**Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury**
*Quarterly of the National School of Judiciary and Public Prosecution*
Zeszyt 4 (56)/2024

**ARTYKUŁY**

# Czy obowiązujący kodeks karny nadąża za algorytmami sztucznej inteligencji?

DOI: 10.53024/8.4.56.2024

FILIP JERZY SZKIŁĄDŹ*

**Streszczenie**
Celem niniejszego opracowania jest odpowiedź na tytułowe pytanie, tj. w jakim zakresie obowiązujące przepisy kodeksu karnego są wystarczające wobec braku innych przepisów, w przypadku wykorzystywania algorytmu sztucznej inteligencji do popełnienia czynu zabronionego lub wystąpienia szkody. Powyższy problem nie był bezpośrednim przedmiotem innych badań. Należy jedynie wskazać, że w literaturze wskazuje się na ewentualne propozycje, iż w przypadku wystąpienia takiej konieczności, można posiłkować się wybranymi regulacjami kodeksu karnego. Nie mniej, dynamicznie zmieniająca się sytuacja prawna sztucznej inteligencji sugeruje, że należałoby dostosowywać przepisy do aktualnej pozycji tegoż systemu oraz jego wykorzystywania. Podkreślić należy, że stosowanie przepisów, które są przestarzałe i docelowo stworzone do innych przestępstw jest niezasadne i kłóciłoby się to z podstawowymi zasadami prawa karnego materialnego i procesowego. Przedmiotowe badania mają na celu weryfikację, na ile obecne przepisy kodeksu karnego można skutecznie wykorzystywać, a także na ile obowiązujące regulacje dają możliwość skutecznego przypisania odpowiedzialności właściwemu podmiotowi. Jednocześnie podkreślić należy, że negatywna odpowiedź na niniejsze wątpliwości będzie dowodziła, iż zasadnym jest natychmiastowe podjęcie prac w celu stworzenia odrębnych regulacji, czy też dodatkowych przepisów, które będą odpowiadały aktualnym potrzebom ustawodawczym. Szerokie pole algorytmu

* Filip Jerzy Szkiłądź, magister prawa, doktorant Szkoły Doktorskiej Uniwersytetu w Białymstoku, aplikant aplikacji sedziowskiej, ORCID: 0000-0003-3897-3927.

sztucznej inteligencji uzasadnia stwierdzenie, że właściwe regulacje są niezbędne, aby zapewnić bezpieczne i zgodne z literą prawa posługiwanie się tym fascynującym systemem.

**Słowa kluczowe:** sztuczna inteligencja, kodeks karny, właściwość przepisów

## 1. WPROWADZENIE

W obowiązujących ustawach prawa karnego próżno jest szukać jakichkolwiek definicji czy też odniesień dotyczących sztucznej inteligencji (SI)[1]. W części szczególnej kodeksu karnego można dostrzec jedynie pojedyncze przestępstwa komputerowe jak na przykład: oszustwa, wykorzystywanie złośliwych oprogramowań[2], a także inne o których więcej informacji pojawi się w rozwinięciu niniejszego opracowania.

Przedmiotowe rozważania należy rozpocząć stawiając jasną tezę, tj.: w obowiązujących przepisach prawa karnego, nie ma regulacji, które odpowiadają *stricte* czynom zabronionym popełnianym przez podmioty posługujące się algorytmami sztucznej inteligencji.

W obowiązującym stanie prawnym Unii Europejskiej mamy do czynienia jedynie z propozycją przepisów jak np. AI Act (Artificial Intelligence Act)[3], czyli pierwsza tego typu regulacja dotycząca sztucznej inteligencji. Ich skuteczne wejście w życie sprawi, że będą to pierwsze na świecie przepisy ogólne dotyczące stosowania algorytmów sztucznej inteligencji. W dużym uproszczeniu, projekt ma na celu ochronę podstawowych praw oraz bezkonfliktowe stosowanie przedmiotowego systemu. W projekcie uwzględniono wiele zabezpieczeń i wyjątków dotyczących aplikacji oraz zapewniono stosowne podziały tychże algorytmów. Nadmienić należy, że na wzór Unii Europejskiej podążają ta drogą także inne państwa. Joe Biden, prezydent Stanów Zjednoczonych, 30 października 2023 r. podpisał dekret dotyczący sztucznej inteligencji. *Order on Safe, Secure, and Trustworthy Artificial Intelligence*[4] ma wyznaczać nowe standardy dla bezpieczeństwa algorytmu AI, ochronę prywatności obywateli, ochronę podstawowych praw obywatelskich, ochronę konsumentów i pracowników oraz umacniać amerykańskie przywództwo na świecie[5]. Wśród różnych państw i instytucji występują także inne propozycje

---

1 W. Filipkowski, *Prawo karne wobec sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020, s. 117.

2 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. Nr 88, poz. 553).

3 Committee on artificial intelligence (CAI) Draft Framework Convention On Artificial Intelligence, Human Rights Democracy And The Rule Of Law. Council Of Europe. Strasburg 18 December.

4 https://www.whitehouse.gov/ „Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023".

5 *Ibidem*.

regulacji, porozumień, wstępnych umów, jak np. Międzynarodowa umowa w sprawie sztucznej inteligencji: Wspólne dążenie do bezpiecznych technologii[6].

Wobec powyższych propozycji usystematyzowania sytuacji prawnej systemów sztucznej inteligencji należy wskazać, że żadna z nich nie porusza kwestii odpowiedzialności karnej. Faktem jest, że odpowiedzialność karna nie jest na pierwszym miejscu jeśli chodzi o dostosowanie jej do bieżących potrzeb informatycznych czy też technologicznych. Można by rzec, że jest niejako marginalizowana. Prymat wiedzie w tej kwestii prawo cywilne, o czym świadczą nowelizacje w tym zakresie kodeksu postępowania cywilnego, dokonane już dekadę temu[7], wówczas gdy nowelizacje kodeksu postępowania karnego dotyczące elektronicznych doręczeń są przewidziane na 2029 r.[8]

Na potrzeby tego opracowania wskazać należy, że sztuczna inteligencja może być zarówno narzędziem w rękach sprawców, jak i przedmiotem wykonawczym czynu lub może zostać uznana jako „sprawca" przestępstwa[9]. Analizując sytuacje, w których można rozważać odpowiedzialność karną za szkody wyrządzone przez takie systemy, wymienić można je w kilku potencjalnych sytuacjach. Po pierwsze, wykorzystanie systemu jako narzędzia w rękach sprawcy w celu popełnienia czynu zabronionego. Po drugie, błąd w nadzorze lub kontroli nad systemem, który nie jest w pełni autonomiczny, a jego prawidłowe funkcjonowanie zależy od operatora. Po trzecie, brak reakcji człowieka, który pełni funkcję „bezpiecznika" w przypadku systemów w pełni autonomicznych[10]. Reasumując nieco powyższe rozważania, wskazać należy, że powyższa odpowiedzialność powinna polegać na dostosowaniu zasad odpowiedzialności karnej osoby fizycznej do rodzaju uwzględniającego lub nie udział człowieka w pętli decyzyjnej – wina w wyborze (*man in the loop*), nadzorze (*man on the loop*) lub wina osób dostarczających SI (*man out of the loop*)[11].

Niezwykle problematyczną kwestią w przedmiotowych badaniach zdaje się być zakwalifikowanie odpowiedzialności konkretnych podmiotów obecnych w całym lub części procesu wytworzenia, a następnie zbycia produktu, tj. gotowego już systemu. Wielość twórców, pośredników, sprzedawców jest kłopotliwa w tym

---

6 https://www.cisa.gov/ „Guidelines for Secure AI System Development, November 26, 2023".

7 Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. Nr 43, poz. 296).

8 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. Nr 89, poz. 555).

9 W. Filipkowski, *Kryminologiczne problemy sztucznej inteligencji – przyczynek do dyskusji*, [w:] *O wolność i prawo. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Rzeplińskiemu*, red. B. Błońska, Ł. Chojniak, B. Gruszczyńska, A. Kosyło, K. Witkowska-Rozpara, D. Woźniakowska-Fajst, Warszawa 2022.

10 R. Rejmaniak, *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, „Roczniki Nauk Prawnych" 2021, Tom XXXI, nr 3, s. 101-107.

11 W. Filipkowski, R. Rejmaniak, *Criminal Liability in the Context of the Functioning of a Smart City*, [w:] *Internet and New Technologies Law, Perspective and Challenges*, red. D. Szostek, M. Załucki. Nomos 2021, s. 304-305.

znaczeniu, że nie ma żadnych regulacji, które wykazałyby do kogo należy kierować potencjalne zarzuty.

Stosunkowo oczywistym zdaje się być fakt, że w przypadku bezpośredniego wykorzystywania systemu w celu popełnienia czynu zabronionego odpowiedzialność winien ponieść sprawca czynu. Za powyższą tezą przemawiają podstawowe zasady odpowiedzialności karnej zawarte w takich przepisach, jak art. 42 ust. 1 Konstytucji Rzeczypospolitej Polskiej[12] oraz art. 1 § 1 k.k. Problem pojawia się w przypadku wyrządzenia szkody, np. nieumyślnie lub wyłącznie przez autonomiczny system, który podlega bądź nie podlega czyjejś kontroli. Jako przykład niniejszego problemu można przytoczyć drony bojowe, których pierwotnym zadaniem jest wyeliminowanie określonego „celu" w postaci pojazdu wojskowego lub innego obiektu. Zatem co w przypadku, gdy ten dron niepoprawnie rozpozna obiekt, a następnie zniszczy zwykły pojazd cywilny bądź świadczący pomoc humanitarną, wyrządzając przy tym inne szkody. Kolejnym bardziej przyziemnym przykładem może być wyrządzenie szkody przez pojazd autonomiczny, który wskutek błędu w systemie spowodował wypadek. Takie przykłady były przedmiotem rozważań w literaturze[13]. Autorzy starają się skrupulatnie podejść do tych rozważań, jednak wobec braku stosownych regulacji prawnych, zagadnienia te są wciąż aktualne. Wobec powyższych zagadnień rozważać należy odpowiedzialność takich podmiotów jak: programista, deweloper, producent, osoby szkolące, wdrażające produkt, sprzedawca oraz zwykły klient.

Obowiązujące przepisy kodeksu karnego oraz innych ustaw nie dają żadnej odpowiedzi w przypadku powyższych problemów. Wobec przedmiotowych stanów faktycznych kreują się następujące problemy szczegółowe: w jakim zakresie przepisy kodeksu karnego są wystarczające w przypadku popełnienia czynów zabronionych z wykorzystaniem algorytmu sztucznej inteligencji, a także na ile obowiązujące regulacje dają możliwość skutecznego przypisania odpowiedzialności właściwemu podmiotowi?

W literaturze proponuje się rozwiązywać powyższe zagadnienia w oparciu o aktualnie obowiązujące przepisy kodeksu karnego. Jednocześnie na podstawie obecnych badań nie wskazuje się na realną potrzebę tworzenia odpowiednich regulacji[14]. Niniejsze opracowanie ma na celu sprawdzenie zasadności i aktualności tejże tezy. Kwestia odpowiedzialności prawnej w przypadku SI, jest na tyle dynamiczna i rozwojowa, że omawiane kwestie mogą zmieniać się niezwykle szybko. Wobec

---

[12] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483, ze zm.).

[13] J. Kaczmarek, A. Sampolski, *Wybrane zagadnienia odpowiedzialności karnej pojazdów autonomicznych*, „Monitor Prawniczy" 2018, nr 9; R. Rejmaniak, *Odpowiedzialność karna za skutki..., op. cit.*

[14] W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 122.

tego niniejsze badania mają na celu także uaktualnienie tegoż stanowiska. Tym samym w opracowaniu zostanie dokonana analiza znamion właściwych przepisów pod kątem możliwości ich zastosowania w odpowiednich przypadkach, odpowiedź na powyższe problemy badawcze, a także wskazanie, czy obecne przepisy kodeksu karnego rzeczywiście są wystarczające aby móc skutecznie, a także zgodnie z literą prawa rozstrzygać konkretne stany faktyczne.

## 2. POSZCZEGÓLNE REGULACJE KODEKSU KARNEGO A POTENCJALNA WŁAŚCIWOŚĆ ICH UŻYCIA W PRZYPADKU WYRZĄDZENIA SZKODY PRZEZ PODMIOT POSŁUGUJĄCY SIĘ SI

Na potrzeby niniejszych rozważań należy wskazać przepisy, które na chwilę obecną mogą służyć jako właściwe do rozpatrywania stosownych stanów faktycznych. W prawie karnym do przestępstw komputerowych zalicza się w szczególności czyny z art. 267 § 1 i 2, art. 268 § 2, art. 268a, art. 269 § 1 i 2, art. 269a, art. 269b, a także art. 287 k.k., czyli oszustwo komputerowe[15]. Nie oznacza to jednak, że zastosowanie każdego z powyższych przepisów można rozważać pod kątem ich użycia wobec stanów faktycznych związanych z SI. Tym samym, w literaturze wskazuje się jedynie na ich część[16]. Aby skutecznie zobrazować cel przedmiotowych badań, w pierwszej kolejności zostaną opisane wybrane przestępstwa, a dopiero później zostanie dokonana ich szczegółowa analiza:

1) zgodnie z art. 268a § 1 k.k. (szkoda w bazach danych), pierwsze zachowanie godzi w dostęp do danych informatycznych, a także polega na niszczeniu, uszkadzaniu, usuwaniu, zmianie oraz utrudnianiu dostępu do nich. Drugie i właściwie kluczowe wobec rozważań jest zachowanie, które polega na godzeniu w proces prawidłowego automatycznego przetwarzania[17], gromadzenia czy przekazywania danych informatycznych, np. przez zakłócanie, czy też uniemożliwienie tego procesu[18];
2) strona przedmiotowa art. 269 k.k., (sabotaż komputerowy), co do zasady polega na niszczeniu, uszkodzeniu, zmianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji czy też funkcjonowania administracji rządowej, w tym na zakłóceniu lub uniemożliwieniu automatycznego przetwarzania, gromadzenia bądź przekazywania danych wymienionych w tym przepisie. Jednocześnie podkreślić należy, że § 2 niniejszego

---

15 A. Marek, V. Konarska-Wrzosek, *Prawo karne*, Warszawa 2016, s. 580; M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7-8, s. 241 i n.

16 W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 117.

17 Pojęcie „automatyczności", które to zostanie szczegółowo opisane w dalszej części opracowania być może okazać się kluczowym rozstrzygnięciem wobec przedmiotowych rozważań ponieważ próżno jest usilnie dokonywać subsumpcji w przypadku gdy znamiona przestępstwa nie odpowiadają elementarnym znaczeniom wobec algorytmów SI.

18 S. Hoc, Art. 268a, [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2023/Legalis.

przepisu polega na dopuszczeniu się czynu określonego w § 1 przez niszczenie lub wymianę informatycznego nośnika danych bądź niszczenie lub uszkodzenie urządzenia służącego do automatycznego przetwarzania, gromadzenia bądź przekazywania danych informatycznych[19];

3) art. 287 k.k. (oszustwo komputerowe) – znamiona tego czynu polegają na bezprawnym wpływaniu na automatyczne przetwarzanie danych oraz bez upoważnienia na przetwarzanie, gromadzenie lub przekazywanie danych informatycznych. Ponadto może polegać na zmianie lub usunięciu danych istniejących w systemie informatycznym. Może również przybrać postać wprowadzenia nowych danych do systemu informatycznego, a to wszystko w celu osiągnięcia korzyści majątkowej;
4) art. 269b k.k. (bezprawne wykorzystywanie programów i danych), polega na wytwarzaniu narzędzi hakerskich, które są efektem działalności sprawcy, wykonywaną wyłącznie przez działanie, pozyskiwanie oznaczające uzyskanie dostępu do narzędzi gotowych. Zbywanie, polegające na przeniesieniu narzędzi na inną osobę a także udostępnianie, co oznacza, że sprawca zachowuje władztwo czy dostęp do takich narzędzi[20].

Tytułem wyjaśnienia zasadnym jest nawiązanie do cech wspólnych powyższych przestępstw. Mianowicie niemalże wszystkie dotyczą automatycznego przetwarzania, a także naruszenia danych informatycznych. W tym kontekście rozważać można, czy wspomniane już terminy są odpowiednie w przypadku nowych technologii, w tym algorytmów SI. Zgodnie z dyspozycją art. 1 lit. b Konwencji o cyberprzestępczości[21], „dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny[22]. Tym samym można uznać, że powyższe pojęcie odnosi się także do algorytmów SI[23].

Problemy interpretacyjne pojawiają się w przypadku pojęcia automatyczności w rozumieniu powyższych przepisów. Na samym początku rozważań, należy wskazać, że autonomiczność nie jest równoznaczna z automatyzmem. Są to dwa różne pojęcia, których nie należy używać zamiennie[24]. Ciekawe ujęcie porównaw-

---

19 S. Hoc, Art. 269, [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2023/Legalis.

20 R.G. Hałas, art. 269b, [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2021/Legalis.

21 Konwencja Rady Europy o cyberpczestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).

22 F. Radoniewicz, *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, „Cybersecurity and Law" 2022, vol. 8, nr 2, s. 149 i n.

23 W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 119.

24 K. Kowalczewska, *Sztuczna inteligencja na wojnie. Perspektywa MPHKZ. Przypadek autonomicznych systemów śmiercionośnej broni*, Warszawa 2021, s. 33 i n.

cze w tym zakresie można dostrzec w literaturze przedmiotu[25], gdzie „system automatyczny" oznacza iż, przyszłe działania są możliwe do przewidzenia, gdyż nie ma możliwości odmiennej reakcji. Nieco odmiennie prezentuje się kwestia „systemów zautomatyzowanych", gdyż tu możliwość działania jest większa, jednakże ograniczona do sytuacji, które zostały uprzednio zaprogramowane[26]. W przypadku „systemów autonomicznych", które zostały obdarowane wysokim poziomem decyzyjności w środowisku, często trudno przewidzieć efekt działań[27]. Powyższe wnioski są bardzo zastanawiające wobec potencjalnej możliwości stosowania tychże przepisów w przypadku pojawienia się takiej potrzeby. Przy ścisłym założeniu, że należy precyzyjnie przestrzegać sensu pojedynczych znamion, wówczas dostępne przepisy nie mogą być stosowane. Jednakże w literaturze wskazuje się na mniej rygorystyczne podejście w tym zakresie[28]. Tłumaczy się bowiem pojęcie automatyczny również jako działający samoczynnie, za pomocą odpowiedniego urządzenia lub wykonywany za pomocą automatu. Wskazując że w przypadku sztucznej inteligencji automatyzacja bez wątpienia znajduje się na wysokim poziomie[29], można dokonać powyższej interpretacji w ten sposób, lecz jedynie warunkowo. Autor niniejszego opracowania skłania się bardziej ku ścisłej interpretacji pojęć „automatyczny" mając na uwadze niemożność stosowania tego pojęcia zamiennie z „autonomiczny".

W literaturze dostrzega się także możliwość wykorzystywania innych przepisów, niezwiązanych bezpośrednio z przestępczością komputerową. Dość kontrowersyjne założenia pojawiły się w przypadku naruszenia prawa przez działanie autonomicznego robota bojowego[30]. Zgodzić należy się ze stwierdzeniem, że jego działania, autoryzowane przez człowieka, są przedłużeniem woli i działań operatora, gdyż sam robot nie decyduje o podjęciu określonego działania. Sam zaś system jest jedynie narzędziem w rękach człowieka.[31] W przypadku gdy człowiek sprawuje jedynie nadzór nad robotem oraz w przypadku robotów autonomicznych przyjęto nieco odmienne stanowisko. Propozycje w tym zakresie opierają się na wykorzystaniu konstrukcji odpowiedzialności karnej za szkody spowodowane przez zwierzęta, z akcentem na odpowiedzialność gwaranta nienastąpienia negatywnego skutku w przypadku braku umyślności[32]. Odchodząc nieco od przedmiotowych rozważań, wskazać należy na ciekawe spostrzeżenie w literaturze, że robot może

---

25 *Ibidem*.
26 K. Kowalczewska, *Sztuczna inteligencja na wojnie, op. cit.*, s. 33 i n.
27 *Ibidem*.
28 W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 117 i n.
29 *Ibidem*.
30 R. Rejmaniak, *Odpowiedzialność karna za skutki..., op. cit.*, s. 35.
31 W. Filipkowski, *Criminal Law and Artificial Intelligence – Selected Aspects*, [w:] *Legal and Technical Aspects of Artificial Intelligence*, red. L. Lai, M. Świerczyński, Warszawa 2020, s. 118.
32 R. Rejmaniak, *Odpowiedzialność karna za skutki..., op. cit.*, s. 38.

być traktowany w przypadku odpowiedzialności karnej jak narzędzie, np. broń palna, nóż[33]. Wobec braku ogólnych regulacji w tym zakresie mogą to być bardzo pouczające wnioski względem przyszłych regulacji dotyczących odpowiedzialności karnej.

Interesującą koncepcją jest również możliwość zastosowania przepisów rozdziału XVI k.k., czyli „Przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne". W literaturze rozważania toczą się nad możliwością zastosowania art. 123 § 1 pkt 4 k.k. w przypadku zabicia ludności cywilnej poprzez działanie autonomicznego robota bojowego[34]. Należy zgodzić się z powyższą tezą, zważywszy na fakt, że ustawodawca nie wyszczególnia jakimi narzędziami czy też w jaki sposób ma dojść do zabójstwa. Wobec powyższego nadzorujący powinien, w przypadku spełnienia innych przesłanek prawem przewidzianych, ponosić odpowiedzialność jako gwarant.

Z punktu widzenia obowiązujących regulacji wobec stanów faktycznych z udziałem algorytmu SI bardzo istotną funkcję pełni art. 2 k.k. Zgodnie z brzmieniem tego przepisu, odpowiedzialność karną za przestępstwo skutkowe popełnione przez zaniechanie ponosi ten, na kim ciążył prawny i szczególny obowiązek zapobiegnięcia skutkowi. Instytucja ta jest niejako określana „gwarantem"[35]. Interpretując odniesienia zawarte w literaturze[36], zauważyć należy, że możliwe jest traktowanie osoby upoważnionej do nadzorowania urządzenia jako wyżej zdefiniowanego gwaranta. To na tej osobie zwykle ciąży szczególny i prawny obowiązek zapobiegnięcia skutkowi popełnienia czynu zabronionego. Ponadto wskazać należy, że zgodnie z literą prawa, gwarant może ponosić odpowiedzialność tylko za zawinione nie zapobiegnięcie skutkowi. Z praktycznego punktu widzenia może to rodzić swego rodzaju problemy interpretacyjne wobec algorytmów SI. Udowodnienie winy w tym zakresie może stać się swego rodzaju wyzwaniem oraz będzie wymagało wiedzy specjalistycznej z zakresu prawa karnego, a także informatyki. Tym samym wskazać należy, że algorytmy SI są poniekąd stworzone do tego aby działać dynamicznie i natychmiast[37].

Aby uzmysłowić sobie istotę problemu należy zaprezentować przykładowy stan faktyczny. Autonomiczny dron porusza się zgodnie z wyznaczoną mu trasą. W trakcie lotu napotyka przeszkodę w postaci zmierzającego w jego kierunku dużego ptaka. Dron wykonuje gwałtowny manewr, w wyniku którego uderzył w budynek, po czym spada z dużą prędkością uderzając w dziecko, które wskutek

---

33 *Ibidem*, s. 35.
34 R. Rejmaniak, *Odpowiedzialność karna za skutki..., op. cit.*, s. 38.
35 A. Grześkowiak, art. 2 k.k, [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2024/Legalis.
36 R. Rejmaniak, *Odpowiedzialność karna za skutki..., op. cit.*, s. 37.
37 W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 121.

zdarzenia straciło życie. Przeanalizować należy w tym przykładzie, a tym samym także w kontekście instytucji gwaranta. Po pierwsze, czy, a jeśli tak, to kto nadzorował poruszający się obiekt, po drugie, czy mógł zapobiec tej szkodzie, po trzecie, dlaczego tego nie zrobił. Jeżeli w trakcie postępowania dowodowego by stwierdzono, że system działał na tyle szybko, iż człowiek nie był w stanie zareagować ze względów naturalnych, wówczas zgodnie z podstawowymi zasadami prawa karnego nie powinien on ponosić odpowiedzialności karnej. Kwestia moralności nie pozwala jednoznacznie stwierdzić, że nikt nie powinien ponosić odpowiedzialności z tego punktu widzenia. Waga problemu sugeruje, że jakkolwiek powinno to zostać uregulowane. Dlatego tak ważne jest badanie przedmiotowych zdarzeń z punktu widzenia odpowiedzialności karnej. Niniejsze badanie z całkowitą dozą pewności należy pogłębiać w dalszych opracowaniach.

Wobec zaprezentowanego przykładu należy poruszyć kwestię, która z praktycznego punktu widzenia również okazuje się być istotna. Mowa o stronie podmiotowej czynu, tj. umyślności oraz nieumyślności [38]. Wskazać należy, że wskazywane uprzednio przestępstwa mogą być popełnione jedynie umyślnie. Tym samym w literaturze w razie potrzeby wskazuje się pewnego rodzaju potencjalne odstępstwa, poprzez wykorzystanie art. 155, art. 156 § 2, a także art. 157 § 3 k.k.[39]. Wszystkie te teorie są jedynie propozycjami, gdyż – jak wskazano wyżej – sytuacja prawna SI w prawie karnym nie jest w żaden sposób uregulowana. Wobec tego każda potencjalna koncepcja przybliża świat nauk prawnych do pewności prawa w tym zakresie.

Na początku niniejszego opracowania wskazano problem dotyczący sprawcy. Obowiązujące przepisy nie wskazują, kto dokładnie powinien ponosić odpowiedzialność w powyższych stanach faktycznych. Uznać należy, że ogólne zasady wynikające z art. 1 k.k.[40], są po prostu niewystarczające w rozumieniu podmiotów posługujących się algorytmami SI. Właśnie dlatego tak ważne jest umiejętne określenie udziału człowieka w pętli decyzyjnej. W trakcie procesu powstawania, programowania, sprzedaży i finalnie korzystania z urządzenia bierze udział kilka, często kilkanaście lub kilkadziesiąt osób. Jak skutecznie przypisać kwestię odpowiedzialności? Na to pytanie nie ma odpowiedzi wśród przepisów kodeksu karnego oraz innych ustaw. Między innymi z tego powodu istniejący pogląd w literaturze dotyczący braku potrzeby tworzenia nowych odmian przestępstw powinien zostać zaktualizowany[41].

---

38 W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 114.
39 R. Rejmaniak, *Odpowiedzialność karna za skutki..., op. cit.*, s. 39.
40 A .Marek, V. Konarska-Wrzosek, *Rozdział IV. Ustawa karna, jej budowa i stosowanie. Prawo karne*, Warszawa 2016, s. 56.
41 W. Filipkowski, *Criminal Law and Artificial Intelligence…, op. cit.*, s. 121.

Abstrahując od powyższych rozważań należy wyraźnie podkreślić, że każde z wymienionych przestępstw zostało skonstruowane przez ustawodawcę w pierwotnie innym zamiarze. Z całkowitą pewnością, tworząc przedmiotowe przepisy nie przewidywano ich warunkowego wykorzystywania w innych ewentualnych przypadkach. Nie bez powodu doświadczamy regularnych nowelizacji, często takich, które marginalnie różnią się od poprzedniego brzmienia przepisu. Wobec tego, niezasadnym byłoby lekceważenie aktualnej sytuacji SI wobec odpowiedzialności karnej. Ponadto wiele państw, a także organizacji aktualnie zmaga się z dostosowaniem prawa do sytuacji jakie tworzy obecność sztucznej inteligencji. Ustawodawcy dostosowują prawo cywilne i ogólne zasady, ponieważ SI będzie wkrótce czymś znacznie więcej niż algorytmem, który usprawnia funkcjonowanie ich użytkownikom.

## 3. WNIOSKI PŁYNĄCE Z NINIEJSZYCH ROZWAŻAŃ ORAZ PROPOZYCJE USTAWODAWCZE

Tytułem odpowiedzi na powyższe pytania badawcze: powyżej wskazane regulacje mogą być na chwilę obecną wykorzystywane w obecnym stanie prawnym, jednakże nie należy tracić z pola widzenia konieczności poczynienia postępów związanych ze stworzeniem nowych rozwiązań ustawodawczych. Dopuszczalna możliwość wynika z tego, że w obecnym stanie prawnym nie ma żadnych regulacji, które swą pierwotną istotą mogłyby dotyczyć algorytmów SI. Jest to nieco odmienne stanowisko od obecnie wskazywanych w literaturze gdzie przyjmuje się się, iż tworzenie nowych typów czynów zabronionych nie jest konieczne[42]. Za powyższym stwierdzeniem stoi argument dotyczący wzrostu zainteresowania przedmiotową problematyką, a tym samym rosnącymi problemami w tym zakresie[43].

Zgodzić należy się z autorami literatury, że obecne regulacje mogą być na chwilę obecną podstawą wymiaru sprawiedliwości w konkretnych przypadkach. Nie oznacza to jednak, że nie są potrzebne zmiany w tym zakresie. Jednocześnie należy wyraźnie podkreślić, iż nie jest konieczna jak najszybsza rewolucyjna zmiana kodeksu karnego oraz innych ustaw karnych. Faktem jest, że dynamiczna sytuacja prawna SI doprowadzi do tego, iż w przypadku braku stosownych regulacji, stany faktyczne będą rozstrzygane w oparciu o powyższe regulacje. Zaznaczyć należy, że przy poprawnym posługiwaniu się obecnymi instrumentami prawnymi powyższe nie będzie stanowiło błędu skutkującego podstawą odwoławczą w rozumieniu art. 428 k.p.k., ani bezwzględną przyczyną odwoławczą w rozumieniu art. 439 § 1

---

42 *Ibidem*; zob. także: W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 122.

43 K. Mamak, K. Kowalczewska, *Military robots should not look like a humans*, "Ethics and Information Technology" 2023, 25(3), s. 42.

k.p.k., gdyż sądy będą musiały opierać swoje rozstrzygnięcie na jakiejś podstawie. Przy założeniu, że nie będą naruszane elementarne zasady prawa karnego w postaci zakazu stosowania analogii i wykładni rozszerzającej subsumpcja będzie prawidłowa. Jednakże, jeżeli dojdzie do pierwszych tego typu naruszeń wówczas będzie to jednoznaczny sygnał, iż obecne regulacje przestały być wystarczające i będą konieczne jak najszybsze zmiany ustawodawcze.

Niektóre stany faktyczne z użyciem algorytmów SI, winno rozwiązywać się wyłącznie w oparciu o dotychczasowe przepisy. Za przykład można wskazać rozsyłanie złośliwych oprogramowań, które algorytm nadaje wskazanym adresatom. Wówczas będzie miał zastosowanie art. 269a k.k., który został szczegółowo opisany powyżej. Tu podkreślić należy, że sam fakt wykorzystania tejże technologii nie uzasadnia natychmiastowej potrzeby wykorzystania nowych regulacji skierowanych wyłącznie do podmiotów posługujących się algorytmami SI. To stan faktyczny, przesłanki i znamiona przestępstwa są niejako wskaźnikiem poprawnej subsumpcji. Niestety należy porzucić utopijne nadzieje, że każdy stan faktyczny z wykorzystaniem algorytmu SI będzie można rozstrzygać w oparciu o obowiązujące przepisy.

Jak wskazano wyżej, problematyka dotycząca strony podmiotowej jest aktualnie istotnym brakiem wobec analizowanych stanów faktycznych[44]. Wskazane przepisy, które sugeruje się stosować warunkowo w przedmiotowych przypadkach można popełnić jedynie umyślnie. Wobec powyższego, zgodnie z art. 9 § 1 k.k.[45], czyn sprawcy może być przestępstwem wyłącznie, gdy ma on zamiar jego popełnienia czy też przewidując możliwość jego popełnienia na to się godzi[46]. Tym samym, dokonując oczywistej analizy, należy wyraźnie podkreślić, że w przypadku gdy zachowanie będzie miało charakter nieumyślny, wówczas sprawca nie realizuje znamion strony podmiotowej i nie popełnia przestępstwa. Podstawowe zasady prawa karnego sugerują takowe zakończenie tegoż problemu. Wówczas należy rozważać inne dopuszczalne formy odpowiedzialności, jak np. cywilna czy administracyjna.

Ciekawym rozwiązaniem byłoby uregulowanie odpowiedzialności w przedmiotowym zakresie w oparciu o przepisy dotyczące produktów niebezpiecznych. Rozważania dotyczące tejże propozycji pojawiło się już dotychczas w literaturze[47]. Wówczas zastosowanie miałyby przepisy kodeksu cywilnego, tj. art. $449^1$-$449^{10}$ k.c.[48]. Jak wynika z dostępnych źródeł, powyższa propozycja jest uzasadniona potencjalną

---

44 W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, op. cit.*, s. 114.

45 A. Marek, V. Konarska-Wrzosek, *Rozdział III. Strona podmiotowa przestępstwa. Wina i jej formy. Prawo karne*, Warszawa 2016, s. 135.

46 R. Rejmaniak, *Odpowiedzialność karna za skutki..., op. cit.*, s. 39.

47 J. M. Kondek, *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję. Uwagi de lege i de lege ferenda*, Warszawa 2021. s. 6-9.

48 Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. Nr 16 poz. 93).

interpretacją dyrektywy Rady 85/374/EWG z 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących odpowiedzialności za produkty wadliwe[49]. Przedmiotowa odpowiedzialność za produkt miałaby zostać rozszerzona na oprogramowanie[50].

Naturalnie powyższe zasady prawa karnego, w tym głównie *nullum crimen sine lege*, są podstawowymi wyznacznikami w tymże zakresie. Należy się jednak zastanowić, czy nie warto byłoby rozszerzyć część szczególną kodeksu karnego o dodatkowe przepisy lub typy przestępstw. Z ustawodawczego punktu widzenia, jeżeli czyn zabroniony został popełniony nieumyślnie, a czyn można popełnić wyłącznie umyślnie, to wówczas sprawca nie popełnia przestępstwa. Wewnętrzna moralność sugeruje jednak, że powinny być przypadki, gdy nieumyślność również powinna zostać penalizowana. Wobec tych przesłanek można wskazać np. szkodę w wielkich rozmiarach, przypadek wystąpienia szkody na dużą skalę oddziaływania, spowodowanie skutków o rażącym charakterze, np. śmierć. W powyższych przypadkach nieumyślne popełnienie czynu mogłoby skutecznie realizować funkcję sankcjonowania zgodnie z podstawowymi zasadami prawa karnego. Pod uwagę należy brać także kwestię wyłączenia winy w całym procesie tworzenia produktu, gdyż wówczas sprawca nie popełnia przestępstwa.

Tytułowe zagadnienie jest niezwykle trudne z ustawodawczego punktu widzenia. Niniejsze opracowanie dowodzi, że na chwilę obecną obowiązujące regulacje prawne są warunkowo wystarczające, aby skutecznie i zgodnie z literą prawa rozwiązywać stany faktyczne z udziałem algorytmów SI. Nie mniej, ogólna sytuacja związana z pojęciem sztucznej inteligencji jest na tyle dynamiczna, że nie można zamykać się na nowe propozycje w tym zakresie. Prace nad powstawaniem nowych regulacji karnych są więc koniecznością. Jak wskazuje się w przedmiotowej literaturze[51], w przyszłości doświadczymy braku odpowiedzialności karnej w tym zakresie. Ponadto nieaktualne prawodawstwo być może będzie czynnikiem hamującym w przypadku rozwoju technologicznego i sztucznej inteligencji[52].

Niniejszy temat dotyczący odpowiedzialności karnej w związku z algorytmami sztucznej inteligencji jest aktualnie czymś nowym w naukach prawnych. Tym samym wskazać należy, że niniejszy przedmiot badań z pewnością będzie stopniowo aktualizowany. Jednocześnie, z dużą dozą prawdopodobieństwa przedmiotowe wnioski będą się różnić wraz z upływem czasu. Jednoznaczna odpowiedź o treści

---

[49] Dyrektywa Rady z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz. Urz. WE L 210, s. 29, ze zm.).

[50] J.M. Kondek, *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję, op. cit.*, s. 6, zob. także: M. Jagielska, [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa 2020, s. 75.

[51] K. Mamak, *Prawo karne przyszłości*, Warszawa 2017, s. 83.

[52] S. Traczyk, *Aktualne problemy prawa karnego*, [w:] *Problemy Prawa w XXI wieku. Aspekty Teoretyczne i Praktyczne*, A. Koman, A. Szyszka (red.), Kielce-Lublin 2020, s. 93 i n.

„tak" lub „nie" na tytułowe pytanie nie jest możliwa. Właśnie dlatego niniejsze opracowanie wykazało w jakim zakresie aktualne regulacje prawne są właściwe aby skutecznie rozwiązywać stany prawne z użyciem algorytmów SI.

## BIBLIOGRAFIA

### Akty prawne

Committee on artificial intelligence (CAI) Draft Framework Convention On Artificial Intelligence, Human Rights Democracy And The Rule Of Law. Council Of Europe. Strasburg 18 December.
Dyrektywa Rady z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz. Urz. WE L 210, s. 29 ze zm.).
Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483, ze zm.).
Konwencja Rady Europy o cyberpczestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).
Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. Nr 43, poz. 296).
Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. Nr 16, poz. 93).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. Nr 88, poz. 553).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. Nr 89, poz. 555).

### Literatura

Filipkowski W., *Criminal Law and Artificial Intelligence – Selected Aspects*, [w:] *Legal and Technical Aspects of Artificial Intelligence*, red. L. Lai, M. Świerczyński, Warszawa 2020.
Filipkowski W., *Kryminologiczne problemy sztucznej inteligencji – przyczynek do dyskusji* [w:] *O wolność i prawo. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Rzeplińskiemu*, red. B. Błońska, Ł. Chojniak, B. Gruszczyńska, A. Kosyło, K. Witkowska-Rozpara, D. Woźniakowska-Fajst, Warszawa 2022.
Filipkowski W., *Prawo karne wobec sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa 2020.
Filipkowski W., Rejmaniak R., *Criminal Liability in the Context of the Functioning of a Smart City*, [w:] *Internet and New Technologies Law, Perspective and Challenges*, red. D. Szostek, M. Załucki. Nomos 2021.
Grześkowiak A., art. 2 k.k, [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak. Warszawa 2024/ Legalis.
Hałas R.G., art. 269b, [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2021/Legalis.
Hoc S., Art. 268a, [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2023/Legalis.
Jagielska M., [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa 2020.
Kaczmarek J., Sampolski A., *Wybrane zagadnienia odpowiedzialności karnej pojazdów autonomicznych*, „Monitor Prawniczy 2018, nr 9.
Kondek J.M., *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję. Uwagi de lege i de lege ferenda*, Warszawa 2021.
Kowalczewska K., *Sztuczna inteligencja na wojnie. Perspektywa MPHKZ. Przypadek autonomicznych systemów śmiercionośnej broni*, Warszawa 2021.
Mamak K., Kowalczewska K., *Military robots should not look like a humans*, "Ethics and Information Technology" 2023, 25(3).
Mamak K., *Prawo karne przyszłości*, Warszawa 2017.
Marek A., V. Konarska-Wrzosek*, Prawo karne*, Warszawa 2016.
Traczyk S., *Aktualne problemy prawa karnego*, [w:] *Problemy Prawa w XXI wieku. Aspekty Teoretyczne i Praktyczne*, A. Koman, A. Szyszka (red.), Kielce-Lublin 2020.

Radoniewicz F., *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, „Cybersecurity and Law" 2022, 8 nr 2.
Rejmaniak R., *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, „Roczniki Nauk Prawnych" 2021, Tom XXXI, nr 3.
Rejmaniak R., *Odpowiedzialność karna za skutki spowodowane przez autonomiczne roboty bojowe – zarys problemu*, [w:] *Wykorzystanie dronów i robotów w systemach bezpieczeństwa. Wybrane aspekty*, red. R. Kamprowski, M. Skarżyński, Poznań 2019.
Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7-8.

### Źródła internetowe

https://www.cisa.gov/ „Guidelines for Secure AI System Development, November 26, 2023".
https://www.whitehouse.gov/ „Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023"

## Can the current criminal code keep up with artificial intelligence algorithms?

### Summary

The purpose of this study is to answer the title question, i.e. to what extent the existing provisions of the Criminal Code are sufficient, in the absence of other provisions, in the case of the use of an artificial intelligence algorithm to commit a criminal act or the occurrence of damage. The above problem has not been the direct subject of other studies. It should only be pointed out that the literature points to possible proposals where, if necessary, selected regulations of the Criminal Code can be used. Nevertheless, the dynamically changing legal situation of artificial intelligence suggests that it would be necessary to adapt the regulations to the current position of the system and its use. It should be emphasized that the application of regulations that are outdated and ultimately created for other crimes is unjustified and would conflict with the basic principles of substantive and procedural criminal law. The research in question is aimed at verifying to what extent the current provisions of the Criminal Code can be used effectively, as well as to what extent the current regulations provide the opportunity to effectively attribute responsibility to the relevant entity. At the same time, it should be emphasized that a negative answer to the current questions will prove that it is reasonable to immediately undertake an effort to create separate regulations, or additional provisions that will meet current legislative needs. The wide field of activity of the artificial intelligence algorithm justifies the statement that appropriate regulations are necessary to ensure that this fascinating system is used safely and in accordance with the letter of the law.

**Keywords:** artificial intelligence, criminal code, jurisdiction of laws