t. LXXVI • nr 12/2023 (906) • DOI 10.33226/0137-5490.2023.12.3

Dr hab. Dariusz Szostek, prof. UŚ

Uniwersytet Śląski w Katowicach
ORCID: 0000-0002-8924-6969
e-mail: dariusz.szostek@us.edu.pl

Dr hab. inż. Paweł Kasprowski, prof. PŚ

Politechnika Śląska w Gliwicach
ORCID: 0000-0002-2090-335X
e-mail: pawel.kasprowski@polsl.pl

Problematyka prawnej kontroli algorytmów

Problems of legal control of algorithms

Streszczenie

Coraz częściej prawo jest implementowane w kodach algorytmicznych, czego przykładem jest np. smart kontrakt. Od lat mamy instytucje oraz procedury odnoszące się do kontroli prawa. Pojawia się zatem pytanie badawcze, czy w związku z coraz częstszym łączeniem prawa z algorytmami nie powinniśmy wprowadzić kontroli algorytmów, przynajmniej tych, które mogą wpływać na prawa i obowiązki człowieka. W niektórych państwach już dzisiaj powstają organy monitorujące implementację prawa w algorytmach. Czy Polska nie powinna pójść w ich ślady?

Słowa kluczowe: algorytm, implementacja prawa w kodach, smart kontrakt, sztuczna inteligencja, LegalTech, odpowiedzialność za funkcjonowanie algorytmów

Abstract

Increasingly, law is being implemented in algorithmic codes, an example of which is the smart contract. For years we have had institutions and procedures relating to the control of law. Therefore the research question arises whether, in connection with the increasing combination of law with algorithms, we should not introduce control of algorithms, at least those that may affect human rights and obligations. Some countries already have bodies monitoring the implementation of law into algorithms. Shouldn't Poland follow in their footsteps?

Keywords: algorithm, implementation of law in codes, smart contract, artificial intelligence, LegalTech, responsibility for algorithm performance

JEL: K20, K24

„W poniższym tekście poruszane są zagadnienia związane z wyzwaniem regulacji algorytmów w kontekście rosnącego znaczenia sztucznej inteligencji i innych algorytmów w różnych dziedzinach, w tym prawnej. W artykule podnosi się iż Polska wciąż odstaje w wykorzystaniu technologii prawnych (LegalTech) w porównaniu do krajów zachodnich. W pracy omówiono koncepcję prawa w kodzie algorytmicznym, wskazując, że coraz częściej przepisy prawne są implementowane w postaci kodów programistycznych czytelnych dla maszyn. Przejście od prawa w tradycyjnej formule do prawa jako kodu staje się rzeczywistością. Kody i algorytmy pełnią coraz większą rolę w podejmowaniu decyzji i mają potencjalne skutki prawne dla obywateli. Z tego powodu podniesiono kwestię konieczności kontroli tych algorytmów oraz wprowadzenia regulacji w tym zakresie. W kontekście kontroli kodu w środowisku informatycznym, wskazano na istniejące narzędzia i techniki testowania poprawności kodu, które są powszechnie stosowane w programowaniu. Jednakże, w umowach i dokumentach prawnych rzadko uwzględnia się wymagania dotyczące testowania oprogramowania. Wykazano, że regulacje prawne powinny uwzględniać zasady testowania i kontroli poprawności kodu, zwłaszcza w przypadku oprogramowania używanego w kluczowych dziedzinach. Podsumowując, tekst porusza kwestię potrzeby regulacji i kontroli algorytmów oraz implementacji prawa w kodzie”[1].

"The following text addresses the challenge of regulating algorithms in the context of the growing importance of artificial intelligence and other algorithms in various fields, including legal. The paper argues that Poland is still lagging behind Western countries in the use of legal technologies (LegalTech). The paper discusses the concept of law in algorithmic code, pointing out that more and more legal regulations are implemented in the form of machine-readable programming codes. The shift from law in the traditional formula to law as code is becoming a reality. Codes and algorithms are playing an increasingly important role in decision-making and have potential legal implications for citizens. For this reason, the need to control these algorithms and to regulate them has been raised. In the context of code control in the IT environment, existing tools and techniques for testing the correctness of code that are commonly used in programming were pointed out. However, software testing requirements are rarely included in contracts and legal documents. It is shown that legal regulations should take into account the principles of testing and code correctness control, especially for software used in key domains. In conclusion, the text addresses the need for regulation and control of algorithms and implementation of law in code."

Wprowadzenie

Wyzwaniem trzeciej dekady XX w., i to nie tylko dla prawników, staje się konieczność regulacji sposobu korzystania zarówno z tzw. sztucznej inteligencji, jak również z innych algorytmów. Coraz większy automatyzm dokonywanych czynności w sferze faktycznej, prawnej, jak chociażby w obszarze decyzji administracyjnych, bądź w obszarze prawa prywatnego (nie tylko smart kontrakty, ale także tokenizacja procesów, wykorzystanie uczenia maszynowego w kancelariach prawnych bądź w wymiarze sprawiedliwości) czy w sferze finansów (compliance, dopuszczalność wykorzystania systemów AI w finansach i inne) nasuwa pytanie, czy należy kontrolować lub audytować algorytmy, w których zaimplementowane są reguły prawne, i kto powinien to robić.

Polska w chwili obecnej pozostaje mocno w tyle w wykorzystaniu algorytmów w tak zwanym LegalTech (Wagner, 2020, s. 2; Grupp, 2014, s. 660–665; Hartung i in., 2018, s. 5; Szostek (Red.), 2021, s. 3 i n.), czyli w zakresie powiązania prawa i technologii. W większości organizacji, w tym w kancelariach prawnych, wykorzystywane są narzędzia LegalTech 1.0 (technologia wspierająca prawników, ale także biznes), rzadziej LegalTech 2.0 (zastępowanie czynności ludzi zautomatyzowanymi systemami, wykorzystanie bardziej złożonych algorytmów)[2]. Natomiast LegalTech 3.0, charakteryzujący się nie tylko automatyzacją podejmowania decyzji, ale także możliwością podejmowania autonomicznych decyzji, w tym mających skutki prawne dla człowieka, w Polsce praktycznie nie jest wykorzystywany, co najwyżej w projektach badawczych czy też w pilotażach. W Polsce, jak pokazuje *Raport LegalTech 2022* (C.H.Beck, 2022), prawnicy skupiają się na „zwykłej komunikacji" elektronicznej i wykorzystaniu kwalifikowanego podpisu elektronicznego, a 40% polskich prawników w ogóle nie jest zainteresowanych narzędziami LegalTech[3]. Natomiast zachodni prawnicy rozwoju branży upatrują w tokenizacji, w automatyzacji procesów, szerokim wykorzystywaniu narzędzi sztucznej inteligencji[4], blockchainu czy też smart kontraktów. Różnica w zaawansowaniu technologicznym i podejściu polskich oraz zachodnich prawników jest tu wyraźnie widoczna.

Prawo w kodzie algorytmicznym

W zachodniej doktrynie coraz częściej wskazuje się na problematykę kodu jako prawa, czy też kwestie związane z implementacją prawa w kodzie (Lessig, 1999, s. 3 i n.; Reidenberg, 1998, s. 553 i n.). W Polsce zagadnienie to nie jest szerzej dyskutowane[5].

Koncepcja prof. L. Lessiga (1999, s. 3 i n.), że kodeks jest prawem, a system prawny składa się w pewnej części z „puzli", które można ze sobą łączyć i formować, m.in. w cyberprzestrzeni, staje się w dzisiejszych czasach rzeczywistością. Nie jest to już koncepcja teoretyczna, ale ma postać faktycznie realizowanych projektów, w których język ludzki – używany do tej pory do informowania społeczeństwa o zasadach prawnych, których należy przestrzegać – jest zastępowany kodami programistycznymi czytelnymi dla maszyn wyposażonych w procesory i bezpośrednio przez nie wykonywanymi. Taki proces odbywa się bez transkrypcji kodu komputerowego na symbole, litery, słowa, frazy i zdania w sposób, który nie może być bezpośrednio postrzegany przez ludzi[6]. Przepis prawny lub umowa zaczyna funkcjonować jako program komputerowy, a nie jako tekst, w którym przepisy prawne są złożone z liter i znaków interpunkcyjnych przedstawionych w języku naturalnym[7]. Klasycznym przykładem takiej sytuacji jest smart kontrakt (Szostek, 2018 s. 113 i n.; Kowacz & Wielgus, 2021, s. 15 i n. oraz cytowana tam literatura). Prawo i technologia coraz intensywniej współdziałają[8] ze sobą poprzez złożony system relacji i korelacji, gdyż obie te sfery przyczyniają się do regulacji zachowań podmiotów, gdzie prawo reguluje takie elementy jak system nakazów i zakazów, a kody programowe stanowią faktyczne ograniczenie wolności tych[9], którzy korzystają z niego w cyberprzestrzeni (Szpringer, 2018, s. 40). Do tej pory kodeksy ograniczały głównie wolność osób działających w cyberprzestrzeni. Można postawić pytanie, dlaczego nie mogą ograniczyć kodów, w tym sztucznej inteligencji.

Zachodni naukowcy wskazują na kod jako architekturę cyberprzestrzeni, a fragmenty kodu jako element konstrukcyjny takiej architektury. Wszystko, co widzimy w Internecie, jest dostarczane za pomocą kodu, tylko kod może pozwolić na obecność reguł społecznych w cyberprzestrzeni. W ten sposób kod działa również jako regulator (Schrebak, 2014).

Funkcje kodów w cyberprzestrzeni w podobny sposób opisuje L. Lessig. Twierdzi, że cyberprzestrzeń nie jest strefą pełnej wolności. Jest regulowana. Autor stwierdza, że „tym regulatorem jest kod – oprogramowanie i sprzęt, które sprawiają, że cyberprzestrzeń jest taka, jaka jest. Ten kod lub architektura określa warunki, w których doświadczane jest życie w cyberprzestrzeni. Określa, jak łatwo jest chronić prywatność lub jak łatwo jest cenzurować mowę. Określa, czy dostęp do informacji jest ogólny, czy też informacje są strefowane. Wpływa na to, kto i co widzi lub co jest monitorowane i niewidzialne. Kod reguluje cyberprzestrzeń w sposób, którego nie można zobaczyć, dopóki nie zacznie się rozumieć natury tego kodu. Zmienia się kod cyberprzestrzeni. A ponieważ ten kod się zmienia (Fenwick i in., 2018, s. 88), zmieni się również charakter cyberprzestrzeni" (Lessig, 2000).

Kontrolujemy regulacje prawne, mając rozbudowane narzędzia oraz instytucje kontrolne. Nie mieliśmy jednak dotychczas zaawansowanych narzędzi ani też procedur w zakresie kontroli kodów algorytmicznych, do których coraz częściej może być implementowane prawo[10]. Dlatego w UE coraz poważniej dyskutuje się nad problem nie tylko odpowiedzialności za kody[11], ale także nad zagadnieniem ich kontroli. Ewoluuje również koncepcja transkrypcji prawa na kody, co jest związane z przejściem doktrynalnym od rozważań *lex informatica* do *lex cryptographia*, na co zwracają uwagę m.in. G. Wood i in., wykazując, iż nowe ujęcie powoduje realizację prawa jako kodu (Wood i in., 2014). Już 25 lat temu, gdy algorytmizacja oraz wykorzystanie kodów w sferze prawnej ledwo raczkowały, M. S. Miller zwracał uwagę na rozpoczynający się proces odchodzenia od

prawa w tradycyjnej formule na rzecz jego implementacji, jak to wówczas wskazywał, w „nowych technologiach”[12]. Zauważał, iż zmniejszać się będzie znaczenie prawa jako takiego w budowaniu globalnego zaufania globalnego społeczeństwa, a wzrastać będzie rola technik bezpieczeństwa czy, jak to dzisiaj określamy, cyberbezpieczeństwa, w tym kryptografii (Miller, 1997).

Kody, algorytmy – jak wskazano na wstępie – wykorzystywane są w wielu sferach, w tym także prawnych. Należy w związku z tym postawić pytanie badawcze: „Skoro kontrolujemy prawo, a przynajmniej mamy procedury, które w demokratycznym kraju umożliwiają kontrolę prawa, to czy w przypadku jego implementacji w kodach nie należałoby podobnej kontroli poddawać algorytmy, zawierające regulacje prawne czy umowy?”.

Przez lata algorytmy były uznawane wyłącznie jako nośnik, a co za tym idzie – nie podlegały jakimkolwiek regułom czy też kontroli. Tyle że w ostatnich latach z nośnika stają się coraz częściej, zwłaszcza w ramach LegalTech 2.0 lub 3.0, narzędziem podejmującym decyzje, czy też będącym umową mającą znaczenie, a nawet skutki prawne dla obywatela. Błąd w ich funkcjonowaniu może skutkować poważnymi, może nawet nieodwracalnymi, konsekwencjami i to nie tylko finansowymi. Z tego też powodu zarówno w całej Unii Europejskiej, jak i w niektórych państwach członkowskich wprowadza się regulacje umożliwiające, przynajmniej w szczególnych sytuacjach, kontrolowanie algorytmów.

Zagadnienie kontroli kodu w środowisku informatycznym

Zagadnienie kontroli poprawności działania kodu jest obecne w środowisku informatycznym od momentu powstania pierwszych programów. Każdy programista wie, że bez narzędzi do testowania poprawności nie da się napisać kodu, który będzie spełniać określone wymagania. Istnieje wiele sposobów testowania kodu jak np.: testowanie jednostkowe (testowanie konkretnych elementów kodu – metod, klas), testowanie integracyjne (kontrola poprawności współpracy różnych modułów kodu) czy testowanie akceptacyjne (wykonywane zwykle przez końcowego odbiorcę). Ważne są także testowanie wydajnościowe czy tak zwane smoke testy – testowanie granic wydajności systemu[13].

Istnieje cały zbiór narzędzi do testowania oraz technik mówiących, co i jak należy testować, aby zminimalizować prawdopodobieństwo błędu. Pomimo istniejących formalizmów i opracowanych technologii z nieznanych powodów wymagania dotyczące procedur opracowywania i przeprowadzania testów są rzadko włączane do dokumentów prawnych związanych z umowami pomiędzy podmiotami gospodarczymi. Często pozostawia się w nich tylko ogólne zapisy mówiące o „zagwarantowaniu należytej staranności” wykonania oprogramowania, co jest później trudne do udowodnienia (lub obalenia) w przypadku sporów prawnych. Z tego powodu można wskazać wiele przypadków, w których oprogramowanie wykorzystywane do obsługi krytycznych operacji nie spełniało wymagań i powodowało błędy (na przykład podczas wyborów samorządowych w Polsce w 2014 r.[14]).

Wydaje się, że wprowadzenie regulacji prawnych opartych na istniejących i znanych w środowisku informatycznym zasadach testowania i kontroli poprawności kodu powinno rozwiązać wiele problemów związanych z oprogramowaniem użytkowanym w kluczowych dla gospodarki czy zdrowia ludzi dziedzinach – tym bardziej, że oprogramowanie to coraz bardziej wpływa na nasze życie. Niestety sytuacja nie jest taka prosta w przypadku aplikacji i systemów wykorzystujących mechanizmy popularnie określane jako „sztuczna inteligencja”. Tego typu systemy nie są klasycznymi aplikacjami, których działanie jest z góry definiowane przez programistę. W klasycznej aplikacji to programista tworzy całą logikę systemu – to on decyduje, jak system ma działać dla każdego rodzaju danych wejściowych. W przeciwieństwie do tego systemy „sztucznej inteligencji” nie są z góry zaprogramowane. Ich cechą charakterystyczną jest uczenie się na podstawie dostarczonych danych. Z tego powodu ich zachowanie dla wprowadzonych konkretnych danych nie jest z góry zdeterminowane. Powoduje to, że testowanie takich aplikacji jest znacznie trudniejsze i nie zostało jeszcze sformalizowane. Wydaje się, że powinno to być jedno z ważnych zadań dla programistów w najbliższej przyszłości.

Kontrola kodów – nakreślenie problemu

Problematykę weryfikacji czy też kontroli kodów należy na potrzeby niniejszego artykułu rozpatrywać co najmniej na dwóch płaszczyznach: prywatnoprawnej oraz publicznoprawnej. Sfera publicznoprawna jest obecnie coraz mocniej rozbudowywana. W monografii LegalTech wskazano na cztery podejścia w tendencjach regulacyjnych odnośnie do kontroli kodów (Szostek (Red.), 2021, s. 31 i n.). W opracowanym raporcie A. Hook wymienia (Hook, b.d.):

1) podejście *wait and see*, czyli wyczekiwanie na obowiązek regulacyjny wynikający z przepisów wspólnotowych – brak systemowego podejścia do problematyki LegalTech, brak instytucji kontrolnych;

2) negację oraz zakaz stosowania niektórych rodzajów technologii przy ograniczeniu ich dostępu do rynku internetowych usług prawniczych (np. Taiwan Bar Association zabroniło uczestniczenia swoim członkom w giełdach usług prawniczych);

3) próbę rozszerzenia aktualnie obowiązujących regulacji w celu objęcia nimi problemu kontroli nad sektorem LegalTech, a także nad kodami;

4) wprowadzenie instytucji oraz regulacji prawnych mających na celu możliwość kontroli kodów.

Coraz częściej w regulacjach unijnych, czasem pośrednio, wskazuje się na konieczność kontroli algorytmów, a przynajmniej wprowadzenie ich rozliczalności. Nie dotyczy to wszystkich kodów i algorytmów, ale określonych w odpo-

wiednich sektorach prawa. Podział ten nie jest związany z klasycznym podziałem prawa na gałęzie, ale raczej z segmentami regulacyjnymi, których dotyczy. Powstają też wyspecjalizowane organy państwowe, o czym dalej, których celem jest nadzór nad niektórymi algorytmami.

Unia Europejska dostrzegła problem kontroli kodów i podjęła w tym zakresie szereg działań legislacyjnych. W wielu dokumentach wskazała na potrzebę przejrzystości i rozliczalności – początkowo algorytmów działających jako AI, a ostatecznie także innych algorytmów. Wskazywano na to m.in. w przyjętej 16.02.2017 r. przez Parlament Europejski rezolucji w sprawie przepisów prawa cywilnego w dziedzinie robotyki oraz AI, w rezolucji Parlamentu Europejskiego i Rady z 20.10.2020 r. zawierającej rekomendacje dla Komisji Europejskiej w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (AI), w publikacji Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania (Komisja Europejska, 2020), a bardziej wyczerpująco w raporcie *Getting the Future Right. Artificial Intelligence and Fundamental Right* (European Union Agency for Fundamental Rights, (2020), wskazując na konieczność uwzględniania przy tworzeniu algorytmów: godności człowieka, prawa do prywatności i ochrony danych, prawa dostępu do wymiaru sprawiedliwości, równości i niedyskryminacji oraz ochrony konsumentów. W jednym z najnowszych raportów Komisji Europejskiej pt. *Study on Safety and Liability Related Aspects of Software* (European Commission, 2021b), przygotowanym przez prof. Ch. Wenderhorst wskazano rekomendacje dla regulacji algorytmów:

1) wprowadzenie nowego, półhoryzontalnego i opartego na analizie ryzyka systemu bezpieczeństwa oprogramowania (wraz z dalszymi krokami w celu modernizacji dorobku prawnego w zakresie bezpieczeństwa),

2) przegląd dyrektywy w sprawie odpowiedzialności za produkty,

3) wprowadzenie nowych ram regulacyjnych dla sztucznej inteligencji,

4) wprowadzenie nowego instrumentu dotyczącego odpowiedzialności za sztuczną inteligencję,

5) kontynuowanie kontroli sprawności cyfrowej całego dorobku prawnego.

Szczególnie warte przytoczenia jest uzasadnienie: „Prawodawca europejski powinien wprowadzić nowy system bezpieczeństwa oprogramowania. System ten miałby charakter półhoryzontalny, ponieważ miałby zastosowanie do oprogramowania (np. wbudowanego, dodatkowego lub samodzielnego) w bardzo szerokim i neutralnym technologicznie znaczeniu, obejmującym np. SaaS. Przezwyciężyłoby to niedociągnięcia w istniejącym prawodawstwie dotyczącym bezpieczeństwa, które albo nie obejmuje oprogramowania, w szczególności oprogramowania samodzielnego, albo jest słabo wyposażone do obsługi oprogramowania. Prawodawca europejski mógłby zatem rozważyć wprowadzenie nowej dyrektywy w sprawie bezpieczeństwa oprogramowania (SSD), której musiałyby towarzyszyć wybrane dalsze kroki w kierunku modernizacji dorobku prawnego w zakresie bezpieczeństwa.

Związek SSD z istniejącym i przyszłym prawodawstwem sektorowym opierałby się na komplementarności. Dyrektywa SSD zajmowałaby się kwestiami przekrojowymi, takimi jak rozgraniczenie między produktami z elementami oprogramowania, oprogramowaniem dodatkowym dla innych produktów i samodzielnym oprogramowaniem, które w odmienny sposób współdziała z innymi produktami, oraz podziałem odpowiedzialności między różnymi producentami w obu przypadkach. Dotyczyłaby ochrony prywatności już w fazie projektowania, cyberbezpieczeństwa, obowiązków w zakresie nadzoru po wprowadzeniu do obrotu, kwestii pojawiających się w kontekście aktualizacji i podobnych zagadnień" (European Commission, 2021b).

Unia Europejska nie tylko w raportach i rekomendacjach odnosi się do regulacji i kontroli kodów algorytmicznych. W najnowszych projektach legislacyjnych – wprost proponuje odpowiednie rozwiązania. W chwili obecnej na szczególną uwagę zasługują: wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie produktów maszynowych (European Commission, 2021a), wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt prawny o sztucznej inteligencji) i zmieniającego niektóre unijne akty ustawodawcze (European Parliament, 2023)[15] oraz wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia ram europejskiej tożsamości cyfrowej (Komisja Europejska, 2021).

W praktyce już od dawna obowiązują przepisy dotyczące kontroli, czy też audytu algorytmów. Jednym z nich jest Rozporządzenie eIDAS[16], w ramach którego wprowadzono tryb kontroli, ale równocześnie nałożono obowiązek ich przeprowadzania odnośnie do kwalifikowanych usług zaufanych, w tym systemów informatycznych, w jakich usługi te są świadczone. Badaniu podlega sama usługa, ale także jej zgodność z przepisami wspólnotowymi, przepisami wykonawczymi oraz kody służące jej świadczeniu. Następuje tu kontrola nie tylko dokumentacji, ale także systemu informatycznego. W konsekwencji zaudytowana usługa uzyskuje status prawny kwalifikowanej usługi zaufanej, a co za tym idzie, zostaje powiązana z domniemaniami prawnymi. Takie rozwiązanie należy uznać za słuszne. Odpowiada ono z jednej strony bezpieczeństwu, w tym cyberbezpieczeństwu i bezpieczeństwu prawnemu, z drugiej strony wychodzi naprzeciw potrzebom nie tylko społeczeństw, ale także państw członkowskich. Algorytmy te są akceptowane przez państwa członkowskie i funkcjonują w powiązaniu z prawem w systemach krajowych. Przykładem są chociażby domniemania prawne związane z kwalifikowanym podpisem elektronicznym, kwalifikowaną pieczęcią elektroniczną, kwalifikowanym doręczeniem, a w niedługim czasie – z kwalifikowanymi atrybutami czy też European ID.

Także na poziomie krajowym wprowadzane są coraz częściej regulacje, a za nimi – instytucje mające na celu kontrolę algorytmów. Przykładem jest Malta Digital Innovation Authority – MDIA (Maltański Urząd Nadzoru Cyfrowych Innowacji) będący odpowiednikiem maltańskiego regulatora

tradycyjnego rynku finansowego. Zadaniem MDIA jest m.in. kontrola kodów źródłowych dla smart kontraktów (czyli algorytmów), na podstawie której jest wydawana decyzja o przyznaniu lub odmowie wydania licencji, a także audyt kodów źródłowych DAO, wykorzystywanych przez podmioty, które chcą legalnie działać na terytorium Malty.

Innym przykładem jest hiszpańska Agencja Nadzoru Sztucznej Inteligencji (Spanish AI Agency). Powstała ona w 2022 r. i jest odpowiedzialna za nadzór oraz monitorowanie projektów w ramach Hiszpańskiej Narodowej Strategii AI[17].

Podobne organy będą musiały w niedalekiej przyszłości powstać także w innych państwach, do czego zobliguje je AI Act. Państwa członkowskie będą zobowiązane do ustanowienia lub wyznaczenia właściwego organu krajowego na potrzeby stosowania i wdrażania AI Act (art. 59 projektu rozporządzenia). Dlatego zasadne wydaje się rozpoczęcie w Polsce dyskusji nad ustawieniem takiego organu oraz określeniem jego struktury, kompetencji, w tym kontrolnych, w odniesieniu do określonych przepisami prawa algorytmów. Kwestia jest o tyle istotna, iż z jednej strony istnieje konieczność zapewnienia odpowiedniego nadzoru, a z drugiej – zapewnienie swobody kontraktów, a także neutralności oraz bezstronności. Organy wskazane w AI Act będą miały w kompetencjach nadzór nad niektórymi algorytmami zarówno wykorzystywanymi w administracji, jak i używanymi przez podmioty prywatne.

Podsumowanie

Problematyka implementacji prawa w kodach algorytmicznych jest rozpatrywana od ponad 25 lat. Jednakże dopiero teraz z etapu koncepcji teoretyczno-prawnej przeszła do etapu realizacji w praktyce. Wydaje się, iż w Polsce w kontekście nie tylko nowych, wymuszających pewne działania, regulacji unijnych, ale w ogóle w interesie polskiego społeczeństwa, a także przejrzystości prawa, w tym implementowanego w kodach algorytmicznych, konieczna jest debata nad wprowadzeniem regulacji krajowej oraz niezależnej, mającej odpowiedni autorytet, instytucji nadzorującej. Niniejszy artykuł należy traktować jako głos zaledwie wszczynający dyskusję.

Przypisy/Notes

[1] Niniejszy tekst (oznaczony jako cytat) został wygenerowany przez ChatGPT na podstawie przygotowanego przez nas artykułu. Wykorzystywanie ChatGPT w zakresie tworzenia publikacji wykracza poza zakres niniejszej publikacji. Wskazuje jednakże na konieczność kontroli kodów algorytmicznych, także typu generative AI, którego przykładem jest ChatGPT.

[2] W zakresie wykorzystania LegalTech 2.0 prym wiodą instytucje finansowe, w tym banki (zob. WIB PAB, 2022).

[3] Szerzej https://legalis.pl/raport-legaltech-2022/ (pobrano 22.06.2023).

[4] Szerzej https://www.wolterskluwer.com/pl-pl/know/future-ready-lawyer-2022 (pobrano 23.05.2023).

[5] Warto w tym miejscu wskazać na publikację M. Araszkiewicza (2011, s. 55 i n.).

[6] Zwrócono na to uwagę w literaturze już przeszło 20 lat temu – zob. Wiebe, 2002, s. 350; Szostek, 2004, s. 39.

[7] Więcej o transkrypcji języka mówionego na kody algorytmiczne – zob. Araszkiewicz, 2021, s. 55 i n.

[8] Przykładem może być analiza prawidłowego wdrożenia 42 dyrektyw w Irlandii, Luksemburgu i we Włoszech przeprowadzona przez system ekspercki (Nanda i in., 2019, s. 1999 i n.). Zobacz także Boulet i in., 2018, s. 23 i n.

[9] Transformacja prawa w kody programistyczne to nowa dyscyplina naukowa, która łączy prawo i informatykę i tym samym tworzy tzw. LegalTech. Szerzej: Schrebak, 2014, s. 1–33; Corrales i in., 2019, s. 5 i n.

[10] Problematyka ta nadaje się na osobne omówienie, w niniejszym artykule jest jedynie wzmiankowana.

[11] Już sama kwestia pojęć jest bardzo zagmatwana. Tytułem przykładu można wskazać chociażby na problem definicji algorytmu, która nie jest jednolita nawet w sferze informatycznej. Ostatecznie reguły dotyczące kontroli mają charakter opisowy, a zakazy czy też nakazy związane z algorytmami dotyczą nie tyle samych algorytmów, ile celów przez nie osiąganych lub sposobu ich osiągnięcia. Problem jest o wiele szerszy, na co wskazuje chociażby brak jednolitej definicji programów czy też kodów programistycznych w prawie nie tylko krajowym, ale również europejskim.

[12] Pojęcie także niedookreślone.

[13] https://udigroup.pl/blog/testowanie-oprogramowania-typy-rodzaje-poziomy/ (pobrano 12.05.2023).

[14] https://niebezpiecznik.pl/post/problemy-w-pkw-zliczanie-glosow-wyborcow-sie-opoznia-zawiodl-system-informatyczny/ (pobrano 12.05.2023).

[15] W dniu 14.06.2023 r. Parlament Europejski przyjął stanowisko negocjacyjne w sprawie aktu o sztucznej inteligencji. Zob. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html (pobrano 2.07.2023).

[16] Rozporządzenie Parlamentu Europejskiego I Rady (UE) nr 910/2014 z dnia 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014R0910&from=PL (pobrano 22.01.2023).

[17] https://espanadigital.gob.es/lineas-de-actuacion/agencia-nacional-de-supervision-de-la-inteligencia-artificial (pobrano 26.02.2023).

Bibliografia/References

Araszkiewicz, M. (2021). Algorytmizacja myślenia prawniczego. Modele, możliwości, ograniczenia. W: D. Szostek (Red.), *LegalTech*. C.H.Beck.

Boulet, R., Mazzega, P., & Bourcier, D. (2018). Network approach to the French system of legal codes. Part II: The role of the weights in a network. *Artificial Intelligence and Law*, *26*. https://doi.org/10.1007/s10506-017-9204-y

C.H.Beck (2022). *Raport LegalTech 2022*. Legalis.

Corrales, M., Fenwick, M., & Haapio, H. (2019). *LegalTech, Smart Contracts and Blockchain*. Springer. https://doi.org/10.1007/978-981-13-6086-2

European Commission. (2021a). *Proposal for a Regulation of the European Parliament and of the Council on machinery products*. https://ec.europa.eu/docsroom/documents/45508 (pobrano 5.02.2023).

European Commission. (2021b). *Study on Safety and Liability Related Aspects of Software*. https://digital-strategy.ec.europa.eu/en/library/study-safety-and-liability-related-aspects-software (pobrano 7.04.2023).

European Union Agency for Fundamental Rights. (2020). *Getting the Future Right. Artificial Intelligence and Fundamental Right*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf (pobrano 8.03.2023).
Fenwick, M., Vermeulen, E. P. M., & Corrales, M. (2018). Business and Regulatory Responses to Artificial Intelligence: Dynamic regulation, innovation ecosystems and the strategic management of disruptive technology. W: M. Corrales, M. Fenwick, & N. Forgó (Red.), *Robotics, AI and the future of law*. Springer. https://doi.org/10.1007/978-981-13-2874-9
Grupp, M. (2014). Legal tech – impulse für Streitbeilegung und Rechtsdienstleistung. *Anwaltsblatt*, (8–9).
Hartung, M., Bues, M., & Halblieb, G. (2018). *Legal tech. How Technology is Changing the Legal World*. C.H.Beck.
Hook, A. (b.d.). *The Use and Regulation of Technology in the Legal Sector beyond England and Wales*. https://www.legalservicesboard.org.uk/wp-content/uploads/2019/07/International-AH-Report-VfP-4-Jul-2019.pdf (pobrano 22.01.2023).
Komisja Europejska. (2020). *Biała księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania*. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (pobrano 7.02.2023).
Komisja Europejska. (2021). *Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej*. https://op.europa.eu/pl/publication-detail/-/publication/5d88943a-c458-11eb-a925-01aa75ed71a1/language-en/format-PDF/source-search (pobrano 6.02.2023).
Kowacz, K., & Wielgus, K. (2021). *Smart kontrakty w prawie umów*. Księgarnia Akademicka Publishing. https://doi.org/10.12797/9788381385107
Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.
Lessig, L. (2000). Code is Law. On Liberty in Cyberspace. *Harvard Magazine*. https://harvardmagazine.com/2000/01/code-is-law-html (pobrano 19.04.2022).
Miller, M. S. (1997). *The Future of Law*. http://www.caplet.com/security/futurelaw/tsld001.htm (pobrano 23.01.2023).
Nanda, R., Siragusa, G., Di Caro, L., Boella, G., Grossio, L., Gerbaudo, M., & Costamanga, F. (2019). Unsupervised and supervised text similarity systems for automated identification of national implementing measures of European Directives. *Artificial Intelligence and Law*, *27*.
Reidenberg, J. (1998). Lex Informatica: The formulation of information policy rules through technology. *Texas Law Review*, (76).
Rozporządzenie Parlamentu Europejskiego I Rady (UE) NR 910/2014 z dnia 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014R0910&from=PL (pobrano 22.01.2023).
Schrebak, S. (2014). *Integrating Computer Science into Legal Discipline: The Rise of Legal Programming*. http://dx.doi.org/10.2139/ssrn.2496094
Szostek, D. (2004). *Czynność prawna a środki komunikacji elektronicznej*. Zakamycze.
Szostek, D. (2018). *Blockchain a prawo*. C.H.Beck.
Szostek, D. (Red.) (2021). *LegalTech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym kancelarii oraz dziale prawnym*. C.H.Beck.
Szpringer, W. (2018). *Blockchain jako innowacja systemowa. Od Internetu informacji do wartości Internetu. Wyzwania dla sektora finansowego*. Poltext.
Wagner, J. (2020). *Legal Tech und Legal Robots. Der Wandel im Rechtswesen durch neue Technologien und Kunsliche Intelligenz*. Springer Gabler.
WIB PAB (2022). *Zastosowanie Sztucznej Inteligencji w Bankowości – szanse oraz zagrożenia*. Warszawski Instytut Bankowości – Program Analityczno-Badawczy. https://us.edu.pl/pierwszy-w-ue-raport-dot-wplywu-ai-i-nowych-regulacji-prawnych-na-rynek-fintech/ (pobrano 22.06.2023).
Wiebe, A. (2002). *Die elektronische Willenserklarung*. Mohr Siebeck.
Wood, G. i in. (2014). *Ethereum: A secure decentralized generalised transaction ledger*. Ethereum Project Yellow Paper, No. 151, 1–32. https://gavwood.com/paper.pdf, (pobrano 23.04.2023).

Dr hab. Dariusz Szostek, prof. UŚ

Profesor Wydziału Prawa i Administracji Uniwersytetu Śląskiego, dyrektor Centrum Cyber Science (wspólne centrum UŚ, UE, PŚ oraz NASK), partner i założyciel kancelarii Szostek_Bar i Partnerzy. Członek PAN Katowice, ekspert Obserwatorium Sztucznej Inteligencji Parlamentu Europejskiego; ekspert, wykładowca, autor wielu publikacji w tym zagranicznych, m.in. monografii *Blockchain a prawo* (2018), *Blockchain and the Law* (2019), *LegalTech* (2020) i innych.

Dr hab. Dariusz Szostek, prof. UŚ

Professor at the Faculty of Law and Administration of the University of Silesia, Director of the Cyber Science Center (joint center of the University of Silesia, UE, PŚ and NASK), partner and founder of the Szostek_Bar and Partners Law Firm. Member of the Polish Academy of Sciences Katowice, expert of the Artificial Intelligence Observatory of the European Parliament; expert, lecturer, author of many publications, including foreign ones, i.a. monographs: *Blockchain a prawo* (2018), *Blockchain and the Law* (2019), *LegalTech* (2020) and others.

Dr hab. inż. Paweł Kasprowski, prof. PŚ

Naukowiec, trener, programista. W branży od 1995 r. (firma Paulosoft). Wiele projektów z czołowymi polskimi firmami (ComArch, Polkomtel, Wasko itp.). Profesor nadzwyczajny Politechniki Śląskiej. Uczelniany koordynator Priorytetowego Obszaru Badawczego: Sztuczna Inteligencja i Przetwarzanie Danych, koordynator uczelniany kierunku informatyka. Doświadczenie w bazach danych, eksploracji danych i uczeniu głębokim. Specjalizacja: analiza Eye Tracking.

Dr hab. inż. Paweł Kasprowski, prof. PŚ

Researcher, trainer, programmer. In business since 1995 (Paulosoft company). A lot of projects with the leading Polish companies (ComArch, Polkomtel, Wasko, etc.). Associate professor at the Silesian University of Technology. University coordinator of the Priority Research Area: Artificial Intelligence and Data Processing, university coordinator of the computer science (informatics). Experience in databases, data mining, and deep learning. Specialization: eye tracking analysis.