Promotorka: dr hab. Kinga Flaga-Gieruszyńska prof. US

Promotorka pomocnicza: dr Aleksandra Klich

Streszczenie rozprawy doktorskiej

mgr Klaudii Maciejewskiej

pt. „Prawne aspekty wykorzystania sztucznej inteligencji jako narzędzia podwyższającego efektywność i bezpieczeństwo systemów teleinformatycznych przetwarzających dane osobowe".

Cyfrowa transformacja, która odbywa się z wykorzystaniem modeli i algorytmów AI, może stanowić zagrożenie w budowaniu ekosystemu zaufania opartego na unijnych wartościach i prawach podstawowych. Oddziaływanie systemów AI na preferencje użytkowników może skutkować manipulacją i ograniczeniem autonomii człowieka. Delegowanie decyzji na modele i algorytmy AI wywiera z kolei wpływ na brak ich zrozumienia, a także przyczynia się do powstawania wątpliwości co do odpowiedzialności za ich wykorzystywanie. Stronniczość danych wykorzystywanych w modelach sztucznej inteligencji może skutkować naruszeniem podstawowych praw i wolności człowieka, w tym przetwarzania danych osobowych. Systemy sztucznej inteligencji powinny być wytwarzane w sposób rzetelny i bezpieczny, aby z wyprzedzeniem diagnozować możliwe do wystąpienia ryzyka, a także zapobiegać potencjalnym szkodom. Transparentność, interpretowalność i przejrzystość systemów informatycznych i teleinformatycznych wykorzystujących rozwiązania AI powinny być zapewnione na trzech płaszczyznach: danych, systemów i komunikacji. Przy czym do kluczowych kwestii należy: 1) poszanowanie praw podstawowych i autonomii człowieka, 2) zapobieganie szkodom i zagrożeniom zarówno technicznym, jak i społecznym, 3) transparentność i wytłumaczalność modeli opartych na algorytmach sztucznej inteligencji, 4) odpowiedzialność prawna za szkody wyrządzone przy zastosowaniu sztucznej inteligencji, 5) ochrona praw własności intelektualnej.

Przedmiotem badawczym niniejszej pracy uczyniono ustalenie implikacji stosowania nowych technologii i usług cyfrowych dla koncepcji odpowiedzialności z perspektywy praw podstawowych. Skupiono się, a zarazem ograniczono, do technologii AI, ze szczególnym uwzględnieniem uczenia maszynowego, sieci neuronowych, modeli AI ogólnego przeznaczenia, w tym generatywnej sztucznej

inteligencji. W nawiązaniu do kluczowego celu badawczego sformułowano główną hipotezę badawczą stanowiącą, że technologie sztucznej inteligencji przyniosły i przyniosą znaczne korzyści, w szczególności poprzez zwiększenie wydajności, dokładności, terminowości i wygody świadczenia wielu usług. Przy tym wiele takich zastosowań można rozumieć jako zwiększające praktyczny zasięg i rozszerzające zakres bezpieczeństwa informacji oraz korzystania z praw i wolności człowieka.

W opracowaniu skoncentrowano się również na analizie znaczenia sztucznej inteligencji dla bezpieczeństwa teleinformatycznego w inteligentnych sieciach i systemach, wykorzystywania inteligentnych systemów bezpieczeństwa w procesach technologicznych i społecznych, jak również wykorzystywania sztucznej inteligencji w tworzeniu bezpiecznych systemów teleinformatycznych, informatycznych, a także bezpiecznych systemów gromadzenia danych, weryfikacji, archiwizacji i przekazywania danych osobowych. W ramach opracowania podjęto się rozwiązania następujących szczegółowych problemów badawczych:

1) zdiagnozowania zakresu zastosowania sztucznej inteligencji na potrzeby tworzenia inteligentnych sieci i systemów teleinformatycznych, w szczególności w zakresie bezpiecznych systemów gromadzenia danych,
2) zbadania wpływu systemów AI na pojęcie odpowiedzialności, w szczególności w zakresie, w jakim mogą one utrudniać korzystanie z praw człowieka i podstawowych wolności, oraz w kwestii odpowiedzialności za te zagrożenia i konsekwencje,
3) odzwierciedlenia stosowania sztucznej inteligencji w przepisach prawa powszechnie obowiązującego, na polu odpowiedzialności cywilnoprawnej za szkody wyrządzone przy wykorzystaniu systemów sztucznej inteligencji oraz ochrony własności intelektualnej,
4) ustalenia wartości wdrożeniowej dla przedsiębiorcy (Currenda Sp. z o.o.) działającego na rynku usług informatycznych w związku z zastosowaniem sztucznej inteligencji w systemach teleinformatycznych dla wymiaru sprawiedliwości i zawodów prawniczych.

Mając na względzie interdyscyplinarny charakter sztucznej inteligencji oraz udział autorki opracowania w programie Ministerstwa Nauki i Szkolnictwa Wyższego „Doktorat wdrożeniowy", efektem prowadzonych badań jest wprowadzenie na rynek innowacyjnego systemu informacji prawnej do monitorowania zmian aktów prawnych przy wykorzystaniu sztucznej inteligencji – AIMON, a także opracowanie

u przedsiębiorcy (Currenda Sp. z o.o.) dokumentacji projektowej opartej na etycznej sztucznej inteligencji oraz sporządzeniu koncepcji audytowania systemów AI.

W ramach przeprowadzonych badań, w pracy przedstawiono wnioski *de lege ferenda* odnoszące się do: 1) bezpieczeństwa i zagrożeń związanych z zastosowaniem rozwiązań sztucznej inteligencji w sieciach i systemach teleinformatycznych, 2) cyberbezpieczeństwa, 3) systemu zarządzania ryzykiem, 4) audytowania sztucznej inteligencji, 5) odpowiedzialności za szkody wyrządzone przy zastosowaniu sztucznej inteligencji, 6) zgodności systemów AI z prawem przetwarzania danych osobowych oraz obowiązkiem zapobiegania lub minimalizowania wpływu przetwarzania danych na prawa i podstawowe wolności osób, których dane dotyczą, 7) ochrony własności intelektualnej systemów teleinformatycznych wytworzonych przez rozwiązania sztucznej inteligencji, 8) autorstwa treści wytworzonych z wykorzystaniem rozwiązań AI, 9) własności dzieł stworzonych przez sztuczną inteligencję, 10) danych osobowych wykorzystywanych do opracowywania systemów AI dla wymiaru sprawiedliwości i zawodów prawniczych.

Systemy AI powinny być odporne na błędy, usterki i niespójności przez możliwość kompleksowego i ciągłego monitorowania modeli AI oraz zarządzania nimi. Wytłumaczalna sztuczna inteligencja może zwiększać zaufanie użytkowników końcowych do rozwiązań wykorzystujących AI. Pozwala przy tym kontrolować modele i algorytmy AI, a także korzystać z nich w produktywny sposób. Powyższe stanowi kluczowy warunek do implementowania odpowiedzialnej sztucznej inteligencji, działającej na rzecz ludzi i społeczeństwa. Należy zatem zapewnić, aby opracowywanie, wytwarzanie i wykorzystywanie systemów AI oparte było na godnej zaufania sztucznej inteligencji oraz wyrażone przez przewodnią i nadzorczą rolę człowieka, bezpieczeństwo informacji i solidność techniczną, ochronę prywatności i danych osobowych. Wdrażanie na rynek rozwiązań AI musi być zgodne z przepisami prawa, z normami i standardami, a także oparte na zasadach etycznych, albowiem tylko w ten sposób możliwe jest budowanie systemów sztucznej inteligencji opartych na zaufaniu i transparentności. Dzięki zharmonizowanym przepisom prawa na poziomie europejskim oraz wdrożeniu odpowiedniej kontroli, systemy AI mogą stanowić narzędzia podwyższające efektywność i bezpieczeństwo przetwarzania danych osobowych.

Słowa kluczowe: sztuczna inteligencja, wytłumaczalna sztuczna inteligencja, cyberbezpieczeństwo, bezpieczeństwo informacji, ochrona danych osobowych, systemy

sztucznej inteligencji, bezpieczeństwo systemów sztucznej inteligencji, odpowiedzialność za szkody, ochrona własności intelektualnej, ethics by design, audyt sztucznej inteligencji, zarządzanie ryzykiem