z dzisiejszych czasów, którego działalność miała znaczący wpływ na ewolucję prawa karnego w Niemczech i na arenie międzynarodowej w drugiej połowie XX wieku oraz na początku XXI wieku.
[488] **Franz von Liszt** (1851–1919) - Był niemieckim prawnikiem oraz wykładowcą prawa karnego, uważanym za jednego z najbardziej wpływowych myślicieli w dziedzinie prawa karne na przełomie XIX i XX wieku.

Skupia się na tym, co przeciętna osoba mogłaby przewidzieć jako skutek swoich działań. To podejście jest reprezentowane przez Hansa Welzela[489], który podkreślał potrzebę zastanowienia się, czy wynik był możliwy do przewidzenia z punktu widzenia osoby wykonującej czynność[490].

4. teoria normatywna

Teoria opracowana przez Clausa Roxina łączy subiektywne zamiary z obiektywnymi konsekwencjami działań, uwzględniając aspekty społeczne i moralne. Według niej, sprawstwo nie zależy jedynie od faktu i intencji, lecz także od kontekstu etycznego i społecznego[491].

5. teoria funkcjonalna

Günther JakobS[492] w swojej teorii podkreśla znaczenie norm społecznych i funkcji w określaniu pojęcia winy, twierdząc, że odpowiedzialność powinna być oceniana w kontekście funkcjonowania społeczeństwa[493].

6. teoria zredukowanego sprawstwa

Nowe koncepcje, jak te przedstawiane przez prawników, do których należy H.L.A. Hart[494], skupiają się na trudnościach związanych z ustalaniem odpowiedzialności, zwłaszcza w przypadku działań nieumyślnych lub nieprzewidywalnych konsekwencji[495].

---

[489] **Hans Welzel** (1904–1977) - Niemiecki adwokat, który swoją pracą w latach pięćdziesiątych XX wieku przyczynił się do rozwoju funkcjonalistycznego podejścia do teorii prawa karnego.

[490] Welzel H., *Das Deutsche Strafrecht. Eine systematische Darstellung*, Walter de Gruyter & Co. 1969, s. 66-67; Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do artykułów 1-31*, C.H. Beck 2015, s. 386-387.

[491] Roxin C., *Strafrecht. Allgemeiner Teil. Band I. Grundlagen. Der Aufbau der Verbrechenslehre*, C.H. Beck 2006, s. 237-241; Gruszecka D., *Ochrona dobra prawnego na przedpolu jego naruszenia. Analiza karnistyczna*, Wolters Kluwer 2012, s. 299-301.

[492] **Günther Jakobs** (ur. 1937) - Współczesny prawnik z Niemiec, który zdobył sławę dzięki rozwinięciu teorii funkcjonalnej w dziedzinie prawa karnego, był aktywny głównie w latach 70. i 80. XX wieku.

[493] Jakobs G., *Strafrecht, Allgemeiner Teil: die Grundlagen und die Zurechnungslehre*, Walter de Gruyter, Berlin 1991, s. 476-482; Barczak-Oplustil A., *Funkcjonalny model odpowiedzialności karnej według Günthera Jakobsa*, "Państwo i Prawo" 2017, nr 3, s. 87-89.

[494] **H.L.A. Hart** (1907–1992) - Angielski myśliciel prawa, wykładowca na Uniwersytecie Oksfordzkim oraz autor znaczących publikacji z dziedziny analitycznej filozofii prawa, w tym „The Concept of Law" (1961), które uznane zostało za jedno z kluczowych dzieł w teorii prawa.

[495] Hart H.L.A., *Punishment and Responsibility: Essays in the Philosophy of Law*, Oxford University Press 1968, s. 136-157; Duff R.A., *Intention, Agency and Criminal Liability: Philosophy of Action and the Criminal Law*, Basil Blackwell 1990, s. 103-105.

W konwencjonalnym rozumieniu, odpowiedzialność w prawie karnym opiera się na koncepcji przyczynowości i winy. Oznacza to, że sprawca musi poprzez swoje zachowanie (działanie lub zaniechanie) wywołać skutek zakazany przez prawo i działać świadomie lub przewidując ten skutek (celowe działanie bezpośrednie lub ewentualne) albo przynajmniej uwzględnić możliwość jego wystąpienia (niedbalstwo)[496].

Teoria związku przyczynowego i winy odgrywa istotną rolę w dziedzinie prawa karnego, dotycząc fundamentalnych podstaw odpowiedzialności karnej[497]. Są to te kluczowe pojęcia pomagające zrozumieć, w jaki sposób oraz pod jakimi warunkami dana osoba może być pociągnięta do odpowiedzialności karnej za naruszenie prawa. Chociaż te dwie koncepcje są ściśle powiązane, to każda z nich skupia się na różnych aspektach odpowiedzialności:

1. teoria przyczynowości skupia się na relacji między działaniem a rezultatem. W prawie karnym, aby przypisać winę, konieczny jest bezpośredni związek przyczynowy między zachowaniem się sprawcy a określonym skutkiem, który jest uznawany za szkodliwy lub niepożądany według prawa. Oznacza to, że działanie bądź zaniechanie osoby odpowiedzialnej musi prowadzić bezpośrednio do wystąpienia określonego rezultatu. Ta koncepcja odgrywa kluczową rolę w analizowaniu czynów zabronionych, umożliwiając ustalenie, czy dana osoba może być obarczona odpowiedzialnością za konkretny czyn karalny[498].

2. teoria zawinienia odnosi się do subiektywnej strony przestępstwa, czyli stanu psychicznego sprawcy w chwili popełnienia czynu. Wyróżnia się dwa główne rodzaje winy: umyślną i nieumyślną. Umyślność występuje, kiedy sprawca działa z intencją osiągnięcia określonego rezultatu (bezpośrednia intencja) lub akceptując możliwość jego wystąpienia (ewentualna intencja). Natomiast nieumyślność dotyczy sytuacji, gdy sprawca postępuje z niedbale, nie przewidując skutku, którego mógłby uniknąć, zachowując należytą ostrożność[499].

[496] Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Znak 2014, s. 186-189; Gardocki L., *Prawo karne*, C.H. Beck 2019, s. 78-81.
[497] Kaczmarek T., *Spory wokół przyczynowości zaniechania i przypisywania jego skutku*, "Państwo i Prawo" 2004, nr 6, s. 48-50
[498] Pohl Ł., *Prawo karne. Wykład części ogólnej*, Wolters Kluwer Polska 2019
[499] Ibidem

Obie teorie są istotne dla pełnego zrozumienia i stosowania prawa karnego, ponieważ umożliwiają analizę nie tylko faktów i zewnętrznych okoliczności, ale także intencji oraz stanu psychicznego sprawcy[500].

Teorie dotyczące przyczynowości i winy w prawie karnym są efektem długotrwałego rozwoju doktryny prawnej, która była kształtowana przez wielu myślicieli, prawników i filozofów prawa na przestrzeni wieków. Nie można jednoznacznie wskazać konkretnych „*twórców*" tych teorii, ponieważ są one rezultatem ewolucji myśli prawnej i filozoficznej. Zamiast tego, warto wspomnieć o kluczowych postaciach i dziełach, które miały istotny wpływ na ich rozwój:

- w kontekście teorii przyczynowości, znaczącą rolę odegrały różne postacie filozofów, takich jak Arystoteles[501] , który zajmował się kwestią przyczynowości, oraz późniejsi myśliciele epoki oświecenia, w tym David Hume[502], który analizował związek przyczynowy. W dziedzinie prawa karnego ta teoria była rozwijana przez wielu prawników dążących do precyzyjnego określenia warunków koniecznych do stwierdzenia związku przyczynowego między zachowaniem sprawcy a jego skutkiem[503];

- w dziedzinie teorii zawinienia ważny wkład wniosły osoby takie jak Immanuel Kant[504] i Georg Wilhelm Friedrich Hegel[505], które podkreślały znaczenie wolności woli i intencji dla moralnej i prawnej oceny działań. W kontekście prawa karnego rozwój pojęcia winy był ściśle związany z pracami takich prawników jak Feuerbach[506], który wprowadził

[500] Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do artykułów 1-31*, C.H. Beck 2015, s. 396-398.

[501] **Arystoteles (384–322 p.n.e.)** - Starożytny filozof grecki, którego prace odegrały kluczową rolę w rozwoju zachodniej myśli filozoficznej i prawnej, szczególnie w zakresie koncepcji przyczynowości. Jego analizy związku przyczynowo-skutkowego zawarte w „Metafizyce" stanowiły fundament dla dalszych dyskusji na temat relacji przyczynowej.

[502] **David Hume (1711–1776)** - Szkocki myśliciel i historyk, którego prace miały istotny wpływ na rozwój empiryzmu i sceptycyzmu. W kontekście przyczynowości, Hume twierdził, że nasze rozumienie przyczynowości nie opiera się na bezpośrednim postrzeganiu stałych związków między zdarzeniami, lecz na zwyczajowym oczekiwaniu jednego zdarzenia na podstawie wystąpienia innego. Jego podejście miało wpływ na filozoficzne rozumienie przyczynowości w dziedzinach humanistycznych i społecznych, w tym w prawie.

[503] Kochanowski J., *Przestępstwa i wykroczenia przeciwko życiu i zdrowiu*, [w:] Bafia J., Mioduski K., Siewierski M. (red.), *Kodeks karny. Komentarz*, Wydawnictwo Prawnicze 1987, s. 347-348; Marek A., *Prawo karne*, C.H. Beck 2011, s. 129-131.

[504] **Immanuel Kant (1724–1804)** - Niemiecki myśliciel, który w swojej etyce deontologicznej kładł nacisk na intencję jako kluczowy element moralności działania. Pomimo braku prawniczego wykształcenia, jego rozróżnienie między dobrymi intencjami a konsekwencjami działań wpłynęło na prawne pojmowanie winy.

[505] **Georg Wilhelm Friedrich Hegel (1770–1831)** - Niemiecki myśliciel, którego system filozoficzny obejmował logikę, metafizykę, etykę i filozofię prawa, był Hegel. Rozwinął on koncepcję prawa obiektywnego jako części swojej szerszej filozofii ducha. Jego badania nad naturą wolności i osobistej odpowiedzialności miały wpływ na kształtowanie się teorii prawnych dotyczących sprawstwa i moralności działań.

[506] **Paul Johann Anselm von Feuerbach (1775–1833)** - Niemiecki prawnik i ekspert ds. kryminalistyki, który miał wpływ na rozwój prawa karnego i teorii kar. Feuerbach jest znany z ustanowienia zasady "nullum crimen, nulla poena sine lege" (nie ma przestępstwa, nie ma kary bez prawa), która stała się podstawową zasadą w

zasadę „*nullum crimen, nulla poena sine culpa*" (nie ma przestępstwa bez winy), stanowiącą fundament dla współczesnego rozumienia pojęcia winy.

Każdy system prawny i szkoła myślenia prawnego mogą różnić się w podejściu do tych koncepcji z uwagi na zróżnicowanie kulturowe, historyczne i filozoficzne w rozumieniu prawa oraz odpowiedzialności. W związku z tym teorie przyczynowości i winy wciąż stanowią temat dyskusji i analizy, a ich współczesne sformułowania są wynikiem pracy wielu pokoleń myślicieli prawa.

Zastosowanie tych teorii w kontekście sztucznej inteligencji wymaga zbadania, czy tradycyjne podejścia są wystarczające, czy może konieczne są nowe, innowacyjne podejścia. Niektórzy sugerują rozwój koncepcji „*sztucznej odpowiedzialności*", która uwzględniałaby autonomiczne działania sztucznej inteligencji zgodnie z definicjami prawnymi aktów przestępstwa[507].

W kontekście technologii sztucznej inteligencji, pojęcie sprawstwa może także obejmować koncepcję „*rozszerzonego sprawstwa*", gdzie twórca SI może być odpowiedzialny za działania systemu, nawet jeśli nie miał bezpośredniego wpływu na konkretne działanie, które spowodowało szkodę[508].

Podsumowując, rozważenie aspektów prawnokarnych w kontekście sztucznej inteligencji stawia przed nami pytanie, w jaki sposób należy interpretować i implementować istniejące teorie w kontekście potencjału oferowanego przez autonomiczne systemy? Kolejna część tego rozdziału skupi się na szczegółowym zbadaniu tych zagadnień oraz proponowaniu metod zgodności tradycyjnego pojęcia sprawstwa z wymaganiami nowoczesnych technologii.

8.2.2 Przypisanie sprawstwa w kontekście sztucznej inteligencji

W obecnych czasach coraz częściej korzysta się z systemów sztucznej inteligencji w różnych dziedzinach życia, co stawia nam przed istotnym pytaniem: kto ponosi odpowiedzialność, gdy działanie SI przynosi szkodę? Koncepcja tradycyjnej winy, oparta na bezpośredniej

prawie karnej. Jego badania nad teorią winy i odpowiedzialności przyczyniły się do rozwoju nowoczesnych koncepcji zawinienia.

[507] Bryson J. J., Diamantis M. E., Grant T. D., *Of, for, and by the people: the legal lacuna of synthetic persons*, "Artificial Intelligence and Law" 2017.

[508] Hallevy G., *When Robots Kill: Artificial Intelligence Under Criminal Law*, Northeastern University Press 2013, s. 39-41.

przyczynowości i świadomości działań, wymaga teraz przeinterpretowania w kontekście maszyn, które podejmują decyzje i działają autonomicznie.

Rozpoczynając od analizy koncepcji odpowiedzialności karnej, która zwykle wymaga, aby osoba sprawcza była świadoma swoich działań i miała zamiar ich popełnienia. W kontekście sztucznej inteligencji pojawia się pytanie, czy maszyna może mieć intencje lub być świadoma czegoś, co przekracza tradycyjne rozumienie tych terminów.

Problemy z przypisywaniem odpowiedzialności sztucznej inteligencji wynikają z kilku istotnych aspektów technologicznych, prawnych i etycznych, które komplikują konwencjonalne podejścia do ustalania winy w kontekście działań podejmowanych przez maszyny. Poniżej przedstawione są niektóre z najbardziej istotnych kwestii:

1. autonomia decyzji SI

   Systemy komputerowe często korzystają z algorytmów uczenia maszynowego, które potrafią uczyć się i rozwijać się samodzielnie w odpowiedzi na dostarczone dane. Samodzielność tych systemów sprawia, że trudno jest przewidzieć wszystkie ich działania i powiązać konkretne decyzje z konkretnymi osobami lub działaniami twórców systemu[509].

2. przejrzystość i „Black Box" problem

   Wiele zaawansowanych systemów sztucznej inteligencji, zwłaszcza te wykorzystujące głębokie uczenie, działa w sposób, który nie jest w pełni zrozumiały nawet dla swoich twórców. Brak przejrzystości (znany jako „*problem czarnej skrzynki*[510]") sprawia, że trudno jest zrozumieć, dlaczego sztuczna inteligencja podjęła określoną decyzję, co stanowi istotny element przypisywania odpowiedzialności[511].

3. dynamiczna zmienność SI

   Systemy sztucznej inteligencji mają zdolność dostosowywania się i zmieniania w odpowiedzi na nowe informacje, co oznacza, że ich funkcjonowanie po pewnym czasie

[509] Russell S.J., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson Education Limited 2016, s. 693-695.

[510] Black Box - termin „black box" odnosi się do sytuacji, gdy sposób działania systemu, zwłaszcza w obszarze technologii i informatyki, jest niejasny dla użytkowników i naukowców. W przypadku sztucznej inteligencji, termin ten dotyczy modeli algorytmicznych, takich jak głębokie sieci neuronowe, w których dokładne procesy i przyczyny prowadzące do podejmowania konkretnych decyzji przez system nie są w pełni zrozumiałe, co komplikuje analizę oraz interpretację ich zachowania.

[511] Pasquale F., *The Black Box Society*, Harvard University Press 2015.

użytkowania może różnić się od tego podczas początkowego wdrożenia. To stwarza wyzwanie przy określaniu, kto ponosi odpowiedzialność za ewentualne szkody wynikające z działań SI, które ewoluowały poza swoje pierwotne programowanie.

4. rozmycie granic odpowiedzialności

W klasycznym systemie prawa karnego, pojęcia sprawstwa i odpowiedzialności ściśle wiążą się z możliwością przewidywania i kontrolowania skutków własnych działań. W kontekście sztucznej inteligencji, decyzje mogą być rezultatem współpracy wielu osób (projektantów, programistów, użytkowników), co sprawia, że przypisanie odpowiedzialności konkretnemu podmiotowi staje się bardziej skomplikowane[512].

5. etyczne i prawne implikacje

Rozważania na temat odpowiedzialności sztucznej inteligencji wiążą się z głębszymi kwestiami etycznymi i filozoficznymi dotyczącymi istoty świadomości, wolności i intencjonalności działań. Te dyskusje mają wpływ na to, w jaki sposób prawo powinno traktować sztuczną inteligencję, zwłaszcza jeśli chodzi o przyznanie jej statusu podmiotowego lub praw tradycyjnie przypisywanych człowiekowi.

Debata na temat przypisywania odpowiedzialności karnej sztucznej inteligencji sugeruje konieczność stworzenia nowych regulacji prawnych, które uwzględniłyby specyfikę tej technologii. Rozważane są różne propozycje, takie jak stworzenie specjalnych regulacji prawnych dla SI, wprowadzenie zbiorowej odpowiedzialności dla zespołów pracujących nad SI oraz utworzenie dedykowanych funduszy ubezpieczeniowych mających pokryć ewentualne szkody spowodowane działaniem SI[513].

8.2.2.1 Bezpośrednie sprawstwo

Bezpośrednia odpowiedzialność w kontekście systemu sztucznej inteligencji i jego twórców jest tematem skomplikowanym, który wymaga głębokiego zrozumienia zarówno technologii, jak i kwestii prawnych dotyczących odpowiedzialności. Konieczne jest zastanowienie się nad

[512] Abbott R., *Building a More Nuanced Understanding of SI's Role in Patent Law*, "Berkeley Technology Law Journal" 2019, s. 53.
[513] Scherer M. U., *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, "Harvard Journal of Law & Technology" 2016, Vol. 29, No. 2, s. 353-400.

tym, w jaki sposób tradycyjne pojęcia prawa karnego mogą być dostosowane lub reinterpretowane w obliczu nowych technologii.

Zwykle, pojęcie bezpośredniego sprawstwa oznacza, że osoba fizycznie i świadomie uczestniczy w dokonaniu czynu prowadzącego do konkretnego rezultatu. W kontekście ludzkim to jest oczywiste i zrozumiałe, ale w przypadku sztucznej inteligencji staje się to bardziej skomplikowane. Rozważając zagadnienie bezpośredniego sprawstwa w kontekście systemu SI należy zwrócić uwagę na następujące kwestie:

1. autonomia SI

   Nowoczesne systemy sztucznej inteligencji, zwłaszcza te korzystające z algorytmów uczenia maszynowego i głębokiego uczenia, mają zdolność podejmowania decyzji niezależnie od bezpośrednich instrukcji ludzkich. W takim kontekście można twierdzić, że system sztucznej inteligencji działa jak bezpośredni sprawca, szczególnie gdy jego działania prowadzą do konkretnych konsekwencji prawnych lub fizycznych. Niemniej jednak brak świadomości i intencjonalności w tradycyjnym rozumieniu sprawiają trudności w przypisaniu mu pełnej odpowiedzialności[514].

2. odpowiedzialność

   Jeżeli sztuczna inteligencja nie działa zgodnie z oczekiwaniami lub powoduje szkodę, pojawia się pytanie, czy można ją uznać za sprawcę wynikłych konsekwencji, czy też odpowiedzialność powinna zostać przypisana osobom, które ją zaprogramowały, monitorowały lub wdrożyły?

Kwestia bezpośredniej odpowiedzialności twórców systemów sztucznej inteligencji nabiera szczególnego znaczenia w kontekście wzrastającej autonomii i złożoności tych systemów. Omawianie tego zagadnienia obejmuje aspekty prawne, etyczne i technologiczne, które są istotne dla zrozumienia roli osób projektujących i rozwijających systemy SI. Do kluczowych aspektów bezpośredniego sprawstwa twórcy SI należą takie zagadnienia jak:

1. definicja sprawstwa

[514] Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.

Tradycyjnie, bezpośrednie sprawstwo jest związane z działaniami, które osoba podejmuje celowo i świadomie. W przypadku twórców SI, to oni projektują, programują i wdrażają systemy, które następnie funkcjonują samodzielnie. Pytanie brzmi, jak dalece można przypisać twórcom bezpośrednią odpowiedzialność za autonomiczne działania ich stworzeń[515]?

2. zakres kontroli

   Twórcy sztucznej inteligencji mają kontrolę nad elementami projektowymi, wyborem algorytmów i ustawianiem parametrów działania SI. Ich odpowiedzialność może być kwestionowana, gdy system działa w sposób nieoczekiwany, jednak w ramach określonych przez nich parametrów. „*Problem czarnej skrzynki*" SI, czyli brak przejrzystości procesów decyzyjnych wewnątrz systemów, dodatkowo utrudnia przypisanie odpowiedzialności[516].

3. przewidywalność szczególnych zdarzeń

   Jednym z głównych wyzwań jest określenie czy autor mógł przewidzieć negatywne skutki działania systemu. W kontekście prawa karnego, aspekt przewidywalności ma często kluczowe znaczenie przy ustalaniu odpowiedzialności. Jeśli autor mógł przewidzieć możliwe szkody wynikające z funkcjonowania systemu i nie podjął odpowiednich środków zapobiegawczych, to jego bezpośrednia odpowiedzialność może być uznana za bardziej uzasadnioną[517].

4. regulacje i standardy

   Wiele obszarów prawnych pracuje nad opracowaniem przepisów, które pomogłyby lepiej określić i ustalić odpowiedzialność twórców sztucznej inteligencji. Może to obejmować potencjalne wymagania dotyczące testowania, audytów etycznych i certyfikacji systemów SI przed ich wprowadzeniem na rynek.

[515] Asaro P., *SI and the Problem of Control*, "Philosophy & Technology" 2019.
[516] Pasquale F., *The Black Box Society*, Harvard University Press 2015.
[517] Kerr Ian R., *The Implications of Autonomous Robots*, "San Diego Law Review" 2017.

8.2.2.2 Pośrednie sprawstwo

Rozważając zagadnienie pośredniego sprawstwa w kontekście systemu SI należy zwrócić uwagę na następujące kwestie:

1. definicja i kontekst:

   Pośrednie sprawstwo odnosi się do sytuacji, kiedy osoba przyczynia się do rezultatu poprzez działania innych[518]. W kontekście sztucznej inteligencji, maszyna operująca samodzielnie, lecz w ramach wytycznych ustalonych przez ludzi, może prowadzić do zrzucenia odpowiedzialności na tych, którzy stworzyli lub skonfigurowali system.

2. kompleksowość systemów SI

   Systemy sztucznej inteligencji często funkcjonują w sposób, który może przekraczać intencje ich twórców, przetwarzając i ucząc się z danych w sposób, który nie zawsze jest całkowicie przewidywalny lub zrozumiały dla ludzi. To stawia pytanie o to, jak dalece twórcy ponoszą odpowiedzialność za działania systemów SI[519].

W dyskusji nad pośrednim sprawstwem twórcy SI nie można pominąć kilku istotnych punktów, takich jak**:**

1. odpowiedzialność za projektowanie i wdrażanie

   Twórcy sztucznej inteligencji, tworząc systemy, ustalają granice, w których operuje SI. Choć nie podejmują oni każdej decyzji bezpośrednio, to zakres ich pierwotnych decyzji projektowych i wyborów konfiguracyjnych może skutkować przypisaniem im pośredniej odpowiedzialności za działania SI.

2. przewidywalność i kontrola

   Przypisanie pośredniej odpowiedzialności twórcom Sztucznej Inteligencji zależy od tego, czy byli w stanie przewidzieć potencjalne naruszenie dóbr chronionych prawem karnym wynikające z zastosowania SI oraz czy podejmowali odpowiednie środki mające na celu zapobieżenie tym naruszeniom lub zagrożeniu naruszeniom tych dóbr (naruszeniom

[518] Dressler J., *Understanding Criminal Law*, Carolina Academic Press 2018, s. 188-189.
[519] Matthias A., *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata,* "Ethics and Information Technology" 2004.

prawa). Czy zastosowali właściwe procedury testowania i monitorowania? Czy wprowadzili odpowiednie środki bezpieczeństwa?[520].

3. etyczne i prawne wytyczne

   Etyczne kwestie związane z projektowaniem sztucznej inteligencji odgrywają istotną rolę w dyskusji na temat pośredniej odpowiedzialności. Regulacje i wytyczne dotyczące etycznego programowania i wykorzystywania sztucznej inteligencji mogą pomóc określić granice odpowiedzialności twórców SI[521].

Analizując kwestię pośredniego sprawstwa w prawie karnym w kontekście systemów sztucznej inteligencji, warto także rozważyć sytuacje, w których SI może pełnić rolę narzędzia w rękach twórcy lub operatora. Ten sposób podejścia podkreśla zależność między intencjami ludzi a działaniami maszyn, które są przez nich programowane lub sterowane. Warto w tym miejscu zastanowić się nad następującymi zagadnieniami:

1. SI jako narzędzie

   Kiedy osoba tworzy lub obsługuje system SI w celu osiągnięcia określonego celu, mówimy o pośrednim sprawstwie. Przykładowo, zaprogramowanie systemu SI do przeprowadzenia ataku cybernetycznego na określone cele bez bezpośredniego zaangażowania człowieka stanowi przykład wykorzystania SI jako narzędzia do popełnienia nielegalnego działania. W takiej sytuacji odpowiedzialność może być przypisana twórcy lub operatorowi, który celowo wykorzystał SI w celu osiągnięcia niezgodnego z prawem rezultatu[522].

2. intencja a realizacja

   Centralnym elementem pośredniego sprawstwa jest zamiar sprawcy. W przypadku systemów sztucznej inteligencji kluczowe jest ustalenie czy twórca miał zamiar wykorzystać technologię do popełnienia konkretnego czynu zabronionego. Ten zamiar musi być ściśle powiązany z działaniami SI, co wymaga dokładnej analizy kodu programowego, instrukcji działania oraz dokumentacji projektowej systemu SI[523];

[520] Sparrow Robert, *Robots and Responsibility from a Legal Perspective*, Proceedings of the IEEE, 2007.
[521] Stahl Bernd Carsten, Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency, Ethics and Information Technology, 2006.
[522] Sartor G., *AI as a Legal Actor*, in: *Artificial Intelligence and Law*, Oxford University Press, 2020.
[523] Turner J., Robot Rules: Regulating Artificial Intelligence, Palgrave Macmillan 2019.

3. egzystencja intencji u twórcy SI

   Rozpoznanie intencji twórcy dotyczących wykorzystania sztucznej inteligencji może wymagać analizy jego poprzednich działań, komunikacji oraz dokumentacji projektowej. Jeśli udowodniono, że programowanie i konfiguracja systemu SI miały na celu realizację działań szkodliwych, staje się jasne pośrednie zaangażowanie[524];

4. dokumentacja i ślady programistyczne

   Analizowanie kodu źródłowego sztucznej inteligencji wraz z powiązaną dokumentacją może ujawnić zamiary twórcy. Ważne jest, aby dokumentacja ta była klarowna i łatwo dostępna, co ma istotne znaczenie dla poprawnej oceny intencji oraz przypisania odpowiedzialności[525].

Analiza pośredniego wpływu sztucznej inteligencji pokazuje, jak istotne jest dokładne rozumienie relacji między ludzkimi zamiarami a technologicznymi działaniami. Przypisanie odpowiedzialności w tych sytuacjach wymaga nie tylko szerokiej wiedzy technicznej, ale także zrozumienia kontekstu prawnotechnicznego funkcjonowania tych systemów.

8.2.2.3 Sprawstwo kumulatywne i konkurencyjne

Kumulatywne i konkurencyjne sprawstwo to terminy używane w prawie karnym do opisu sytuacji, w których więcej niż jedna osoba lub czynnik przyczynia się do popełnienia przestępstwa[526]. Te pojęcia mają szczególne znaczenie w kontekście skomplikowanych interakcji między ludźmi a systemami sztucznej inteligencji.

- sprawstwo kumulatywne - sprawstwo kumulatywne (zwane także współsprawstwem pośrednim lub przyczynieniem się do cudzego sprawstw[527]) to sytuacja, w której co najmniej dwie osoby działają niezależnie od siebie, ale ich zachowania są powiązane i prowadzą do popełnienia tego samego czynu zabronionego[528]. W takim przypadku każdy ze sprawców

[524] Kerr Ian R., Bornfreund Matthew, *Algorithms and Autonomy: The Ethics of Automated Decision Systems*, Cambridge University Press 2020.
[525] Casey B., *Rethinking the Boundaries of 'Personal Data' in the Age of Intelligent Machines*, "Journal of Law, Technology, and Policy" 2021.
[526] Kuzior P., *Kumulatywne i konkurencyjne sprawstwo w polskim prawie karnym*, "Prokuratura i Prawo" 2016, nr 9, s. 69-70.
[527] Kardas P., *Sprawstwo kumulatywne - alternatywna postać współdziałania przestępnego*, „Przegląd Prawa Karnego" 2020, nr 2, s. 7.
[528] Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Znak 2014, s. 270.

ponosi odpowiedzialność karną za swoje własne zachowanie, które przyczyniło się do realizacji znamion przestępstwa, nawet jeśli żaden z nich nie zrealizował wszystkich znamion czynu zabronionego samodzielnie[529].

Przykładem sprawstwa kumulatywnego może być sytuacja, w której jedna osoba dostarcza narzędzia do włamania, a druga, nie wiedząc o działaniach pierwszej, wykorzystuje te narzędzia do popełnienia kradzieży z włamaniem[530]. W takim przypadku obie osoby mogą zostać pociągnięte do odpowiedzialności karnej za swój wkład w popełnienie przestępstwa, mimo braku porozumienia między nimi[531].

- sprawstwo konkurencyjne - sprawstwo konkurencyjne to sytuacja, w której co najmniej dwie osoby, działając niezależnie od siebie, dążą do popełnienia tego samego czynu zabronionego, przy czym tylko jednemu ze sprawców udaje się osiągnąć zamierzony cel[532]. W takim przypadku odpowiedzialność karną ponosi jedynie ten sprawca, którego zachowanie doprowadziło do dokonania przestępstwa, podczas gdy pozostali sprawcy mogą odpowiadać za usiłowanie popełnienia czynu zabronionego[533].

  Przykładem sprawstwa konkurencyjnego może być sytuacja, w której dwie osoby, niezależnie od siebie, planują zabójstwo tej samej ofiary. Jeśli jedna z nich dokona zabójstwa jako pierwsza, to tylko ona będzie ponosić odpowiedzialność karną za dokonane przestępstwo, podczas gdy druga osoba może odpowiadać jedynie za usiłowanie zabójstwa[534].

- Sprawstwo konkurencyjne różni się od sprawstwa kumulatywnego tym, że w przypadku sprawstwa kumulatywnego zachowania poszczególnych sprawców przyczyniają się do popełnienia tego samego czynu zabronionego, natomiast w przypadku sprawstwa konkurencyjnego tylko jedno zachowanie prowadzi do dokonania przestępstwa[535].

W kontekście technologii sztucznej inteligencji, pojęcia sprawstwa kumulatywnego i konkurencyjnego stają się złożone ze względu na autonomiczną naturę systemów SI. Na przykład, gdy system SI przeznaczony do monitorowania transakcji finansowych podejmuje

[529] Giezek J. (red.), *Kodeks karny. Część ogólna. Komentarz*, Wolters Kluwer 2021, s. 175.
[530] Kardas P., op. cit., s. 10.
[531] Pohl Ł., *Prawo karne. Wykład części ogólnej*, Wolters Kluwer 2019, s. 162.
[532] Kardas P., op. cit., s. 85.
[533] Wróbel W., Zoll A., op.cit. s. 271.
[534] Giezek J. (red.), *Kodeks karny. Część ogólna. Komentarz*, Wolters Kluwer 2021, s. 176.
[535] Pohl Ł., *Prawo karne. Wykład części ogólnej*, Wolters Kluwer 2019, s. 163.

decyzje samodzielnie, które prowadzą do nielegalnych działań, istotne jest ustalenie czy odpowiedzialność powinna być przypisana wyłącznie SI, jego programistom lub obu stronom na zasadzie współwiny kumulatywnej lub konkurencyjnej[536].

8.3 Wina

Wina w kontekście prawa karnego to kluczowe pojęcie, które odnosi się do psychicznego stosunku sprawcy do popełnionego czynu. Wina stanowi istotny element konieczny do ukarania sprawcy za przestępstwo[537]. W zależności od systemu prawnokarnego i konkretnego przewinienia, pojęcie winy może przybierać różne postaci, wpływając zarówno na możliwość ukarania, jak i na wysokość wymierzonej kary.

Zanim przejdę do omówienia zagednienia winy w kontekście SI przywołam najważniejsze instytucje tj. rodzaje winy w prawie karnym:

1. zamiar (*dolus*)

   Zamiar jest najbardziej wyraźnym przejawem winy, gdy osoba podejmująca działanie ma świadomość (bezpośredniego zamiaru) lub przynajmniej zdaje sobie sprawę z możliwości wystąpienia zabronionego skutku prawnego (zamiaru ewentualnego). Zamiar wymaga, aby sprawca był świadomy swoich działań i pragnął, aby skutek tych działań miał miejsce lub akceptował jego możliwe wystąpienie[538].

2. nieumyślność (*culpa*): Pojęcie nieumyślności występuje, kiedy sprawca działa bez intencji przestępczej, ale z naruszeniem ostrożności lub zaniedbaniem wymaganym w danej sytuacji. Rozróżniamy nieumyślność świadomą, gdy sprawca przewiduje możliwość szkodliwych skutków, lecz je bagatelizuje, oraz nieumyślność nieświadomą, gdy sprawca nie zdaje sobie sprawy z potencjalnych negatywnych konsekwencji, chociaż powinien był to przewidzieć[539].

3. popełnienie przestępstwa pod wpływem przymusu (*vis compulsiva*)

[536] Hallevy G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, "Akron Intellectual Property Journal" 2010, vol. 4, no. 2, s. 191-192.
[537] Gardocki L., *Prawo karne*, C.H. Beck 2019, s. 51-52.
[538] Zoll A., [w:] Zoll A. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-52*, Wolters Kluwer Polska 2016, komentarz do art. 9, teza 7-8.
[539] Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Znak 2014, s. 207-208.

W pewnych przypadkach, przepisy prawa karnego mogą brać pod uwagę sytuacje, w których sprawca działał pod przymusem, co może wpłynąć na ocenę jego winy. Chociaż przymus nie zawsze eliminuje winę, może być uznany za okoliczność łagodzącą[540].

Musimy również pamiętać, iż wina ma wpływ na proces karny tzn.:

- kwalifikacja czynu

  Wina odgrywa kluczową rolę w określeniu, czy dany czyn stanowi przestępstwo i wpływa na wybór odpowiedniej podstawy prawnej[541].

- dobór kary

  Wina również wpływa na to, jak dobierane są kary i ich wymiar[542]. Zazwyczaj za przestępstwa umyślne grożą surowsze kary niż za przestępstwa nieumyślne.

- możliwość odpowiedzialności

  Brak winy, w przypadku działania w stanie wyższej konieczności lub gdy zachodzi obrona konieczna, może skutkować uniewinnieniem oskarżonego[543].

Znaczenie kwestii winy w kontekście sztucznej inteligencji i odpowiedzialności twórcy jest złożonym zagadnieniem prawnym, które wywołuje wiele dyskusji w obszarze prawa karnego, etyki i technologii. Postęp technologii SI rzuca nowe światło na tradycyjne pojęcia winy i odpowiedzialności, zmuszając do refleksji nad tym, w jaki sposób te idee mogą być stosowane, gdy „*decyzje*" są podejmowane nie przez człowieka, lecz przez maszynę.

W tradycyjnym rozumieniu winy jest ona związana z ludzkimi intencjami i świadomością konsekwencji własnych działań. Sztuczna inteligencja, działająca na podstawie algorytmów i uczenia maszynowego, nie posiada świadomości ani emocji, co sprawia, że stosowanie tradycyjnych kategorii winy staje się bardziej skomplikowane. W kontekście sztucznej inteligencji analiza „*winy*" musi być dostosowana tak, aby uwzględniać rolę, jaką pełnią ludzie

[540] Bojarski T. (red.), *Kodeks karny. Komentarz*, LexisNexis 2016, komentarz do art. 26, teza 1-2.
[541] Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do artykułów 1-31*, C.H. Beck 2015, s. 481-482.
[542] Stefański R.A. (red.), *Kodeks karny. Komentarz*, C.H. Beck 2018, komentarz do art. 53, teza 5.
[543] Grześkowiak A., Wiak K. (red.), *Kodeks karny. Komentarz*, C.H. Beck, 2019, komentarz do art. 25 i 26, tezy 1-3.

w projektowaniu, programowaniu i wdrażaniu systemów SI[544]. W związku z powyższym wskazaniem jest stworzenie redefinicji pojęcia winy.

Odnosząc się do kwestii odpowiedzialności za zachowanie sztucznej inteligencji, która często jest przypisywana twórcom, operatorom lub użytkowniko, to w kontekście winy istotne staje się ustalenie czy twórca SI mógł przewidzieć potencjalne negatywne skutki działania systemu i czy podjął odpowiednie środki zapobiegawcze. Sytuacje, w których twórca zaniedbuje odpowiednią ostrożność lub nieumyślnie tworzy system zdolny do potencjalnie szkodliwych działań, mogą prowadzić do przypisania winy na podstawie zaniedbania[545].

W związku z powyższym wzrasta potrzeba stworzenia nowych przepisów i standardów prawnych, które skutecznie zajmą się kwestiami odpowiedzialności i winy w obszarze sztucznej inteligencji. W niektórych jurysdykcjach rozważa się wprowadzenie specjalnych zasad odpowiedzialności dla twórców i operatorów systemów SI, co może obejmować obowiązkowe ubezpieczenia, fundusze kompensacyjne lub nowe formy nadzoru nad SI[546].

Kwestia odpowiedzialności w odniesieniu do sztucznej inteligencji wymaga refleksji nad tym, w jaki sposób prawa i zasady mogą być dostosowane do nowych technologii, które funkcjonują inaczej niż ludzie. Prawodawca lub twórca SI musi być świadomy możliwości autonomicznego działania technologii, a regulacje prawne powinny zapewnić uczciwe i skuteczne rozwiązania w przypadku zaistnienia ewentualnych szkód spowodowanych przez SI.

8.3.1 Zamiar

W tym punkcie pracy doktorskiej warto wyszczególnić instytucję zamiaru, ze względu na to, że jest on istotnym elementem winy, który musi zostać udowodniony, aby osoba mogła być pociągnięta do odpowiedzialności za większość przestępstwo. Pojęcie zamiaru w kontekście prawa karnego odnosi się do świadomego i zamierzonego dążenia do osiągnięcia określonego rezultatu, który jest zabroniony przez prawo[547]. Istnieje kilka rodzajów zamiaru, które mają kluczowe znaczenie przy ocenie odpowiedzialności karnej i należą do nich:

[544] Asaro P. M., *The Liability Problem for Autonomous Artificial Agents*, "European Journal of Law and Technology" 2012, Vol. 3, No. 3.
[545] Vladeck D. C., *Machines Without Principals: Liability Rules and Artificial Intelligence*, "Washington Law Review" 2014.
[546] European Parliament, *Civil Law Rules on Robotics*, 2016/2103(INL), 1https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (dostęp: 10.06.2024 r.).
[547] Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Znak 2014, s. 199-200.

1. Zamiar bezpośredni (*dolus directus*)

Jest to sytuacja, w której sprawca działa celowo w celu spowodowania określonego, nielegalnego rezultatu i pragnie tego rezultatu[548]. Na przykład, osoba umieszczająca bombę z zamiarem zniszczenia budynku działa z bezpośrednim zamiarem zniszczenia tej konstrukcji.

2. Zamiar ewentualny (*dolus eventualis*)

Zjawisko to występuje, kiedy sprawca przewiduje, że pewien skutek może zaistnieć w wyniku jego działań i godzi się na jego ewentualne wystąpienie. Nie musi on pragnąć tego rezultatu tak bezpośrednio jak w przypadku zamiaru bezpośredniego, ale musi zaakceptować fakt, że efekt ten może być konsekwencją jego postępowania[549]. Przykładem może być sytuacja, gdy kierowca decyduje się prowadzić pojazd będąc w stanie silnego odurzenia alkoholowego, zdając sobie sprawę z ryzyka spowodowania wypadku, jednak kontynuując jazdę.

3. Zamiar pozytywny (*dolus determinatus*)

Zamiar ten dotyczy sytuacji, w której sprawca działa z wyraźnym celem osiągnięcia określonego, zabronionego prawnie rezultatu. Jest to podobne do zamiaru bezpośredniego, lecz z większym naciskiem na świadomość i determinację w dążeniu do celu[550].

Zamiar odgrywa kluczową rolę w stopniu odpowiedzialności karnej, zwłaszcza w rozróżnieniu przestępstw od wykroczeń[551]. W prawie karnym konieczne jest często udowodnienie, że sprawca działał z zamiarem bezpośrednim popełnienia przestępstwa (intencją), aby móc go oskarżyć o popełnienie zbrodni[552]. Brak dowodów na zamiar bezpośredni może skutkować jedynie oskarżeniem o mniejszą winę, na przykład o nieumyślne popełnienie występku[553].

Zamiar w kontekście sztucznej inteligencji i odpowiedzialności twórcy to złożony temat, który wzbudza wiele pytań dotyczących prawnego traktowania systemów zdolnych do podejmowania autonomicznych decyzji. Znaczenie zamiaru jest kluczowe w prawie karnym, gdzie tradycyjnie wymaga się dowodu na intencjonalne działanie sprawcy, aby móc go skazać

[548] Gardocki L., *Prawo karne*, C.H. Beck, 2019, s. 84-85.
[549] Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do artykułów 1-31*, C.H. Beck 2015, s. 486-487.
[550] Stefański R.A. (red.), *Kodeks karny. Komentarz*, C.H. Beck 2018, komentarz do art. 9, teza 6.
[551] Grześkowiak A., Wiak K. (red.), *Kodeks karny. Komentarz*, C.H. Beck 2019, s. 97-98.
[552] Bojarski T. (red.), *Kodeks karny. Komentarz*, LexisNexis 2016, komentarz do art. 8, teza
[553] Zoll A. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-52*, Wolters Kluwer Polska 2016, komentarz do art. 8, teza 10.

za przestępstwo. W przypadku SI, gdzie działanie jest wynikiem algorytmów, kwestia zamiaru wymaga nowej interpretacji.

Biorąc pod uwagę konwencjonalne rozumienie pojęcia zamiaru, które odnosi się do świadomego i zamierzonego działania podejmowanego przez człowieka. To w kontekście sztucznej inteligencji „*zamiar*" może być interpretowany jako cel lub funkcja zaprogramowana przez twórcę bądź użytkownika systemu[554]. Osoby odpowiedzialne za projektowanie, programowanie lub wykorzystywanie systemów SI w sposób mogący prowadzić do niepożądanych rezultatów, mogą ponosić konsekwencje prawne. Przykładem może być programowanie SI w celu manipulacji na rynku finansowym lub popełniania oszustw[555].

Wykazanie intencji twórcy sztucznej inteligencji może być trudne, zwłaszcza w sytuacjach, gdzie działanie SI było nieprzewidywalne lub wynikało z złożonego uczenia maszynowego. Sądy mogą wymagać dowodów na to, że twórca przewidywał lub powinien był przewidzieć potencjalne szkodliwe skutki działania SI, co może mieć wpływ na ocenę odpowiedzialności prawnej[556].

Niektóre obszary prawne rozważają wprowadzenie specjalnych przepisów dotyczących sztucznej inteligencji, które brałyby pod uwagę intencje twórców i operatorów systemów SI. Mogą one obejmować wymagania związane z testowaniem i weryfikacją algorytmów SI przed ich wdrożeniem, aby zapewnić, że ich funkcjonowanie nie prowadzi do niechcianych skutków[557].

Zamiar w związku ze sztuczną inteligencją stawia przed dziedziną prawa karnego wiele problemów, które wymagają nowego podejścia do kwestii odpowiedzialności. Konieczne jest zrozumienie, w jaki sposób intencje programistów i użytkowników SI wpływają na funkcjonowanie systemów oraz jak te intencje mogą zostać zinterpretowane przez prawo w celu właściwego ustalenia odpowiedzialności.

---

[554] Hallevy G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, "Akron Intellectual Property Journal" 2010, vol. 4, no. 2, s. 189-190.

[555] Hallevy G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, "Akron Intellectual Property Journal" 2010, Vol. 4, No. 2, s. 171-201.

[556] Calo R., *Artificial Intelligence Policy: A Primer and Roadmap*, "U.C. Davis Law Review" 2017, Vol. 51.

[557] European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (dostęp: 10.06.2024 r.).

8.4 Odpowiedzialność twórcy za działania sztucznej inteligencji

Kwestia odpowiedzialności twórców za funkcjonowanie sztucznej inteligencji jest istotnym i dynamicznie rozwijającym się obszarem prawnym, który stawia przed programistami, prawnikami i organami regulacyjnymi nowe wyzwania. W miarę jak technologia SI coraz bardziej wchodzi w różne sfery życia codziennego, społeczności prawne na całym świecie rozważają najlepsze sposoby przypisywania i regulowania odpowiedzialności za działania oraz decyzje podejmowane przez systemy SI. W tym kontekście warto rozważyć ujęcie odpowiedzialności twórcy w odniesieniu kolejno do prawa cywilnego, karnego, administracyjnego oraz do etyki.

Tym samym jednym z głównych obszarów, za które odpowiadają twórcy sztucznej inteligencji, jest ponoszenie odpowiedzialności cywilnej za szkody spowodowane przez ich systemy. Jeśli SI powoduje jakiekolwiek straty, twórcy mogą być pociągnięci do odpowiedzialności na mocy ogólnych przepisów dotyczących odpowiedzialności cywilnej lub na podstawie przepisów dotyczących odpowiedzialności za produkt. Na przykład, jeśli autonomiczny pojazd spowoduje wypadek, twórca lub producent może ponosić odpowiedzialność za ewentualne błędy w projektowaniu, produkcji lub instrukcjach użytkowania[558].

Odnosząc tą odpowiedzialność do prawa karnego, w niektórych obszarach rozważa się również możliwość karania karą kryminalną twórców SI za działania swoich wynalazków. Problem pojawia się, gdy SI działa w sposób szkodliwy i nieprzewidywalny, a można udowodnić, że twórcy mieli świadomość potencjalnego zagrożenia i zlekceważyli odpowiednie środki ostrożności. Takie sytuacje są rzadkie, ale dyskusja na ten temat trwa, zwłaszcza w kontekście systemów autonomicznych zdolnych do podejmowania decyzji mogących prowadzić do szkód lub śmierci[559].

Kolejno, odpowiedzialność regulacyjna (administracyjna), która w wielu krajach wprowadza szczególne przepisy dotyczące sztucznej inteligencji, a te mogą nakładać dodatkowe obowiązki na twórców, takie jak wymóg przeprowadzania audytów etycznych, testów bezpieczeństwa

[558] Calo R., *Robotics and the Lessons of Cyberlaw*, "California Law Review" 2015, Vol. 103.
[559] Hallevy Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, "Journal of Criminal Law and Criminology" 2011, Vol. 101, No. 2.

oraz spełniania przepisów dotyczących ochrony danych osobowych. Nieprzestrzeganie tych regulacji może prowadzić do nałożenia sankcji administracyjnych lub karanych[560].

Poza aspektami formalno-prawnymi, twórcy sztucznej inteligencji muszą także uwzględniać kwestie odpowiedzialności etycznej związanej z ich technologiami. To oznacza projektowanie systemów w taki sposób, aby zapewnić sprawiedliwość, przejrzystość i szacunek dla prywatności użytkowników. Etyczne podejście do tworzenia i implementacji sztucznej inteligencji staje się coraz bardziej istotne dla społeczeństwa i może wpływać na reputację oraz akceptację technologii na rynku[561].

W dysertacji aspekt tych czterech form odpowiedzialności zostanie szczegółowo opisany w podpunktach poniżej. Powyższe za cel miało wprowadzić do tematyki, by następnie szczegółowo temat opisać.

8.4.1 Odpowiedzialność cywilna

Odpowiedzialność prawnocywilna twórcy sztucznej inteligencji stanowi istotny element rozważań dotyczących regulacji i zarządzania ryzykiem związanym z implementacją technologii SI. Istotne jest zrozumienie różnorodnych czynników, które mogą wpłynąć na ustalenie tej odpowiedzialności w przypadku powstania szkód spowodowanych przez systemy sztucznej inteligencji. Oto kilka kluczowych aspektów, które należy brać pod uwagę:

1. defekt produktu

Odpowiedzialność za wady produktu stanowi istotny sposób, w jaki twórcy sztucznej inteligencji mogą być pociągnięci do odpowiedzialności cywilnej. Kluczowe jest ustalenie czy szkoda wynikała z wad produktu, takich jak błędy w oprogramowaniu czy brakujące procedury bezpieczeństwa. Wady te obejmują możliwe błędy projektowe, usterki produkcyjne oraz niewystarczające ostrzeżenia lub instrukcje[562].

2. standardy i zgodność z przepisami

[560] European Commission, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (dostęp: 10.06.2024 r.).
[561] Bryson J. J., *SI & Global Governance: No One Should Trust SI*, United Nations University Centre for Policy Research 2018.
[562] Vladeck D. C., *Machines Without Principals: Liability Rules and Artificial Intelligence*, "Washington Law Review" 2014.

Kreatorzy sztucznej inteligencji muszą respektować obowiązujące normy i przepisy dotyczące projektowania, testowania i wdrażania systemów SI. To obejmuje przestrzeganie regulacji dotyczących ochrony danych osobowych (jak na przykład RODO[563]), standardów bezpieczeństwa produktów oraz specyficznych uregulowań branżowych. Niedopełnienie tych norm może stanowić podstawę do ustalenia odpowiedzialności cywilnej[564].

3. przewidywalność szkody

Ocena odpowiedzialności cywilnej opiera się na przewidywalności szkód. Czy autor mógł rozsądnie przewidzieć ewentualne konsekwencje działania systemu SI? To zagadnienie staje się szczególnie skomplikowane w kontekście systemów SI, które uczą się i adaptują w sposób, który może być nie do końca przewidywalny nawet dla swoich twórców[565].

4. środki zaradcze i ostrzeżenia

Odpowiedzialność może być ograniczona, gdy twórca podejmie odpowiednie środki w celu poinformowania użytkowników o ewentualnych zagrożeniach lub zastosuje skuteczne środki zaradcze w celu zmniejszenia ryzyka szkody[566]. Ważna jest jasna komunikacja z użytkownikami na temat ograniczeń i zagrożeń związanych z produktem SI[567].

5. etyka i odpowiedzialność społeczna

Odpowiedzialność cywilna nie dotyczy tylko przestrzegania przepisów; obejmuje również szersze aspekty etyczne i społeczne. Osoby tworzące sztuczną inteligencję powinny starannie dbać o to, aby ich systemy były uczciwe, przejrzyste i nie powodowały niepotrzebnych szkód[568].

[563] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

[564] Casey B. et al., *Rethinking the Liability of Robots and AI*, "Emory Law Journal" 2015, Vol. 64.

[565] Calo R., *Robotics and the Lessons of Cyberlaw*, "California Law Review" 2015, Vol. 103.

[566] Pietrzykowski T., *Odpowiedzialność za sztuczną inteligencję - wyzwania dla prawa cywilnego i karnego*, "Przegląd Prawniczy Uniwersytetu Warszawskiego" 2021, vol. 20, nr 1, s. 35-36.

[567] Asaro P. M., *The Liability Problem for Autonomous Artificial Agents*, "European Journal of Law and Technology" 2012, Vol. 3, No. 3.

[568] Bostrom N., Yudkowsky E., *The Ethics of Artificial Intelligence*, red. Keith Frankish, William Ramsey, "Cambridge Handbook of Artificial Intelligence" 2014.

Istotne jest zrozumienie tych elementów, które wpływają na sposób, w jaki prawo dostosowuje się do nowych wyzwań technologicznych i zapewnia, że twórcy sztucznej inteligencji ponoszą odpowiedzialność za swoje produkty w sposób sprawiedliwy i skuteczny.

8.4.2 Odpowiedzialność karna

Odpowiedzialność karna twórcy sztucznej inteligencji to zagadnienie o szerokim zakresie, które dotyczy praktycznych i teoretycznych aspektów prawa karnego. W kontekście systemów SI istotne staje się zrozumienie, w jaki sposób tradycyjne pojęcia odpowiedzialności karnej, takie jak wina, zamiar czy przyczynowość, mogą być stosowane w przypadku popełnienia przestępstwa przez maszynę. Istnieje kilka kwestii wartych uwagi:

1. przypisanie winy

Tradycyjnie, kwestia odpowiedzialności karnej w przypadku sztucznej inteligencji polega na ustaleniu winy, co jest skomplikowane ze względu na brak świadomości czy zamiaru w tradycyjnym ludzkim rozumieniu. Dlatego w kontekście SI często dyskutuje się o możliwości przypisania odpowiedzialności osobom za projektowanie, programowanie i użytkowanie systemów SI. Kluczowym zagadnieniem staje się pytanie, czy twórcy lub operatorzy mogli przewidzieć potencjalne szkodliwe skutki działania SI i czy podjęli odpowiednie środki zapobiegawcze[569].

2. przewidywalność i unikanie szkody

Twórca systemu sztucznej inteligencji może ponieść odpowiedzialność, jeśli mógł przewidzieć narażenie lub naruszenie dóbr chronionych prawem karnym przez system i nie podjął działań w celu ich uniknięcia lub zminimalizowania rozmiarów naruszenia. Ocena opiera się na zastosowaniu najlepszych praktyk branżowych, standardów bezpieczeństwa oraz przestrzeganiu odpowiednich protokołów testowych[570].

3. rola przepisów i regulacji

Specjalne przepisy dotyczące sztucznej inteligencji mogą nałożyć dodatkowe obowiązki na twórców i użytkowników systemów SI, co może mieć wpływ na ich odpowiedzialność karą.

[569] Hallevy G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, "Akron Intellectual Property Journal" 2010, Vol. 4, No. 2, s. 171-201.
[570] Calo R., *Artificial Intelligence Policy: A Primer and Roadmap*, "U.C. Davis Law Review" 2017 Vol. 51.

Na przykład, złamanie przepisów dotyczących ochrony danych osobowych przez system SI może skutkować karalnością twórców tego systemu[571].

4. użycie SI w kontekście nielegalnym

Jedną z istotnych kategorii problemów stanowi wykorzystanie sztucznej inteligencji w celach nielegalnych, takich jak ataki cybernetyczne, oszustwa czy manipulacje na rynkach. W takich sytuacjach twórca lub użytkownik SI może ponosić bezpośrednią odpowiedzialność za działania systemu, jeśli udowodniono, że świadomie wykorzystali SI do realizacji niezgodnych z prawem celów[572].

Rozważenie kwestii odpowiedzialności karnej za twórców sztucznej inteligencji wymaga dostosowania tradycyjnych zasad prawa karnego do nowych wyzwań technologicznych oraz ciągłego monitorowania postępujących technologii i ich wpływu na społeczeństwo oraz system prawny.

8.4.3 Odpowiedzialność regulacyjna (administracyjna)

Tworzenie sztucznej inteligencji musi odbywać się zgodnie z przepisami, które regulują procesy projektowania, rozwoju, wdrożenia i użytkowania. Ważne jest, aby twórcy SI ponosili odpowiedzialność za zapewnienie bezpieczeństwa, zgodności z etyką i przestrzegania prawa. Istnieje kilka kluczowych aspektów, które należy uwzględnić:

1. zgodność z przepisami o ochronie danych

Ochrona danych osobowych to jedno z kluczowych zagadnień regulacyjnych związanych z sztuczną inteligencją. Twórcy systemów sztucznej inteligencji muszą zagwarantować, że ich rozwiązania są zgodne z lokalnymi i międzynarodowymi przepisami, takimi jak *Ogólne Rozporządzenie o Ochronie Danych* (RODO) w Unii Europejskiej. Wartościowe są tu kwestie minimalizacji danych, bezpieczeństwa informacji oraz praw osób, których dane są przetwarzane, do dostępu, poprawiania i usuwania swoich danych[573].

[571] European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (dostęp: 10.06.2024 r.).
[572] Lemley M., *The Role of AI in the Criminal Justice System*, "Stanford Law Review" 2019, Vol. 61.
[573] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

2. standardy bezpieczeństwa i certyfikacja

Twórcy sztucznej inteligencji są zobowiązani do przestrzegania określonych norm bezpieczeństwa technicznego i operacyjnego. Wiele systemów różnych państw narzuca wymagania dotyczące certyfikacji dla systemów SI, które muszą zostać spełnione przed wprowadzeniem produktu na rynek. Nieuczestniczenie w tych standardach może skutkować sankcjami administracyjnymi, włączając w to kary finansowe[574].

3. przestrzeganie specyficznych regulacji branżowych

Sztuczna inteligencja jest wykorzystywana w różnych dziedzinach, takich jak finanse, opieka zdrowotna, transport i inne, które często podlegają specjalnym regulacjom. Twórcy sztucznej inteligencji muszą być świadomi i przestrzegać branżowych przepisów regulujących wykorzystanie SI w każdym z tych sektorów, co może obejmować wymagania dotyczące przejrzystości działania SI, odpowiedzialności za błędy oraz etyczne aspekty korzystania z SI[575].

4. przepisy dotyczące autonomicznych i samouczących się systemów

Specjalną uwagę należy zwrócić na systemy sztucznej inteligencji oparte na uczeniu maszynowym, które mogą wykazywać nieprzewidywalne zachowania poza pierwotnym zakresem. Przepisy mogą wymagać mechanizmów kontroli, audytów oraz możliwości interwencji ludzkiej w przypadku, gdy działanie systemu SI odbiega od zamierzonego przeznaczenia[576].

Tworzenie sztucznej inteligencji wiąże się z wieloma aspektami, zarówno technicznymi, jak i prawnymi. Ważne jest odpowiednie zarządzanie tymi kwestiami dla zapewnienia legalności, bezpieczeństwa i akceptacji społecznej tej technologii.

8.4.4 Odpowiedzialność etyczna

Tworzenie sztucznej inteligencji wiąże się z wieloma kwestiami etycznymi, które są kluczowe dla rozwoju i wdrożenia tej technologii. Odpowiedzialność twórców SI nie ogranicza się

[574] Weller A., Challenges for Transparency and Accountability in Machine Learning, Nature Machine Intelligence 2019, Vol. 1.
[575] Calo R., Artificial Intelligence Policy: A Primer and Roadmap,"U.C. Davis Law Review" 2017, Vol. 51.
[576] European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (dostęp: 10.06.2024 r.)

jedynie do przestrzegania przepisów prawnych, ale również dotyczy szerszych zagadnień społecznych i moralnych związanych z wpływem SI na społeczeństwo. Istnieje wiele istotnych aspektów, które trzeba uwzględnić podczas tego procesu:

1. transparentność działania SI

Jednym z kluczowych elementów etyki w opracowywaniu sztucznej inteligencji jest zapewnienie przejrzystości jej funkcjonowania. Twórcy powinni starać się o to, aby algorytmy były zrozumiałe dla użytkowników i innych zainteresowanych stron. Przejrzystość odgrywa istotną rolę w budowaniu zaufania oraz umożliwia ocenę i kontrolę nad systemami SI[577].

2. sprawiedliwość i brak „*bias*" (ang. unbiased)[578]

Systemy sztucznej inteligencji powinny być projektowane i implementowane w taki sposób, aby unikać dyskryminacji i uprzedzeń. Twórcy SI powinni stosować techniki redukcji uprzedzeń i regularnie testować swoje systemy pod kątem ewentualnych, niezamierzonych skojarzeń, które mogłyby negatywnie wpłynąć na różne grupy społeczne[579].

3. odpowiedzialność za decyzje SI

Twórcy sztucznej inteligencji powinni ponosić odpowiedzialność za decyzje podejmowane przez ich systemy. To oznacza nie tylko przestrzeganie zasad odpowiedzialności prawnej i regulacyjnej, ale także gotowość etyczną do konfrontacji z konsekwencjami wynikającymi z działania ich technologii. Rozważania na temat tego, kto „*prowadzi grę*", gdy sztuczna inteligencja podejmuje kluczowe decyzje, są istotne dla etycznej odpowiedzialności[580].

4. zabezpieczenie prywatności i ochrona danych

W kontekście sztucznej inteligencji, ważne staje się zapewnienie ochrony danych osobowych i prywatności użytkowników. Programiści muszą upewnić się, że systemy SI przestrzegają obowiązujących przepisów dotyczących ochrony danych oraz wprowadzają dodatkowe środki

[577] Gebru T., *Datasheets for Datasets*, "Communications of the ACM" 2021, Vol. 64, No. 12.
[578] Unbiased – w odniesieniu do uczenia maszynowego, modele, które nie faworyzują ani nie dyskryminują żadnej grupy, dokonując przewidywań w oparciu o reprezentatywne i zrównoważone dane treningowe.
[579] Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, "Proceedings of Machine Learning Research" 2018, Vol. 81, s. 1-15.
[580] Calo R., *Artificial Intelligence and the End of Open Society*, "Stanford Law Review" 2020, Vol. 72.

zabezpieczające prywatność, zgodnie z zasadą „*projektowanie z uwzględnieniem prywatności*" (ang. privacy by design)[581].

5. zrównoważony rozwój i wpływ społeczny

Kreatorzy sztucznej inteligencji powinni brać pod uwagę długoterminowe konsekwencje wprowadzania swoich technologii. Wpływ sztucznej inteligencji na rynek pracy, społeczne nierówności oraz środowisko naturalne wymagają przemyślanych strategii, które zmniejszają negatywne skutki, jednocześnie maksymalizując korzyści dla społeczeństwa[582].

Te elementy odpowiadają na konieczność właściwego zarządzania rozwojem i wdrażaniem SI, aby zagwarantować, że ta technologia służy wspólnemu dobru, a jej negatywne konsekwencje są skutecznie ograniczane.

8.5 Problematyka związana z klasyfikacją czynów dokonywanych przez systemy SI uważanych za przestępne

Rozwój technologii opartych na sztucznej inteligencji wymusza rewizję tradycyjnych reguł prawnych, szczególnie w kontekście klasyfikacji czynów podejmowanych przez SI jako przestępstwa. Kwestia ta dotyka zarówno aspektów teoretycznych, jak i praktycznych związanych z rozumieniem funkcjonowania oraz odpowiedzialności za systemy SI.

Analiza problemów związanych z klasyfikacją działań podejmowanych przez systemy sztucznej inteligencji jako przestępstwa stanowi jedno z najbardziej skomplikowanych i innowacyjnych zagadnień w dziedzinie prawa karnego. Istnieje pogląd, że sztuczna inteligencja może prowadzić do działań, które naruszają prawo, jednak kwestia ustalenia odpowiedzialności za te czyny pozostaje nierozstrzygnięta. Obecne regulacje prawne są dostosowane do sytuacji, w których za przestępstwo odpowiada człowiek jako sprawca, co powoduje trudności w bezpośrednim stosowaniu tych regulacji do działań podejmowanych przez SI.

[581] Cavoukian A., *Privacy by Performance: The 7 Foundational Principles*, https://www.datatilsynet.no/globalassets/global/english/7foundationalprinciples_anncavoukian2.pdf (dostęp: 10.06.2024 r.)

[582] Crawford K., *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence,* Yale University Press 2021.

Ważnym aspektem w tym miejscu pracy doktorskiej jest wyjaśnienie pojęcia czynu, które w polskim prawie karnym jest pojęciem fundamentalnym i oznacza zachowanie człowieka, które może podlegać ocenie prawnej i ewentualnej odpowiedzialności karnej[583]. Zgodnie z kodeksem karnym[584], aby dane zachowanie zostało uznane za czyn, musi spełniać następujące warunki[585]:

1. musi być zachowaniem człowieka - tylko osoba fizyczna może popełnić czyn w rozumieniu prawa karnego[586].

2. musi być zachowaniem zewnętrznym - sama myśl, postanowienie lub wewnętrzne przeżycie nie stanowi czynu[587].

3. musi być zachowaniem dowolnym (zależnym od woli człowieka) - zachowania niezależne od woli, takie jak odruchy lub czynności podejmowane pod wpływem przymusu fizycznego, nie są czynami[588].

Czyny mogą być działaniem (zrobieniem czegoś) lub zaniechaniem (niezrobieniem czegoś, co sprawca był zobowiązany zrobić). Aby czyn był karalny, musi wypełniać znamiona przestępstwa określone w kodeksie karnym lub innych ustawach[589]. Ponadto, sprawca musi działać w sposób zawiniony (umyślnie lub nieumyślnie), a jego czyn musi być bezprawny i społecznie szkodliwy w stopniu wyższym niż znikomy[590].

Prawo karne reguluje, jakie czyny są przestępstwami, jakie kary grożą za ich popełnienie oraz w jakich okolicznościach sprawca może zostać uznany za niewinnego lub jego odpowiedzialność może być ograniczona (np. ze względu na niepoczytalność lub działanie w obronie koniecznej)[591].

Kontynuując zagadnienie problematyki związanej z klasyfikacją czynów dokonywanych przez systemy SI uważanych za przestępne, kluczowym wyzwaniem jest określenie czy czyny

[583] Gardocki L., *Prawo karne*, C.H. Beck 2019, s. 51-55, 60-63.
[584] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2024 r. poz. 17 z późn. zm.)
[585] Gardocki L., op.cit. s. 51-55, 60-63.
[586] Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-31*, C.H. Beck, 2017, s. 202-208, 221-225.
[587] Ibidem
[588] Ibidem
[589] Gardocki L., op.cit. s. 51-55, 60-63.
[590] Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-31*, C.H. Beck, 2017, s. 202-208, 221-225.
[591] Gardocki L., *Prawo karne*, C.H. Beck 2019, s. 51-55, 60-63.

popełniane przez systemy sztucznej inteligencji mogą być uznane za przestępstwa zgodnie z obowiązującym prawem karnym, które zakłada człowieka jako sprawcę. Systemy SI, działając samodzielnie, mają potencjał generowania negatywnych konsekwencji (narażenie na naruszenie lub naruszenie dóbr chronionych prawem), które w tradycyjnych regulacjach prawnych mogłyby zostać zakwalifikowane jako przestępstwa, takie jak naruszenia prywatności, oszustwa czy nawet szkody fizyczne[592]. Proces klasyfikacji działań podejmowanych przez SI jako przestępstwa wymaga przede wszystkim ustalenia, czy dana aktywność SI może być uznana za czyn zabroniony, co jest bezpośrednio powiązane z problemem świadomości, intencji oraz zdolności do przewidzenia konsekwencji działań przez system SI. W kontekście prawnym istotne staje się pytanie o *mens rea* - czyli o intencję popełnienia przestępstwa lub świadomość naruszenia prawa - co jest niezbędne do pociągnięcia do odpowiedzialności za większość rodzajów przestępstw[593].

W temacie problematyki w odniesieniu do sprawstwa i odpowiedzialności istotnym zagadnieniem jest ustalenie, kto ponosi odpowiedzialność za działania systemów sztucznej inteligencji prowadzące do popełnienia czynu zabronionego. Konwencjonalne pojęcie sprawstwa, oparte na świadomości i intencjach, napotyka trudności w przypadku algorytmów maszynowych i procesów podejmowania decyzji[594]. W związku z tym należy rozważyć, czy twórcy lub operatorzy systemów SI mogą być pociągnięci do odpowiedzialności za czyny dokonane przez te systemy. W kontekście sztucznej inteligencji rozważa się różne modele odpowiedzialności, począwszy od bezpośredniego przypisania odpowiedzialności twórcom, użytkownikom lub właścicielom systemów SI, aż do bardziej złożonych modeli ubezpieczeń lub funduszy rekompensacyjnych, które mogłyby pokryć szkody spowodowane przez autonomiczne działania SI.

Zadaniem prawników oraz ustawodawców jest dostosowanie przepisów prawa karnego w sposób umożliwiający skuteczne reagowanie na wyzwania wynikające z rozwoju technologii sztucznej inteligencji. W różnych jurysdykcjach rozważane są różne podejścia, począwszy od wprowadzenia nowych kategorii przestępstw skoncentrowanych na działaniach SI, przez zmiany definicji winy, aż po stworzenie nowych form odpowiedzialności prawnej[595]. Unia

[592] N Bostrom N., Müller Y., *Future Progress in Artificial Intelligence: A Survey of Expert Opinion*, "Journal of Artificial Intelligence Research" 2014.
[593] Hallevy G., *When Robots Kill: Artificial Intelligence under Criminal Law*, Northeastern University Press 2013.
[594] Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.
[595] Edwards L., *Law, Policy, and the AI Dilemma*, Routledge, New York 2022.

Europejska, przykładowo, w ramach Europejskiego *Aktu o Sztucznej Inteligencji*[596], dąży do stworzenia regulacji prawnych określających klasyfikację systemów SI według ryzyka oraz ustanawia szczegółowe wymagania dla systemów o wysokim poziomie ryzyka. Niemniej jednak ten akt skupia się głównie na aspektach cywilnych i regulacyjnych, nie poruszając bezpośrednio kwestii odpowiedzialności karnej za działania SI.

8.6 Jakie czynniki powinny wpływać na proces kwalifikacji prawnej działalności SI

Proces kwalifikacji prawnej działalności sztucznej inteligencji jest złożony, gdyż musi uwzględniać zarówno techniczne aspekty technologii, jak i prawną infrastrukturę, która często nie nadąża za szybkim rozwojem cyfrowych innowacji. Oto kluczowe czynniki, które powinny wpływać na proces kwalifikacji prawnej działalności SI:

1. zgodność z istniejącymi przepisami

   Istotnym aspektem jest sprawdzenie czy działania podejmowane przez system sztucznej inteligencji są zgodne z obowiązującymi przepisami prawa. To obejmuje przepisy prawa cywilnego, karnego, dotyczące praw autorskich, ochrony danych osobowych oraz specjalistyczne regulacje dotyczące poszczególnych sektorów, takich jak finanse czy opieka zdrowotna[597].

2. intencjonalność i autonomia decyzji

   Rozważania na temat tego, czy sztuczna inteligencja podejmuje decyzje samodzielnie czy też stanowi narzędzie w rękach użytkownika, mają istotne znaczenie. W kontekście prawa karnego, intencjonalność działań odgrywa kluczową rolę w ustalaniu winy. W przypadku SI, trudno mówić o tradycyjnym zamiarze, dlatego istotne jest określenie stopnia autonomii systemu oraz możliwości przewidzenia jego działań przez twórców[598].

3. przewidywalność skutków działania SI

[596] Komisja Europejska, *Artificial Intelligence Act*, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (dostęp 10.06.2024 r.).
[597] Calo R., *Robotics and the Lessons of Cyberlaw*, "California Law Review" 2015, Vol. 103.
[598] Hallevy Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, "Journal of Criminal Law and Criminology" 2011, Vol. 101, No. 2.

Ocena czy twórca lub operator systemu mógł rozsądnie przewidzieć potencjalne negatywne skutki sztucznej inteligencji, wymaga spełnienia obowiązków związanych z testowaniem systemów, oceną ryzyka oraz wdrożeniem odpowiednich zabezpieczeń. Duża przewidywalność konsekwencji działań SI może mieć wpływ na zakres odpowiedzialności prawnej[599].

4. przezroczystość i kontrola nad systemem

Ważne jest także, czy działanie sztucznej inteligencji było przejrzyste dla jej twórców i użytkowników, oraz czy istniały odpowiednie mechanizmy kontroli i interwencji. Systemy „*czarnej skrzynki*", w których procesy decyzyjne nie są transparentne, mogą utrudniać ocenę prawną[600].

5. wpływ społeczny i etyczny

Kwestie etyczne oraz potencjalny oddziaływanie społeczne sztucznej inteligencji są również brane pod uwagę. Warto zwrócić uwagę na zagadnienia związane z dyskryminacją, ochroną prywatności oraz wpływem na demokrację i prawa człowieka przy analizie funkcjonowania SI. Istotne jest uwzględnienie szerokich konsekwencji społecznych wynikających z wykorzystania sztucznej inteligencji[601].

Te wszystkie elementy razem kreują kompleksowy obraz trudności związanych z kwalifikacją działalności prawnej SI, podkreślając konieczność nieustannej adaptacji przepisów prawa do ewoluujących technologii.

[599] Pasquale F., *The Black Box Society*, Harvard University Press 2015.
[600] Balkin J. M., *The Three Laws of Robotics in the Age of Big Data*, "Ohio State Law Journal" 2017, Vol. 78.
[601] Crawford K., *AI Now Report*, AI Now Institute, New York University 2019.

Rozdział IX. Wyniki badań

9.1 Wprowadzenie do wyników badań

W tym rozdziale prezentowane są wyniki badań skupiające się na analizie odpowiedzialności prawnej w kontekście działań sztucznej inteligencji. W obliczu szybko rozwijającej się technologii SI, tradycyjne podejścia prawne często okazują się niewystarczające lub nieadekwatne do rozwiązania wszystkich aspektów związanych z nowymi wyzwaniami, jakie stawia przed nami automatyzacja. Kluczowym punktem analizy jest stworzony diagramu, który klarownie prezentuje proces określania odpowiedzialności prawnej w przypadkach z udziałem SI, zwłaszcza gdy nie da się przypisać człowiekowi odpowiedzialności za działania maszyny.

W mojej pracy szczegółowo analizowałam sytuacje, w których istniejące przepisy prawne nie uwzględniają możliwości przypisania pełnej odpowiedzialności ludziom za działania związane z użyciem lub przez sztuczną inteligencję. Przypadki, które analizowałam dowodzą, że odpowiedzialność często ogranicza się jedynie do aspektów tworzenia innowacyjnych rozwiązań, które wychodzą poza tradycyjne ramy ludzkiego zarządzania i kontroli nad technologią. Te obserwacje sugerują konieczność opracowania nowych regulacji, które byłyby w stanie usunąć te „*luki prawne*".

Opracowany przeze mnie diagram zaprezentowany w pracy[602] pełni funkcję narzędzia pomocniczego dla legislatorów i praktyków prawa, umożliwiając bardziej efektywne i precyzyjne podejście do zagadnień związanych z sztuczną inteligencją w prawie. Na podstawie zebranych danych i analiz zaproponowałam również dwa nowe podejścia regulacyjne. Pierwsze z nich zakłada wprowadzenie konkretnych przepisów dotyczących odpowiedzialności twórców systemów SI, które mogłyby lepiej reagować na dynamicznie zmieniające się realia technologiczne. Drugie podejście sugeruje rozważenie wprowadzenia form odpowiedzialności maszyn, co stanowiłoby innowacyjne i potencjalnie rewolucyjne rozwiązanie w kontekście globalnego systemu prawnego.

[602] Patrz: strona:180

W kolejnej części tego rozdziału dokładnie opiszę każde z tych rozwiązań, prezentując argumenty za ich wdrożeniem oraz potencjalne trudności związane z ich realizacją.

9.2 Podsumowanie kluczowych odkryć

W obszarze, gdzie wykorzystuje się technologię sztucznej inteligencji, obowiązujące regulacje prawne stanowią solidne podstawy do ustalenia odpowiedzialności człowieka (punkt 10.3 Diagramu). Jednak zakres tej odpowiedzialności jest elastyczny i zależy od wielu czynników, takich jak to, czy winę można przypisać człowiekowi czy grupie, a także od charakteru sztucznej inteligencji jako produktu lub usługi. Co ważne, chociaż przepisy prawne dotyczące sztucznej inteligencji nie są jeszcze w pełni sprecyzowane, istnieją kierunki badawcze wskazujące na elementy, które należy unikać w tworzonych przez ludzi systemach SI, aby uniknąć ponoszenia przez nie karnej odpowiedzialności lub innych sankcji.

W dyskusjach naukowych obecnie zaleca się ostrożność w przypisywaniu sztucznej inteligencji samoświadomości, co wydaje się uzasadnione w kontekście tego badania. Brak wystarczających dowodów na to, że osiągnięcie to jest bliskie możliwościom technologicznym dostępnym obecnie, dlatego skoncentrowanie się na obecnym poziomie rozwoju sztucznej inteligencji wydaje się być najbardziej odpowiednie dla celów tego badania.

Jednakże kluczowe jest to, że twórca sztucznej inteligencji musi przestrzegać wszystkich obowiązujących standardów naukowych i regulacji, aby uniknąć sytuacji, w których SI mogłaby nieumyślnie spowodować skutki podlegające odpowiedzialności karnej (punkt 10.3 Diagramu). Szczególnie ważna jest kwestia autonomicznych systemów sztucznej inteligencji, które mają zdolność podejmowania samodzielnych decyzji. To właśnie te systemy, działające niezależnie od czynnika ludzkiego, mogą prowadzić do incydentów, które prawo karne klasyfikuje jako czyny zabronione.

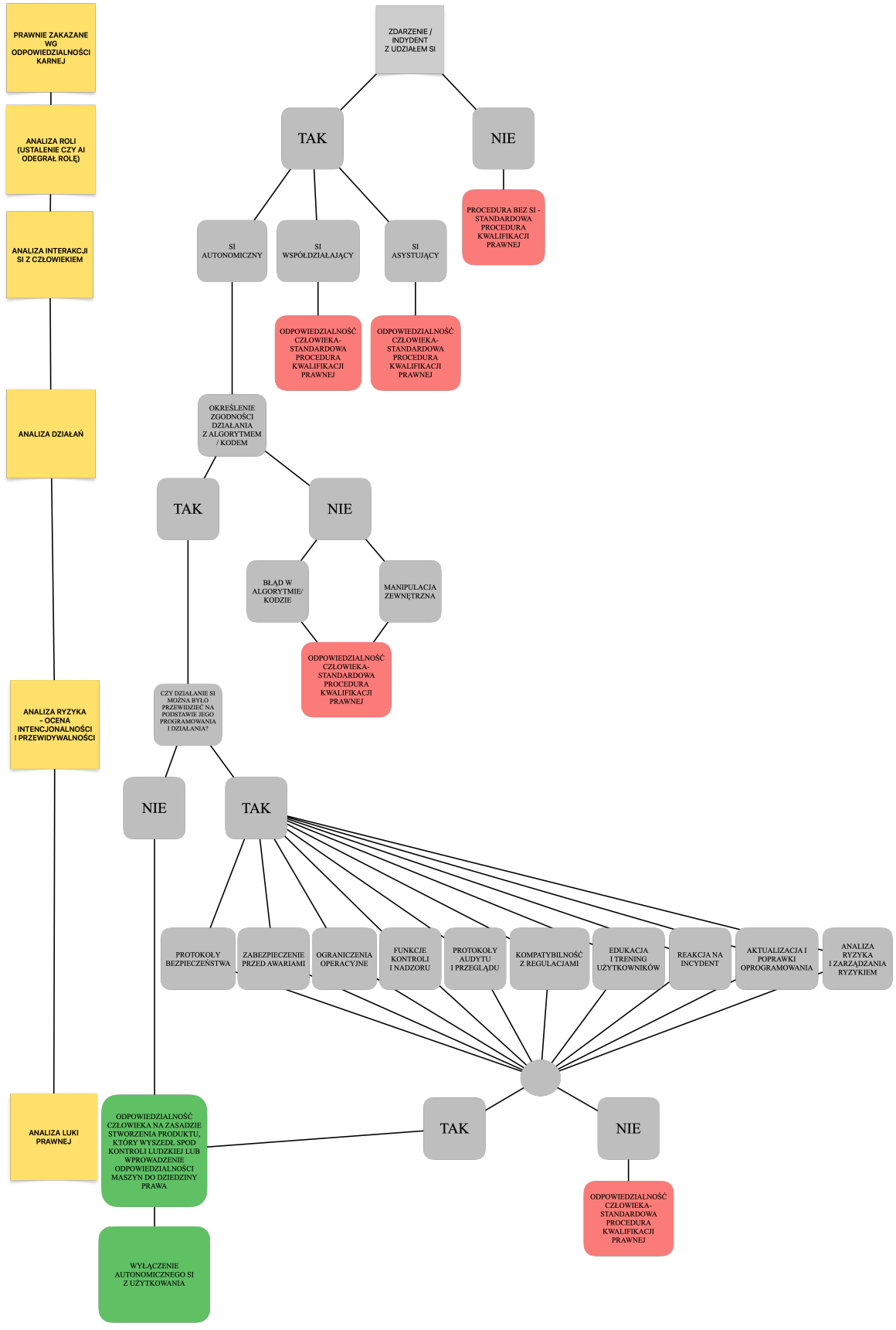
9.3 Diagram

Poniższy diagram ilustruje systematyczne podejście do analizy zdarzeń lub incydentów związanych ze sztuczną inteligencją. Przedstawia on kompleksowy proces badawczy, w którym poszczególne kroki (oznaczone na żółto) prowadzą do ustalenia, czy i w jakim stopniu człowiek może ponosić odpowiedzialność prawna. Ten diagram ma służyć jako narzędzie wsparcia dla

zarówno teoretyków, jak i praktyków prawa, pomagając im dokładniej identyfikować osobę odpowiedzialną oraz podstawy tej odpowiedzialności, gdy w analizowanym zdarzeniu lub incydencie pojawia się udział sztucznej inteligencji.

Pole oznaczone kolorem czerwonym wskazują na obszary, w których stosowane są obecnie obowiązujące przepisy i tradycyjne metody oceny prawnej. Z kolei odcienie zieleni podkreślają braki wynikające z przeprowadzonych badań i analizy prawnej, gdzie aktualne prawo nie określa jeszcze zasad odpowiedzialności dla osób fizycznych lub podmiotów zbiorowych. Te ustalenia sugerują pilną potrzebę stworzenia nowych regulacji, które pozwolą skutecznie reagować na unikalne wyzwania związane z rozwojem i wykorzystaniem sztucznej inteligencji.

DIAGRAM ODPOWIEDZIALNOŚCI PRAWNEJ ZDARZEŃ LUB INCYDENTÓW KARNIE ZABRONIONYCH Z UDZIAŁEM SZTUCZNEJ INTELIGENCJI



Źródło: Opracowanie własne

9.3.1 Szczegółowy opis diagramu

Diagram ukazuje proces ustalania odpowiedzialności karnej w przypadku zdarzeń lub incydentów związanych z sztuczną inteligencją. Kolejne fazy obejmują:

Etap 1. Prawne zakazanie – odpowiedzialność karna

Pierwsza faza diagramu polega na zastanowieniu się nad podstawowym pytaniem, czy działanie, które obserwujemy, narusza przepisy prawa karnego. Tylko takie działania powinny być dalej analizowane pod kątem odpowiedzialności.

Etap 2. Analiza roli

Podczas początkowego etapu analizy zdarzenia z udziałem sztucznej inteligencji istotne jest ustalenie podstawowych faktów i okoliczności incydentu, w tym sprawdzenie, czy doszło do interwencji sztucznej inteligencji. Następnie kluczowe jest precyzyjne określenie roli, jaką mogła odegrać sztuczna inteligencja w kontekście danego zdarzenia oraz ewentualnych skutków prawnych. W oparciu o wyniki tej wstępnej oceny, można uznać sztuczną inteligencję za istotny czynnik wpływający na wydarzenie i poddać ją dalszej analizie lub też wykluczyć ją jako element nieistotny dla oceny prawnej.

Etap 3. Analiza interakcji SI z człowiekiem

Podczas analizy zdarzenia z udziałem sztucznej inteligencji istotne jest zrozumienie, w jaki sposób interakcja między systemem SI a człowiekiem mogła wpłynąć na zaistniałą sytuację, ze szczególnym uwzględnieniem stopnia autonomii systemu SI. W trakcie tej oceny wyróżnia się trzy podstawowe typy sztucznej inteligencji:

1. autonomiczna SI:

   Systemy autonomiczne działają samodzielnie, podejmując decyzje na podstawie własnych algorytmów. Przykładowo, umożliwiają one pojazdom autonomicznym poruszanie się po drogach bez konieczności ingerencji człowieka, reagując na zmieniające się warunki w czasie rzeczywistym[603].

[603] Kosiński J., *Sztuczna inteligencja i jej prawne aspekty*, "Studia Prawnicze" 2019, nr 3, s. 52-53.

2. współdziałająca SI:

   W tej dziedzinie sztuczna inteligencja służy jako wsparcie dla ludzi, proponując sugestie dotyczące możliwych działań lub udzielając rekomendacji, jednak to użytkownik podejmuje ostateczne decyzje. Przykładem mogą być zaawansowane systemy diagnostyczne w medycynie, które pomagają w analizie danych klinicznych i sugerują potencjalne diagnozy, ale decyzja dotycząca leczenia zawsze należy do lekarza[604].

3. asystująca SI:

   Te systemy nie mają zdolności do podejmowania decyzji samodzielnie i działają jako asystenci użytkownika, wykonując proste czynności zgodnie z jego poleceniami. Przykładem tego są *chatboty* obsługi klienta, które odpowiadają na typowe pytania i przekazują bardziej skomplikowane sprawy do człowieka[605].

Powyższe grupy różnią się między sobą pod względem zdolności działania i wymagają innego podejścia do kwestii odpowiedzialności prawnej. Z tego powodu, jeśli chodzi o kwestie odpowiedzialności, analiza będzie koncentrowała się głównie na systemach SI działających autonomicznie, ponieważ to one operują niezależnie i mogą wymagać szczególnych rozważań prawnych. W przypadku systemów SI współpracujących i asystujących, kluczowym elementem w przypisaniu odpowiedzialności pozostaje człowiek, co stawia pod znakiem zapytania indywidualną odpowiedzialność samego systemu SI.

Etap 4. Analiza działań

W trakcie tego etapu dokładnie analizuje się sytuację w celu sprawdzenia czy działania systemu sztucznej inteligencji zgadzają się z założeniami zaimplementowanego kodu i algorytmów. Badanie koncentruje się na określeniu, czy powstałe wydarzenia są wynikiem błędu programistycznego czy też niepożądanego ingerowania z zewnątrz, które mogło wpłynąć na funkcjonowanie systemu. Identyfikacja natury i źródła potencjalnej usterki jest istotna dla zrozumienia mechanizmów odpowiedzialności i podejmowania dalszych działań.

[604] Bieliński A., *Prawo wobec wyzwań sztucznej inteligencji - wybrane zagadnienia*, "Monitor Prawniczy" 2021, nr 16, s. 856-857.
[605] Kosiński J., *Sztuczna inteligencja i jej prawne aspekty*, "Studia Prawnicze" 2019, nr 3, s. 54.

Etap 5. Ocena intencjonalności i przewidywalności działań SI

Ten etap skoncentrowany jest na rozważeniu, czy działanie SI nosiło znamiona intencjonalności oraz czy było możliwe do przewidzenia w świetle jego zaprogramowanych parametrów i poprzedniego zachowania. Krytyczne jest tu zbadanie, jakie środki zapobiegawcze zostały wdrożone, aby zniwelować ryzyko niepożądanych efektów działań SI. Przy ocenie brane są pod uwagę następujące aspekty:

- przegląd procedur bezpieczeństwa - dokładne sprawdzenie, czy obecne wytyczne zapewniają skuteczną ochronę przed incydentami, błędami operacyjnymi lub działaniami nieuprawnionymi;
- przegląd systemu zabezpieczeń - analiza, czy stosowane środki są wystarczające do zapobiegania potencjalnym problemom technicznym oraz błędom w kodzie, które mogłyby spowodować nieprawidłowe działanie sztucznej inteligencji;
- ograniczenia operacyjne - analiza czy narzucenie ograniczeń na funkcjonowanie systemu w określonych warunkach może zapobiec ryzyku nadużyć i niebezpiecznych sytuacji;
- funkcje kontroli i nadzoru - funkcje weryfikacji umożliwiające monitorowanie działania sztucznej inteligencji oraz zdolność interwencji i przejęcia kontroli nad systemem w przypadku wykrycia zagrożeń;
- protokoły audytu i przeglądu - przegląd narzędzi audytowych stworzonych do oceny skuteczności systemu informatycznego i implementacji niezbędnych uaktualnień w celu zapewnienia jego bezpiecznej pracy;
- kompatybilność z regulacjami - upewnienie się, że stosowane środki zapobiegawcze są zgodne z przepisami prawnymi i normami etycznymi;
- edukacja i trening użytkowników - analizowanie gotowości użytkowników systemu sztucznej inteligencji do efektywnego i bezpiecznego korzystania z niego;
- reakcja na incydenty - ocena sposobu działania w przypadkach awarii lub błędów systemu sztucznej inteligencji;

- aktualizacje i poprawki oprogramowania - aktualizacja oprogramowania systemów sztucznej inteligencji w celu zapewnienia poprawności i bezpieczeństwa procesu;

- analiza ryzyka i zarządzanie nim - badanie sposobów analizy i zarządzania ryzykiem w obszarze operacyjnym sztucznej inteligencji, mających na celu rozpoznanie i ograniczenie ewentualnych zagrożeń.

Etap 6. Analiza luki prawnej

Ostatni etap analizy koncentruje się na identyfikacji i rozważaniu obszarów prawnych, które nie są objęte regulowanymi przepisami. Szczególnie skupia się na identyfikacji obszarów, w których nie można przypisać odpowiedzialności człowiekowi za działania sztucznej inteligencji ze względu na brak regulacji w obecnym systemie prawnym. Istnieją bowiem braki w adekwatnych mechanizmach prawnych umożliwiających rozliczenie za zdarzenia generowane przez SI. Zidentyfikowanie tej luki prawnej jest kluczowe dla opracowania nowych regulacji prawnych, które mogą dostosować się do dynamicznych zmian technologicznych i ich wpływu na aspekty odpowiedzialności. Ten etap stanowi istotę badania - podkreśla pilną potrzebę działań legislacyjnych i otwiera dyskusję na temat potencjalnych kierunków rozwoju prawa zdolnego radzić sobie z złożonymi wyzwaniami wynikającymi z postępującej sztucznej inteligencji.

Diagram przedstawia trzy kolory, które reprezentują różne drogi i ich skutki:

- żółty - etap analizy i oceny, które należy przeprowadzić w celu ustalenia odpowiedzialności;

- czerwony - sytuacje, w których odpowiedzialność karna „*standardowa*" tj. kodeksowa jest możliwa bez szczególnych regulacji dotyczących SI**;**

- zielony - obszary, w których zauważa się brak zapisów prawnych i potrzebę wprowadzenia nowych regulacji.

Należy zaznaczyć, że diagram nie jest stałym narzędziem, ale dynamicznym modelem analitycznym, który powinien być dostosowywany i rozwijany wraz z postępem w dziedzinie sztucznej inteligencji i prawa. Celem takiego podejścia jest umożliwienie elastycznego reagowania na nowe wyzwania i postęp technologiczny, co może przyczynić się do lepszej ochrony prawnej zarówno dla twórców SI, użytkowników, jak i społeczeństwa jako całości.

9.4 Analiza wyników badań

W trakcie analiz i badań w kontekście mojej rozprawy doktorskiej dotyczącej prawnokarnych aspektów technologii opartych na sztucznej inteligencji, ze szczególnym naciskiem na kwestie związane z kwalifikacją prawną, przypisaniem winy i odpowiedzialnością karną twórcy, zidentyfikowano obszar wymagający szczególnej uwagi prawniczej w kontekście prawa karne. Ten obszar został wyodrębniony na przygotowanym diagramie w niniejszym rozdziale, pokazując brak odpowiednich uregulowań prawnych, które mogłyby regulować sytuacje, w których działania sztucznej inteligencji prowadzą do naruszenia przepisów prawa karnego i odpowiedzialności prawnokarnej.

Jeśli twórca sztucznej inteligencji podejmuje wszelkie kroki, aby uniknąć naruszania prawa karnego przez SI, niezależnie od sterowania przez człowieka (autonomiczna SI), konieczne jest rozważenie trzech scenariuszy po przeprowadzonej analizie.

Pierwszym z tych scenariuszy jest zaangażowanie ludzi w odpowiedzialność za stworzenie produktu lub usługi, które wymknęły się spod kontroli człowieka. Drugim scenariuszem jest wprowadzenie odpowiedzialności maszyn do regulacji prawnych. Jednakże, wydaje się, że konieczne jest także ustanowienie regulacji nakładających obowiązek na twórcę wprowadzenia mechanizmu dezaktywacji autonomicznego SI z użytkowania jako trzeciego scenariusza.

Badanie tych wyników ma na celu zidentyfikowanie potencjalnych rozwiązań prawnych, które mogłyby skutecznie kontrolować wykorzystanie sztucznej inteligencji przez prawo karne, jednocześnie dbając o ochronę interesów społecznych oraz bezpieczeństwo obywateli.

9.4.1 Odpowiedzialność człowieka za działanie produktu lub usługi, które wyszły spod kontroli ludzkiej

Rozważając problem odpowiedzialności człowieka w przypadku produktów lub usług, których działanie przekracza ludzką kontrolę, wdrożenie autonomicznych systemów sztucznej inteligencji stawia istotne pytania dotyczące określenia winy za ewentualne szkody lub naruszenia prawa.

Istnieje pilna konieczność uregulowania kwestii odpowiedzialności karnej w sytuacji, gdy autonomiczna sztuczna inteligencja działa samodzielnie, bez nadzoru ludzkiego i doprowadza do naruszeń prawa karnego. Warto rozważyć wprowadzenie przepisów prawnych

umożliwiających pociągnięcie do odpowiedzialności za czyny systemu autonomicznego SI jego twórcę, które prowadzą do naruszenia prawa karnego.

W kontekście badania tej kwestii należy brać pod uwagę:

- sposoby prawne umożliwiające ustalenie tożsamości i przypisanie odpowiedzialności za czyny autonomicznej sztucznej inteligencji;
- zalecenia dotyczące precyzji w projektowaniu i monitorowaniu autonomicznych systemów SI, aby zapobiec niezamierzonym działaniom;
- możliwe sankcje lub kary dla twórców autonomicznej SI w przypadku naruszenia prawa karnego przez działania tego systemu.

Zapewnienie jasno określonych regulacji prawnych dotyczących odpowiedzialności za systemy autonomiczne SI staje się coraz ważniejsze w obliczu dynamicznego rozwoju tej technologii i jej coraz powszechniejszego wykorzystania w różnych obszarach życia społecznego.

9.4.1.1 Mechanizmy prawne umożliwiające identyfikację i przypisanie odpowiedzialności za działania autonomicznej sztucznej inteligencji

W kontekście wprowadzania przepisów dotyczących odpowiedzialności za działania autonomicznej sztucznej inteligencji, istotne może być stworzenie rejestru sztucznej inteligencji, analogicznego do istniejącego rejestru danych osobowych[606] zgłaszanych do organu nadzorczego, takiego jak *Inspektor Ochrony Danych Osobowych*[607]. Taka inicjatywa umożliwiłaby skuteczniejsze nadzorowanie i kontrolowanie podmiotów odpowiedzialnych za kreowanie i wykorzystywanie autonomicznej sztucznej inteligencji.

W praktyce, w kontekście przepisów na poziomie Unii Europejskiej, firmy zainteresowane wprowadzaniem produktów lub świadczeniem usług opartych na sztucznej inteligencji

[606] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

[607] Inspektor Ochrony Danych Osobowych (IOD) to specjalista ds. ochrony danych osobowych, którego powołanie jest obowiązkowe w niektórych organizacjach zgodnie z art. 37 RODO. IOD nadzoruje przestrzeganie przepisów o ochronie danych, doradza w tym zakresie administratorowi i współpracownikom oraz pełni funkcję punktu kontaktowego dla organu nadzorczego i osób, których dane dotyczą.

musiałyby złożyć stosowne zgłoszenie do dedykowanego organu. Podobnie jak w przypadku *Administratora Danych Osobowych*[608], podmiot odpowiedzialny za sztuczną inteligencję musiałby zostać zgłoszony jako podmiot nadzorujący jej funkcjonowanie i działanie.

Stworzenie takiego rejestru miałoby na celu zapewnienie przejrzystości oraz łatwej identyfikacji podmiotów odpowiedzialnych za rozwijanie i stosowanie sztucznej inteligencji. Ponadto, firmy korzystające z tej technologii w swoich produktach, które mogą być modyfikowane, również byłoby wymagane zgłoszenie rejestracji do odpowiednich organów nadzoru.

Wszelkie zmiany w działaniu sztucznej inteligencji, które mogą wpłynąć na jej autonomię lub sposób funkcjonowania, powinny być zgłaszane do odpowiednich organów nadzoru w celu aktualizacji informacji. Dzięki temu organy nadzorcze będą miały pełen wgląd w działania i rozwój sztucznej inteligencji, a także będą mogły egzekwować odpowiedzialność za jej działania u odpowiednich podmiotów.

Jednocześnie, konieczne jest nałożenie kar za zaniechanie zgłoszenia sztucznej inteligencji do rejestru, co może być podstawą do wycofania produktu lub usługi z terytorium Unii Europejskiej w przypadku naruszenia tego obowiązku. Niemniej jednak, w świetle szybkiego postępu technologicznego, egzekwowanie tego rodzaju przepisów może okazać się problematyczne, jednak ich wprowadzenie jest kluczowe dla zapewnienia spójności i odpowiedzialności w obszarze wykorzystania sztucznej inteligencji.

Wprowadzenie takiej metodyki miałoby na celu zapewnienie bezpieczeństwa oraz ochrony prawnej w kontekście wykorzystywania sztucznej inteligencji, a także ułatwienie procesu identyfikacji i przejęcia odpowiedzialności za jej działania w przypadku naruszeń lub złamania przepisów prawa karnego.

Akt o Sztucznej Inteligencji[609], wprowadzany przez Unię Europejską, zawiera wiele środków mających na celu regulację systemów SI, zwłaszcza tych uznanych za wysokiego ryzyka. Te

[608] Administrator Danych Osobowych to podmiot, który decyduje o celach i sposobach przetwarzania danych osobowych. Może nim być osoba fizyczna, osoba prawna, organ publiczny lub jednostka organizacyjna nieposiadająca osobowości prawnej. Administrator ponosi odpowiedzialność za zgodność przetwarzania danych z przepisami RODO i musi wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić ochronę praw osób, których dane dotyczą.

[609] Komisja Europejska, *Artificial Intelligence Act*, 13 March 2024. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, (dostęp 10.06.2024 r.).

środki obejmują konieczność rejestracji, monitorowania po wprowadzeniu na rynek oraz odpowiedzialność dostawców za spełnienie wymagań ustawy.

Chociaż te regulacje stanowią znaczący krok w kierunku odpowiedzialnego wdrażania i nadzorowania technologii SI, mogą być one niewystarczające w niektórych aspektach. W kontekście przypisania odpowiedzialności i identyfikacji twórcy, obowiązki te skupiają się głównie na systemach wysokiego ryzyka, pozostawiając mniej rygorystyczne ramy dla systemów o niższym ryzyku, które również mogą powodować szkody. Ponadto, choć system rejestracji i monitorowania pozwala na identyfikację i śledzenie systemów SI, to nie dostarcza pełnej transparentności działania każdego zastosowania SI w każdym kontekście.

Zainspirowani rozporządzeniem RODO, gdzie każdy podmiot przetwarzający dane osobowe musi starannie udokumentować swoje działania i być w stanie wykazać, że przetwarzanie odbywa się zgodnie z prawem, można rozważyć wprowadzenie bardziej szczegółowych i uporządkowanych wymagań dotyczących dokumentacji i raportowania dla wszystkich rodzajów systemów informatycznych, niezależnie od poziomu ryzyka.

Można także rozważyć wprowadzenie bardziej zaawansowanego „*rejestru twórców i operatorów sztucznej inteligencji*", podobnego do rejestru administratorów danych w RODO, co przyczyniłoby się do zwiększenia przejrzystości oraz ułatwiło egzekwowanie odpowiedzialności w przypadku naruszeń. Taki rejestr mógłby również obejmować obowiązek przeszkolenia i uzyskania certyfikacji dla twórców i operatorów systemów SI, co podniosłoby ich świadomość wymogów prawnych i etycznych.

Rozszerzenie tych przepisów w celu uwzględnienia wszystkich systemów sztucznej inteligencji, nie tylko tych uznanych za wysokie ryzyko oraz zaostrzenie wymagań dotyczących dokumentacji, szkolenia i raportowania może przyczynić się do lepszego określenia odpowiedzialności i skuteczniejszego nadzoru nad działaniami SI.

9.4.1.2 Wymogi dotyczące staranności w tworzeniu i nadzorowaniu autonomicznych systemów SI, aby uniknąć niekontrolowanego działania

W kontekście rosnącej autonomii systemów sztucznej inteligencji, ważne jest wprowadzenie szczegółowych wymagań dotyczących staranności przy ich tworzeniu i nadzorowaniu,

mających na celu zminimalizowanie ryzyka niekontrolowanego działania. Podmioty odpowiedzialne za rozwój i wdrożenie autonomicznych systemów SI powinny wprowadzić zaawansowane mechanizmy monitorujące, które umożliwią wczesne wykrywanie potencjalnie niebezpiecznych odchyleń od zamierzonych funkcji systemu. Takie mechanizmy powinny także umożliwiać regularne informowanie odpowiednich organów nadzorczych o wszelkich zagrożeniach, które mogą wystąpić podczas użytkowania systemów.

Akt dotyczący Sztucznej Inteligencji Unii Europejskiej, mimo że stanowi solidną podstawę do regulacji stosowania systemów SI, nie uwzględnia w pełni mechanizmów odpowiedzialności w przypadkach, gdy SI działa w sposób nieprzewidziany przez twórców. W związku z tym konieczne wydaje się wprowadzenie dodatkowych przepisów regulujących procesy identyfikacji i nadzoru w sposób bardziej rygorystyczny. Propozycje takich regulacji mogą obejmować ustanowienie obowiązkowego systemu certyfikacji dla wszystkich autonomicznych systemów SI o wysokim ryzyku, co zwiększyłoby przejrzystość procesów ich wdrażania oraz umożliwiło skuteczniejsze zarządzanie potencjalnymi zagrożeniami.

Aby zagwarantować maksymalne bezpieczeństwo społeczności, zaleca się ustalenie międzynarodowych norm bezpieczeństwa i etyki dla sztucznej inteligencji, co pomoże w standaryzacji praktyk i wymagań na skalę światową. Współpraca międzynarodowa oraz wymiana bezwzględnie najlepszych praktyk mogą znacząco przyczynić się do stworzenia bezpiecznego oraz odpowiedzialnego środowiska dla rozwoju i wdrożenia autonomicznych systemów SI.

W końcu, należy rozważyć wprowadzenie przepisów, które nakładałyby obowiązek na twórców sztucznej inteligencji w celu implementacji mechanizmów wyłączających system w przypadkach wykrycia działań mogących prowadzić do naruszenia praw lub zagrożenia bezpieczeństwu publicznemu. Stanowiłoby to istotny element zabezpieczający przed niekontrolowanym funkcjonowaniem technologii.

9.4.1.3 Możliwe sankcje lub kary dla twórców autonomicznej SI w przypadku naruszenia prawa karnego przez działania tego systemu

W kontekście systemów autonomicznej sztucznej inteligencji ważne jest ustalenie odpowiednich kar lub sankcji dla twórców tych systemów w przypadku naruszenia prawa karnego. Przypisanie odpowiedzialności prawnokarnej za ewentualne naruszenie dóbr chronionych prawem spowodowanych przez autonomiczny system SI może być oparte na zasadzie ryzyka. To oznacza, że twórca może zostać pociągnięty do odpowiedzialności za szkody, jakie jego produkt lub usługa wyrządziły, nawet jeśli nie działał bezpośrednio ani nie miał zamiaru spowodowania uszkodzeń.

Ważnym elementem jest w tym kontekście określenie pojęcia „*utraty kontroli ludzkiej*", które odnosi się do sytuacji, gdy sztuczna inteligencja podejmuje działania niezgodne z jej programowaniem lub oczekiwaniami twórców, prowadząc do naruszenia norm prawnych. Badacze mogą dalej rozwijać tę kategorię, aby precyzyjnie określić moment, w którym sztuczna inteligencja przekracza ustalone granice bezpieczeństwa i legalności.

Nakładanie kar na osoby tworzące sztuczną inteligencję w przypadku naruszenia prawa przez ich systemy powinno uwzględniać, że zbyt surowe kary mogą zahamować postęp technologiczny i innowacje. Z drugiej strony, brak odpowiedzialności stwarza ryzyko nadużyć i szkód społecznych. Dlatego wprowadzenie odpowiedzialności opartej na ryzyku wydaje się być rozwiązaniem, które uwzględnia oba te aspekty.

O elementach łagodzących kary możemy mówić, gdy twórca systemu sztucznej inteligencji wypełnił wszystkie obowiązki wynikające z odpowiednich protokołów i mechanizmów bezpieczeństwa, jakie zostały zidentyfikowane na diagramie. Wówczas to odpowiedzialność mogłaby być złagodzona. Na przykład, jeśli twórca wykazał staranność w procesie projektowania, testowania i monitorowania systemu, zastosował skuteczne środki zapobiegawcze oraz szybko reagował na wykryte nieprawidłowości, te działania mogłyby stanowić podstawę do zmniejszenia kary lub nawet uwolnienia od odpowiedzialności.

W kontekście wniosków o nowe przepisy, istotne jest także utworzenie instytucji nadzorczych, które będą monitorować działania sztucznej inteligencji oraz jej zgodność z prawem. Takie

organy mogłyby również zajmować się rejestracją systemów SI, co ułatwiłoby identyfikację i przypisanie odpowiedzialności twórcom w przypadku naruszeń.

9.4.2 Prawna odpowiedzialność maszyn

W trakcie pisania swojej dysertacji pt. „*Prawnokarne aspekty technologii wykorzystującej sztuczną inteligencję ze szczególnym uwzględnieniem kwalifikacji prawnej, przypisaniem sprawstwa i odpowiedzialności twórcy*", problem odpowiedzialności maszyn w kontekście prawa staje się coraz istotniejszy w obliczu rosnącej autonomii systemów SI. Wprowadzenie regulacji dotyczących odpowiedzialności prawnej maszyn mogłoby pomóc w uzupełnieniu istniejących „*luk prawnych*", które zostały zidentyfikowane podczas przeprowadzonych badań. Realizacja tego kroku byłaby jednak wyzwaniem, wymagającym również stworzenia norm prawnych dla samych maszyn, co stanowiłoby znaczące wyzwanie zarówno pod względem prawnym, jak i kulturowym.

Wprowadzenie odpowiedzialności prawnej dla maszyn wymagałoby nie tylko znaczących zmian w przepisach i regulacjach, ale także rewizji sposobu, w jaki społeczeństwo postrzega maszyny i sztuczną inteligencję. Przejście na takie rozwiązania może wydawać się zbyt radykalne w obecnym punkcie naszego rozwoju kulturowego i technologicznego. Implementacja praw dla maszyn stawia przed nami wyzwania wykraczające poza obecną strukturę prawną, co wymaga od ustawodawców, naukowców oraz społeczeństwa głębokiego zastanowienia się nad etycznymi i praktycznymi konsekwencjami takiej decyzji.

Na obecnym etapie trudno jednoznacznie określić, czy wprowadzenie odpowiedzialności maszyn jest właściwym rozwiązaniem. Wydaje się, że konieczne jest przeprowadzenie dalszych badań i analiz z różnych dziedzin, które mogłyby dostarczyć odpowiedzi na pytanie o przyszłe kierunki rozwoju prawa w kontekście zaawansowanych technologii. Takie analizy powinny pomóc organom ustawodawczym w ocenie, czy i w jaki sposób należy wprowadzić taką formę odpowiedzialności.

W kontekście niniejszej pracy doktorskiej istotne jest zauważenie, że chociaż wprowadzenie odpowiedzialności maszyn może wydawać się obiecującym rozwiązaniem w celu zapełnienia wykrytej luki prawnej, na obecnym etapie nie można jednoznacznie rozstrzygnąć tej kwestii. Konieczność dalszych badań i refleksji jest więc nieunikniona, aby w przyszłości podejmować świadome i odpowiedzialne decyzje legislacyjne.

9.4.3 Wyłączenie autonomicznego SI z użytkowania

Jednym z kluczowych zagadnień w kontekście wyników jest możliwość wyłączenia autonomicznej sztucznej inteligencji. Konieczne jest interdyscyplinarne podejście do tego problemu, aby skutecznie zarządzać ryzykiem związanym z autonomią SI. Wdrożenie obowiązku zapewnienia bezpieczeństwa poprzez projektowanie (security by design) powinno uwzględniać kryptograficzne mechanizmy ochrony systemów SI, które umożliwią ich dezaktywację w sytuacji, gdy maszyna nabierze samoświadomości lub działa poza ludzką kontrolą, podejmując działania sprzeczne z prawem.

Gdy sztuczna inteligencja nie ma jeszcze osobowości prawnej ani nie jest jasne, czy w ogóle ją otrzyma, wyłączenie SI powinno być traktowane jako środek zapobiegawczy, a nie kara. Podobnie jak w przypadku konfiskaty mienia używanego do popełnienia przestępstwa lub wycofania niebezpiecznego produktu z rynku, takie działanie powinno służyć prewencyjnej ochronie społecznej przed potencjalnymi skutkami działalności SI.

Twórca powinien być odpowiedzialny, ale nie powinien ponosić konsekwencji, jeśli zrobił wszystko, co w jego mocy, aby zapobiec niezamierzonym działaniom swojego produktu zgodnie z najlepszymi praktykami i dostępną wiedzą. W przypadkach, gdy nie można ustalić właściciela lub zarządzającego SI, istotne jest wprowadzenie procedur prawnych umożliwiających przejęcie kontroli nad autonomicznym systemem przez odpowiednie instytucje państwowe w celu jego dezaktywacji.

W praktyce wprowadzenie tych zasad wymagałoby rozważenia konieczności ustanowienia nowych przepisów prawnych, które określałyby procedury dezaktywacji oraz zakres odpowiedzialności zarówno twórców, jak i użytkowników autonomicznych systemów sztucznej inteligencji. Celem jest zapewnienie bezpieczeństwa publicznego oraz zachowanie postępu technologicznego.

9.5 Propozycje zmian legislacyjnych

W tym fragmencie mojej rozprawy doktorskiej skupiam się na zaproponowaniu nowych przepisów prawnych dotyczących technologii sztucznej inteligencji. Analizuję konkretne rekomendacje prawne, które mogą być wprowadzone w odpowiedzi na wyzwania związane z rozwojem i wdrażaniem SI. Moim celem jest nie tylko rozwiązanie obecnych problemów, ale

także stworzenie podstaw prawnych dla przyszłych, jeszcze nieprzewidzianych scenariuszy wynikających z dalszego postępu technologicznego.

W kontekście prawnym, dużą uwagę skupia się na kwestiach związanych z odpowiedzialnością cywilną i karną, a także przepisach dotyczących ochrony danych osobowych i prywatności. Istotne pytanie brzmi, w jaki sposób te prawa mogą być dostosowane lub poszerzone, aby skutecznie regulować nowe technologie, które często wychodzą poza tradycyjne ramy działania maszyn czy programów.

9.5.1 Ogólne propozycje zmian w prawodawstwie dotyczące sztucznej inteligencji

Wyzwania związane z rosnącym wpływem technologii sztucznej inteligencji na różne sfery życia społecznego i gospodarczego wymagają kompleksowego podejścia legislacyjnego. Obecne przepisy prawne nie zawsze w pełni uwzględniają specyfikę działania i konsekwencje systemów SI, co sprawia, że ustawodawcy muszą dostosować regulacje w celu zapewnienia bezpieczeństwa i sprawiedliwości w kontekście ich stosowania.

Podczas analizy przeprowadzanej w ramach niniejszej pracy doktorskiej odkryłam „*lukę prawną”*, która wskazuje na brak odpowiednich mechanizmów zapewniających skuteczną odpowiedzialność zarówno cywilną, jak i karną za działania sztucznej inteligencji, które wykraczają poza kontrolę ludzką. W celu rozwiązania tego problemu sugerowane jest wprowadzenie zmian legislacyjnych obejmujących nie tylko prawo karne, ale także inne obszary prawa, aby zapewnić spójną regulację wszystkich aspektów prawnych funkcjonowania SI.

Propozycje zmian mogłyby obejmować ustalenie klarownej definicji sytuacji, w których mówimy o działaniach sztucznej inteligencji, które „*uciekły spod kontroli człowieka*”. Takie definicje powinny znaleźć się w dedykowanym Kodeksie etycznym lub być określone w szczegółowych przepisach zawartych w odpowiedniej ustawie specjalnej. Taki kodeks mógłby określać zasady odpowiedzialności, procedury postępowania oraz etyczne ramy działania sztucznej inteligencji.

Dodatkowo, sugestia zakłada stworzenie dedykowanej agendy nadzorczej, której zadaniem będzie kontrola, dokumentacja oraz nadzór nad funkcjonowaniem systemów sztucznej inteligencji. Taka instytucja, wzorując się na organach monitorujących ochronę danych

osobowych, miałaby możliwość skutecznego zapobiegania ryzykom związanym z nieprawidłowym wykorzystaniem autonomicznych systemów SI poprzez prowadzenie rejestrów i zatwierdzanie podmiotów odpowiedzialnych za rozwój i implementację tych technologii.

Jednocześnie, w kontekście wyłączenia autonomicznego sztucznej inteligencji z użytkowania, ważne będzie wprowadzenie regulacji umożliwiających skuteczne i bezpieczne wyłączanie systemów SI, które stanowią zagrożenie. Specjalna ustawa mogłaby dostarczyć solidnych regulacji prawnych, podobnych do tych stosowanych w przypadku ochrony danych osobowych, jednocześnie zapewniając ochronę interesów publicznych i indywidualnych użytkowników.

W skrócie, właściwe regulacje i zmiany prawne odgrywają kluczową rolę w kontrolowaniu ryzyka związanego z rosnącą autonomią sztucznej inteligencji, co z kolei przyczynia się do budowania zaufania społecznego do nowych technologii oraz bezpiecznego ich wprowadzania.

9.5.2 Postulat zmian w Kodeksie karnym w odpowiedzi na wyzwania postawione przez SI

9.5.2.1 Odpowiedzialność na zasadzie ryzyka w związku z działaniem systemów autonomicznych

W odpowiedzi na wzrastające wyzwania związane z autonomicznymi systemami komputerowymi, szczególnie w kontekście sztucznej inteligencji, istnieje pilna potrzeba wprowadzenia specjalnych przepisów prawnych, które bezpośrednio odnosiłyby się do kwestii odpowiedzialności karnej w związku z działalnością tych technologii. W ramach propozycji zmian w Kodeksie karnym, w niniejszej dysertacji przedstawiam projekt nowej regulacji mającej na celu uregulowanie odpowiedzialności na zasadzie ryzyka za ewentualne szkody spowodowane przez autonomiczne systemy.

Nowo proponowany artykuł Kodeksu karnego „*Odpowiedzialność na zasadzie ryzyka w związku z działaniem systemów autonomicznych*” wprowadza koncepcję odpowiedzialności karnej za czynności podejmowane przez autonomiczne systemy informatyczne, które, choć działają samodzielnie, mogą potencjalnie skutkować znaczącymi naruszeniami dóbr chronionych prawem. Zaproponowany przepis stanowi, że *producent lub dystrybutor systemu ponosi odpowiedzialność karną w przypadku szkody wynikającej z ryzyka normalnego*

funkcjonowania tego systemu. Istotnym aspektem jest fakt, że taka odpowiedzialność ma zastosowanie nawet w sytuacjach, gdy autonomiczny system wymknął się spod kontroli producenta lub dystrybutora.

Kolejne akapity przewidują możliwość zwolnienia z odpowiedzialności, jeśli producent lub dystrybutor może udowodnić, że naruszenie dobra zostało spowodowane siłą wyższą, działaniami poszkodowanego lub osobami trzecimi, za które nie ponoszą odpowiedzialności, albo jeśli przed wprowadzeniem systemu na rynek podjęto wszystkie odpowiednie środki zapobiegawcze.

Dodatkowo, przepis przewiduje, że w szczególnie poważnych przypadkach, takich jak te prowadzące do śmierci, uszczerbku na zdrowiu lub znacznych szkód materialnych, sąd może orzec o odpowiedzialności producenta lub dystrybutora biorąc pod uwagę charakterystykę ryzyka autonomicznego działania systemu.

Propozycje regulacji sugerują także potrzebę wprowadzenia szczegółowych wymagań odnośnie do projektowania, testowania oraz weryfikacji bezpieczeństwa systemów autonomicznych, a także procedur postępowania w przypadku ich nieprzewidzianego działania, które zostaną ustalone przez odpowiednie instytucje regulacyjne.

Takie podejście ma na celu poprawę bezpieczeństwa w zastosowaniach autonomicznych technologii sztucznej inteligencji, minimalizację ryzyka dla użytkowników i poszkodowanych oraz zapewnienie klarowności i przewidywalności odpowiedzialności prawnej. To kluczowe dla zachowania zaufania społecznego i promowania odpowiedzialnego rozwoju technologicznego.

Oto propozycja sformułowania takiego przepisu:

Art. [numer] - Odpowiedzialność na zasadzie ryzyka w związku z działaniem systemów autonomicznych

1. *Odpowiedzialność karna za szkody wyrządzone przez autonomiczne systemy informatyczne, w tym systemy sztucznej inteligencji, które podejmują decyzje samodzielnie, ponosi producent lub dystrybutor systemu, jeżeli szkoda wynika z ryzyka związanego z normalnym funkcjonowaniem takiego systemu, nawet jeśli system wyszedł spod kontroli producenta lub dystrybutora.*

2. *Odpowiedzialności, o której mowa w ust. 1, nie ponosi producent lub dystrybutor, jeżeli wykaże, że:*

   a. *szkoda powstała w wyniku działania siły wyższej,*

   b. *szkoda powstała wyłącznie w wyniku działania lub zaniechania osoby poszkodowanej lub osób trzecich, za które producent lub dystrybutor nie ponosi odpowiedzialności,*

   c. *wszystkie dostępne i stosowne środki prewencyjne zostały zastosowane przed wprowadzeniem systemu na rynek i system był regularnie aktualizowany oraz monitorowany w celu zapobiegania wypadkom.*

3. *W przypadku gdy system autonomiczny, który wyszedł spod kontroli, spowoduje śmierć, uszczerbek na zdrowiu lub znaczne szkody materialne, sąd może orzec o odpowiedzialności producenta lub dystrybutora, biorąc pod uwagę stopień ryzyka związanego z autonomicznym działaniem systemu i jego potencjalną zdolność do wyrządzenia szkody.*

4. *Przepisy szczegółowe dotyczące wymagań dla systemów autonomicznych, w tym zasady ich projektowania, testowania, weryfikacji bezpieczeństwa oraz procedury w przypadku stwierdzenia ich niekontrolowanego działania, zostaną określone przez ministra właściwego do spraw informatyzacji w drodze rozporządzenia.*

5. *Działania naprawcze po wystąpieniu incydentu z udziałem autonomicznego systemu sztucznej inteligencji powinny obejmować nie tylko ustalenie przyczyn i eliminację wad, ale również obligatoryjne informowanie odpowiednich organów regulacyjnych oraz społeczeństwo o potencjalnych zagrożeniach.*

6. *W przypadku gdy system autonomiczny, który wyszedł spod kontroli, wywoła skutek w postaci śmierci, uszczerbku na zdrowiu lub znaczne szkody materialne, sąd może orzec o odpowiedzialności producenta lub dystrybutora, biorąc pod uwagę stopień ryzyka związanego z autonomicznym działaniem systemu i jego potencjalną zdolność do wyrządzenia szkody.*

7. *Przepisy szczegółowe dotyczące wymagań dla systemów autonomicznych, w tym zasady ich projektowania, testowania, weryfikacji bezpieczeństwa oraz procedury w przypadku*

stwierdzenia ich niekontrolowanego działania, zostaną określone przez ministra właściwego do spraw informatyzacji w drodze rozporządzenia.

8. *Działania naprawcze po wystąpieniu incydentu z udziałem autonomicznego systemu sztucznej inteligencji powinny obejmować nie tylko ustalenie przyczyn i eliminację wad, ale również obligatoryjne informowanie odpowiednich organów regulacyjnych oraz publikę o potencjalnych zagrożeniach.*

9.5.2.2 Wyłączenie z użytkowania systemów sztucznej inteligencji

W odpowiedzi na wyzwania stawiane przed prawem karnym, proponowane są zmiany mające na celu wzmocnienie odpowiedzialności prawnej związanej z używaniem autonomicznych systemów sztucznej inteligencji. Kolejna propozycja koncentruje się na wprowadzeniu odpowiedzialności za nieprawidłowe zarządzanie i monitorowanie takich systemów, aby skutecznie reagować na rzeczywiste zagrożenia wynikające z ich działania. Zaproponowany artykuł powinien znaleźć swoje miejsce w ustawie specjalnej dotyczącej sztucznej inteligencji, co skutkować będzie bezpośrednim odniesieniem do odpowiedzialności karnej.

Proponuję, aby przepis dotyczący *wyłączenie z użytkowania systemów sztucznej inteligencji,* zawierał takie elementy jak:

1. obowiązek wycofania niebezpiecznego systemu SI

   Jeśli zostanie zauważone, że system sztucznej inteligencji stanowi bezpośrednie niebezpieczeństwo dla zdrowia, życia lub mienia ludzi, producent lub dystrybutor jest zobowiązany do natychmiastowego wyłączenia go i poinformowania odpowiednich organów regulacyjnych oraz użytkowników o zagrożeniu.

2. możliwość interwencji przez organ nadzorczy

   Decyzję o zaprzestaniu korzystania z systemu może również podjąć organ nadzorczy, jeśli uzna, że system nie może być dalej bezpiecznie kontrolowany. W takiej sytuacji, organ może także zażądać od producenta lub dystrybutora wprowadzenia koniecznych zmian w systemie.

3. procedury wycofania produktu

Producent albo dystrybutor musi przestrzegać procedur dotyczących wycofania produktu, włączając w to analizę ryzyka, tworzenie i wdrażanie planu wycofania oraz monitorowanie systemu po zakończeniu procesu wycofywania.

A o to propozycja przepisu:

Art. [numer] - Wyłączenie z użytkowania systemów sztucznej inteligencji

1. *W przypadku stwierdzenia, że autonomiczny system informatyczny stanowi bezpośrednie zagrożenie dla zdrowia, życia ludzi lub mienia, producent lub dystrybutor jest zobowiązany do niezwłocznego wycofania systemu z eksploatacji i powiadomienia właściwych organów regulacyjnych oraz użytkowników o wystąpieniu zagrożenia.*

2. *Decyzja o wycofaniu systemu z użytkowania może być także wydana przez właściwy organ nadzorczy, jeśli ten uzna, że działanie systemu SI nie może być już bezpiecznie kontrolowane lub zneutralizowane przez producenta czy dystrybutora. Organ nadzorczy, w uzasadnionych przypadkach, może również zobowiązać producenta lub dystrybutora do przeprowadzenia niezbędnych modyfikacji w systemie w celu eliminacji zagrożenia.*

3. *Producent lub dystrybutor ma obowiązek przestrzegania procedur wycofywania produktu, które obejmują etapy takie jak: analiza ryzyka, opracowanie planu wycofania, jego realizacja i monitoring po wycofaniu, a także informowanie o ryzyku i działaniach podjętych w odpowiedzi na wykryte zagrożenie.*

Powyższa propozycja przepisu, w mojej ocenie powoduje, iż należy wprowadzić jeszcze jeden nowy przepis do ustawy specjalnej dotyczącej sztucznej inteligencji, co również, jak w przypadku poprzedniej propozycji, będzie on skutkować odpowiedzialnością karną. Przepis ten dotyczy zaniedbania w wyłączaniu systemu sztucznej inteligencji i powinien brać pod uwagę:

- odpowiedzialność karną nałożoną na producenta lub dystrybutora, który nie dezaktywował systemu SI, mimo wiedzy o istniejącym zagrożeniu, co skutkowało powstaniem szkód;

- kara może zawierać zarówno kary finansowe, jak i inne rodzaje odpowiedzialności, w zależności od wielkości szkód i stopnia zaniedbania;

Propozycja przepisu jest następująca:

Art. [numer] - Odpowiedzialność za niewycofanie niebezpiecznego systemu sztucznej inteligencji

1. ***[Podstawowa odpowiedzialność]*** *Producent lub dystrybutor autonomicznego systemu informatycznego, który, mimo stwierdzenia zagrożenia, nie podejmuje działań w celu jego natychmiastowego wycofania z użytkowania, odpowiada karnie za szkody wyrządzone przez ten system. Odpowiedzialność ta dotyczy sytuacji, gdy mimo obowiązku wynikającego z artykułu [numer] - Wyłączenie z użytkowania systemów sztucznej inteligencji, system pozostaje aktywny.*

2. ***[Działania wymagane od producenta lub dystrybutor]*** *W przypadku rozpoznania zagrożenia przez autonomiczny system sztucznej inteligencji, producent lub dystrybutor jest zobowiązany do niezwłocznego jego wyłączenia, powiadomienia właściwych organów regulacyjnych oraz użytkowników. Niezastosowanie się do tych obowiązków skutkuje odpowiedzialnością karną za każdą szkodę spowodowaną przez system po stwierdzeniu zagrożenia.*

3. ***[Zaostrzenie kar]*** *W sytuacjach, gdy działanie niebezpiecznego systemu sztucznej inteligencji skutkuje poważnymi szkodami materialnymi, uszczerbkiem na zdrowiu lub śmiercią, sąd może nałożyć szczególnie surowe kary. W takich przypadkach brane pod uwagę będą stopień zaniedbania oraz potencjalne zagrożenie dla zdrowia publicznego i bezpieczeństwa.*

4. ***[Regulacje szczegółowe]*** *Szczegółowe wymagania dotyczące procedur wycofania systemu AI, w tym etapy analizy ryzyka, przygotowania i realizacji planu wycofania, monitoring po wycofaniu, oraz informowanie o ryzyku i podjętych działaniach, zostaną określone w rozporządzeniu wydanym przez ministra właściwego do spraw informatyzacji.*

Te postulaty *de lege lata* mają na celu zwiększenie odpowiedzialności producentów i dystrybutorów systemów sztucznej inteligencji, zapewniając, że niebezpieczne systemy zostaną szybko wycofane z użytkowania w celu ochrony publicznej i minimalizacji ryzyka wyrządzenia szkód. Nowe przepisy stawiają szczególny nacisk na obowiązki

i odpowiedzialność tych podmiotów w zarządzaniu ryzykiem związanym z autonomicznymi systemami SI.

Wprowadzenie tych przepisów ma na celu nie tylko zwiększenie odpowiedzialności firm, które decydują się wprowadzić na rynek produkty korzystające z technologii sztucznej inteligencji, ale także zapewnienie bezpieczeństwa użytkownikom. Istotne jest, aby prawo postępowało krok za krokiem wraz ze szybkim rozwojem technologicznym, dostarczając skuteczne środki regulacyjne zdolne skutecznie reagować na nowe wyzwania i zagrożenia.

9.5.3 Interdyscyplinarny kontekst zmian

Ważne jest, aby rozważać perspektywę zmian prawnych dotyczących technologii sztucznej inteligencji w taki sposób, który uwzględnia równowagę pomiędzy innowacyjnością technologiczną a troską o bezpieczeństwo i odpowiedzialność.

Aby reformy prawne były skuteczne i nie ograniczały innowacyjności, konieczne jest zastosowanie interdyscyplinarnego podejścia, które integruje wiedzę z różnych dziedzin: prawa, etyki, technologii oraz społecznych aspektów korzystania z sztucznej inteligencji. Taki sposób postępowania zapewni, że nowe przepisy będą odpowiednio reagować na wyzwania związane z rozwojem i wdrożeniem autonomicznych systemów informatycznych, jednocześnie dbając o interesy społeczeństwa i indywidualnych użytkowników.

Osiągnięcie tego celu wymaga ciągłej współpracy między różnymi dziedzinami, które powinny wspólnie rozważać zarówno techniczne możliwości sztucznej inteligencji, jak i potencjalne ryzyko oraz konsekwencje społeczne i etyczne związane z jej zastosowaniami. Ponadto, wprowadzenie klarownych przepisów prawnych powinno uwzględniać dynamiczne dostosowywanie się do postępu technologicznego, co umożliwi szybką reakcję na nowe wyzwania oraz eliminację przestarzałych lub nieskutecznych regulacji.

Na poziomie prawnym, zmiany powinny uwzględniać nie tylko konkretne przepisy dotyczące prawa karnego, ale również poszerzyć zakres ochrony poprzez prawo cywilne, przepisy administracyjne oraz zasady dotyczące odpowiedzialności firm. Rozwiązania prawne powinny być tak skonstruowane, aby nie tylko karać za nadużycia, ale także promować najlepsze praktyki i zachęcać do odpowiedzialnego rozwoju i wykorzystywania technologii.

Nie wolno zapominać także o znaczeniu edukacji i świadomości, zarówno wśród twórców technologii, jak i użytkowników. Znajomość możliwości i ograniczeń systemów sztucznej inteligencji, a także zrozumienie przepisów regulujących ich zastosowanie, są kluczowe dla zapewnienia bezpiecznego i etycznego wykorzystania. Edukacja w tym obszarze powinna obejmować aspekty techniczne oraz prawnoetyczne, przygotowując wszystkich do kompetentnego i świadomego korzystania z nowych technologii.

Podsumowując, złożony kontekst zmian w ustawodawstwie dotyczącym sztucznej inteligencji stanowi nie tylko wyzwanie, ale także okazję do stworzenia przemyślanego i efektywnego systemu prawnego, który będzie w stanie nadążyć za tempem rozwoju technologii. Jednocześnie ma zapewnić bezpieczeństwo, sprawiedliwość i ochronę dla wszystkich zainteresowanych stron. Rozwój ten wymaga stałej refleksji, debaty i gotowości do przemyślanych zmian w odpowiedzi na dynamicznie ewoluujący świat sztucznej inteligencji.

9.5.4 Międzynarodowy kontekst zmian

Wprowadzenie zmian w przepisach dotyczących sztucznej inteligencji stanowi wyzwanie, które wymaga globalnego podejścia. W przypadku Polski jako kraju, który nie jest liderem w innowacjach związanych z SI, istotne jest poszukiwanie rozwiązań sprzyjających postępowi technologicznemu przy jednoczesnym uwzględnieniu odpowiednich regulacji prawnych. W tym kontekście kluczową rolę odgrywa ujednolicenie przepisów w ramach Unii Europejskiej, co pozwoli uniknąć rozdrobnienia rynku i stworzyć spójne warunki dla wszystkich państw członkowskich.

W kontekście wprowadzania zmian legislacyjnych na arenie międzynarodowej, osiągnięcie globalnego porozumienia wydaje się być trudne ze względu na różnice kulturowe oraz rozbieżności interesów ekonomicznych poszczególnych państw. Chociaż stworzenie powszechnych regulacji międzynarodowych dotyczących sztucznej inteligencji byłoby idealnym rozwiązaniem, mogącym przyczynić się do ustanowienia jednolitych standardów i zasad, realizacja tego celu może okazać się długotrwałym i skomplikowanym procesem, szczególnie w obliczu współczesnych napięć geopolitycznych oraz wyraźnie zarysowanych interesów narodowych.

Skoncentrowanie się na prawodawstwie europejskim wydaje się być bardziej realistycznym i efektywnym podejściem. Unia Europejska już udowodniła swoją zdolność do wprowadzania innowacyjnych i skutecznych regulacji, jak to miało miejsce w przypadku RODO, które ustaliły wysokie standardy ochrony danych osobowych i stały się wzorcem dla innych krajów. Europejski system prawny zapewnia unikalną platformę do testowania i wdrażania przepisów regulujących technologie SI, co może również posłużyć jako model dla innych regionów.

Przyjęcie konkretnego europejskiego podejścia umożliwi skoordynowanie działań i polityk na poziomie kontynentalnym, co jest szczególnie istotne w obliczu szybkiego postępu technologii SI i jej zastosowań. Takie podejście umożliwi także lepsze zarządzanie ryzykiem związanym z nowymi technologiami, zapewniając jednocześnie, że innowacje nie zostaną ograniczone przez nadmiernie restrykcyjne przepisy.

Próba ustanowienia wspólnych regulacji prawnych na poziomie UE może także przyczynić się do wzmocnienia pozycji Europy jako światowego lidera w obszarze etycznych i zrównoważonych technologii. Chociaż proces harmonizacji prawa SI na skalę globalną może być skomplikowany, Unia Europejska, dzięki swojemu doświadczeniu i zasobom, posiada potencjał do bycia pionierem w tej dziedzinie, pokazując, że można łączyć innowacyjność z odpowiedzialnym regulowaniem.

Z uwagi na charakter zmian w Unii Europejskiej, istnieje argument za podejściem, które sugeruje, że stosowanie wyłącznie krajowych regulacji może być niewystarczające i prowadzić do izolacji polskiego rynku. W takiej sytuacji globalni producenci i twórcy technologii sztucznej inteligencji mogą skoncentrować swoje wysiłki na bardziej liberalnych i przyjaznych rynkach, pomijając Polskę. W rezultacie może to prowadzić do dyskryminacji polskich konsumentów i użytkowników. To ukazuje konieczność dostosowywania prawa do światowych trendów oraz potrzeb rynku, gdzie Polska powinna dążyć do aktywnego uczestnictwa w procesie ustalania międzynarodowych standardów.

Tak samo jak w przypadku sukcesu *Rozporządzenia Ogólnego o Ochronie Danych*[610], które ustanowiło jednolite standardy ochrony danych osobowych w całej UE, Polska powinna wspierać i promować inicjatywy mające na celu stworzenie równie skutecznych przepisów

[610] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

dotyczących sztucznej inteligencji. Proponowane regulacje powinny uwzględniać nie tylko kwestie odpowiedzialności za działanie SI, ale także aspekty etyczne i bezpieczeństwa.

Należy więc skoncentrować się na stworzeniu propozycji zmian w Kodeksie karnym oraz innych aktach regulujących działalność związana z sztuczną inteligencją. Te zmiany powinny jasno i zrozumiale określać zasady odpowiedzialności producentów i dystrybutorów. Warto również rozważyć wprowadzenie mechanizmów zapewniających, że każdy nowy produkt oparty na sztucznej inteligencji, który trafi na europejski rynek, jest zgodny z obowiązującymi przepisami prawnymi i etycznymi. Tego rodzaju podejście może przyczynić się do wzrostu siły i innowacyjności sektora sztucznej inteligencji w Europie w dłuższej perspektywie czasowej.

Konieczne będzie nie tylko wprowadzenie zmian w przepisach prawnych, ale także szeroko zakrojone działania edukacyjne i społeczne, aby zapewnić odpowiednie przygotowanie wszystkich zainteresowanych stron do funkcjonowania w zmieniającym się środowisku regulacyjnym. Realizacja tych zmian będzie wymagała współpracy na wielu szczeblach, począwszy od lokalnych inicjatyw, aż po międzynarodowe porozumienia, co może stanowić solidną podstawę dla przyszłego rozwoju i wdrożenia sztucznej inteligencji na skalę globalną.

9.6 Dyskusja

9.6.1 Dyskusja nad tematem wprowadzenia odpowiedzialności twórcy na zasadzie ryzyka

9.6.1.1 Aspekty prawne odpowiedzialności na zasadzie ryzyka

Trwają intensywne debaty akademickie na temat wprowadzenia koncepcji odpowiedzialności opartej na ryzyku dla twórców i operatorów sztucznej inteligencji. Istotne zagadnienia tych dyskusji skupiają się głównie na potencjalnych wyzwaniach prawnych i etycznych związanych z SI, zwłaszcza w kontekście odpowiedzialności za ewentualne szkody lub błędy spowodowane przez systemy SI.

Jednym z głównych zagadnień jest kwestia odpowiedzialności prawnej, która obejmuje identyfikację strony odpowiedzialnej, ustalenie związków przyczynowych oraz skomplikowania w przejrzystości procesów podejmowania decyzji przez SI. To sprawia, że

trudno jest określić, kto winien ponosić odpowiedzialność w przypadku awarii systemu SI lub powstania szkody[611].

W odpowiedzi na te wyzwania, niektórzy sugerują konkretną regulację prawną dotyczącą odpowiedzialności sztucznej inteligencji. Przykładowo, niektóre propozycje prawne sugerują, by twórcy i operatorzy SI mogliby być pociągani do odpowiedzialności za wszelkie naruszenia dóbr spowodowane przez systemy, bez względu na winę. Taka strategia jest porównywalna do podejścia stosowanego w przypadku innych produktów i technologii, które mogą nieść za sobą istotne ryzyko[612].

Ponadto, podkreśla się konieczność aktualizacji przepisów regulacyjnych w celu skutecznego zarządzania tymi obowiązkami, co sugeruje, że Unia Europejska zmierza w kierunku podejścia opartego na ryzyku w kontekście odpowiedzialności za sztuczną inteligencję. W ramach tego podejścia proponowany jest surowy system odpowiedzialności dla systemów SI o wysokim ryzyku, zalecając, aby twórcy i operatorzy zagwarantowali bezpieczeństwo i niezawodność systemu w celu zapobieżenia ewentualnym szkodom[613].

Te rozmowy stanowią część szerszego uznania, że dynamiczny postęp w dziedzinie technologii sztucznej inteligencji wymaga nowego podejścia do regulacji prawnych i etycznych, aby wyważyć innowacje z ochroną przed potencjalnymi zagrożeniami[614].

Dyskusja akademicka na temat odpowiedzialności twórców i operatorów sztucznej inteligencji jest kształtowana przez konieczność rozwiązania pojawiających się problemów prawnych, etycznych i praktycznych związanych z technologią SI. Dążenie do bardziej restrykcyjnych regulacji odzwierciedla starania mające na celu zapewnienie ponoszenia odpowiedzialności i zapewnienie bezpieczeństwa podczas implementacji systemów SI.

Analizując artykuły naukowe można zobaczyć, w jaki sposób autorzy tych artykułów podchodzą do wprowadzenia odpowiedzialności twórcy sztucznej inteligencji z perspektywy ryzyka oraz jakie zarzuty pod adresem tego podejścia pojawiają się w literaturze przedmiotu.

---

611 Gecić Law, *Who's Responsible? Addressing Liability in the Age of AI*, dostępny w geciclaw.com, https://www.geciclaw.com/whos-responsible-addressing-liability-in-the-age-of-artificial-intelligence/ (dostęp: 10.06.2024 r.).

612 Ibidem

613 Ibidem

614 ISACA, *The Promise and Peril of the AI Revolution: Managing Risk*, dostępny w isaca.org, https://www.isaca.org/resources/white-papers/2023/the-promise-and-peril-of-the-ai-revolution (dostęp: 10.06.2024 r.).

W odniesieniu do zaproponowanego przeze mnie przepisu wprowadzającego odpowiedzialność na zasadzie ryzyka, słowa poparcia można znaleźć w tekście opublikowanym w „*Odpowiedzialność za sztuczną inteligencję*" (Cambridge Handbook of Responsible Artificial Intelligence)[615], gdzie omówiono propozycję *Aktu o Sztucznej Inteligencji* (AIA), który ma na celu zapewnienie, że systemy SI wprowadzone na rynek Unii Europejskiej są bezpieczne i zgodne z obowiązującym prawem dotyczącym fundamentalnych praw i wartości Unii. Autorzy podkreślają konieczność uwzględnienia wymogów dotyczących SI w istniejącym oraz przyszłym prawodawstwie dotyczącym bezpieczeństwa produktów, co obejmuje wprowadzenie odpowiedzialności związanej z ryzykiem dla systemów SI uznanych za wysokiego ryzyka. To rozwiązanie pod krytykę poddają autorzy artykułu opublikowanego w „*Raporcie Grupy Ekspertów dotyczącym Odpowiedzialności za Sztuczną Inteligencję i Inne Nowoczesne Technologie Cyfrowe*" (European Journal of Risk Regulation)[616], którzy krytykują jednolite podejście do regulacji odpowiedzialności za SI. Zaznaczają, że traktowanie SI jako jednorodnej kategorii aplikacji uniemożliwia dostosowanie regulacji do konkretnych zastosowań i kontekstów, w których technologia jest wykorzystywana. Twierdzą, że różnorodność zastosowań SI wymaga bardziej zróżnicowanego podejścia do odpowiedzialności, co pozwoliłoby lepiej uwzględnić różnorodne społeczne obawy związane z każdym zastosowaniem.

Podsumowując, propozycje wprowadzenia odpowiedzialności na zasadzie ryzyka są uważane za kluczowy element bezpiecznego i etycznego rozwoju technologii sztucznej inteligencji. Jednakże krytycy tego podejścia twierdzą, że takie standaryzowane rozwiązania mogą okazać się niewystarczająco elastyczne do skutecznego regulowania tak zróżnicowanej i dynamicznie rozwijającej się dziedziny jak sztuczna inteligencja. Oba stanowiska podkreślają konieczność ciągłej debaty i dostosowywania przepisów prawnych, aby adekwatnie reagować na postęp technologiczny.

---

[615] Wendehorst C., Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks, in: Voeneky S., Kellmeyer P., Mueller O., Burgard W. (eds.), The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives, Cambridge Law Handbooks, Cambridge University Press, s. 187-209, https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/liability-for-artificial-intelligence/12A89C1852919C7DBE9CE982B4DE54B7 (dostęp: 10.06.2024 r.).

[616] Škorvánek I., Talus K., Smuha N. A., *Raport grupy ekspertów dotyczący odpowiedzialności za sztuczną inteligencję oraz inne nowoczesne technologie cyfrowe: krytyczna ocena*, European Journal of Risk Regulation, Vol. 11, No. 2, s. 390-398, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/expert-groups-report-on-liability-for-artificial-intelligence-and-other-emerging-digital-technologies-a-critical-assessment/45FD6BB0E113E7C4A9B05128BC710589 (dostęp: 10.06.2024 r.).

9.6.1.2 Aspekty technologiczne odpowiedzialności na zasadzie ryzyka

Wprowadzenie koncepcji odpowiedzialności opartej na ryzyku dla twórców sztucznej inteligencji budzi mieszane uczucia w społeczności technologicznej. Niektórzy eksperci i naukowcy uważają taki krok za konieczny w celu zapewnienia bezpieczeństwa i odpowiedzialności w epoce rosnącej autonomii maszyn, podczas gdy inni obawiają się, że może to zahamować innowacje. Dlatego w tym miejscu warto przedstawić słowa krytyki oraz poparcia dla propozycji nowego przepisu w odniesieniu do odpowiedzialności na zasadzie ryzyka. W poniższym podpunkcie, przeciwnie niż w poprzednim podpunkcie, odnoszą się do aspektów technicznych.

I tak w kontekście poparcia wprowadzenia dla odpowiedzialności na zasadzie ryzyka, założenia wprowadzenia tej odpowiedzialności zakładają, że twórcy i użytkownicy systemów sztucznej inteligencji powinni być w pełni odpowiedzialni za ewentualne szkody spowodowane przez ich produkty, niezależnie od tego, czy są one wynikiem ich winy. Argumentacja za takim podejściem opiera się na konieczności zwiększenia zaufania społecznego do technologii SI, co jest kluczowe dla ich dalszego rozwoju i integracji z naszym codziennym życiem. Na przykład w artykule „*Podejście w postaci regulacyjnych piaskownic do regulowania wysokiego ryzyka aplikacji sztucznej inteligencji*”[617] podkreśla się, że podejście regulacyjne oparte na koncepcji piaskownicy może stanowić dopełnienie reżimu odpowiedzialności ścisłej, równoważąc potrzebę ochrony społecznej z zachętami do innowacji. Termin „*piaskownica*” (ang. sandbox) w kontekście regulacji i technologii odnosi się do kontrolowanego środowiska testowego, w którym nowe technologie, produkty lub usługi mogą być eksperymentowane i testowane bez całkowitego spełnienia obowiązujących przepisów. Koncepcja piaskownicy regulacyjnej umożliwia przetestowanie innowacji w warunkach rzeczywistych, zapewniając jednocześnie ochronę użytkowników oraz umożliwiając organom nadzoru monitorowanie i ocenę nowych rozwiązań przed ich pełnym wdrożeniem i komercjalizacją. „*Piaskownice*” (ang. sandboxes) są powszechnie wykorzystywane w sektorach silnie regulowanych, takich jak finanse, opieka zdrowotna czy transport, gdzie surowe przepisy mogłyby odstraszać przed wprowadzaniem nowych, potencjalnie przełomowych technologii. Dzięki „*piaskownicom*” firmy mogą

[617] Truby J., Brown R. D., Ibrahim I. A., Parellada O. C., *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, European Journal of Risk Regulation, Vol. 13, No. 2, s. 270-294, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence-applications/C350EADFB379465E7F4A95B973A4977D (dostęp: 10.06.2024 r.)

współpracować z organami regulacyjnymi, aby zapewnić bezpieczeństwo i zgodność innowacji z prawem, jednocześnie przyspieszając ich rozwój i dostępność na rynku.

Krytyczne podejście do wprowadzenia odpowiedzialności na zasadzie ryzyka w aspekcie technologicznym pokazuje, że sceptycy tej koncepcji argumentują, iż surowa odpowiedzialność może nierówno obciążać mniejsze i średnie firmy, które nie posiadają finansowych zasobów większych korporacji do radzenia sobie z ewentualnymi roszczeniami. Ostrzega się również, że taka strategia może odstraszać przed eksperymentowaniem z nowymi, potencjalnie przełomowymi technologiami ze względu na obawy przed konsekwencjami prawnymi[618].

Podsumowując, koncepcja odpowiedzialności na zasadzie ryzyka w kontekście twórców sztucznej inteligencji niesie ze sobą wiele potencjalnych korzyści i wyzwań. Ważne jest znalezienie odpowiedniej równowagi, aby zachować innowacyjny charakter przy jednoczesnym zapewnieniu bezpieczeństwa i ochrony użytkowników.

9.6.1.3 Aspekty etyczne odpowiedzialności na zasadzie ryzyka

Wprowadzenie zasady odpowiedzialności opartej na ryzyku dla twórców sztucznej inteligencji rodzi istotne dylematy etyczne, które są intensywnie dyskutowane w kręgach naukowych i technologicznych. Głównym argumentem za takim podejściem jest konieczność poprawy bezpieczeństwa i odpowiedzialności w kontekście wykorzystania SI. Idea ta zakłada, że twórcy i użytkownicy systemów SI powinni ponosić odpowiedzialność za ewentualne szkody wynikające z działania tych systemów, niezależnie od ich winy. To zobowiązanie ma na celu zmotywowanie firm do wprowadzenia bardziej rygorystycznych procedur testowych oraz zapewnienia bezpieczeństwa produktów opartych na sztucznej inteligencji[619].

Istnieje jednak obawa, że zbyt restrykcyjne przepisy mogą ograniczać rozwój technologicznej innowacji. Odpowiedzialność oparta na zasadzie ryzyka może stanowić przeszkodę dla mniejszych firm i start-upów, które nie dysponują wystarczającymi zasobami, aby sprostać

[618] Pietrzykowski T., *Odpowiedzialność za sztuczną inteligencję - wyzwania dla prawa cywilnego i karnego*, "Przegląd Prawniczy Uniwersytetu Warszawskiego" 2021, vol. 20, nr 1, s. 38-39.

[619] European Commission, *AI Liability Directive*, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en (dostęp: 10.06.2024 r.).

wymogom regulacyjnym. To z kolei może spowolnić postęp w dziedzinie nowych, potencjalnie przełomowych technologii sztucznej inteligencji.

Etyczne rozważania dotyczą również sprawiedliwości i odpowiedzialności. Istnieje ryzyko, że systemy sztucznej inteligencji, działając niezamierzonymi ścieżkami, mogą przyczynić się do szkód lub dyskryminacji. Dlatego kluczowe jest, aby projektować i wdrażać te systemy w sposób transparentny, uwzględniając właściwe zasady etyczne oraz szanując prawa człowieka. Warto rozważyć kwestię czy odpowiedzialność powinna spoczywać wyłącznie na twórcach systemów SI czy być rozszerzona na operatorów i użytkowników tychże systemów[620].

Podsumowując, wprowadzenie zasady odpowiedzialności opartej na ryzyku dla twórców sztucznej inteligencji jest istotnym krokiem w zapewnieniu bezpieczeństwa i etycznej odpowiedzialności w dobie rozwoju sztucznej inteligencji. Niemniej jednak każde rozwiązanie regulacyjne musi uwzględniać potrzebę ochrony społeczeństwa oraz konieczność zachowania zdrowego ekosystemu innowacji technologicznych.

9.6.2 Dyskusja na temat wprowadzenia obowiązku wdrożenia mechanizmów umożliwiających wyłączenia SI, które stanowią zagrożenie

9.6.2.1 Aspekty prawne wyłączania systemów SI

W kontekście prawnym, wprowadzenie wymogu implementacji mechanizmów umożliwiających dezaktywację systemów sztucznej inteligencji, które prezentują ryzyko, jest szeroko omawiane w literaturze przedmiotu. Dyskusja ta skupia się na konieczności zabezpieczenia przed ewentualnymi szkodami wynikającymi z działania systemów SI bez kontroli.

Poparcie dla wprowadzenia obowiązku wdrożenia mechanizmów wyłączających wynika z postrzegania sztucznej inteligencji jako technologii o potencjalnie wysokiego ryzyka, która może stanowić zagrożenie dla bezpieczeństwa, prywatności i innych fundamentalnych praw

[620] AI-Regulation, *Ethical Framework, Civil Liability and Intellectual Property Rights for AI*, https://www.ai-regulation.com/ (dostęp: 10.06.2024 r.)

człowieka. W kontekście bezpieczeństwa i odpowiedzialności, obowiązkowe mechanizmy wyłączające mogą pełnić rolę środka ostrożności, zapewniając, że systemy SI mogą być szybko i skutecznie wyłączone w przypadku awarii lub gdy ich działanie zaczyna odbiegać od zamierzonych funkcji. Takie podejście znajduje uznanie w różnych przepisach dotyczących certyfikacji i standardów bezpieczeństwa na poziomie Unii Europejskiej[621].

Z drugiej strony krytyka wprowadzenia tego obowiązku wskazuje, iż istnieją obawy dotyczące wpływu takich przepisów na innowacyjność i postęp technologiczny. Przeciwnicy argumentują, że rygorystyczne wymagania mogą hamować rozwój nowych technologii i zniechęcać do eksperymentowania, co jest kluczowe dla rozwoju sztucznej inteligencji. Dodatkowo, zbyt restrykcyjne regulacje mogą skutkować znacznymi kosztami dla firm, zwłaszcza dla mniejszych przedsiębiorstw i startupów, które mogą mieć trudności z dostosowaniem się do finansowych i technicznych wymogów związanych z wdrażaniem zaawansowanych systemów bezpieczeństwa[622].

Debata na temat konieczności wprowadzenia obowiązkowych mechanizmów wyłączających dla systemów sztucznej inteligencji podkreśla istotę znalezienia równowagi między zapewnieniem bezpieczeństwa a zachowaniem ducha innowacyjności. Kluczowe jest zrozumienie, w jaki sposób te regulacje wpłyną na różnorodne zastosowania SI oraz jak efektywnie zharmonizować nowe przepisy prawne z dynamicznym tempem rozwoju technologicznego. W ostatecznym rozrachunku, każda forma regulacji powinna wspierać zarówno bezpieczeństwo, jak i zdrowy postęp innowacji w obszarze sztucznej inteligencji.

9.6.2.2 Aspekty technologiczne wyłączania systemów SI

Mechanizmy umożliwiające dezaktywację systemów sztucznej inteligencji, które mogą stanowić zagrożenie, łączą się z różnymi aspektami technologicznymi. Omawianie tej kwestii obejmuje zarówno korzyści, jak i negatywne konsekwencje ewentualnych regulacji prawnych w tej sferze.

---

621 Zisov N., Targov T., *Risks of Artificial Intelligence – Safety Aspects*, Chambers and Partners, https://chambers.com/articles/risks-of-artificial-intelligence-safety-aspects (dostęp: 10.06.2024 r.).

622 Holland & Knight, *What to Know About the New Artificial Intelligence Executive Order*, https://www.hklaw.com/en/insights/publications/2023/10/what-to-know-about-the-new-artificial-intelligence-executive-order (dostęp: 10.06.2024 r.).

Poparcie dla wprowadzenia obowiązku wdrożenia mechanizmów wyłączających wskazuje, iż z punktu widzenia bezpieczeństwa, istnieje uzasadnienie dla wprowadzenia takich zabezpieczeń ze względu na potencjalne ryzyko, jakie nieskrępowane systemy SI mogą stanowić dla społeczeństwa. Te mechanizmy, nazywane często „*wyłącznikiem awaryjnym*" (ang. kill switch), umożliwiają szybką reakcję w sytuacjach, gdy działanie SI przekracza ustalone parametry lub staje się niebezpieczne. Przykładowo, w przypadku autonomicznych pojazdów, utrata połączenia lub błędy w algorytmach mogą prowadzić do wypadków, dlatego możliwość natychmiastowego wyłączenia tych systemów jest kluczowa dla bezpieczeństwa publicznego[623].

Z drugiej strony, krytyka wprowadzenia tego obowiązku, wskazuje iż istnieją obawy dotyczące wpływu takich regulacji na innowacyjność oraz postęp technologiczny. Mechanizmy wygaszania mogą być postrzegane jako ograniczenie dla twórców sztucznej inteligencji, co potencjalnie może hamować rozwój tej dziedziny. Dodatkowo istnieje ryzyko nadużywania takich systemów, co może prowadzić do problemów związanych z kontrolą i cenzurą. Krytycy argumentują, że zbyt restrykcyjne podejście może tłumić innowacje oraz postęp technologiczny w obszarze sztucznej inteligencji[624].

Wprowadzenie mechanizmów umożliwiających wyłączenie systemów sztucznej inteligencji, które stanowią zagrożenie, to zagadnienie wymagające głębokiej analizy i zrozumienia zarówno technologicznych, jak i etycznych implikacji tego typu rozwiązań. Pomimo priorytetowego znaczenia bezpieczeństwa, istotne jest unikanie niepotrzebnego ograniczania przestrzeni dla innowacji. Konieczne są dalsze badania i debaty w celu znalezienia właściwej równowagi między tymi dwoma istotnymi celami.

9.6.2.3 Aspekty etyczne wyłączania systemów SI

Wprowadzenie środków umożliwiających dezaktywację systemów sztucznej inteligencji, które stanowią zagrożenie, stawia istotne pytania dotyczące etyki. Poparcie dla takich rozwiązań opiera się na argumentach związanych z koniecznością ochrony społeczności przed

[623] Zisov N., Targov T., *Risks of Artificial Intelligence – Safety Aspects*, Chambers and Partners, https://chambers.com/articles/risks-of-artificial-intelligence-safety-aspects (dostęp: 10.06.2024 r.).

[624] Holland & Knight, *What to Know About the New Artificial Intelligence Executive Order*, https://www.hklaw.com/en/insights/publications/2023/10/what-to-know-about-the-new-artificial-intelligence-executive-order (dostęp: 10.06.2024 r.).

potencjalnie niebezpiecznymi działaniami nieskrępowanych systemów SI. Mechanizmy, takie jak „*wyłącznik awaryjny*" (ang. kill switch), mogą być postrzegane jako narzędzie zapewniające bezpieczeństwo i kontrolę nad technologią, która w przeciwnym razie mogłaby działać w nieprzewidywalny sposób i tworzyć zagrożenia[625].

Jednakże, krytyka tego podejścia skupia się na obawach dotyczących potencjalnego nadużycia takich mechanizmów oraz ewentualnych ograniczeń dla innowacji. Istnieje obawa, że zbyt rygorystyczna kontrola może zahamować rozwój technologii i innowacji, szczególnie w dynamicznie rozwijającej się dziedzinie sztucznej inteligencji. Dodatkowo istnieje ryzyko, że nierozważne wdrożenie tych mechanizmów może prowadzić do nieetycznego wykorzystania oraz ograniczeń w dostępie do technologii[626].

W związku z tym, istotne wydaje się odnalezienie harmonii między troską o dobro społeczeństwa a umożliwieniem rozwoju technologicznego. Konieczne są dalsze dyskusje i badania, aby dobrze zrozumieć, jak najlepiej włączyć te mechanizmy w sposób moralny i efektywny.

[625] Rakowski R., Polak P., Kowalikova P., *Ethical Aspects of the Impact of AI: the Status of Humans in the Era of Artificial Intelligence*, Soc 58, s. 196–203, https://doi.org/10.1007/s12115-021-00586-8 (dostęp: 10.06.2024 r.).

[626] Chen Z., *Ethics and discrimination in artificial intelligence-enabled recruitment practices*, Humanit Soc Sci Commun 10, https://doi.org/10.1057/s41599-023-02079-x (dostęp: 10.06.2024 r.).

Podsumowanie i wnioski

1. Podsumowanie kluczowych wyników

W mojej dysertacji doktorskiej przeprowadziłam gruntowną analizę, badania nad wpływem sztucznej inteligencji na obszar prawa karnego. Skoncentrowałam się zarówno na teoretycznych, jak i praktycznych aspektach prawnych, technologicznych oraz etycznych związanych z dynamicznym rozwojem technologii SI. Poniżej zamieszczam kluczowe wnioski z mojej pracy:

1. definicja i klasyfikacja sztucznej inteligencji

   W badaniu określono i sklasyfikowano sztuczną inteligencję, co pozwoliło na wypracowanie klarownych ram pojęciowych. Identyfikacja różnorodnych form SI oraz ich technologicznych specyfikacji stanowi podstawę dla dalszych analiz prawnych i etycznych.

2. rola i odpowiedzialność twórcy SI

   Omówiono i przeanalizowano odpowiedzialność prawnokarną twórców systemów sztucznej inteligencji. Dyskusja wskazuje na konieczność wprowadzenia klarownych regulacji, które precyzyjnie określają obowiązki oraz odpowiedzialność osób projektujących i implementujących technologie oparte na sztucznej inteligencji, szczególnie w kontekście ryzyka i zapewnienia bezpieczeństwa.

3. przegląd regulacji prawnych

   Przejrzano obowiązujące i sugerowane przepisy prawne, zarówno na szczeblu krajowym, jak i międzynarodowym. Badanie to ujawniło braki w obecnych regulacjach oraz różnice w podejściach legislacyjnych, które powinny być rozwiązane w przyszłości, aby skuteczniej reagować na wyzwania związane z sztuczną inteligencją.

4. etyczne i filozoficzne implikacje

   Omówiono kwestie etyczne i filozoficzne dotyczące autonomii w podejmowaniu decyzji przez sztuczną inteligencję oraz ewentualnej samoświadomości. Te rozważania są istotne

dla zrozumienia, jak prawa i przepisy powinny reagować na postępy w technologii SI, uwzględniając jej możliwości i wpływ na społeczeństwo.

5. studia przypadków

   Przeprowadzono szczegółową analizę konkretnych przykładów wykorzystania sztucznej inteligencji w różnych branżach, co pozwoliło na praktyczne ukazanie wyzwań i możliwości związanych z wprowadzaniem tych technologii. Badania te pomagają w zrozumieniu realnych konsekwencji prawnych i etycznych związanych z funkcjonowaniem sztucznej inteligencji.

Podsumowując, moja praca doktorska przynosi pełną analizę, która wskazuje na pilną potrzebę dostosowania przepisów prawa karnego do nowoczesnych realiów technologicznych oraz dynamicznych zmian wynikających z rozwoju sztucznej inteligencji. Zaleca się regularne monitorowanie postępu technologicznego oraz aktualizację przepisów prawnych, co ma kluczowe znaczenie dla zapewnienia bezpieczeństwa i sprawiedliwości w erze cyfryzacji i automatyzacji.

2. Wnioski teoretyczne

Analiza teoretyczna przeprowadzona w ramach niniejszej rozprawy doktorskiej zapewnia głębsze spojrzenie na relacje między aspektami prawny, etycznym i technologicznym sztucznej inteligencji. Praca ta wyjaśnia, jak rozwój SI wpływa na obecne regulacje prawne oraz jakie teoretyczne podstawy są konieczne do zrozumienia i kształtowania przyszłości prawniczej w tej dynamicznie rozwijającej się dziedzinie. Poniżej prezentuję kluczowe wnioski teoretyczne wynikające z moich badań:

1. rozszerzenie definicji odpowiedzialności

   Klasyczne pojęcie odpowiedzialności prawnej musi być dostosowane do nowych wyzwań, jakie stawia sztuczna inteligencja. Sugeruję, by tą definicją powinna obejmować nie tylko bezpośrednich twórców i operatorów systemów SI, ale także osoby odpowiedzialne za ich utrzymanie i aktualizację. Taka ekspansja pomoże w zrozumieniu i regulowaniu złożoności interakcji między człowiekiem a autonomicznymi systemami.

2. nowe podejścia do odpowiedzialności na zasadzie ryzyka

   Proponuję teoretyczne fundamenty dla wprowadzenia modelu odpowiedzialności opartego na zasadzie ryzyka, który bardziej wiernie odzwierciedlałby wrodzone ryzyko związane z funkcjonowaniem systemów sztucznej inteligencji. Wnioski te wynikają z faktu, że systemy SI mogą wykazywać zachowania nieprzewidziane przez ich twórców, co wymaga prawnego rozpatrzenia ewentualnych szkód w sposób innowacyjny i przemyślany.

3. etyczne i prawne implikacje autonomii SI

   Praca podkreśla ważność łączenia norm etycznych z przepisami prawnymi w celu kierowania autonomicznymi decyzjami podejmowanymi przez systemy SI. Dyskusje teoretyczne na temat autonomii maszyn powinny prowadzić do stworzenia jasnych wytycznych, które będą pomocne przy tworzeniu odpowiednich ram prawnych.

4. wpływ technologicznego postępu na interpretacje prawne

   Postęp w dziedzinie technologii sprawia, że konieczna staje się ponowna ocena niektórych tradycyjnych koncepcji prawnych. Badanie podkreśla konieczność ciągłego aktualizowania literatury prawniczej i teorii w odpowiedzi na postęp technologiczny, aby prawo mogło skutecznie reagować na nowe wyzwania.

5. teoria odpowiedzialności zbiorowej

   Rozważałam także opcję rozszerzenia odpowiedzialności na podmioty zbiorowe, takie jak firmy i organizacje, które wdrażają technologie sztucznej inteligencji. Hipoteza teoretyczna sugeruje, że w przypadkach, gdy ustalenie indywidualnej odpowiedzialności jest problematyczne, odpowiedzialność zbiorowa może stanowić skuteczne narzędzie prawnicze.

Podsumowując, wnioski teoretyczne sugerują, że konieczne jest holistyczne podejście do ustalania przepisów dotyczących sztucznej inteligencji, które powinny uwzględniać zarówno dynamiczny rozwój technologiczny, złożoność etyczną, jak i praktyczne aspekty wdrożenia. Taki sposób postępowania zapewni solidne teoretyczne podstawy dla przyszłych regulacji, które będą mogły skutecznie odpowiedzieć na wyzwania wynikające z szybkiego rozwoju technologii informatycznych.

3. Praktyczne implikacje dla twórców i użytkowników SI

Badania i analizy przeprowadzone w trakcie realizacji tego doktoratu mają istotne konsekwencje dla osób projektujących oraz korzystających z systemów sztucznej inteligencji. Poniżej przedstawiam kluczowe praktyczne aspekty, które powinny zostać uwzględnione podczas tworzenia, wprowadzania oraz użytkowania tych technologii:

1. wzmocnienie protokołów bezpieczeństwa

   Twórcy sztucznej inteligencji powinni skoncentrować się na włączeniu zaawansowanych protokołów bezpieczeństwa i zasad etycznych już na etapie projektowania systemów – „*bezpieczeństwo i etyka od samego początku*" (ang. „security and ethics by design"). Taka praktyka nie tylko zmniejsza ryzyko nieprzewidywalnych działań SI, lecz także buduje zaufanie użytkowników do technologii. Twórcy powinni systematycznie aktualizować swoje systemy, aby spełniały najnowsze standardy bezpieczeństwa oraz przepisy prawne.

2. edukacja i świadomość

   Warto inwestować w programy edukacyjne dla twórców i użytkowników sztucznej inteligencji, które zwiększają świadomość na temat potencjalnych zagrożeń oraz najlepszych praktyk związanych ze sztuczną inteligencją. Edukacja powinna uwzględniać nie tylko aspekty techniczne, ale także etyczne i prawne, aby wszyscy byli świadomi swoich obowiązków i możliwych konsekwencji wynikających z wykorzystania sztucznej inteligencji.

3. transparentność działania systemów SI

   Twórcy systemów sztucznej inteligencji powinni starać się zapewnić pełną przejrzystość działania swoich produktów. To oznacza jasne informowanie użytkowników o sposobie przetwarzania danych, podejmowanych decyzjach przez system oraz zastosowanych środkach bezpieczeństwa. Przejrzystość ma kluczowe znaczenie dla budowania zaufania i umożliwienia użytkownikom łatwego zrozumienia i kontroli nad technologią.

4. implementacja mechanizmów odpowiedzialności

Wprowadzenie klarownych mechanizmów odpowiedzialności w przypadku błędów lub nadużyć jest niezbędne. Twórcy sztucznej inteligencji powinni być przygotowani na ewentualne awarie lub nieprzewidziane działania ich systemów i odpowiednio reagować, wprowadzając procedury, które umożliwią szybkie rozpoznanie i naprawę problemów.

5. zgodność z przepisami prawnymi

   Twórcy i użytkownicy sztucznej inteligencji powinni być świadomi obowiązujących przepisów prawnych dotyczących SI w różnych obszarach prawnych. Szczególnie istotne jest zwracanie uwagi na regulacje dotyczące prywatności, ochrony danych oraz odpowiedzialności, co wymaga bliskiej współpracy z prawnikami specjalizującymi się w prawie technologicznym.

6. przygotowanie na zmiany regulacyjne

   Sektor sztucznej inteligencji prężnie się rozwija i podlega ciągłym zmianom w obszarze regulacji. Osoby tworzące i korzystające z systemów SI powinny być gotowe do dostosowania się do nowych wymogów prawnych, co może wymagać elastyczności w projektowaniu systemów oraz aktywnego monitorowania zmian legislacyjnych.

Podsumowując, praktyczne konsekwencje wynikające z tej pracy mają na celu nie tylko zwiększenie bezpieczeństwa i efektywności systemów sztucznej inteligencji, ale także zapewnienie, że proces wdrożenia będzie prowadzony w sposób odpowiedzialny i zgodny z najwyższymi standardami etycznymi i prawnymi. Prawidłowe zarządzanie tymi kwestiami jest kluczowe dla długoterminowego powodzenia technologii sztucznej inteligencji oraz dla ochrony i promocji praw użytkowników.

4. Rekomendacje prawne

W kontekście rosnącego wpływu sztucznej inteligencji na różne obszary życia, istnieje pilna potrzeba dostosowania ram prawnych, które skutecznie regulowałyby działanie i wdrożenie tych zaawansowanych technologii. Poniżej przedstawiam zbiór sugestii prawnych mających na celu wsparcie ustawodawców, twórców SI oraz społeczeństwa w odpowiedzialnym korzystaniu z możliwości, jakie oferuje sztuczna inteligencja:

1. tworzenie dedykowanego ustawodawstwa dla SI:

- wprowadzenie specjalnych ustaw, które skupiałyby się na regulacjach dotyczących sztucznej inteligencji, obejmując aspekty odpowiedzialności, bezpieczeństwa, transparentności oraz etyczne wyzwania związane z SI;

- zdefiniowanie i regularne aktualizowanie definicji oraz kategorii sztucznej inteligencji, aby przepisy mogły być na bieżąco z dynamicznym rozwojem technologii.

2. ustanowienie jasnych zasad odpowiedzialności:

- wskazanie warunków, w jakich twórcy i dystrybutorzy systemów sztucznej inteligencji mogą ponosić odpowiedzialność prawną za działania swoich systemów.

- wprowadzenie zasady odpowiedzialności opartej na ryzyku, która uwzględniałaby szczególne cechy funkcjonowania autonomicznych systemów sztucznej inteligencji.

3. promowanie zasad bezpieczeństwa i etyki „*by design*"[627]:

- przed uruchomieniem nowych systemów sztucznej inteligencji, zaleca się wprowadzenie obowiązkowych audytów etycznych i oceny wpływu na prywatność (PIA);

- twórcy sztucznej inteligencji powinni być zobowiązani do uwzględnienia standardów bezpieczeństwa i etyki już na etapie projektowania produktów. W ramach tych standardów należy przewidzieć możliwość wyłączenia systemów SI, które zaczynają działać w sposób niezamierzony lub stanowią zagrożenie, poprzez zapewnienie mechanizmów „*kill switch*", umożliwiających szybkie i skuteczne wyłączenie systemu w przypadku wykrycia działania naruszającego prawa lub bezpieczeństwo użytkowników.

4. zasady odnoszące się do przejrzystości i zrozumiałości sztucznej inteligencji:

[627] "By design" oznacza podejście, w którym określone cechy lub funkcje produktu, usługi lub systemu są wbudowane w jego projekt od samego początku, zamiast być dodawane później. Koncepcja ta jest szczególnie istotna w kontekście ochrony prywatności i bezpieczeństwa danych, gdzie "privacy by design" odnosi się do uwzględniania kwestii prywatności na każdym etapie projektowania i rozwoju systemu. Patrz w: Cavoukian A., *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2009, s. 1-2.

- wprowadzenie obowiązkowe przez twórców systemów sztucznej inteligencji funkcji tłumaczenia decyzji podejmowanych przez ich systemy, co zwiększyłoby przejrzystość działania SI;

- dostarczenie użytkownikom informacji na temat sposobu funkcjonowania sztucznej inteligencji oraz potencjalnych uprzedzeniach zastosowanych w tych systemach.

5. Stworzenie mechanizmów monitorowania i nadzoru:

- utworzenie instytucji nadzorującej systemy sztucznej inteligencji, która miałaby zajmować się przyjmowaniem skarg, monitorowaniem przestrzegania regulacji oraz inicjowaniem śledztw w przypadku nadużyć. Taki podmiot powinien mieć również możliwość wymuszania wyłączenia systemów SI, które łamią przepisy prawa, stanowią zagrożenie dla bezpieczeństwa publicznego lub naruszają prawa obywatelskie;

- firmy wykorzystujące sztuczną inteligencję są zobowiązane do regularnego raportowania na temat funkcjonowania i wpływu swoich systemów na społeczeństwo.

6. wsparcie dla innowacji i rozwoju SI:

- utworzenie „*piaskownic*" (ang. „sandbox") regulacyjnych, które umożliwiłyby testowanie nowych technologii sztucznej inteligencji w kontrolowanych warunkach przed ich wprowadzeniem na rynek;

- wspieranie międzynarodowej współpracy w celu opracowania globalnych norm dotyczących sztucznej inteligencji, mających na celu zharmonizowanie przepisów i promowanie globalnej konkurencyjności.

Zalecenia te mają na celu nie tylko zapewnienie bezpieczeństwa i ochrony prawnej dla użytkowników i społeczeństwa, ale także tworzenie sprzyjających warunków dla dalszego rozwoju technologii sztucznej inteligencji. Wprowadzenie klarownych, przemyślanych i elastycznych regulacji prawnych jest kluczowe dla wykorzystania potencjału SI przy minimalizowaniu związanych z nią ryzyk.

5. Ograniczenia badań

Podczas pisania mojej rozprawy doktorskiej na temat prawnych aspektów technologii opartych na sztucznej inteligencji, natknęłam się na wiele problemów, które mogły wpłynąć na głębokość i zakres moich analiz. Warto zwrócić uwagę na kilka istotnych kwestii, które mogą stanowić przeszkody w pełnym zrozumieniu tematu oraz w formułowaniu ogólnych rekomendacji prawnych.

1. Dynamika rozwoju technologii SI

   Rozwój technologii sztucznej inteligencji cechuje niezwykła dynamika, co powoduje, że przepisy prawne mogą szybko tracić na aktualności. Szybkie tempo postępu technologicznego sprawia, że legislatorom trudno nadążyć za bieżącymi potrzebami regulacyjnymi, a badania naukowe mogą nie zdołać w pełni odzwierciedlić najnowszych trendów i praktyk stosowanych w rzeczywistości.

2. Zróżnicowanie jurysdykcji

   Różnice w podejściu do regulacji sztucznej inteligencji pomiędzy różnymi systemami prawnymi na całym świecie stwarzają wyzwanie przy formułowaniu globalnych zaleceń. Trudności wynikające z dysproporcji jurysdykcyjnych w interpretacji i stosowaniu prawa sprawiają, że tworzenie uniwersalnych rozwiązań prawnych, które byłyby skuteczne na szeroką skalę, jest utrudnione.

3. Interdyscyplinarność tematu

   Sztuczna inteligencja łączy wiele obszarów, takich jak informatyka, etyka i prawo. Złożoność technologiczna SI oraz jej interdyscyplinarny charakter wymagają głębszej wiedzy i współpracy między ekspertami z różnych dziedzin. Brak dostępu do specjalistycznej wiedzy lub jej niepełne zrozumienie może ograniczyć perspektywę badawczą.

4. Zmienność percepcji społecznej

   Sztuczna inteligencja wywołuje zróżnicowane reakcje w społeczeństwie, począwszy od entuzjazmu po obawy dotyczące kwestii etycznych i bezpieczeństwa. Postrzeganie

społeczne SI zmienia się z czasem, co może mieć wpływ na kierunki badań naukowych oraz rekomendacje prawne. To dynamiczne środowisko wymaga ciągłej analizy i dostosowywania podejść badawczych.

5. Dostęp do danych i ich prywatność

   Przeprowadzanie badań w obszarze sztucznej inteligencji często wymaga dostępu do obszernych zbiorów danych, co stawia pytania dotyczące ochrony prywatności i bezpieczeństwa informacji. Przepisy prawne regulujące ochronę danych osobowych mogą mieć wpływ na możliwości prowadzenia badań, ograniczając dostęp do informacji koniecznych do przeprowadzenia kompleksowej analizy.

6. Wpływ przesłanek komercyjnych

   Aspekty biznesowe związane z rozwojem i wdrażaniem technologii sztucznej inteligencji mogą wpływać na kierunki badań oraz ich obiektywność. Nacisk rynkowy i interesy ekonomiczne mogą ograniczać pełną i otwartą dyskusję na temat potencjalnych ryzyk czy niedoskonałości technologii SI.

Podsumowując, mimo tych ograniczeń, praca dostarcza istotnych spostrzeżeń na temat aspektów prawnych związanych ze sztuczną inteligencją, stanowiąc solidną podstawę do dalszych, bardziej szczegółowych badań w tej dynamicznie rozwijającej się dziedzinie. Wyraźne ograniczenia podkreślają potrzebę ciągłego monitorowania i dostosowywania regulacji prawnych w celu skutecznego zarządzania wyzwaniami wynikającymi z nowych technologii.

6. Sugestie do dalszych badań

Analiza prawnych aspektów technologii wykorzystujących sztuczną inteligencję, mimo że obszerna i szczegółowa, otwiera wiele możliwości dla przyszłych badań. Postęp technologiczny oraz dynamiczne zmiany w przepisach prawnych generują stałą potrzebę aktualizacji wiedzy i dostosowania prawa do nowych realiów. Poniżej przedstawiam kilka kluczowych obszarów, które zasługują na dalsze dogłębne badania:

1. Międzynarodowa harmonizacja przepisów

Mając na uwadze globalny charakter technologii oraz różnice w regulacjach krajowych, konieczne jest przeprowadzenie badań mających na celu ocenę możliwości i metod harmonizacji przepisów dotyczących sztucznej inteligencji. Prace badawcze mogłyby skoncentrować się na analizie najlepszych praktyk i strategii, które mogą przyczynić się do standaryzacji ram prawnych dotyczących działania sztucznej inteligencji na arenie międzynarodowej.

2. Etyczne aspekty sztucznej inteligencji

   Rozwój sztucznej inteligencji stwarza wiele kwestii etycznych, które wymagają ciągłego nadzoru i regulacji. Przyszłe badania mogłyby skoncentrować się na opracowaniu powszechnych zasad etycznych dla twórców i użytkowników systemów SI, które mogłyby być uzupełnieniem obowiązujących przepisów prawnych.

3. Technologiczne ograniczenia sztucznej inteligencji

   Badania nad technologicznymi ograniczeniami oraz zdolnościami autonomicznych systemów sztucznej inteligencji są istotne. Zrozumienie tych kwestii ma kluczowe znaczenie dla skutecznej regulacji prawnej, zwłaszcza w kontekście odpowiedzialności za działania systemów SI. Przyszłe badania mogą skupić się na ocenie ryzyka i przewidywalności zachowań autonomicznych systemów.

4. Przyszłość odpowiedzialności prawnej

   W obliczu wzrastającej autonomii systemów sztucznej inteligencji, istotne będzie zbadanie potencjalnych opcji wprowadzenia nowych form odpowiedzialności prawnej, które skuteczniej uwzględnią złożoność i specyfikę działania SI. Przyszłe badania mogą również rozważyć możliwość wprowadzenia przepisów dotyczących maszyn jako nowej kategorii podmiotu ponoszącego odpowiedzialność prawną w tym karną.

5. Skutki wprowadzenia regulacji

   Ważne jest zrealizowanie badań empirycznych dotyczących wpływu regulacji na postęp technologiczny oraz innowacyjność. Analiza tych informacji mogłaby pomóc w ocenie, czy obowiązujące przepisy sprzyjają czy hamują rozwój technologiczny, co ma kluczowe znaczenie dla tworzenia skutecznych i zrównoważonych polityk prawnych.

6. Interdyscyplinarne podejście do regulacji

   Sugeruje się przeprowadzenie badań, w których zaangażowani byliby eksperci z różnych dziedzin - prawnicy, inżynierowie, filozofowie, socjolodzy - aby wspólnie opracowywać kompleksowe rozwiązania regulacyjne. Taka współpraca mogłaby prowadzić do bardziej całościowego i efektywnego podejścia do wyzwań związanych ze sztuczną inteligencją.

Podsumowując, każda z wymienionych dziedzin stwarza szerokie możliwości dla przyszłych badań, które mogą istotnie przyczynić się do rozwoju prawnego oraz technologicznego kontekstu stosowania sztucznej inteligencji. Ważne jest kontynuowanie tych działań, aby zagwarantować bezpieczne i odpowiedzialne wykorzystanie tej innowacyjnej technologii w społeczeństwie.

Bibliografia

Piśmiennictwo

— Abbott R., *Building a More Nuanced Understanding of SI's Role in Patent Law*, "Berkeley Technology Law Journal" 2019.

— Abbott R., Sarch A. F., *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, "UC Davis Law Review" 2019, Vol. 53.

— Ajunwa I., Friedler S., Scheidegger C., Venkatasubramanian S., *Hiring by algorithm: Predicting and preventing disparate impact*, "SSRN Electronic Journal" 2016.

— Albanese J. S., *Transnational Crime and the 21st Century: Criminal Enterprise, Corruption, and Opportunity*, Oxford University Press 2011.

— Allen C., Wallach W., *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press 2011.

— Alpaydin E., *Introduction to Machine Learning*, MIT Press 2014.

— Arksey H., O'Malley L., *Scoping studies: towards a methodological framework*, "International Journal of Social Research Methodology" 2005, vol. 8, no. 1.

— Asaro P. M., *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making*, "International Review of the Red Cross "2012, Vol. 94, No. 886.

— Asaro P. M., *The Liability Problem for Autonomous Artificial Agents*," European Journal of Law and Technology" 2012, Vol. 3, No. 3.

— Asaro P., *SI and the Problem of Control*, "Philosophy & Technology" 2019.

— Ashley K. D., *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambridge University Press 2017.

— Balkin J. M., *The Three Laws of Robotics in the Age of Big Data*, “Ohio State Law Journal” 2017, Vol. 78.

— Barczak-Oplustil A., *Funkcjonalny model odpowiedzialności karnej według Günthera Jakobsa*, "Państwo i Prawo" 2017, nr 3.

— Barfield W., Pagallo U. (eds.), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing 2018.

— Barocas S., Selbst A. D., *Big data's disparate impact*, “California Law Review” 2016, vol. 104.

— Bernal P., *Data Privacy: Between Regulation and Rights*, Cambridge University Press 2021.

— Bieliński A., *Prawo wobec wyzwań sztucznej inteligencji - wybrane zagadnienia*, "Monitor Prawniczy" 2021, nr 16.

— Bishop C. M., *Pattern Recognition and Machine Learning*, Springer 2006

— Bogen M., Rieke A., *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Pew Research Center 2018.

— Bojarski T. (red.), *Kodeks karny. Komentarz*, LexisNexis 2016.

— Bostrom N., *Ethical Issues in Advanced Artificial Intelligence*, Cognitive, “Emotive and Ethical Aspects of Decision Making in Humans and in Artificial Intelligence” 2003, Vol. 2.

— Bostrom N., *Ethics of Artificial Intelligence and Robotics*, “Stanford Encyclopedia of Philosophy” 2020.

— Bostrom N., Müller Y., *Future Progress in Artificial Intelligence: A Survey of Expert Opinion*, “Journal of Artificial Intelligence Research” 2014.

— Bostrom N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press 2014.

— Bostrom N., Yudkowsky E., *The Ethics of Artificial Intelligence*, "The Cambridge Handbook of Artificial Intelligence" 2014, Cambridge University Press.

— Boyle J., *The Public Domain: Enclosing the Commons of the Mind*, Yale University Press 2008.

— Breiman L., *Random Forests*, "Machine Learning" 2001, Vol. 45, No. 1.

— Brenner S. W., *Cybercrime: Criminal Threats from Cyberspace*, "ABC-CLIO" 2010.

— Brenner S. W., *Law in an Era of "Smart" Technology*, Oxford University Press 2007.

— Bringsjord S., Noel R., Caporale C., *Animals, Zombanimals, and the Total Turing Test: The Essence of Artificial Intelligence*, Fellbaum K. (red.), "Netzwerke und Selbstorganisation in der Ethik", LIT Verlag, Münster 2000.

— Brkan M., Psychogiopoulou E., *The Future of Privacy Certification in Europe: An Exploration of the GDPR Provisions on Criteria and Procedures for Certification*, "European Journal of Law and Technology" 2018, Vol. 9, No. 1.

— Broadbent E., *Interactions with Robots: The Truths We Reveal about Ourselves*, "Annual Review of Psychology" 2017, Vol. 68.

— Brownsword R., Scotford E., Yeung K. (eds.), *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press 2017.

— Brynjolfsson E., McAfee A., *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company 2014.

— Bryson J. J., Diamantis M. E., Grant T. D., *Of, for, and by the people: the legal lacuna of synthetic persons*, "Artificial Intelligence and Law" 2017.

— Bryson J. J., *SI & Global Governance: No One Should Trust SI*, United Nations University Centre for Policy Research 2018.

— Bryson J., *Patiency Is Not a Virtue: The Design of Intelligent Systems and Systems of Ethics*, "Ethics and Information Technology" 2018, Vol. 20, No. 1.

— Buchanan B., Grant T., *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*, IGI Global 2018.

— Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, "Proceedings of Machine Learning Research" 2018, Vol. 81.

— Bygrave L. A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International 2002.

— Calo R., *Artificial Intelligence and the End of Open Society*, "Stanford Law Review" 2020, Vol. 72.

— Calo R., *Artificial Intelligence Policy: A Primer and Roadmap*, U.C. "Davis Law Review" 2017, Vol. 51.

— Calo R., *Robotics and the Lessons of Cyberlaw*, "California Law Review" 2015, Vol. 103.

— Casey B. et al., *Rethinking the Liability of Robots and AI*, "Emory Law Journal" 2015, Vol. 64.

— Casey B., Farhangi A., Vogl R., *Rethinking Explainable Machines: The GDPR's „Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, "Berkeley Technology Law Journal" 2019.

— Casey B., *Rethinking the Boundaries of 'Personal Data' in the Age of Intelligent Machines*, "Journal of Law, Technology, and Policy" 2021.

— Casey B., *Rethinking the Boundaries of Law in the Age of SI*, "Columbia Law Review" 2019, Vol. 119.

— Casey B., *The Impact of Artificial Intelligence on Rules, Standards, and Principles in Law*, "Harvard Journal of Law & Technology" 2018, Vol. 31, No. 2.

— Casey E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press 2011.

— Cath C. et al., *Artificial Intelligence and the "Good Society": the US, EU, and UK approach*," Science and Engineering Ethics" 2018, Vol. 24, No. 2.

— Cath C., *Governing artificial intelligence: ethical, legal and technical opportunities and challenges*, “Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences” 2018, Vol. 376, No. 2133.

— Chalmers D. J., *Facing Up to the Problem of Consciousness*, “Journal of Consciousness Studies” 1995, Vol. 2, No. 3.

— Chalmers D., *The Conscious Mind: In Search of a Fundamental Theory*, Oxford University Press, 1996.

— Chalmers D.J., *The Conscious Mind: In Search of a Fundamental Theory*, Oxford University Press 1996.

— Chella A., Manzotti R., *Artificial Consciousness*, Imprint Academic, Exeter 2007.

— Chella A., Manzotti R., *Artificial Consciousness: Theoretical and Practical Issues*, "Frontiers in Robotics and AI" 2020, Frontiers Media SA, vol. 7.

— Chesney R., Citron D., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, “California Law Review” 2018, Vol. 107.

— Chesney R., Citron D., *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*, F”oreign Affairs” 2019, Vol. 98, No. 1.

— Chesney R., Citron D.K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, "California Law Review" 2019, vol. 107, no. 6.

— Chiesa A., Ducci S., *Profiling the New Face of Cyber Criminals*, “Emerging Trends in ICT Security” 2007, Vol. 1.

— Choo K. K. R., *The Cyber Threat Landscape: Challenges and Future Research Directions*, “Computers & Security” 2011, Vol. 30, No. 8.

— Chynoweth P., *Legal research in the built environment: a methodological framework*, "International Journal of Law in the Built Environment" 2009, vol. 1, no. 1.

— Clarke R., Knake R. K., *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins 2010.

— Coeckelbergh M., *AI Ethics*, MIT Press 2020.

— Collins R. K. L. et al., *The Privacy Implications of Digital Voice Assistants: Alexa, Are You Listening?*, "American Business Law Journal" 2021, Vol. 58, No. 4.

— Crawford K., *AI Now Report*, AI Now Institute, New York University 2019.

— Crawford K., *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press 2021.

— Crevier D., *AI: The Tumultuous History of the Search for Artificial Intelligence*, Basic Books 1993.

— Danaher J., *The Threat of Algocracy: Reality, Resistance and Accommodation*, "Philosophy & Technology" 2016, Vol. 29, No. 3.

— De Vries I., *Legal implications of AI listening practices: A look into Google's data handling*, "AI & Law Journal" 2020, Vol. 28, No. 1.

— Dennett D. C., *Consciousness Explained*, Little, Brown and Co 1991.

— Dennett D. C., *Freedom Evolves*, Viking 2003.

— Dignum V., *Ethics in artificial intelligence: introduction to the special issue*, "Ethics and Information Technology" 2018, Vol. 20, No. 1.

— Dignum V., *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer "Nature" 2019.

— Ding J., *Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI*, "Future of Humanity Institute" 2018, University of Oxford.

— Dressel J., Farid H., *The accuracy, fairness, and limits of predicting recidivism*, "Science Advances" 2018.

— Dressler J., *Understanding Criminal Law*, Carolina Academic Press 2018.

— Dreyfus H. L., *What Computers Still Can't Do: A Critique of Artificial Reason*, MIT Press, 1992.

— Duff R.A., *Intention, Agency and Criminal Liability: Philosophy of Action and the Criminal Law*, Basil Blackwell 1990.

— Durkin J., *Expert Systems: Design and Development*, Macmillan Publishing Co 1994.

— Edwards L., *Law, Policy, and the AI Dilemma*, Routledge 2022.

— Edwards L., Veale M., *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, "Duke Law & Technology Review" 2017, Vol. 16.

— Elish M. C., Boyd D., *Situating methods in the magic of Big Data and AI*, "Communication Monographs" 2017, Vol. 84, No. 1.

— Fagan C., Newman A., *AI and Cybersecurity: Opportunities and Challenges*, "International Journal of Cybersecurity Intelligence & Cybercrime" 2021, Vol. 4, No. 1.

— Ferguson A. G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, NYU Press 2017.

— Floridi L., Cowls J., *A Unified Framework of Five Principles for AI in Society*, "Harvard Data Science Review" 2019.

— Foley S., Karlsen J. R., Putniņš T. J., *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?*, "The Review of Financial Studies" 2019, Vol. 32, No. 5.

— Ford H., *Moje życie i dzieło*, Wydawnictwo Naukowe PWN 2022.

— Gallagher S., Zahavi D., *The Phenomenological Mind*, 2nd ed., London: Routledge 2012.

— Gallagher S., Zahavi D., *The Phenomenological Mind: An Introduction to Philosophy of Mind and Cognitive Science*, Routledge 2008.

— Gardocki L., *Prawo karne*, C.H. Beck 2019.

— Garvie C., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, "Georgetown Law Center on Privacy & Technology" 2016.

— Gavaghan C., *Defining the Challenge for 21st Century NZ: Robots and the Law*, New Zealand Law Foundation 2016.

— Gebru T., *Datasheets for Datasets*, "Communications of the ACM" 2021, Vol. 64, No. 12., 2021.

— Gercke M., *Understanding Cybercrime: A Guide for Developing Countries*, ITU, 2012.

— Gerke S., Minssen T., Cohen G., *Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare*, "Artificial Intelligence in Healthcare" 2020.

— Giarratano J., Riley G., *Expert Systems: Principles and Programming*, PWS Publishing Co.1998.

— Giezek J. (red.), *Kodeks karny. Część ogólna. Komentarz*, Wolters Kluwer 2021.

— Gillespie T., *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press 2018.

— Gless S., Silverman E., Weigend T., *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, "New Criminal Law Review" 2016, vol. 19, no. 3.

— Goertzel B., Pennachin C. (Eds.), *Artificial General Intelligence*, Springer 2007.

— Goldsmith J., Wu T., *Cybercrime: Digital Cops in a Networked Environment*, NYU Press, 2006.

— Gonzalez R. C., *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificially Intelligent'?*, "Computer Law & Security Review" 2018, Vol. 34, No. 2.

— Goodall N. J., *Can you program ethics into a self-driving car?*, "IEEE Spectrum" 2016, Vol. 53, No. 6.

— Goodall N.J., *Machine ethics and automated vehicles*, w: *Road Vehicle Automation*, red. Gereon Meyer, Springer 2014.

— Goodfellow I., Bengio Y., Courville A., Bengio Y., *Deep Learning*, Vol. 1, MIT Press Cambridge 2016.

— Goodison S. E., Davis R. C., Jackson B. A., *Digital Evidence and the U.S. Criminal Justice System*, RAND Corporation 2015.

— Goodman B., Flaxman S., *European Union regulations on algorithmic decision-making and a "right to explanation"*, "AI Magazine" 2017, Vol. 38, No. 3.

— Goodman M., Brenner S. W., *The Emerging Consensus on Criminal Conduct in Cyberspace*, "International Journal of Law and Information Technology" 2002, Vol. 10, No. 2.

— Goodman M., *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*, Doubleday 2015.

— Goodman R., *A guide to the ethics of autonomous cars*, "Ethics and Information Technology" 2016, Vol. 18, No. 3.

— Grabosky P., *Cybercrime*, "Oxford Handbook of Crime and Public Policy" 2011, Oxford University Press.

— Grabosky P., *Virtual Criminals: Old Wine in New Bottles?*, "Social & Legal Studies" 2001, Vol. 10, No. 2.

— Greenwood D., *Incident Response in the Age of Cloud*, "Data Protection Leader" 2021.

— Gruszecka D., *Ochrona dobra prawnego na przedpolu jego naruszenia. Analiza karnistyczna*, Wolters Kluwer 2012.

— Grześkowiak A., Wiak K. (red.), *Kodeks karny. Komentarz*, C.H. Beck 2019.

— Gunkel D. J., *The Machine Question: Critical Perspectives on AI, Robots, and Ethics*, MIT Press 2012.

— Hagendorff T., *The ethics of AI ethics: An evaluation of guidelines*, "Minds and Machines" 2020, Vol. 30.

— Hallevy G., *Liability for Crimes Involving Artificial Intelligence Systems*, Springer International Publishing 2015.

— Hallevy G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, "Akron Intellectual Property Journal" 2010, Vol. 4, No. 2.

— Hallevy G., *When Robots Kill: Artificial Intelligence under Criminal Law*, Northeastern University Press 2013.

— Hallevy G., *Liability for Crimes Involving Artificial Intelligence Systems*, "Journal of Criminal Law and Criminology" 2011, Vol. 101, No. 2.

— Harari Y. N., *Homo Deus: A Brief History of Tomorrow*, Harper 2017.

— Hart H.L.A., *Punishment and Responsibility: Essays in the Philosophy of Law*, Oxford University Press 1968, s. 136-157.

— Hildebrandt M., *Law for Computer Scientists and Other Folk*, Oxford University Press 2020.

— Hildebrandt M., *The new laws of robotics: Defending human expertise in the age of AI*, Harvard University Press 2016.

— Hildt E., *Artificial Intelligence: Does Consciousness Matter?*, "Frontiers in Psychology" 2019, vol. 10.

— Hinton G. E., Sejnowski T. J., *Unsupervised Learning: Foundations of Neural Computation*, MIT Press 1999.

— Hirschberg J., Manning C. D., *Advances in natural language processing*, "Science" 2015, Vol. 349, No. 6245,.

— Holt T. J., Bossler A. M., Seigfried-Spellar K. C., *Cybercrime and Digital Forensics: An Introduction*, Routledge 2014.

— Infocomm Media Development Authority (IMDA), *Model Governance Framework for Artificial Intelligence in Singapore*, 2nd ed., Infocomm Media Development Authority, Singapore 2020.

— Jakobs G., *Strafrecht, Allgemeiner Teil: die Grundlagen und die Zurechnungslehre*, Walter de Gruyter 1991.

— Jobin A. et al., *The global landscape of AI ethics guidelines*, "Nature Machine Intelligence" 2019, Vol. 1, No. 9.

— Johnson L., *Risk Management in Software Development and Software Engineering Projects*, "TechWorld Association" 2019.

— Jurafsky D., Martin J. H., *Speech and Language Processing*, Cambridge University Press, 2019.

— Kahn J. P., *Amazon Echo and the Hot Tub Mishap: Case Study on Privacy in Connected Homes*, "Technology & Ethics" 2016, Vol. 8, No. 1.

— Kamarinou D., Millard C., Singh J., *Machine learning with personal data*, Queen Mary School of Law Legal Studies 2016.

— Kaplan A., *Where Does Artificial Intelligence Stand?*, Proceedings of the International Conference on Artificial Intelligence 2016.

— Kardas P., *Sprawstwo kumulatywne - alternatywna postać współdziałania przestępnego*, „Przegląd Prawa Karnego" 2020, nr 2.

— Kardas P., *Sprawstwo pojedyncze i sprawstwo współdziałające - zagadnienia konstrukcyjne i konsekwencje praktyczne*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2004, z. 1.

— Karnow C. E. A., *Liability for Distributed Artificial Intelligences*, "Berkeley Technology Law Journal", 1966 Vol. 11, No. 1.

— Katz D. M., Bommarito M. J. II, Blackman J., *A General Approach for Predicting the Behavior of the Supreme Court of the United States*, PLOS ONE 2017.

— Kerr Ian R., Bornfreund Matthew, *Algorithms and Autonomy: The Ethics of Automated Decision Systems*, Cambridge University Press 2020.

— Kerr Ian R., *The Implications of Autonomous Robots*, "San Diego Law Review" 2017.

— Kerr O. S., *Computer Crime Law* (5th ed.), West Academic Publishing 2021.

— Kerr O. S., *Search Warrants in an Era of Digital Evidence*, "Mississippi Law Journal" 2005, Vol. 75.

— Kim P., *Auditing Algorithms for Discrimination*, "Harvard Law Review" 2017.

— Kochanowski J., *Przestępstwa i wykroczenia przeciwko życiu i zdrowiu*, [w:] Bafia J., Mioduski K., Siewierski M. (red.), *Kodeks karny. Komentarz*, Wydawnictwo Prawnicze 1987.

— Kołecki H., *Dowody elektroniczne - przepisy i standardy*, "Prokuratura i Prawo" 2013, nr 6.

— Koops B.-J., *The Trouble with European Data Protection Law*, "International Data Privacy Law" 2014, Vol. 4, No. 4.

— Kosiński J., *Sztuczna inteligencja i jej prawne aspekty*, "Studia Prawnicze" 2019, nr 3.

— Królikowski M., Zawłocki R. (red.), *Kodeks karny. Część ogólna*. *Tom I. Komentarz do art. 1-31*, C.H. Beck 2017.

— Kurzweil R., *The Singularity Is Near: When Humans Transcend Biology*, Viking 2005.

— Kuzior P., *Kumulatywne i konkurencyjne sprawstwo w polskim prawie karnym*, "Prokuratura i Prawo" 2016.

— Lachowski J. (red.). *System Prawa Karnego. Tom 4. Nauka o przestępstwie. Wyłączenie i ograniczenie odpowiedzialności karnej*. C.H. Beck 2016.

— Lacity M. C., Willcocks L. P., *Robotic Process Automation and Risk Mitigation: The Definitive Guide*, SB Publishing 2016.

— LeCun Y., Bengio Y., Hinton G., *Deep learning*, "Nature" 2015, Vol. 521, No. 7553.

— Lee K., *AI Superpowers: China, Silicon Valley, and the New World Order*, "Houghton Mifflin Harcourt" 2018.

— Legg S., Hutter M., *A Collection of Definitions of Intelligence*, "Frontiers in Artificial Intelligence and Applications" 2007, Vol. 157.

— Lemley M., *The Role of AI in the Criminal Justice System*, "Stanford Law Review" 2019, Vol. 61.

— Lessig L., *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, Penguin 2004.

— Levac D., Colquhoun H., O'Brien K.K., *Scoping studies: advancing the methodology*, "Implementation Science" 2010, vol. 5, no. 69.

— Levy S., *Hackers: Heroes of the Computer Revolution*, Doubleday 1984.

— Liao S. H., *Expert system methodologies and applications – a decade review from 1995 to 2004*, "Expert Systems with Applications" 2005, Vol. 28, No. 1.

— Litman J., *Digital Copyright*, Prometheus Books 2001.

— Luger G. F., Stubblefield W. A., *Artificial Intelligence: Structures and Strategies for Complex Problem Solving*, Pearson/Addison-Wesley 2004.

— Lynskey O., *The Foundations of EU Data Protection Law*, Oxford University Press 2017.

— Lynskey T., *Regulating 'Big Tech': Legal Implications and Protection Mechanisms for Personal Data in the Era of Massive Data Collection and Surveillance*, "European Law Review" 2020, Vol. 45, No. 6.

— Lyon D., *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination*, Routledge 2003.

— Manyika J. et al., *A New Look at Data Privacy: Addressing the Challenges of the Digital Age*, McKinsey Global Institute 2020.

— Marchant G. E., Lindor R. A., *The Coming Collision Between Autonomous Vehicles and the Liability System*, "Santa Clara Law Review" 2015, Vol. 55, No. 4.

— Marchuk I., *The Fundamental Concept of Crime in International Criminal Law: A Comparative Law Analysis*, Springer 2014, s. 117-119.

— Marek A., *Prawo karne*, C.H. Beck 2011.

— Matthias Andreas, *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata*, "Ethics and Information Technology" 2004.

— Maurer M., Gerdes J. C., Lenz B., Winner H. (Eds.), *Autonomous Driving: Technical, Legal and Social Aspects*, Springer 2016.

— McCarthy J., Minsky M. L., Rochester N., Shannon C. E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955*, "AI Magazine" 2006, Vol. 27, No. 4.

— McCorduck P., *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence*, A K Peters/CRC Press 2004.

— McNeal G. S., *Children's Consumer Privacy and the Internet of Things: Regulating the Playground of Disruption*, "Loyola Law Review" 2017, Vol. 67, No. 2.

— McTear M., Callejas Z., Griol D., *The Conversational Interface: Talking to Smart Devices*, Springer 2016.

— Metzinger T., *Being No One: The Self-Model Theory of Subjectivity*, MIT Press 2003.

— Miller R., *Collaborative Cybersecurity: Building Effective Alliances in a Fragmented Environment*, Strategic Forum 2017.

— Mittelstadt B., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, "Big Data & Society" 2016.

— Morin A., *Self-Awareness Part 1: Definition, Measures, Effects, Functions, and Antecedents*, "Social and Personality Psychology Compass" 2011, vol. 5, no. 10.

— Morse S. J., *New Neuroscience, Old Problems*, in *Neuroethics: Mapping the Field*, Dana Press 2002

— Murphy K. P., *Machine Learning: A Probabilistic Perspective*, MIT Press 2012.

— Neisser U., *Five Kinds of Self-Knowledge*, "Philosophical Psychology" 1988, vol. 1, no. 1.

— Ng A., *Deep Learning*, “DeepLearning.AI” 2021.

— Nof S. Y. (Ed.), *Handbook of Industrial Robotics*, Wiley 1999.

— O'Neil C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown 2016.

— Pagallo U., *AI and the law: A legal perspective*, in *The Oxford Handbook of Ethics of AI*, Oxford University Press 2018.

— Pagallo U., *The Laws of Robots: Crimes, Contracts, and Torts*, Springer 2013.

— Pan S. J., Yang Q., *A Survey on Transfer Learning*, “IEEE Transactions on Knowledge and Data Engineering” 2010, Vol. 22, No. 10.

— Papernot N., McDaniel P., Goodfellow I., Jha S., Celik Z. B., Swami A., *Practical black-box attacks against machine learning*, “Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security” 2018.

— Parisi F., *Legal Challenges of Deepfake Technology*, “European Journal of Law and Technology” 2020, Vol. 11, No. 1.

— Parisi F., *Legal Responses to Deepfakes: How New EU and US Initiatives Could Set the Global Standard*, “Computer Law & Security Review” 2020, Vol. 36.

— Pasquale F., *The Black Box Society*, Harvard University Press 2015.

— Perry W. L., McInnis B., Price C. C., Smith S. C., Hollywood J. S., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation 2013.

— Persily N., *The 2016 U.S. Election: Can Democracy Survive the Internet?*, “Journal of Democracy” 2017, Vol. 28, No. 2.

— Pfleeger C. P., Pfleeger S. L., *Security in Computing*, Prentice Hall 2006.

— Pietrzykowski T., *Odpowiedzialność za sztuczną inteligencję - wyzwania dla prawa cywilnego i karnego*, "Przegląd Prawniczy Uniwersytetu Warszawskiego" 2021, vol. 20, nr 1.

— Pohl Ł. *Prawo karne. Wykład części ogólnej*. Wolters Kluwer 2019.

— Poole D., Mackworth A., Goebel R., *Computational Intelligence: A Logical Approach*, Oxford University Press 1998.

— Powel A., *Privacy concerns in the rise of smart assistants*, "Journal of Data Protection & Privacy" 2019, Vol. 3, No. 2.

— Price W. N. II, *Artificial Intelligence in Health Care: Applications and Legal Implications*, "The SciTech Lawyer" 2017, Vol. 13, No. 4.

— Rahwan I., *Society-in-the-loop: programming the algorithmic social contract*, "Ethics and Information Technology" 2018, Vol. 20, No. 1.

— Riskin J., *The Defecating Duck, Or, the Ambiguous Origins of Artificial Life*, "Critical Inquiry" 2003, Vol. 29, No. 4.

— Rizzolatti G., Sinigaglia C., *The functional role of the parieto-frontal mirror circuit: interpretations and misinterpretations*, "Nature Reviews Neuroscience" 2010, Vol. 11, No. 4.

— Roberts H., Cowls J., Morley J., Taddeo M., Wang V., Floridi L., *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*, "AI & Society" 2021, vol. 36.

— Rosen J., Hannaford B., Satava R. M., *Surgical Robotics: Systems Applications and Visions*, Springer 2019.

— Rosenblatt B., *Digital Rights Management: Business and Technology*, M&T Books 2005.

— Roxin C., *Strafrecht. Allgemeiner Teil. Band I. Grundlagen. Der Aufbau der Verbrechenslehre*, C.H. Beck 2006, s. 237-241.

— Russell S., Dewey D., Tegmark M., *Research Priorities for Robust and Beneficial Artificial Intelligence*, "AI Magazine" 2015, Vol. 36, No. 4.

— Russell S., *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking 2019.

— Russell S., Norvig P., *Artificial Intelligence: A Modern Approach*, Pearson 2016.

— Ryan M., Stahl B. C., *Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications*, "Journal of Information, Communication and Ethics in Society" 2020.

— Sánchez-Monedero J., Dencik L., Edwards L., *What does the Robot Think? Transparency as a Fundamental Design Requirement for Intelligent Systems*, in: "Proceedings of ICSIL" 2017.

— Sartor G., *AI as a Legal Actor*, in: *Artificial Intelligence and Law*, Oxford University Press 2020.

— Scharre P., *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton & Company 2018.

— Schellekens M., *To regulate or not to regulate? The European Parliament's proposal to grant legal status to robots*, "Computer Law & Security Review" 2015.

— Scherer M. U., *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, "Harvard Journal of Law & Technology" 2016, Vol. 29, No. 2.

— Schneier B., *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W.W. Norton & Company 2018.

— Schneier B., *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company 2015.

— Searle J. R., *Minds, Brains, and Programs*, "Behavioral and Brain Sciences" 1980, Vol. 3, No. 3.

— Searle J.R., *Minds, Brains, and Programs*, "Behavioral and Brain Sciences" 1980, vol. 3, no. 3.

— Selwyn N., *Should Robots Replace Teachers?*, Polity Press 2019.

— Sifferd K.L., *Consciousness and Criminal Responsibility*, "Jurisprudence" 2019, vol. 10, no. 3.

— Smith A., *The Curious Case of the Dollhouse That Ordered Itself*, "AI & Society" 2016, Vol. 32, No. 4.

— Smith B. W., *Automated Vehicles Are Probably Legal in the United States*, "Texas A&M Law Review 2012.

— Smith J., *Cybersecurity: Best Practices and Strategies for the Modern World*, CyberTech Publishing 2018.

— Solove D., *Understanding Privacy*, Harvard University Press, Cambridge, MA, 2008.

— Solum Lawrence B., *Legal Personhood for Artificial Intelligences*, "North Carolina Law Review" 1992.

— Sourdin T., *Judge v Robot? Artificial Intelligence and Judicial Decision-Making*, "UNSW Law Journal" 2018, Vol. 41, No. 4.

— Sourgens F. G., *Artificial Intelligence in the Courtroom: The Significance of OpenAI's GPT-3 for the Legal Profession*, "Journal of Legal Education" 2020, Vol. 69, No. 1.

— Sparrow R., *Killer robots*, "Journal of Applied Philosophy" 2007, Vol. 24, No. 1.

— Sparrow RobertR., *Robots and Responsibility from a Legal Perspective*, "Proceedings of the IEEE" 2007.

— Stahl Bernd B., CarstenC., *Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency*, "Ethics and Information Technology" 2006.

— Stallings W., Brown L., *Computer Security: Principles and Practice*, Pearson 2015.

— Starr S. B., *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, "Stanford Law Review" 2014, Vol. 66.

— State Council of the People's Republic of China, *New Generation Artificial Intelligence Development Plan* 2017.

— Stefański R.A. (red.), *Kodeks karny. Komentarz*, C.H. Beck 2018.

— Surden H., *Artificial Intelligence and Law: An Overview*, "Georgia State University Law Review" 2019, Vol. 35, No. 4.

— Susskind R., Susskind D., *The Future of the Professions: How Technology Will Transform the Work of Human Experts*, Oxford University Press 2015.

— Suter T., Hugenholtz P. B., *Copyright and Digital Rights Management*, in *Handbook on the Economics of Copyright: A Guide for Students and Teachers*, Edward Elgar Publishing 2005.

— Sutton R. S., Barto A. G., *Reinforcement Learning: An Introduction*, MIT Press 2018.

— Svantesson D. J. B., Clarke R., *Privacy and consumer risks in cloud computing*, "Computer Law & Security Review" 2010, Vol. 26, No. 4.

— Taddeo M., Floridi L., *Regulate artificial intelligence to avert cyber arms race*, "Nature" 2018, Vol. 556, No. 7701.

— Tavani H. T., Grodzinsky F. S., *Cyberstalking, Personal Privacy, and Moral Responsibility*, "Ethics and Information Technology" 2002, Vol. 4, No. 2.

— Taylor E., Lee M., Willis M., Gannoni A., *Real-time monitoring of offenders: The high-tech future of crime prevention?*, "Trends & Issues in Crime and Criminal Justice" 2017, No. 532.

— Taylor H., *Building a Culture of Cybersecurity Awareness*, InfoSec Institute 2020.

— Terry N. P., *Liability for Mobile Health and Wearable Technologies*, A"nnals of Health Law" 2016, Vol. 25.

— Tkacz S., *Robotyka i autonomizacja - wpływ na rozwój technologiczny*, Knosala R. (red.), „Innowacje w zarządzaniu i inżynierii produkcji" 2018, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, t.1.

— Turing A. M., *Computing Machinery and Intelligence*, "Mind" 1950, Vol. 59, No. 236.

— Turner J., *Robot Rules: Regulating Artificial Intelligence*, Palgrave Macmillan, 2019.

— Vapnik V., *The Nature of Statistical Learning Theory*, Springer 1995.

— Vincent C., Bengio Y., *Evolutionary Architectures for Learning to Learn*, in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2019.

— Vincent J., *Ethical Dimensions of AI*, in Proceedings of the International Conference on Ethics and AI 2019.

— Vincent J., *Ethics in the Age of Artificial Intelligence*, Oxford University Press 2019.

— Vladeck D. C., *Machines Without Principals: Liability Rules and Artificial Intelligence*, "Washington Law Review" 2014.

— Volonino L., Anzaldua R., Godwin J., *Computer Forensics: Principles and Practices*, Pearson 2014.

— VRT NWS, *How we got to listen to Google Assistant recordings*, VRT NWS 2019.

— Wachter S., Mittelstadt B., *A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI*, "Columbia Business Law Review" 2019.

— Wall D. S., *Cybercrime: The Transformation of Crime in the Information Age*, "Polity" 2007.

— Weber R. H., *Internet of Things – New security and privacy challenges*, "Computer Law & Security Review" 2010, Vol. 26, No. 1.

— Weizenbaum J., *ELIZA—a computer program for the study of natural language communication between man and machine*, "Communications of the ACM" 1966, Vol. 9, No. 1.

— Weller A., *Challenges for Transparency and Accountability in Machine Learning*, "Nature Machine Intelligence" 2019, Vol. 1.

— Welzel H., *Das Deutsche Strafrecht. Eine systematische Darstellung*, Walter de Gruyter & Co. 1969.

— Westerlund M., *The Emergence of Deepfake Technology: A Review*, "Technology Innovation Management Review" 2020, Vol. 10, No. 11.

— Wiak K. (red.). *Prawo karne*. C.H. Beck 2021.

— Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Znak 2014.

— Wróbel, W., Zoll, A. (red.). *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-52*. Wolters Kluwer 2016.

— Yang X. S., *Nature-Inspired Metaheuristic Algorithms*, Luniver Press 2010.

— Yeung K., *Algorithmic regulation: A critical interrogation*, "Regulation & Governance" 2017, Vol. 12, No. 4.

— Zarsky T. Z., *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making*, Science, "Technology, & Human Values" 2016.

— Zarsky T. Z., *Understanding Privacy and Data Protection: What You Need to Know*, "Recode" 2019.

— Zittrain J., *The Future of the Internet and How to Stop It*, Yale University Press, "New Haven" 2008.

— Zoll A. (red.), *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-52*, Wolters Kluwer Polska, 2016.

— Zuboff S., *The Age of Surveillance Capitalism*, PublicAffairs 2019.

Akty prawne

— Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2023 r. poz. 1610 z późn. zm.).

— Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2024 r. poz. 17 z późn. zm.)

Dokumenty prawa ponadnarodowego

— Ustawa o Przestępczości Komputerowej Stanów Zjednoczonych z dnia 29 października 1986 r. w sprawie zwalczania przestępstw komputerowych oraz ochrony systemów informatycznych (Computer Fraud and Abuse Act, 18 U.S.C. § 1030).

— Koenig F., Schmidt P., Friemel C., Riche N. H., Kahn T., Lalmas M., Waldvogel D., *Zagadnienia etyczne i prawne związane z asystentami głosowymi dla dzieci*, "Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services"*2018,* ACM.

— California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (dostęp 10.06.2024 r.).

— Rozporządzenie Wykonawcze Prezydenta USA z dnia 30 października 2023 r. w sprawie bezpiecznego, pewnego i godnego zaufania rozwoju oraz użycia sztucznej inteligencji, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (dostęp 10.06.2024 r.)

— Rada Europy, Konwencja o cyberprzestępczości, Budapeszt, European Treaty Series - Nr 185, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

— Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119/1 z 4.05.2016, s. 1).

— Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informacyjnych w Unii, 2016 (Dz.U. L 194 z 19.7.2016).

— Komisja Europejska, *Artificial Intelligence Act*, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

Wykaz orzeczeń, oświadczeń i decyzji

— California Legislative Information, *AB-730 Elections: deceptive audio or visual media*, 2019.

— EEOC, DOJ, FTC, & CFPB, *Joint Statement on Artificial Intelligence and Algorithmic Bias*, Federal Trade Commission, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf (dostęp 10.06.2024 r.).

Netografia

— AI-Regulation, *Ethical Framework, Civil Liability and Intellectual Property Rights for AI*, 2020, https://www.ai-regulation.com/.

— Allen, N., Barrett, M. N., Millendorf, S. M., Moore, S., & Zhang, R. R. , Highlights From the Biden Administration Executive Order on AI, Foley & Lardner LLP, https://www.foley.com/insights/publications/2023/11/highlights-biden-administration-executive-order-ai/.

— American Civil Liberties Union, *After Third Wrongful Arrest*, *ACLU Slams Detroit Police Department for Continuing to Use Faulty Facial Recognition Technology*, https://www.aclu.org/press-releases/after-third-wrongful-arrest-aclu-slams-detroit-police-department-for-continuing-to-use-faulty-facial-recognition-technology.

— Angwin, J., Larson, J., Mattu, S., Kirchner, L., *Machine Bias*, ProPublica, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

— Art. 29 Grupa Robocza ds. Ochrony Danych, *Wytyczne w sprawie przejrzystości na mocy rozporządzenia 2016/679*, https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf&ved=2ahUKEwjB-sDijdGGAxW8KRAIHWRMBu4QFnoECBUQAQ&usg=AOvVaw3THJIYxE3qtBg7knfbycpt.

— Bellon T., *Liability and Legal Questions Follow Uber Autonomous Car Fatal Accident*, Insurance Journal, https://www.insurancejournal.com/news/national/2018/03/20/483981.htm.

— Bocetta S., *Has an Ai Cyber Attack Happened Yet?* InfoQ, https://www.infoq.com/articles/ai-cyber-attacks/.

— Bonnington C., *NHTSA Finds Tesla Not at Fault in 2016 Autopilot Crash*, Daily Dot, https://www.dailydot.com/debug/nets-results-tesla-autopilot-crash-investigation/.

— Brown A., *Tesla Autopilot Crash Victim Joshua Brown Was an Electric Car Buff and a Navy SEAL,* The Drive, https://www.thedrive.com/news/4249/tesla-autopilot-crash-victim-joshua-brown-was-an-electric-car-buff-and-a-navy-seal.

— Bryson J. J., *Robots should be slaves*, red. Y. Wilks, in: *Close Engagements with Artificial Companions: Key Social, Psychological, Ethical and Design Issues*, John Benjamins Publishing Company, Vol. 8, s. 63-74, https://doi.org/10.1075/nlp.8.11bry.

— Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

— Cadwalladr C., Graham-Harrison E., *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

— Capgemini Research Institute, *Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security*, https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf.

— Capgemini, *AI for Justice – bringing data into the courtroom*, https://www.capgemini.com/insights/expert-perspectives/ai-for-justice-bringing-data-into-the-courtroom/.

— Cavoukian A., *Privacy by Performance: The 7 Foundational Principles*, https://www.datatilsynet.no/globalassets/global/english/7foundationalprinciples_anncavoukian2.pdf.

— Chen Z., *Ethics and discrimination in artificial intelligence-enabled recruitment practices*, Humanit Soc Sci Commun 10, https://doi.org/10.1057/s41599-023-02079-x.

— Church P., *AI & the GDPR: Regulating the minds of machines, Linklaters,* https://www.linklaters.com/en/insights/blogs/digilinks/ai-and-the-gdpr-regulating-the-minds-of-machines.

— Da Silva M., Horsley T., Singh D., Da Silva E., Ly V., Thomas B., Daniel R.C., Chagal-Feferkorn K.A., Iantomasi S., White K., Kent A., Flood C.M., *Legal concerns in health-related artificial intelligence: a scoping review protocol*, Systematic Reviews, Vol. 11, No. 123, https://doi.org/10.1186/s13643-022-01939-y.

— Dastin J., *Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters, https://www.reuters.com/article/idUSKCN1MK0AG/.

— Dastin, J., Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/.

— *Death of Elaine Herzberg*, Wikipedia, https://en.wikipedia.org/wiki/Death_of_Elaine_Herzberg.

— EEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent*

Systems, First Edition, IEEE, https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html.

— European Commission, *AI Liability Directive*, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en.

— European Commission, *Coordinated Plan on Artificial Intelligence*, https://digital-strategy.ec.europa.eu/en/policies/plan-ai.

— European Commission, *Ethics Guidelines for Trustworthy AI*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

— European Commission, *Ethics guidelines for trustworthy AI*, High-Level Expert Group on Artificial Intelligence, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

— European Commission, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064.

— European Commission, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

— European Parliament, Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

— European Parliament, *Civil Law Rules on Robotics*, 2016/2103(INL), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.

— European Parliament, *Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and*

military uses and of state authority outside the scope of criminal justice, (2020/2013(INI)), https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_EN.html.

— European Union Agency for Cybersecurity (ENISA), *Artificial Intelligence Cybersecurity Challenges*, ENISA, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

— Executive Office of the President, National Science and Technology Council, Committee on Technology, *Preparing for the Future of Artificial Intelligence*, Washington, D.C., https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

— Filipkowski W., *Criminal Law and Artificial Intelligence - Selected Aspects*, in: *Legal and Technical Aspects of Artificial Intelligence*, L. Lai, M. Świerczyński (eds.), Rozdział: 8, Wydawnictwo Naukowe Uniwersytetu Kardynała Stefana Wyszyńskiego, https://www.researchgate.net/publication/366701783_Criminal_Law_and_Artificial_Intelligence_-_Selected_Aspects.

— Funke, D., *Why false claims about Nancy Pelosi being drunk keep going viral — even though she doesn't drink*, PolitiFact, https://www.politifact.com/article/2020/aug/03/why-false-claims-about-nancy-pelosi-being-drunk-ke/.

— *G7 Leaders' Statement on the Hiroshima AI Process*, The White House, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/.

— Gecić Law, *Who's Responsible? Addressing Liability in the Age of AI*, dostępny w geciclaw.com, https://www.geciclaw.com/whos-responsible-addressing-liability-in-the-age-of-artificial-intelligence/.

— Gilboy J., *Judge Rules Tesla Knew of Autopilot Dangers Before 2019 Fatal Crash, But Did Nothing*, The Drive, https://www.thedrive.com/news/judge-rules-tesla-knew-of-autopilot-dangers-before-2019-fatal-crash-but-did-nothing.

— Goodman, M. E., Shinohara, T. K., De, R., Kourinian, A., *US FTC, DOJ, EEOC, and CFPB Release Joint Statement on AI, Discrimination and Bias*, Mayer Brown,

https://www.mayerbrown.com/en/insights/publications/2023/04/us-ftc-doj-eeoc-and-cfpb-release-joint-statement-on-ai-discrimination-and-bias.

— Google, *Artificial Intelligence at Google: Our Principles*, https://ai.google/principles/.

— Gul R., Nofely A. M. O., *The Future of Law from The Jurisprudence Perspective for Example: The Influence of Science & Technology to Law SI Law*, Journal Equity of Law and Governance, Vol. 1, No. 1, s. 77–83, https://www.ejournal.warmadewa.ac.id/index.php/sjj/article/view/3556.

— Hall K., Fitall E., *Artificial Intelligence and Diagnostic Errors,* Agency for Healthcare Research and Quality, https://psnet.ahrq.gov/perspective/artificial-intelligence-and-diagnostic-errors.

— Hallevy G*., The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control,* Akron Intellectual Property Journal*,* https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1.

— Harned Z., Lungren M. P., Rajpurkar P., *Machine Vision, Medical AI, and Malpractice*, Harvard Journal of Law & Technology Digest, https://jolt.law.harvard.edu/digest/machine-vision-medical-ai-and-malpractice.

— Harwell D., *A face-scanning algorithm increasingly decides whether you deserve the job*, The Washington Post, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

— Higgins T., *Tesla wins first US Autopilot trial involving fatal crash*, CNBC, https://www.cnbc.com/2023/10/31/tesla-wins-first-us-autopilot-trial-involving-fatal-crash.html.

— High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

— Hill K., *Wrongfully Accused by an Algorithm*, The New York Times, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

— Holland & Knight, *What to Know About the New Artificial Intelligence Executive Order*, https://www.hklaw.com/en/insights/publications/2023/10/what-to-know-about-the-new-artificial-intelligence-executive-order.

— International Organization for Standardization, *ISO/IEC 27001 Information security management*, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

— ISACA, *The Promise and Peril of the AI Revolution: Managing Risk*, isaca.org, https://www.isaca.org/resources/white-papers/2023/the-promise-and-peril-of-the-ai-revolution.

— Kamila, M. K., Jasrotia, S. S., *Ethical issues in the development of artificial intelligence: recognizing the risks.* International Journal of Ethics and Systems, https://doi.org/10.1108/IJOES-05-2023-0107.

— Karinshak E., Jin Y., *AI-driven disinformation: a framework for organizational preparation and response,* Journal of Communication Management, *https://doi.org/10.1108/JCOM-09-2022-0113*.

— Klein A., *Tesla driver dies in first fatal autonomous car crash in US*, New Scientist, https://www.newscientist.com/article/2095740-tesla-driver-dies-in-first-fatal-autonomous-car-crash-in-us/.

— Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji - Europejskie podejście do doskonałości i zaufania*, COM(2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pl.pdf.

— Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Sztuczna inteligencja dla Europy*, COM(2018) 237 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018DC0237.

— Komisja Europejska, *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*, COM(2021) 206 final, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

— Komisja Europejska, *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*, COM/2021/206 final, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0012.02/DOC_1&format=PDF.

— Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Ni Loideain, N., & Svantesson, D. J. B., *Expanding the artificial intelligence-data protection debate,* International Data Privacy, https://doi.org/10.1093/idpl/ipy024.

— Levine D., Jin H., *Tesla wins Autopilot trial involving fatal crash*, Reuters, https://www.reuters.com/business/autos-transportation/tesla-wins-autopilot-trial-involving-fatal-crash-2023-10-31/.

— Macdonald Ch., *Tesla's Autopilot was not to blame for fatal 2019 Model 3 crash, jury finds*, Engadget, https://www.engadget.com/teslas-autopilot-was-not-to-blame-for-fatal-2019-model-3-crash-jury-finds-210643301.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAACf82OlZRHyk_qdet8M9oAOaVHt7KTSPNWmVRG15lgUsQf2w1uStt0hrPnm_ikmOlaRh88o-vMkqkO-vB82eDNekGlm7getbxSjUAxzWbZtmqXN4tyLvyNz4N25PjSB5PUikpyZKkExv7LYpXFgRtIkYS9Ls3LGYYfreGDXu1PtK.

— Mantzarlis, A., *What do we do about the "shallowfake" Nancy Pelosi video and others like it?*, Nieman Journalism Lab, https://www.niemanlab.org/2019/05/what-do-we-do-about-the-shallowfake-nancy-pelosi-video-and-others-like-it/.

— Marsden C., Meyer T., *Regulating Disinformation with Artificial Intelligence: Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism*, European Parliamentary Research Service, PE 624.279, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf.

— Marta, P., Salminen, N., Whitehead, D., Perez, N., & Briggs, P., *AI and Cybersecurity: Possible New Risks and Legal Implications,* New York Law Journal,

https://www.law.com/newyorklawjournal/2023/05/08/ai-and-cybersecurity-possible-new-risks-and-legal-implications/.

— Mielnik D., *Anonimowość w Internecie a problem cyberbezpieczeństwa*, w: *Współczesny wymiar bezpieczeństwa publicznego. Kształtowanie bezpiecznych przestrzeni. Działania profilaktyczne*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, https://www.researchgate.net/publication/340205488_Anonimowosc_w_Internecie_a_problem_cyberbezpieczenstwa_Aspekt_prawny.

— Ministerstwo Cyfryzacji, *Analiza związku Aktu w sprawie Sztucznej Inteligencji z wybranymi obowiązującymi i projektowanymi regulacjami prawnymi*, 2022, https://www.gov.pl/web/ai/raport-analiza-zwiazku-aktu-w-sprawie-sztucznej-inteligencji-z-wybranymi-obowiazujacymi-i-projektowanymi-regulacjami-prawnymi.

— MIT Technology Review, *Preparing for AI-enabled cyberattacks*, https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/.

— Modgil S., *Beyond silos: Why AI Regulation calls for an Interdisciplinary Approach,* King's College, https://nms.kcl.ac.uk/sanjay.modgil/BeyondSilos.pdf.

— Monsees D., Product Lead Google, *More information about our processes to safeguard speech data,* Google Blog, https://blog.google/products/assistant/more-information-about-our-processes-safeguard-speech-data/.

— Naik N., Hameed B.M.Z., Shetty D.K., Swain D., Shah M., Paul R., Aggarwal K., Ibrahim S., Patil V., Smriti K., Shetty S., Rai B.P., Chlosta P. & Somani B.K., *Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?* Frontiers in Surgery, https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322/full.

— Noga B.R., Opris I., Lebedev M.A. & Mitchell G.S., *Editorial: Neuromodulatory Control of Brainstem Function in Health and Disease*, Frontiers in Neuroscience, https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2020.00086/full.

— OECD, *OECD AI Principles overview*, https://oecd.ai/en/ai-principles.

— Parlament Europejski, *Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii*, (2020/2012(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PL.html.

— Polonetsky J., Tene O., *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, T-PD(2018)09Rev, s. 13-15, https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6.

— Rada Ministrów RP*, Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*, Portal Gov.pl, https://www.gov.pl/web/ai/polityka-dla-rozwoju-sztucznej-inteligencji-w-polsce-od-roku-2020.

— Rada Ministrów RP*, Polityka rozwoju SI w Polsce przyjęta przez Radę Ministrów – co dalej?*, Portal Gov.pl, https://www.gov.pl/web/govtech/polityka-rozwoju-ai-w-polsce-przyjeta-przez-rade-ministrow--co-dalej.

— Rakowski R., Polak P., Kowalikova P., *Ethical Aspects of the Impact of AI: the Status of Humans in the Era of Artificial Intelligence*, Soc 58, s. 196–203, https://doi.org/10.1007/s12115-021-00586-8.

— Rossi F.., *Artificial Intelligence: Potential Benefits and Ethical Considerations*, European Parliament, Briefing, https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf.

— Ruddin I., Zein S. Z. SGN, *Evolution of Cybercrime Law in Legal Development in the Digital World*, Journal Multidisiplin Madani, Vol. 4, No. 1, s. 168-173, https://doi.org/10.55927/mudima.v4i1.7962.

— Ryan-Mosley, T., *How generative AI is boosting the spread of disinformation and propaganda*, MIT Technology Review, https://www.bing.com/search?q=How+generative+AI+is+boosting+the+spread+of+disinf

ormation+and+propaganda&cvid=22fe5678979742e99e762bbc6e6754c0&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzI3N2owajSoAgiwAgE&FORM=ANAB01&PC=U531.

— Schaffer S., *Will the Autonomous Car Industry Survive Autopilot's First Fatal Crash?, All About Circuits,* https://www.allaboutcircuits.com/news/self-driving-cars-tesla-model-s-fatal-crash/.

— Sellier A.L., *The impact of the Artificial Intelligence Act on criminal law*, "EU Law Live", no. 91, s. 2-3, https://eulawlive.com/weekend-edition/weekend-edition-no91/.

— Shen M. W., *Trust in AI: Interpretability is not necessary or sufficient, while black-box interaction is necessary and sufficient*, DeepAI, https://deepai.org/publication/trust-in-ai-interpretability-is-not-necessary-or-sufficient-while-black-box-interaction-is-necessary-and-sufficient.

— Shoemaker N., *Here's What We Know about Tesla's First Fatal Crash*, Big Think, https://bigthink.com/technology-innovation/heres-what-we-know-about-teslas-first-fatal-crash/.

— Sirignano A., Ricci G., *Ethical and Legal Challenges of Telemedicine in the Era of the COVID-19 Pandemic*, Medicina, https://doi.org/10.3390/medicina57121314.

— Škorvánek I., Talus K., Smuha N. A., *Raport grupy ekspertów dotyczący odpowiedzialności za sztuczną inteligencję oraz inne nowoczesne technologie cyfrowe: krytyczna ocena*, European Journal of Risk Regulation, Vol. 11, No. 2, s. 390-398, 2020, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/expert-groups-report-on-liability-for-artificial-intelligence-and-other-emerging-digital-technologies-a-critical-assessment/45FD6BB0E113E7C4A9B05128BC710589.

— State of California Department of Justice, *California Consumer Privacy Act (CCPA)*, https://www.oag.ca.gov/privacy/ccpa.

— Statt N., *Thieves are now using AI deepfakes to trick companies into sending them money*, The Verge, https://www.theverge.com/2019/9/5/20851251/deepfake-ai-voice-scam.

— Truby J., Brown R. D., Ibrahim I. A., Parellada O. C., *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, European Journal of Risk Regulation, Vol. 13, No. 2, s. 270-294, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence-applications/C350EADFB379465E7F4A95B973A4977D.

— U.S. Food and Drug Administration, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)*, https://www.fda.gov/media/122535/download.

— UNESCO, *Raport na temat Etyki Sztucznej Inteligencji*, https://unesdoc.unesco.org/ark:/48223/pf0000380455_pol.

— UNESCO, *Rekomendacja w sprawie etyki sztucznej inteligencji*, https://unesdoc.unesco.org/ark:/48223/pf0000373434.

— Vogeler, W., *AI Can Predict Supreme Court Decisions, New Study Finds*, FindLaw, https://www.findlaw.com/legalblogs/supreme-court/ai-can-predict-supreme-court-decisions-new-study-finds/.

— Wendehorst C., *Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks*, in: Voeneky S., Kellmeyer P., Mueller O., Burgard W. (eds.), *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives*, Cambridge Law Handbooks, Cambridge University Press, s. 187-209, https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/liability-for-artificial-intelligence/12A89C1852919C7DBE9CE982B4DE54B7.

— Wikipedia Contributors, *Deepfake*, Wikipedia, https://en.wikipedia.org/wiki/Deepfake.

— Wikipedia Contributors, *Fintech*, Wikipedia, https://en.wikipedia.org/wiki/Fintech.

— Wikipedia, COMPAS (software), https://en.wikipedia.org/wiki/COMPAS_(software).

— Wikipedia*, Facebook–Cambridge Analytica data scandal,* https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

— Wolfson S.., *Amazon's Alexa recorded private conversation and sent it to random contact*, The Guardian, https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation.

— World Economic Forum, *Empowering AI Leadership: An Oversight Toolkit for Boards of Directors*, https://www3.weforum.org/docs/WEF_Empowering_AI_Leadership_2022.pdf.

— World Economic Forum, *Law Enforcement Agencies Develop Best Practices for Using Facial Recognition*, https://www.theverge.com/2019/9/5/20851248/deepfakes-ai-fake-audio-phone-calls-thieves-trick-companies-stealing-money.

— World Health Organization, *Ethics and governance of artificial intelligence for health*, https://www.who.int/publications/i/item/9789240029200.

— Zirpoli Ch.T., *Generative Artificial Intelligence and Copyright Law,* CRS Reports, https://crsreports.congress.gov/product/pdf/LSB/LSB10922.

— Zisov N., Targov T., *Risks of Artificial Intelligence – Safety Aspects*, Chambers and Partners, https://chambers.com/articles/risks-of-artificial-intelligence-safety-aspects.