§ WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI *w kryminalistyce*

apl. adw. Paulina Przybyłowicz
Izba Adwokacka w Łodzi

Wraz z dynamicznym rozwojem nowych technologii możemy zaobserwować rosnącą rolę sztucznej inteligencji (ang. *artificial intelligence,* AI) w wielu dziedzinach życia. To innowacyjne rozwiązanie, w związku z rosnącą z uwagi na rozwój techniki przestępczością, może pomóc również w skutecznym wykrywaniu przestępców. Problematyka zastosowania sztucznej inteligencji cieszy się coraz większym zainteresowaniem wśród społeczeństwa, które również wykazuje chęć wykorzystania AI w kryminalistyce.

WPROWADZENIE

Termin „sztuczna inteligencja" został po raz pierwszy zdefiniowany w 1955 r. przez Johana McCarthy'ego[1]. Obecnie istnieje wiele definicji powyższego terminu. Sztuczna inteligencja „to ekscytujące próby stworzenia myślących komputerów (...) maszyn z umysłami w pełnym tego słowa znaczeniu"[2]. Po-

1 K. Rożnowski, *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007, nr 2, s. 110.

2 J. Haugeland, *Artificial Intelligence: The Very Idea*, „Artificial Intelligence" 1986, nr 29, s. 349–353, K. Rożnowski, *Sztuczna inteligencja. Rozwój, szanse i zagrożenia*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007, nr 2, s. 111.

nadto sztuczna inteligencja definiowana jest jako „nauka o czynnościach, które miałyby spowodować, że maszyny będą wykonywać funkcje, które aktualnie lepiej wykonuje człowiek”[3].

Celem niniejszego opracowania jest przede wszystkim ukazanie możliwości wykorzystania sztucznej inteligencji w kryminalistyce. Ponadto opracowanie skupi się na przedstawieniu zagrożeń, jakie może nieść za sobą korzystanie z rozwiązań, jakie daje sztuczna inteligencja. Wynika to z faktu, iż pomimo wielu pozytywnych aspektów jej stosowania, jednocześnie może ona zagrażać prawom podstawowym. W związku z powyższym artykuł zbada również aktualne regulacje prawne w zakresie AI. Niniejsze opracowanie podkreśli również konieczność ciągłego nowelizowania przepisów dotyczących sztucznej inteligencji w związku z rozwojem nowych technologii. Niestety przypuszczać można, iż z uwagi na dynamikę wskazanego rozwoju regulacje prawne wymagają częstej ich aktualizacji.

Problematyka sztucznej inteligencji z uwagi na jej ciągły rozwój jest aktualnym oraz nowoczesnym tematem, który ciągle ewoluuje. Dnia 13.03.2024 r. Parlament przyjął akt w sprawie sztucznej inteligencji, który ma na celu jednoczesne zapewnienie rozwoju technologicznego AI wraz z zagwarantowaniem bezpieczeństwa podstawowych praw i wolności człowieka. Akt ten ma zapewniać społeczeństwo, iż system AI jest przejrzysty, bezpieczny, zgodny ze środowiskiem oraz niedyskryminujący. Ponadto nowa regulacja ma wprowadzić w przyszłości Europejską Radę ds. Sztucznej Inteligencji, której zadaniem będzie skuteczne egzekwowanie przepisów na poziomie krajowym.

Innowacyjność niniejszego opracowania polega przede wszystkim na zauważeniu skali możliwości wykorzystania sztucznej inteligencji w kryminalistyce, przy jednoczesnym zasygnalizowaniu zagrożeń, jakie mogą wystąpić w związku z korzystaniem z niej. Niewystarczająca regulacja prawna w powyższym zakresie może skutkować pojawieniem się coraz to większej ilości nowych problemów, przede wszystkim z uwagi na ciągły rozwój nowych technologii. Ponadto niniejsze opracowanie zwraca uwagę na fakt, że mimo powstania regulacji prawnych, konieczna jest ich ciągła nowelizacja w tym zakresie. Zatem zarówno Unia Europejska, jak i państwa członkowskie za pomocą przepisów prawnych powinny nie tyle wyłącznie tworzyć nowe regulacje

3 E. Rich, K. Knight, *Artificial Intelligence*, New York 1990, s. 100–101.

prawne, jak dostosowywać je do określonego w danym momencie poziomu technologicznego rozwoju.

ISTOTA SZTUCZNEJ INTELIGENCJI

Z uwagi na prężny rozwój technologii oraz zauważalność możliwości, jakie niesie za sobą wykorzystanie AI, coraz częściej pojawia się pytanie o przyszłe jej wykorzystanie w procesie stosowania prawa. Powyższe może wynikać z faktu, iż AI, jak również komputeryzacja czy szeroko pojęta robotyzacja mają coraz większy wpływ na organizowanie oraz świadczenie usług przez profesjonalnych prawników[4]. Problematyka stosowania rozwiązań zaproponowanych przez sztuczną inteligencję powoduje przede wszystkim niepewność w zakresie ochrony dóbr osobistych człowieka. W obecnych czasach, kiedy rozwój technologii przechodzi dynamiczne zmiany, a w Internecie można odnaleźć wiele danych osobowych poszczególnych obywateli, korzystanie ze sztucznej inteligencji, która miałaby możliwość wykorzystania tak szerokiej bazy danych do swoich działań, może spowodować zawahania w zakresie przestrzegania przez nią ochrony dóbr osobistych człowieka. Naruszone przede wszystkim mogłoby zostać prawo do prywatności, uregulowane zarówno w ustawodawstwie krajowym, jak również międzynarodowym, a uznawane jako prawo podstawowe, tj. fundamentalne. W związku z powyższym państwa, które chciałyby stosować rozwiązania AI, musiałyby odnaleźć balans pomiędzy zapewnieniem ochrony interesu publicznego a ochroną interesu poszczególnych jednostek.

W zakresie dóbr osobistych przez przedstawicieli doktryny poruszany jest również temat posiadania dóbr osobistych przez sztuczną inteligencję. Stwierdzono bowiem, iż AI nie tylko może, ale również powinna stać się podmiotem dóbr osobistych, jednakże nie jest to uznawane za warunek niezbędny[5]. Dobra te mogą przynależeć osobom fizycznym, osobom prawnym, jak również mogą być przypisane dla zwierząt. Powyższa kwestia jest dość problematyczna, przede wszystkim z uwagi na fakt, iż przyznanie jakichkolwiek dóbr osobistych sztucznej inteligencji wiązałoby się z uznaniem, że posiada ona podmiotowość

4 M. Zubańska, *Kryminalistyka w dobie przyspieszenia naukowo-technicznego i technologicznych nadużyć – przytłaczająca wizja zmian, czy inspiracja do rozwoju?*, „Studia Prawnoustrojowe" 2021, nr 52, s. 557.

5 M. Rożnowska, *Dobra osobiste sztucznej inteligencji, a doktrynalna ochrona dóbr osobistych – czy sztuczna inteligencja może być podmiotem dóbr osobistych?*, „Transformacje Prawa Prywatnego" 2023, nr 2, s. 197.

prawną. Rozstrzygnięcie problemów związanych z działalnością sztucznej inteligencji pozwoliłoby na wykorzystanie jej pełnych zasobów, a co za tym idzie – wyciągnięcie korzyści, które za sobą niesie. Między innymi jest to egzekwowanie prawa, prewencja społeczna czy zwalczanie przestępczości.

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) popiera wykorzystanie sztucznej inteligencji w postępowaniach karnych, m.in. w zakresie ścigania przestępstw[6]. Organ uznał, iż wykorzystanie AI przyspieszyłoby pracę organów sądowych oraz podmiotów zajmujących się ściganiem sprawców przestępstw. Poniżej zostaną omówione przykładowe systemy AI wykorzystywane w kryminalistyce, jednakże odnaleźć ich można dużo więcej, jak np. system detekcji deepfake, profilowanie DNA, rozpoznawanie głosu czy analiza big data.

SYSTEM IDENTYFIKACJI ŚLADÓW LINII PAPILARNYCH

Czy stwierdzenie, iż każdy człowiek posiada unikalne linie papilarne, które odróżniają go od pozostałych osób, jest zgodne z prawdą? Czy każdy palec tego samego człowieka różni się układem linii papilarnych? Chcąc sprawdzić oraz wykorzystać możliwości, jakie daje sztuczna inteligencja, naukowcy z Columbia University przygotowali nowy model sztucznej inteligencji, która miała za zadanie porównywanie odcisków palców. AI opracowana przez badaczy z Columbia University potrafi dopasować odciski palców z 99,99 % prawdopodobieństwem uzyskania dobrego wyniku[7]. Ponadto badacze doszli do wniosku, iż linie papilarne nie są tak unikalne u tej samej osoby, jak dotychczas wszystkim się wydawało, lecz były po prostu w nieodpowiedni sposób porównywane.

Aktualnie stosowane metody porównywania linii papilarnych badały je poprzez szczegółową analizę wzorów grzbietów. Natomiast sztuczna inteligencja porównuje te linie poprzez analizę wzorów binarnych, jak również wykorzy-

6 K. Dziedzic, K. Juszka, *Kontrowersyjne nowe technologie w kryminalistyce*, „Studia Prawnoustrojowe" 2022, nr 55, s. 108.

7 G. Guo, A. Ray, M. Izydorczak, J. Goldfeder, H. Lipson, W. Xu, *Unveiling intra-person fingerprint similarity via deep contrastive learning*, Science Advances, vol. 10, issue 2, https://www.science.org/doi/10.1126/sciadv.adi0329?adobe_mc=MCMID%3D56027468956561299854396479018955009130%7CMCORGID%3D242B6472541199F70A4C98A6%2540AdobeOrg%7CTS%3D1704897905 (dostęp: 15.03.2024 r.).

stując gęstość oraz orientację grzbietów. Zatem jej badanie skupia się na analizie kątów oraz krzywizn, co stanowi nowatorskie rozwiązanie wśród dotychczasowych metod badawczych. Oczywiście aby w pełni wprowadzić powyższe rozwiązanie do codziennej praktyki, konieczne jest przetestowanie wniosków przesyłanych przez AI na większej liczbie różnorodnych linii papilarnych.

Obecnie w celu identyfikacji śladów linii papilarnych odnalezionych na miejscu zdarzenia oraz porównania ich ze śladami znajdującymi się w bazie danych jest wykorzystywany system AFIS (Automatyczny System Identyfikacji Daktyloskopijnej). Nie jest on jednak w 100% skuteczny, przede wszystkim z uwagi na fakt, iż porównuje on ślady linii papilarnych znalezionych na miejscu zdarzenia wyłącznie ze śladami znajdującymi się w bazie danych. Aktualnie w zbiorze daktyloskopijnym do końca 2019 r. zgromadzono 4.069.691 kart daktyloskopijnych oraz 112.535 obrazów niezidentyfikowanych śladów linii papilarnych z miejsc zdarzeń[8]. System poprzez porównanie specyficznych cech charakterystycznych poszczególnych linii papilarnych odnajduje w bazie stosowny odcisk, który uprzednio został złożony przez daną osobę.

Dzięki powyższemu rozwiązaniu kryminalistyka jest w stanie walczyć z poszczególnymi kategoriami przestępstw, takimi jak przestępstwa przeciwko wolności seksualnej, przestępstwa związane z praniem brudnych pieniędzy czy terroryzmem, a nawet cyberprzestępstwami. Wprowadzenie AFIS pozwoliło bowiem na: zwiększenie oraz ulepszenie procesów bezpieczeństwa, szybsze poszukiwanie przestępców oraz osób pokrzywdzonych, jak również zwiększenie wsparcia kontroli granicznych.

SYSTEM IDENTYFIKACJI TWARZY

Rozwój sztucznej inteligencji pozwolił również na wykorzystanie algorytmu pozwalającego na identyfikację twarzy, czyli tzw. identyfikację biometryczną. System przetwarza obrazy, biorąc pod uwagę zaprogramowany w nim schemat, a następnie dokonuje weryfikacji oraz identyfikacji danej osoby, co pozwala między innymi na wykrycie sprawcy przestępstwa. Cleaview AI dokonuje porównania twarzy danej osoby z całą bazą zdjęć zamieszczonych w Interne-

8 E. Kot, *Opracowanie zaawansowanego technologicznie systemu informatycznego umożliwiającego zautomatyzowane przetwarzanie informacji zgromadzonych w kryminalistycznych biometrycznych bazach danych w celu zwalczenia przestępstw lub identyfikacji osób*, „Problemy Kryminalistyki" 2020, nr 308 (2), s. 35.

cie, w tym na wszelkich platformach społecznościowych. Powyższe rozwiązanie ma ponadto na celu: ułatwienie egzekwowania prawa, zwalczania przestępczości czy zwiększenie działań prewencyjnych.

Parlament Europejski wyraził swoje niezadowolenie z wykorzystywania przez organy ścigania oraz służby wywiadowcze prywatnych baz danych, które dokonują weryfikacji oraz identyfikacji twarzy. Państwa członkowskie UE zostały wezwane przez Parlament Europejski do przyznania się do korzystania z takich baz danych, przypominając jednocześnie o fakcie, iż korzystanie np. z Cleaview AI nie jest zgodne z regulacjami UE dotyczącymi ochrony danych. Ponadto Parlament Europejski wezwał wszystkie państwa członkowskie do wprowadzenia na ich terytorium zakazu korzystania z prywatnych baz danych mających na celu identyfikację twarzy[9]. Negatywnie do systemu identyfikacji twarzy odniosła się również Europejska Rada Ochrony Danych w Wytycznych 05/22, wersji nr 2 z 26.04.2023 r., uznając, że ma ona wpływ na liczne prawa i wolności, nie tylko ograniczając np. prawo do prywatności czy ochronę danych osobowych, lecz również naruszając jednocześnie wolność zgromadzeń, godność ludzką czy wolność przemieszczania się[10].

Mimo pozytywnych skutków wprowadzenia systemu identyfikacji twarzy, spotkał się on w wielu państwach z krytyką, z uwagi na brak podstawy prawnej do przetwarzania takich informacji. Od 2020 r. do francuskiego organu nadzorczego wpływały liczne skargi na Clearview AI, tj. system mający na celu rozpoznawanie twarzy. Na podstawie licznych interwencji, zgodnie z art. 83 rozporządzenia RODO[11], doszło do ukarania Clearview AI administracyjną karą pieniężną w wysokości 20 mln euro oraz nakazania zaprzestania przetwarzania i zbierania danych osób zamieszkałych we Francji. Ponadto dane już zebrane miały zostać usunięte w terminie dwóch miesięcy[12]. System Clearview AI mimo zakazu jego stosowania w USA, Kanadzie i Wielkiej Brytanii,

9 Rezolucja Parlamentu Europejskiego z 6.10.2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych (2020/2016 (INI)).

10 O. Łuczak, *Wykorzystanie sztucznej inteligencji w kryminalistyce – czyli ile prawdy jest w filmach detektywistycznych?*, https://lgl-iplaw.pl/2023/07/wykorzystanie-sztucznej-inteligencji-w-kryminalistyce-czyli-ile-prawdy-jest-w-filmach-detektywistycznych (dostęp: 15.03.2024 r.).

11 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. nr 119, s. 1 z późn. zm.).

12 Newslatter UODO dla Inspektorów Ochrony Danych, rok 2022, nr 12 (45), s. 14.

miał zostać również wykorzystany w wojnie na Ukrainie, w celu identyfikowania ofiar, osób zaginionych, szpiegów czy zbrodniarzy wojennych[13].

GRANICE ORAZ ZAKAZY SZTUCZNEJ INTELIGENCJI

Mimo szerokich możliwości, jakie daje wykorzystanie sztucznej inteligencji w wielu dziedzinach życia społecznego, niesie ono również za sobą liczne zagrożenia dóbr osobistych, takich jak prawo do prywatności czy wolność zrzeszania się. W związku z istotnością ochrony dóbr osobistych, stanowiących fundamentalne wartości społeczne, zaistniała potrzeba określenia swoistych granic, w ramach których AI może zostać wykorzystywana przez organy stosowania prawa. W tym celu powstała rezolucja Parlamentu Europejskiego z 6.10.2021 r.[14], która uwzględnia m.in.:

1) **Białą Księgę Komisji z 19.02.2020 r. w sprawie sztucznej inteligencji – „Europejskie podejście do doskonałości i zaufania" [COM(2020)0065];**

2) **wysłuchanie w Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) w dniu 20.02.2020 r. na temat sztucznej inteligencji w prawie karnym oraz jej wykorzystania przez policję i organy wymiaru sprawiedliwości w sprawach karnych;**

3) **opinie przedstawione przez Komisję Rynku Wewnętrznego i Ochrony Konsumentów oraz Komisję Prawną;**

4) **wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji (AI), opublikowane przez grupę ekspertów wysokiego szczebla Komisji ds. AI w dniu 8.04.2019 r.;**

13 A. Dębska, *Własność intelektualna w cieniu dramatów ludzkich – cyberwojna na technologie, zalegalizowanie piractwa, niszczenie dziedzictwa kulturowego*, https://lgl-iplaw.pl/2022/03/wlasnosc-intelektualna-w-cieniu-dramatow-ludzkich-zniszczen-cyberwojna-na-technologie-zalegalizowanie-piractwa-niszczenie-dziedzictwa-kulturalnego/ (dostęp: 15.03.2024 r.).

14 Rezolucja Parlamentu Europejskiego z 6.10.2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych (2020/2016 (INI)).

5) **Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS 108) oraz zmieniający ją protokół.**

Z uwagi na fakt, iż ważną rolę w postępowaniu karnym odgrywają jego podstawowe zasady, jak również takie wartości, jak godność człowieka czy zakaz dyskryminacji, AI powinna być wykorzystywana tylko w szczególnych przypadkach oraz w sposób proporcjonalny, zgodny z zasadami sprawiedliwości społecznej oraz adekwatny do standardów ścigania przestępstw. Zgodność ta powinna również uwzględniać wszelkie regulacje ustanowione przez organy unijne, a dotyczące ochrony danych osobowych.

Ponadto powyższa regulacja wprowadziła również liczne zakazy w stosowaniu sztucznej inteligencji, w poszczególnych sytuacjach, takich jak:

1. **jej niezgodność z prawami podstawowymi;**
2. **chęć masowej inwigilacji, w tym przetwarzanie danych biometrycznych w celu masowej inwigilacji w przestrzeni publicznej;**
3. **proponowanie orzeczeń sądowych;**
4. **automatyczna analiza lub rozpoznawanie w przestrzeni publicznej poszczególnych cech ludzkich, takich jak, np. głos, DNA czy elementy behawioralne;**
5. **korzystanie z prywatnych baz danych służących do identyfikacji twarzy;**
6. **masowa kwalifikacja punktowa obywateli.**

Nowo przyjęta przez Parlament Europejski regulacja prawna, tj. akt w sprawie sztucznej inteligencji, określa obowiązki dostawców oraz użytkowników w zależności od poziomu ryzyka[15]. W związku z powyższym systemy, które stwarzają niedopuszczalne ryzyko, a jednocześnie stanowiące zagrożenie dla ludzi oraz ich praw, mają zostać zakazane. Między innymi są to:

15 Parlament Europejski, *Akt ws. sztucznej inteligencji: pierwsze przepisy regulujące sztuczną inteligencję*, https://www.europarl.europa.eu/topics/pl/article/20230601STO93804/akt-ws-sztucznej-inteligencji-pierwsze-przepisy-regulujace-ai (dostęp: 17.03.2024 r.).

1) **systemy identyfikacji biometrycznej podejmujące działania zdalnie oraz w czasie rzeczywistym (np. rozpoznawanie twarzy), z wyłączeniem określonych prawem warunków oraz przy uzyskaniu stosownych zezwoleń;**

2) **klasyfikacja punktowa osób, prognozowanie przestępczości na podstawie cech osobistych jednostki, jej zachowań czy statusu społecznego;**

3) **manipulacja społeczeństwem oraz wykorzystanie słabości poszczególnych jednostek (np. szkodliwe zabawki głosowe);**

4) **kategoryzacja osób fizycznych;**

5) **systemy mające na celu rozpoznawanie emocji w miejscach pracy czy instytucjach naukowych.**

Natomiast na systemy AI, które tworzą nowe treści, tj. ChatGPT, został nałożony wymóg przejrzystości, polegający w szczególności na niegenerowaniu nielegalnych treści oraz ujawnianiu wygenerowanej treści. W odróżnieniu od powyższych systemów, te z ograniczonym ryzykiem muszą spełniać wyłącznie minimalne wymogi związane z ich przejrzystością, w tym umożliwienie społeczeństwu podjęcia świadomych decyzji. Pomimo generalnego zakazu stosowania przez organy ścigania rozwiązań sztucznej inteligencji, nowa regulacja wprowadza od powyższej zasady pewne wyjątki, mianowicie w sytuacjach, które wymagają szybkiej reakcji organów, takich jak ataki terrorystyczne czy poszukiwanie osób zaginionych.

ZAGROŻENIA ORAZ BŁĘDY SZTUCZNEJ INTELIGENCJI

Jednym z największych zagrożeń, jakie niesie za sobą korzystanie ze sztucznej inteligencji, z uwagi na wielkość bazy danych, z których czerpie ona informacje, jest wyciek tych danych. Wszelkie czynności wykonywane w ramach działań kryminalistycznych, takie jak identyfikacja twarzy czy badanie układu linii papilarnych, wymagają gromadzenia danych osobowych, które stanowią tzw. dane wrażliwe. Ich wyciek mógłby spowodować liczne konsekwencje prawne oraz faktyczne. W związku z powyższym to na władzach danego państwa spoczywa obowiązek zapobiegania takim sytuacjom i stworzenia takich zabezpieczeń, które pozwalałyby w jak największym stopniu na zminimalizowanie możliwości wycieku jakichkolwiek danych osobowych do osób czy podmiotów nieuprawnionych.

Parlament Europejski w rezolucji z 6.10.2021 r.[16] zauważył problem przypisania odpowiedzialności prawnej za szkody wyrządzone przez sztuczną inteligencję, jednakże nie określił konkretnie, kto taką odpowiedzialność ma ponosić. Uznano jedynie, że odpowiedzialność musi zostać przypisana zidentyfikowanej osobie fizycznej lub prawnej. W związku z powyższym powstaje pytanie, czy odpowiedzialność taką należy przypisać twórcy sztucznej inteligencji, czy podmiotowi lub użytkownikowi, który z niej w danym celu skorzystał? Moim zdaniem trafne byłoby podzielenie tej odpowiedzialności na oba podmioty i określenie stopnia przyczynienia się ich do zaistnienia powstałej szkody. Wyłączenie odpowiedzialności użytkownika spowodowałoby bowiem sytuację, w której czułby się on bezkarny i winę za wszelkie działania przerzucałby na AI. Natomiast wyłączenie odpowiedzialności twórcy sztucznej inteligencji wykreowałoby sytuację, w której to twórca czułby się bezkarny i wytwarzał produkt o mniejszej jakości, a co za tym idzie – posiadający mniej zabezpieczeń. Ponadto w powyższym przypadku mielibyśmy również do czynienia ze spadkiem zaufania społecznego w zakresie tworzenia i rozwijania

16 Rezolucja Parlamentu Europejskiego z 6.10.2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych [2020/2016 (INI)].

nowych technologii oraz wprowadzenia ich do coraz to szerszego grona dziedzin.

Należy również pamiętać, iż sztuczna inteligencja nie tylko może być wykorzystana przez organy państwowe, lecz również przez przestępców. Mogą oni bowiem wykorzystać potencjał AI do popełniania różnorodnych przestępstw, np. szantażu czy podszywania się pod inną osobę[17]. Szantaż, jakiego mogliby dokonać za pomocą sztucznej inteligencji, posiada szeroki zakres działania, wręcz masowy. Z uwagi na możliwość korzystania przez AI z szerokiej bazy danych, przestępcy mogliby odnajdywać w niej poszczególne elementy, a następnie szantażować podmioty związane z udostępnianą treścią. Ponadto nowe technologie pozwalają już na przetwarzanie oraz modyfikowanie treści cyfrowej, zatem przestępcom z wykorzystaniem AI byłoby łatwo podszyć się pod inną osobę w Internecie. Zwiększy to z pewnością przestępczość polegającą na wyłudzaniu pieniędzy, np. od osób starszych, przez udawanie za pomocą social mediów bliskiej im osoby.

AI jako system, tak samo jak człowiek wykonujący daną czynność, może się pomylić. Mimo możliwie niskiego marginesu błędu nie może on zostać w każdym przypadku wykluczony. System sztucznej inteligencji może zatem błędnie zidentyfikować twarz lub wskazać porównanie do linii papilarnych osoby zapisanej w systemie. Naruszyłoby to zaufanie społeczeństwa do takiego rozwiązania, a nawet wzbudziłoby liczne kontrowersje i panikę w związku z możliwym, przyszłym wskazaniem właśnie tej osoby jako sprawcy danego przestępstwa. Zatem AI powinna być wykorzystana wyłącznie w konkretnych przypadkach, które wymagają jej pomocy, a organy państwowe powinny liczyć się z jej ewentualną pomyłką.

PODSUMOWANIE

Biorąc pod uwagę powyższe rozważania, można stwierdzić, iż sztuczna inteligencja może być skutecznie wykorzystana w kryminalistyce. Dzięki takim rozwiązaniom, jak identyfikacja twarzy czy porównanie linii papilarnych, może przyczynić się ona do zwalczania przestępczości oraz usprawnienia

17 P. Olbert, *Sztuczna inteligencja i przestępczość przyszłości w kontekście kryminalistycznych badań informatycznych*, „Przegląd Policyjny" 2023, nr 1 (149), s. 145.

działania organów ścigania. Należy jednak pamiętać, iż może ona posłużyć również przestępcom do łamania prawa, np. poprzez wykorzystanie masowego szantażu czy podszywanie się pod rzeczywiście istniejące osoby. Wejście w życie aktu ws. sztucznej inteligencji pozwoli na zabezpieczenie podstawowych praw i wolności człowieka, przy jednoczesnym umożliwieniu dalszych innowacji technologicznych. Jednakże wymagane są w późniejszym czasie jego nowelizacje, w szczególności z uwagi na ciągły rozwój nowych technologii. Wprowadzenie bowiem dostosowanych do aktualnego rozwoju społecznego przepisów prawnych pozwoli na wyeliminowanie problemów narastających przez nieustanny rozwój społeczny.

W przypadku wejścia w życie nowej regulacji unijnej, państwa członkowskie powinny nie tylko stosować ją bezpośrednio, lecz również stworzyć własne wewnętrzne przepisy, które określałyby funkcjonowanie instytucji sztucznej inteligencji w poszczególnym państwie o danej strukturze wewnętrznej. Przepisy krajowe nie regulowałyby natomiast istoty sztucznej inteligencji, lecz stosowanie jej rozwiązań w poszczególnym państwie, np. przez poszczególne organy ścigania, uwzględniając jednocześnie dotychczasowe przepisy unijne. Jednakże niezależnie od powyższego oprócz pozytywnych skutków wykorzystania sztucznej inteligencji kluczowym elementem jest uświadomienie społeczeństwu zagrożeń, jakie niesie za sobą jej działanie. W tym w szczególności możliwość wycieku danych osobowych czy popełnienia przez AI błędu, który mógłby nieść za sobą straszne konsekwencje dla danej jednostki, np. osoby, którą sztuczna inteligencja wskazałaby nietrafnie na podstawie porównania linii papilarnych zawartych w bazie danych z odciskami palców pobranymi w miejscu przestępstwa.

BIBLIOGRAFIA

AKTY PRAWNE:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. nr 119, s. 1 z późn. zm.).

2. Rezolucja Parlamentu Europejskiego z 6.10.2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych (2020/2016 (INI)).

LITERATURA:

1. Dziedzic K., Juszka K., *Kontrowersyjne nowe technologie w kryminalistyce*, „Studia Prawnoustrojowe" 2022, nr 55.

2. Haugeland J., *Artificial Intelligence: The Very Idea*, „Artificial Intelligence" 1986, nr 29, s. 349–353.

1. Kot E., *Opracowanie zaawansowanego technologicznie systemu informatycznego umożliwiającego zautomatyzowane przetwarzanie informacji zgromadzonych w kryminalistycznych biometrycznych bazach danych w celu zwalczania przestępstw lub identyfikacji osób*, „Problematyka Kryminalistyki" 2020.

2. Newslatter UODO dla Inspektorów Ochrony Danych, 2022.

3. Olbert P., *Sztuczna inteligencja i przestępczość przyszłości w kontekście kryminalistycznych badań informatycznych*, „Przegląd Policyjny" 2023.

4. Rich E., Knight K., *Artificial Intelligence*, New York 1990.

5. Rożnowska M., *Dobra osobiste sztucznej inteligencji, a doktrynalna ochrona dóbr osobistych – czy sztuczna inteligencja może być podmiotem dóbr osobowych?*, „Transformacje Prawa Prywatnego" 2023.

6. Rożnowski K., *Sztuczna inteligencja. Rozwój, szanse i zagrożenia*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007.

7. Zubańska M., *Kryminalistyka w dobie przyspieszenia naukowo-technicznego i technologicznego nadużyć – przytłaczająca wizja zmian, czy inspirująca do rozwoju?*, „Studia Prawnoustrojowe" 2021, nr 52.

ŹRÓDŁA INTERNETOWE:

1. Dębska A., *Własność intelektualna w cieniu dramatów ludzkich – cyberwojna na technologie, zalegalizowanie piractwa, niszczenie dziedzictwa kulturowego*, https://lgl-iplaw.pl/2022/03/wlasnosc-intelektualna-w-cieniu-dramatow-ludzkich-zniszczen-cyberwojna-na-technologie-zalegalizowanie-piractwa-niszczenie-dziedzictwa-kulturalnego/ (dostęp: 15.03.2024 r.).

2. Guo G., Ray A., Izydorczak M., Goldfeder J., Lipson H., Xu W., *Unveiling intra-person fingerprint similarity via deep contrastive learning*, Science Advances, https://www.science.org/doi/10.1126/sciadv.adi0329?adobe_mc=MCMID%3D56027468956561299854396479018955009130%7CMCORGID%3D242B6472541199F70A4C98A6%2540AdobeOrg%7CTS%3D1704897905 (dostęp: 15.03.2024 r.).

3. Łuczak O., *Wykorzystanie sztucznej inteligencji w kryminalistyce – czyli ile prawdy jest w filmach detektywistycznych?*, https://lgl-iplaw.pl/2023/07/wykorzystanie-sztucznej-inteligencji-w-kryminalistyce-czyli-ile-prawdy-jest-w-filmach-detektywistycznych/ (dostęp: 15.03.2024 r.).

4. Parlament Europejski, *Akt ws. sztucznej inteligencji: pierwsze przepisy regulujące sztuczną inteligencję*, https://www.europarl.europa.eu/topics/pl/article/20230601STO93804/akt-ws-sztucznej-inteligencji-pierwsze-przepisy-regulujace-ai (dostęp: 17.03.2024 r.).

STRESZCZENIE

W wyniku prężnego rozwoju nowych technologii wzrosła możliwość wykorzystania potencjału, jaki niesie za sobą sztuczna inteligencja. Możliwość jej wykorzystania wywarła piętno na licznych dziedzinach nauk, w tym na kryminalistyce. Niewątpliwie może ona pomóc organom wymiaru sprawiedliwości w sprawniejszym działaniu, np. poprzez pomoc w wykryciu sprawcy przestępstwa. Jednakże jej wykorzystanie budzi wiele kontrowersji. Wynika to przede wszystkim z faktu, iż mimo nowoczesności systemu, nie jest on w 100% doskonały i może popełniać błędy, tak samo jak każdy człowiek czy zaprogramowany system. Poniższy artykuł ma na celu ukazanie możliwości wykorzystania sztucznej inteligencji w kryminalistyce, jak również zagrożeń, jakie może nieść za sobą jej wykorzystanie. Niestety mimo licznych korzyści, jakie niesie za sobą sztuczna inteligencja, może ona spowodować wiele zagrożeń. Zatem jej pełne zastosowanie w ważnych sferach życia publicznego nie jest obecnie możliwe. Niniejsze opracowanie ma na celu zasygnalizowanie konieczności nie tyle stworzenia kolejnych regulacji prawnych związanych z działalnością sztucznej inteligencji, ile aktualizowania ich wraz z postępem technologicznym.

Słowa kluczowe: sztuczna inteligencja, kryminalistyka, postępowanie karne, identyfikacja twarzy, linie papilarne

ABSTRACT

As a result of the thriving development of new technologies, the possibility of exploiting the potential of artificial intelligence has increased. The possibility of its use has made its mark on numerous fields of science, including forensics. It is undeniable that it can help justice authorities to operate more efficiently, for example, by helping to detect the perpetrator of a crime. However, its use is controversial. This is mainly due to the fact that despite the modernity of the system, it is not 100% perfect and can make mistakes, just like any human or programmed system. The following article aims to show the possibilities of using artificial intelligence in forensics, as well as the risks that its use may bring. Unfortunately, despite the numerous benefits of artificial intelligence, it can cause many risks. Thus, its full application in important spheres of public life, is currently not possible. The purpose of this study is not so much to signal the need for further regulations related to the activities of artificial intelligence, but to update them with technological progress.

Keywords: artificial intelligence, forensics, criminal proceedings, facial identification face, fingerprints