Cybersecurity and Law

2026 Nr 1(16) Numer specjalny

DOI: 10.35467/cal/226782

Bezpieczeństwo narodowe jako „strefa wolna od prawa" dla rozwoju i eksploracji sztucznej inteligencji

National security as a "law-free zone" for the development and exploration of artificial intelligence

Justyna KUREK-SOBIERAJ
Akademia Sztuki Wojennej
ORCID: 0000-0002-8754-5243
E-mail: j.kurek@akademia.mil.pl

Streszczenie

Sztuczna inteligencja wywiera wpływ na każdy obszar naszego życia a związane z nią skutki wydają się nie możliwe do przewidzenia. Uwzględniając potencjał i ryzyko związane z rozwojem AI na przykład w obszarze praw autorskich, ochrony danych osobowych czy praw własności intelektualnej, stworzenie już na wstępnym etapie rozwoju narzędzi i systemów AI kompleksowej regulacji prawnej, uwzględniającej potencjał sztucznej inteligencji, wydaje się jedynym słusznym rozwiązaniem. Ramy prawne dla rozwoju i stosowania AI stanowi unijne rozporządzenie. Implikacją tej konstrukcji jest pozostawienie całkowicie poza prawną regulacją sfer, które wyłączone są z zakresu zastosowania prawa europejskiego. Celem artykułu jest wskazanie na te wyjątki oraz postawienie pytań o konsekwencje takiego rozwiązania dla zastosowań w obszarach wojskowych, obronności i bezpieczeństwa narodowego. W artykule postawione są pytania o to, czy faktycznie pozostawienie tych obszarów zastosowania narzędzi AI poza prawną kontrolą jest rozwiązaniem pożądanym zarówno z punktu widzenia praw obywatelskich, jak i bezpieczeństwa państwa, czy może konieczna jest autonomiczna regulacja w prawie krajowym oparta o unijny wzorzec jako standard minimalny.

Słowa kluczowe
bezpieczeństwo narodowe, sztuczna inteligencja, modele AI, systemy AI

Abstract

Artificial intelligence impacts every area of our lives, and its consequences seem unpredictable. Considering the potential and risks associated with AI development, for example, in the areas of copyright, personal data protection, and intellectual property rights, creating comprehensive legal regulations that address the potential of AI at the initial stage of development seems the only appropriate solution. An EU regulation provides the legal framework for the development and application of AI. This construction implies that areas excluded from the scope of European law are completely beyond legal regulation. The aim of this article is to highlight these exceptions and raise questions

about the consequences of such a solution for applications in military, defense, and national security. The article asks whether leaving these areas of AI application beyond legal control is truly desirable from the perspective of both civil rights and national security, or whether autonomous regulation in national law, based on the EU model as a minimum standard, is necessary.

Keywords

national security, artifical intellogance, AI models, AI systems

Uwagi ogólne

Od dawna żadna technologia nie wywoływało tylu sprzecznych reakcji społecznych. Z jednej strony - sztuczna inteligencja postrzegana jest jako zjawisko, które ma szanse zrewolucjonizować każdy obszar naszego życia, z drugiej strony - liczne obawy wiążą się z faktem, iż efekty tej rewolucji nie są możliwe do przewidzenia. Stąd za tak istotne uważa się, aby rozwój sztucznej inteligencji od samego początku objęty był szczegółową regulacją, która ukierunkowana jest na stworzenie ram dla kontrolowanego rozwoju technologii, zapewniającej ramy dla bezpiecznego i etycznego[1] korzystania z technologii AI[2], rozwijania technologii przy jednoczesnym dostosowaniu jej do podstawowych praw obywatelskich Unii Europejskiej. Jak wskazano w Konkluzjach Nadzwyczajnego Posiedzenia Rady Europejskiej, „UE musi znaleźć się w światowej czołówce, jeśli chodzi o rozwój bezpiecznej, godnej zaufania i etycznej sztucznej inteligencji”[3]. Biorąc pod uwagę, iż znajdujemy się na początku zastosowań sztucznej inteligencji a narzędzia AI są w zasadzie w fazie rozwoju, zasadne wydaje się postawienie pytań czy rzeczywiście tak wczesna regulacje przyczyni się do wsparcia obserwowanej rewolucji cyfrowej[4] i nie doprowadzi *de facto* do „zabicia innowacji w zarodku”[5]. Uwzględniając potencjał i ryzyko związane z rozwojem AI na przykład w obszarze praw autorskich, ochrony danych osobowych czy praw własności intelektualnej, stworzenie na tym etapie regulacji prawnej, uwzględniającej potencjał sztucznej inteligencji, wydaje się jedynym słusznym rozwiązaniem[6].

Zgodnie z przyjętym modelem, ramy prawne dla rozwoju i stosowania AI stanowi unijne rozporządzenia. Implikacją tej konstrukcji jest pozostawienie

---

[1] W. Drobny, Źródła norm etycznych przy stosowaniu sztucznej inteligencji w służbie publicznej (zarys problemu z perspektywy teoretycznoprawnej) [w:] G. Sibiga (red.), Wpływ Aktu w sprawie sztucznej inteligencji na funkcjonowanie administracji publicznej, Warszawa 2025, s. 184.

[2] Pkt. 26 Preambuły Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (dalej jako „AI Akt” lub „Akt w sprawie sztucznej inteligencji”).

[3] Rada Europejska, Nadzwyczajne posiedzenie Rady Europejskiej (1 i 2 października 2020 r.) – Konkluzje, EUCO 13/20, 2020, s. 6.

[4] Podobnie M. Wyszomirska, AI Act as EU Legislator’s Response to Challenges of Artificial Intelligence Development, Safty and Fire Technology, SFT 2025, vol. 65, no. 1, s. 31.

[5] W publicystyce branżowej zwraca się uwagę na tzw. efekt brukselski którym jest zbyt wczesna i kompleksowa regulacja, która w konsekwencji może przyczynić się do osłabienia pozycji UE na globalnym rynku AI. Por. m.in. artykuł pt. Europa traci wyścig o AI. Nadmiar regulacji hamuje innowacje i konkurencyjność UE https://wartowiedziec.pl/serwis-glowny/aktualnosci/78987-europa-traci-wyscig-o-ai-nadmiar-regulacji-hamuje-innowacje-i-konkurencyjnosc-ue (dostęp 29.05.2026

[6] Podobnie, M. Kaczmarczyk, Quo vadis, sztuczna inteligencjo? Rozważania nad problematyką etyczną i prawną AI, Studia Prawnoustrojowe 2025, nr 68, s. 189-190.

całkowicie poza prawną regulacją sfer, które wyłączone są z zakresu zastosowania prawa europejskiego. Celem niniejszego artykułu jest wskazanie na te wyjątki oraz postawienie pytań o konsekwencje takiego rozwiązania zarówno z perspektywy rozwoju narzędzi sztucznej inteligencji. Biorąc pod uwagę potencjał jaki sztuczna inteligencja może przynieść w takich obszarach jak: zastosowania wojskowe, obszar obronności i bezpieczeństwo narodowe, należy zastanowić się czy faktycznie pozostawienie tych obszarów zastosowania narzędzi AI poza prawną kontrolą jest rozwiązaniem pożądanym zarówno z punktu widzenia praw obywatelskich, jak i bezpieczeństwa państwa.

Ogólne ramy prawne oraz wyjątki w zakresie stosowania sztucznej inteligencji w prawie Unii Europejskiej

Ramy prawne stosowania sztucznej inteligencji reguluje akt w sprawie sztucznej inteligencji. Rozporządzenie to jest bezpośrednio skuteczne we wszystkich państwach Unii Europejskiej. Jak wskazuje się w Preambule jego celem „jest poprawa funkcjonowania rynku wewnętrznego przez ustanowienie jednolitych ram prawnych, w szczególności w zakresie rozwoju, wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji (zwanych dalej „systemami AI") w Unii, zgodnie z wartościami Unii, w celu promowania upowszechniania zorientowanej na człowieka i godnej zaufania sztucznej inteligencji (AI) przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej (zwanej „Kartą")"[7].

Mimo, horyzontalnego charakteru rozporządzenia i jego bezpośredniego skutku, pewne sfery regulacyjne pozostają nie objęte wspólną regulacją. Obowiązujące przepisy obejmuje swoim zakresem jedynie wykorzystywanie systemów AI w ramach prawa unijnego. Poza zakresem prawa UE pozostają więc kluczowe z punktu widzenia obywateli Unii Europejskiej obszary regulacyjne – tj. rozwijanie i stosowanie systemów AI w zakresie czynności wchodzących w obszar bezpieczeństwa narodowego, działalności służb specjalnych, obronności i zastosowań wojskowych. Jak wskazuje się w pkt. 24 Preambuły AI Aktu, „jeżeli i w zakresie, w jakim systemy AI wprowadza się do obrotu, oddaje do użytku lub wykorzystuje się je ze zmianami lub bez zmian – do celów wojskowych, obronnych lub celów bezpieczeństwa narodowego, systemy te należy wyłączyć z zakresu stosowania niniejszego rozporządzenia niezależnie od tego, jaki podmiot wykonuje te działania – nie ma znaczenia na przykład, czy jest on podmiotem publicznym czy prywatnym."[8] Oprócz wyłączeń o charakterze materialnoprawnym wskazanych w art. 2 ust. 3 AI Aktu, regulacja ta zawiera także inne wyjątki, które z uwagi na ograniczone ramy niniejszego opracowania

[7] Pkt. 1 Preambuły do AI Aktu.

[8] Pkt. 24 Preambuły do AI Aktu. Jak dalej wskazuje się w tym punkcie „W przypadku celów wojskowych i obronnych, takie wyłączenie jest uzasadnione zarówno art. 4 ust. 2 TUE, jak i specyfiką polityki obronnej państw członkowskich i wspólnej polityki obronnej Unii objętej tytułem V rozdział 2 TUE, które podlegają prawu międzynarodowemu publicznemu stanowiącemu zatem bardziej odpowiednie ramy prawne dla regulacji systemów AI w kontekście stosowania śmiercionośnej siły i innych systemów AI w kontekście działań wojskowych i obronnych. W przypadku celów bezpieczeństwa narodowego wyłączenie to jest uzasadnione zarówno faktem, że za bezpieczeństwo narodowe wyłączną odpowiedzialność ponoszą państwa członkowskie zgodnie z art. 4 ust. 2 TUE, jak i faktem, że działania w zakresie bezpieczeństwa narodowego mają szczególny charakter, wiążą się ze szczególnymi potrzebami operacyjnymi i że stosuje się do nich szczególne przepisy krajowe*".*

nie będą poddane szczegółowej analizie[9]. Należy także wskazać, iż poza zakresem regulacji pozostają kwestie pozostające w wyłącznej domenie regulacyjnej państw członkowskich. Dlatego pełna transpozycja przepisów do krajowych porządków prawnych wymaga przyjęcia krajowych środków implementujących, które uregulować będą kwestie, które nie są objęte wspólną unijną regulacją, między innymi zasady nadzoru nad modelami i systemami sztucznej inteligencji a także systemu kar w przypadku naruszenia obowiązków przy wprowadzaniu i stosowaniu technologii AI.

Eksploracja modeli i narzędzi AI poza obszarem prawa UE

Kluczowe dla zdefiniowania zakresu kompetencji UE w obszarze regulacji zastosowań AI jest wskazanie ram prawodawczych prawa europejskiego. Kompetencje Unii Europejskiej są wyłączone w przypadku działalności wykraczającej poza zakres prawa Unii. Wynika to wprost z art. 72 i 73 TFUE[10]. Precyzyjne określenie zakresu wyłączeń wymaga więc określenia zakresu kompetencji Unii Europejskiej w stanowieniu prawa oraz tych obszarów, gdzie państwa członkowskie zachowały pełną i arbitralną swobodę prawodawczą[11]. Stosownie do art. 5 TUE, Unia Europejska działa na zasadzie kompetencji przyznanych. Wszelkie kompetencje nieprzyznane Unii w traktatach należą do państw członkowskich.

Zastosowanie systemów sztucznej inteligencji w obszarze bezpieczeństwa narodowego jest poza zakresem ustawodawstwa unijnego. Konsekwencją tego jest nie tylko wyłączenie tego obszaru z Aktu w sprawie sztucznej inteligencji, ale także Konwencji ramowej Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności.[12] Jest to rozwiązanie celowe, stosowane również w innych obszarach regulacyjnych, np. w ochronie danych osobowych[13] i wiąże się z dychotomicznym podziałem kompetencji między państwami członkowskimi a Unią Europejską. Wyłączenie w AI Akcie zastosowań modeli i systemów AI w toku działań wykraczających poza zakres prawa Unii prowadzi w efekcie do swoistego reżimu regulacyjnego o charakterze hybrydowym – część bowiem zastosowań AI objęta jest prawem Unii Europejskiej a część pozostawiona jest do arbitralnej decyzji ustawodawcy krajowego – który może objąć ten zakres dedykowaną krajową regulacją lub też pozostawić bez ram legislacyjnych.

Będzie miało to fundamentalne znaczenie przykładowo w takich obszarach jak: dopuszczalność stosowania zakazanych systemów sztucznej inteligencji, przyjętym modelem nadzoru czy obowiązkami podmiotów stosujących systemy AI

[9] AI Akt nie znajduje zastosowania do niektórych form wykorzystywania AI w celach ścigania przestępstw i współpracy sądowej (art. 2 ust. 4) a także odpowiedzialności dostawców usług pośrednich objętych regulacją Aktu o Usługach Cyfrowych[9] (art. 2 ust. 5 AI Aktu) oraz wykorzystywania modeli i systemów do celów badań naukowych i rozwojowych (art. 2 ust. 6).

[10] Zgodnie z art. 72 TFUE „niniejszy tytuł nie narusza wykonywania przez Państwa Członkowskie obowiązków dotyczących utrzymania porządku publicznego i ochrony bezpieczeństwa wewnętrznego". Zgodnie natomiast z art. 73 TFUE, uprawnienia ustawodawcze Unii Europejskiej są wyłączone w przypadku działań wykraczających poza zakres prawa UE, w szczególności dotyczących bezpieczeństwa narodowego".

[11] J. Kurek, Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big Data. Aspekty prawne, organizacyjne i systemowe, Warszawa 2021, s.10.

[12] https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f

[13] por. J. Kurek-Sobieraj [w:] P. Litwiński, ODO Compliance. Praktyczny komentarz z przykładami i orzecznictwem, Warszawa 2025, s. 32; J. Kurek, Bezpieczeństwo państwa..., s. 18-19.

chociażby w odniesieniu do obowiązku stałej analizy ryzyka w stosunku do stosowanych modeli i systemów AI, przejrzystości w fazie projektowania czy też nadzoru ludzkiego nad trenowanymi modelami i systemami AI.

Pojęcie bezpieczeństwa narodowego w prawie i orzecznictwie UE

Ani przepisy AI Aktu, ani regulacje prawa pierwotnego UE nie definiują pojęcia bezpieczeństwa narodowego. Próba wskazania ram tego pojęcia pojawiła się w kontekście sztucznej inteligencji w Wytycznych Komisji Europejskiej w sprawie zakazanych systemów sztucznej inteligencji[14]. Zgodnie ze wskazaną tak definicją, „Termin ten odnosi się do „głównego interesu" i ochrony podstawowych funkcji państwa i podstawowych interesów społeczeństwa i obejmuje zapobieganie i karanie czynów, które mogą mieć destabilizujący wpływ na podstawowe struktury konstytucyjne, polityczne, gospodarcze lub społeczne kraju, a w szczególności bezpośrednio zagrażające społeczeństwu, ludności lub państwu samo w sobie, takie jak przykładowo działalność terrorystyczna[15]. Bezpieczeństwo narodowe nie obejmuje np. działalność związaną z bezpieczeństwem ruchu drogowego[16], lub organizacja lub administracja wymiaru sprawiedliwości[17]". Definicja ta nie ma oczywiście charakteru wiążącego. Warto ją jednak przywołać jako zgodną z linią orzeczniczą Trybunału Sprawiedliwości UE i jedną z nielicznych prób syntetyzacji wartości narodowych przez organy stanowienia prawa.

Ukształtowane w prawie i praktyce Unii Europejskiej rozumienie pojęcia bezpieczeństwa narodowego jest wynikiem bogatego orzecznictwa unijnych trybunałów. Trybunał zaliczył do obszarów związanych z bezpieczeństwem narodowym takie zagadnienia jak: polityka azylowa, ochrona języka narodowego lub zasady przyznawania tytułów szlacheckich. Są to więc dziedziny zastrzeżone do wyłącznej kompetencji państw członkowskich w obszarze bezpieczeństwa i tożsamości narodowej[18]. W orzecznictwie jednoznacznie wskazuje się, że kwestia określenia ram bezpieczeństwa narodowego oraz zakresu pojęcia została pozostawiona kompetencjom państw członkowskich. Pozostawienie sfery definicyjnej po stronie państw członkowskich i związane z tym pewne luzy interpretacyjne uznaje się za zabieg celowy i zamierzony[19]. Rozwiązanie takie wpisuje się w dynamikę priorytetów państwa, która jest konsekwencją zmienności w czasie wartości podlegających ochronie w zakresie bezpieczeństwa narodowego. Orzecznictwo europejskie pozwoliło więc na zdefiniowanie pewnych założeń wspólnych oraz wskazanie punktów odniesienia

[14] Communication from the Commission C(2025) 5052 final. Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act). Warto wskazać, że wytyczne KE nie mają charakteru wiążącego a jedynie poglądowy. Jedynym podmiotem uprawnionym do dokonania wiążącej wykładni prawa w UE jest Trybunał Sprawiedliwości UE.

[15] Wyrok TSUE z dn.6.10.2020, La Quadrature du Net i inni, w spr. C-511/18, C-512/18 i C-520/18,EU:C:2020:791, § 135; wyrok TSUE z dn.5.06.2023, KE v Polska, C-204/21, EU:C:2023:442, § 318, w zw. ze spr. C-439/19, § 67 i spr. C-306/21, § 40

[16] Wyrok TSUE z dn. 22.06.2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504.

[17] Wyrok TSUE z dn. 5.06. 2023, KE v Polska, C-204/21, EU:C:2023:442, § 319.

[18] Por. m.in. wyrok TS w sprawie C-208/09. Ilonka Sayn-Wittgenstein przeciwko Landeshauptmann von Wien, wyrok TS w sprawie C-391/09, Malgožata Runevič Vardyn, Łukasz Paweł Wardyn przeciwko Vilniaus miesto savivaldybės administracija i in., z wyroku TS w sprawie C-601/15 w sprawie J.N. przeciwko Staatssecretaris van Veiligheid en Justitie.

[19] Por. J. Kurek-Sobieraj [w:] P. Litwiński, ODO Compliance. Praktyczny komentarz, s. 32.

w tym takich obszarach, jak: zabezpieczenie państwa i jego ładu konstytucyjnego oraz demokracji przed zagrożeniami ze strony działań szpiegowskich, terroryzmu oraz separatyzmu[20]. Poszukując uniwersalnej definicji bezpieczeństwa narodowego, warto przywołać poglądy A. Grzelak, która wskazuje, iż „bezpieczeństwo narodowe najczęściej rozumiane jest jako jedna z podstawowych funkcji każdego państwa, która obejmuje problematykę przeciwstawienia się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia oraz rozwoju narodu i państwa. Państwo w trosce o własne bezpieczeństwo narodowe ustala zbiór wartości wewnętrznych, które jego zdaniem powinny być chronione przed zagrożeniami. Bezpieczeństwo narodowe postrzegane jest zatem jako zdolność narodu (państwa) do obrony terytorium i wartości”[21].

Podsumowując, zgodnie z orzecznictwem unijnych trybunałów, pojęcie bezpieczeństwa narodowego obejmuje takie obszary aktywności państwa, które bez względu na obowiązujące sojusze polityczne, gospodarcze i wojskowe pozostać w obszarze wyłącznej kompetencji państwa i które nie powinny być przedmiotem delegacji na rzecz podmiotów i instytucji międzynarodowych. Zapewnienie bezpieczeństwa narodowego stanowi bowiem główną powinność państwa i jego organów konstytucyjnych poprzez zabezpieczenie wartości fundamentalnych dla bytu i tożsamości narodowej.

Krajowa regulacja pojęcia bezpieczeństwa narodowego

Pozostawienie państwom członkowskim swobody w kształtowaniu zakresu przedmiotowego pojęcia bezpieczeństwa narodowego jest zabiegiem zamierzonym i nie stanowi luki w systemie prawa[22]. Jako kluczowy wskazać należy na art. 5 Konstytucji[23] – który może być postrzegany jako konkretyzacja politycznego i społeczno-gospodarczego manifestu jaki stanowi wstęp do ustawy zasadniczej RP. Przepis art. 5 określa bowiem cele, które powinny być uwzględniane w każdym aspekcie funkcjonowania państwa[24]. Przepis ten odwołuję się do tych wartości, które z perspektywy doświadczeń historycznych RP mogą być określone jako podstawowe dla przetrwania i jestestwa narodu jak również gwarantować harmonijny i dostatni rozwój państwa i obywateli. Stanowią one tzw. „twarde jądro”[25] wyznaczające cele i interesy w obszarze bezpieczeństwa narodowego[26].

Jak wskazuje M. Szpunar, działania państwa w sferze prawnie regulowanej powinny się odnosić do ochrony i obrony wartości narodowych – o charakterze zarówno militarnym, jak i niemilitarnym. To te obszary aktywności państwa, które powinny pozostać w domenie polityki krajowej. W doktrynie

[20] Opinia rzecznika generalnego TSUE Francisa Jacobsa przedstawiona w dniu 6.04.1995 r. w sprawie C-120/94 (Komisja przeciw Grecji). s. 2.
[21] A. Grzelak [w:] A. Wróbel (red.), Traktat o Funkcjonowaniu Unii Europejskiej.
[22] J. Kurek, Bezpieczeństwo narodowe (państwa) uwarunkowania traktatowe, Przegląd Konstytucyjny 2022, nr 5 (69), s. 283.
[23] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483 ze zm.).
[24] F. Florczak-Wątor [w:] M. Safjan, L. Bosek (red.), Konstytucja RP. Komentarz, t. 1, Warszawa 2016.
[25] Twarde jądro polskich interesów narodowych wyznacza art. 5 Konstytucji. Podobnie wyrok TK w sprawie K 32/09.
[26] J. Kurek, Bezpieczeństwo narodowe (państwa)..., s. 284.

podkreśla się, iż *ratio legis* tego przepisu odwołuje się do pojęcia suwerenności oraz tożsamości konstytucyjnej[27].

Pojęcie ładu i tożsamości konstytucyjnej poddane zostało interpretacji Trybunału Konstytucyjnego w orzeczeniu nr. K-32/09. Jak słusznie wskazuje L. Garlicki, kompetencje objęte zakazem przekazania stanowią o tożsamości konstytucyjnej, a więc odzwierciedlają wartości, na których opiera się Konstytucja[28]. Trybunał wskazuje, iż tożsamość konstytucyjna jest pojęciem wyznaczającym zakres wyłączenia spod kompetencji przekazania materii należących (…) do „twardego jądra", kardynalnych dla podstaw ustroju danego państwa. Niezależnie od trudności związanych z ustaleniem szczegółowego katalogu kompetencji nieprzekazywalnych, należy zaliczyć do materii objętych całkowitym zakazem przekazania postanowienia określające zasady naczelne Konstytucji oraz postanowienia dotyczące praw jednostki wyznaczające tożsamość państwa, w tym w szczególności wymóg zapewnienia ochrony godności człowieka i praw konstytucyjnych, zasadę państwowości, zasadę demokracji, zasadę państwa prawnego, zasadę sprawiedliwości społecznej, zasadę pomocniczości, a także wymóg zapewnienia lepszej realizacji wartości konstytucyjnych i zakaz przekazywania władzy ustrojodawczej oraz kompetencji do kreowania kompetencji[29]. Są to te wartości, a zarazem żywotne interesy państwa, które objęte są ochroną bezpieczeństwa narodowego i pozostają poza zakresem prawa UE.

Konstytucjonalizacja celów państwa wyraża z jednej strony oczekiwania społeczne wobec priorytetów państwa, ale także gotowość do ich realizacji. Wpływa ona ponadto na ich stabilizację oraz trwałość. Ich ujęcie w Konstytucji gwarantuje, że nie będą one elementem bieżącej gry politycznej i programu aktualnie rządzącej formacji politycznej[30].

Podsumowując jako kluczowe dla określenia obszarów wyznaczających ramy bezpieczeństwa narodowego Rzeczypospolitej Polskiej, należy za Trybunałem Konstytucyjnym wskazać na tzw. „twarde jądro" celów i interesów narodowych w postaci: (1) ochrony niepodległości i integralności terytorialnej, (2) zapewnienia wolności i praw człowieka oraz praw obywatelskich, (3) ochrony dziedzictwa narodowego oraz (4) ochrony środowiska w duchu zrównoważonego rozwoju[31].

Implementacja modeli i systemów sztucznej inteligencji w zgodzie ze standardami praw człowieka i zasadami etyki

Jak wskazuje się w Preambule Aktu w sprawie Sztucznej Inteligencji, „Unijne ramy prawne określające zharmonizowane przepisy dotyczące AI są niezbędne, by wspierać rozwój, wykorzystywanie i upowszechnianie AI na rynku wewnętrznym, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony interesów publicznych, takich jak: zdrowie i bezpieczeństwo oraz ochrona praw podstawowych, w tym demokracji, praworządności i ochrony środowiska,

[27] M. Szpunar [w:] M. Safjan, L. Bosek (red.), Konstytucja RP. Komentarz, t. 2, Warszawa 2016, s. 139.
[28] L. Garlicki, Normy konstytucyjne relatywnie niezmieniane [w:] J. Trzciński (red.), Charakter i struktura norm Konstytucji, Warszawa 1997, s. 148.
[29] Por. m.in. K. Działocha [w:] Konstytucja RP. Komentarz, L. Garlicki (red.), Warszawa 2007, s. 14; K. Wojtyczek, Przekazywanie kompetencji państwa organizacjom międzynarodowym, Kraków 2007, s. 284.
[30] M. Florczak-Wątor, [w:] Konstytucja RP..., s. 284.
[31] Wyrok TK w sprawie K 32/09.

uznanych i chronionych przez prawo Unii”[32]. Cel ten zgodnie z art. 1 ust. 2 AI Aktu, osiągany jest poprzez przyjęcie regulacji w zakresie m.in: (1) zharmonizowanych reguł dotyczących wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów AI w Unii, (2) zakazów dotyczących niektórych praktyk w zakresie AI, (3) szczególnych wymogów dotyczących systemów AI wysokiego ryzyka a także obowiązkach które spoczywają na operatorach takich systemów.

Materialny zakres zastosowania unijnego rozporządzenia ma służyć harmonijnemu i zgodnemu z zasadami etyki i praw człowieka rozwijaniu w Unii Europejskiej modeli i systemów sztucznej inteligencji. Potencjał, który samoucząca i rozwijająca się technologia posiada zostaje zamknięty w ramy prawne, które blokują możliwość rozwijania narzędzi w sposób niekontrolowany a także który szkodziłby prawo człowieka. Biorąc pod uwagę potencjał jaki wynika z wykorzystania technologii w takich kontekstach, jak użycie narzędzi do praktyk manipulacji, wyzysku i kontroli społecznej niektóre praktyki AI zostały objęte zakazem stosowania. Są to te praktyki w przypadku, których poziom ryzyka naruszenia praw podstawowych został uznany przez unijnego prawodawcę jako niedopuszczalny. Przykłady te enumeratywnie wskazane zostały w art. 5 AI Aktu.

Jak wskazuje Komisja Europejska w swoich wytycznych odnoszących się do systemów AI wysokiego ryzyka, są to między innymi systemy, które: (1) mogą prowadzić do szkodliwej manipulacji lub oszustwa m.in. poprzez wykorzystywanie technik podprogowych wykraczających poza świadomość użytkownika; (2) wykorzystują podatności na zagrożenia wynikające ze szczególnych cech użytkownika (np. z uwagi na wiek bądź niepełnosprawność); (3) stosują szkodliwą i dyskryminującą w skutkach punktację społeczną, czyli systemy oceniające lub klasyfikujące użytkowników na podstawie zachowań społecznych bądź cech na podstawie danych pochodzących z niepowiązanych kontekstów społecznych; (4) stosujące indywidualną oceną celem przewidywania prawdopodobieństwa przewidzenia ryzyka popełnienia przestępstwa w oparciu o profil osobowościowy lub cechy użytkownika; (5) są nakierowane na nieukierunkowaną eksplorację Internetu lub nagrań z telewizji przemysłowej celem tworzenia lub rozszerzania baz danych służących rozpoznaniu twarzy; (6) są wykorzystywane do wyciągania wniosków na temat emocji osoby w miejscu pracy lub instytucjach edukacyjnych, bądź też; (7) z wykorzystaniem danych biometrycznych kategoryzują użytkowników celem wnioskowania o danych wrażliwych użytkowników takich jak (rasie, poglądach politycznych, przynależności zawodowej, przekonaniach religijnych, życiu i orientacji seksualnej)[33].

Zakazane praktyki w zakresie AI a eksploracja w obszarze bezpieczeństwa narodowego

Analizując potencjał sztucznej inteligencji, wykorzystanie narzędzi AI w działalności podmiotów odpowiedzialnych za bezpieczeństwo i obronność mogłoby w sposób znaczący przyczynić się do podniesienia ogólnego poziomu bezpieczeństwa. Duży potencjał w zakresie bezpieczeństwa mógłby z całą

[32] Pkt. 8 Preambuły do AI Aktu.

[33] Przykłady przygotowane na podstawie praktyk wylistowanych w Wytycznych KE Commission Guidelines on prohibited artificial intelligence practice, s. 3-4.

pewnością pojawić się w takim obszarze jak, wykorzystanie narzędzi profilowania celem przewidywania prawdopodobieństwa ryzyka popełnienia przestępstwa, nieukierunkowana eksploracja Internetu czy nagrań telewizji przemysłowej celem identyfikacji lub narzędzi służących ocenie osoby w miejscu pracy lub instytucjach edukacyjnych. Konsekwencją wyłączenia zakazów zdefiniowanych w art. 5 AI Aktu do praktyk stosowanych w obszarze bezpieczeństwa narodowego jest *de facto* dopuszczalność stosowania ich m.in. w działalności służb specjalnych, o ile przepisy prawa krajowego nie wprowadzą w tym zakresie dodatkowych obostrzeń.

W przypadku polskiego projektu ustawy transponującej, nie zostały przewidziane żadne szczególne wymogi odnośnie do sfer nie objętych prawem Unii Europejskiej. Polski ustawodawca potwierdza jedynie wyłączenie stosowania AI Aktu w działaniach służb specjalnych, zastosowaniach wojskowych oraz dla celów bezpieczeństwa narodowego. W praktyce oznacza to, że jeżeli służby specjalne – o ile stosowane przez nich systemy nie będą kwalifikowane jako tzw. systemy podwójnego zastosowania mają prawo stosować m.in. zakazane systemy zdefiniowane w art. 5 ust. 1 lit d – tj. służące ocenie lub przewidywaniu ryzyka popełnienia przestępstwa przez osobę fizyczną wyłącznie na podstawie profilowania lub oceny cech osobowości i cech charakterystycznych. Mogły by więc wykorzystywać dane wrażliwe dane odnośnie skazań oraz dane historyczne dane dotyczące przestępczości do trenowania dedykowanych celom bezpieczeństwa narodowego modeli i powiązanych z nimi systemów AI. Takie zastosowanie w wytycznych Komisji uznane było za niedopuszczalne.

Jak wskazuje się w wytycznych KE (pkt. 190), systemy AI do przewidywania przestępczości identyfikują wzorce na podstawie danych historycznych – często danych grupowych – łącząc wskaźniki z prawdopodobieństwem wystąpienia przestępstwa, a następnie generują punktową ocenę ryzyka jako wyniki predykcyjne. Takie wykorzystanie danych historycznych dotyczących popełnionych przestępstw w celu przewidywania przyszłych zachowań innych osób oprócz potencjalnie wysokiego potencjału skuteczności dla celów prezencji przestępczości, może utrwalać, a nawet wzmacniać uprzedzenia i może prowadzić do „pominięcia" kluczowych okoliczności indywidualnych, jeżeli okoliczności te nie są częścią zbioru danych ani nie są uwzględniane w algorytmach, na których opiera się dany system AI. Może to również podważyć zaufanie społeczeństwa do organów ścigania i ogólnie do systemu wymiaru sprawiedliwości[34].

W kontekście niedopuszczalnego ryzyka i zakazanych praktyk, można wskazać na praktykę wykorzystującą profilowanie grupowe. Pojęcie to odnosi się do tworzenia i zastosowania profilu opisowego dla danej grupy, na przykład kategorii sprawców przestępstw (np. terrorystów, gangsterów itp.) skonstruowanych na podstawie danych historycznych dotyczących wcześniej popełnionych przestępstw przez inne osoby. Te profile grupowe mogą być później wykorzystywane do oceny i przewidywania ryzyka popełnienia podobnych przestępstw przez inne osoby. Jeżeli system AI sporządza prognozę i stosuje taki profil (grupowy) do konkretnej osoby fizycznej, stanowi to profilowanie danej

[34] Raport „Bias in algorithms – Artificial intelligence and discrimination [Stronniczość algorytmiczna – sztuczna inteligencja a dyskryminacja] Agencja Praw Podstawowych Unii Europejskiej Agencja Praw Podstawowych Unii Europejskiej (8.12.2022 r.) https://fra.europa.eu/en/publication/2022/bias-algorithm [dostęp 4.05.2026].

osoby i w związku z tym może wchodzić w zakres zakazu określonego w art. 5 ust. 1 lit. d) aktu w sprawie sztucznej inteligencji[35].

Zasady wykorzystywania danych osobowych do trenowania systemów AI a unijny standard ochrony danych osobowych

Analizując skutki wyłączenia unijnych standardów do rozwoju systemów sztucznej inteligencji trzeba jednocześnie wskazać na konsekwencje w postaci wyłączenia zastosowania europejskiego reżimu ochrony danych osobowych. W obszarze bezpieczeństwa narodowego, modele i systemy AI nie będą więc musiały być bez uwzględnienia standardów ochrony danych osobowych. W tym przypadku nie ma więc konieczności gwarantowania ochrony danych osobowych w całym cyklu życia systemów AI[36]. Oznacza to przede wszystkim brak konieczności uwzględnienia ochrony prywatności w fazie projektowania, minimalizacji danych przy przypadku trenowania modeli AI a także braku obowiązku przeprowadzenia oceny skutków dla ochrony danych osobowych.

Europejska Rada ds. Ochrony Danych Osobowych w Opinii nr 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji[37] zwraca uwagę na co najmniej konieczność zagwarantowania zgodności z art. 5 RODO. W kontekście rozwijania systemów SI należy więc zwrócić uwagę, w szczególności na następujące kwestie: (1) obowiązek rozliczalności procesów przetwarzania danych osobowych (2) zgodność z prawem, rzetelność i przejrzystości przetwarzania danych osobowych (3) ograniczenie celu i minimalizację danych (4) zagwarantowanie praw osób których dane dotyczą.

Biorąc jednocześnie pod uwagę wysokie ryzyko dla danych osobowych, które wiążą się z rozwojem narzędzi SI, administrator danych osobowych powinien przed rozpoczęciem trenowania modeli przeprowadzić analizę ryzyka dla danych osobowych. W przypadku rozwijania narzędzi AI brak obowiązku stosowania unijnego reżimu ochrony danych osobowych oznacza, iż w przypadku zastosowań sztucznej inteligencji dla celów wyłącznie bezpieczeństwa narodowego możliwe mogłoby być trenowanie modeli AI poprzez np. masowe pobieranie danych z rejestrów publicznych (także tych zamkniętych) bez przeprowadzenia odpowiedniej oceny skutków dla ochrony danych osobowych i wdrożenia stosowanych zabezpieczeń dla danych osobowych a także konsultacji z krajowym organem ochrony danych osobowych.

W praktyce oznaczałoby to brak konieczności spełnienia kluczowego obowiązku, który powinien być wdrożony w fazie projektowania modeli SI i odpowiednich systemów SI. W ramach przeprowadzanej analizy ryzyka, zgodnie z unijnymi standardami wynikającymi z RODO, podmiot trenujący

[35] Pkt. 196 wytycznych KE Commission Guidelines on prohibited artificial intelligence practice, s. 78.

[36] O obowiązkach wynikających z RODO por. m.in. A. Mednis, Dotychczasowe obowiązki informacyjne z RODO a wymogi zapewnienia prejrzystości i wyjaśnialności przez podmioty stosujące systemy AI wysokiego ryzyka [w:] G. Sibiga (red.), Wpływ Aktu w sprawie sztucznej inteligencji na funkcjonowanie administracji publicznej, Warszawa 2025, s. 165 oraz M. Szpyrka. Uczenie maszynowe a prawa podstawowe. Czyli o obowiązkach organów administracji publicznej, które wdrażają systemy AI wysokiego ryzyka [w:] G. Sibiga (red.), Wpływ Aktu w sprawie sztucznej inteligencji..., s. 86.

[37] Opinia EROD nr 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl [dostęp: 17.08.2026].

modele AI powinien co najmniej wykonać szczegółowy opis wszystkich operacji przetwarzania danych osobowych objętych projektowanym narzędziem, w tym wskazać: jakie dane będą przetwarzane, kro będzie miał do nich dostęp, w jaki sposób dane będą pozyskane i w jakim celu przetwarzane. Przed przystąpieniem do przetwarzania, administrator powinien dokonać oceny, czy faktycznie osiągnięcie zakładanego celu wymaga przetwarzania danych osobowych i czy cel ten nie mógłby zostać osiągnięty poprzez trenowanie modelu danymi anonimowymi lub syntetycznymi. A także w przypadku niezbędności wykorzystania danych osobowych, przeprowadzić swoisty test ważenia interesów i zastanowić się, czy planowane rozwiązanie nie ingeruje w sposób nadmierny w prywatność osób, których dane są przetwarzane. Ocena skutków to także, wykazanie potencjalnych zagrożeń takich jak nieuprawniony dostęp, czy wyciek danych i ocena prawdopodobieństwa wystąpienia taki ryzyk dla danych osobowych wraz z zaprojektowaniem odpowiednich środków ograniczających ryzyka.

Uwagi końcowe

Mimo iż modele i systemy wykorzystujące sztuczną inteligencje dopiero się rozwijają, już dzisiaj widać iż stanowi ona w wielu obszarach zastosowań swoisty game-changer. Stąd za tak istotne uważa się, aby rozwój sztucznej inteligencji od samego początku objęty był szczegółową regulacją, która ukierunkowana jest na stworzenie ram dla kontrolowanego rozwoju technologii, zapewniającej ramy dla bezpiecznego i etycznego korzystania z technologii AI. Z uwagi na uwarunkowania systemowe, prawo Unii Europejskiej nie obejmuje zastosowań i rozwoju AI w dziedzinie bezpieczeństwa narodowego, obronności i zastosowań obronnych. Biorąc pod uwagę zasadę legalizmu z której wynika, że organy państwa działają w granicach i na podstawie prawa stan niepewności co do standardów ochrony, jaką dany podmiot musi stosować oraz podstaw prawnych stanowi zagrożenie dla skutecznego rozwijania narzędzi opartych o technologię sztucznej inteligencji. Brak objęcia materialnym zakresem prawa unijnego (w tym AI Aktu oraz RODO) procesów rozwijania narzędzi AI stosowanych dla wyłącznych celów bezpieczeństwa narodowego nie oznacza zakazu stosowania unijnych standardów. To sfera wymaga jednak autonomicznej regulacji w przepisach krajowych.

Autonomizacja regulacji prawnej w ramach działań wchodzących w zakres bezpieczeństwa narodowego może paradoksalnie stać się remedium na problemy, którym nie da się przeciwdziałać w skali ponadnarodowej. Biorąc pod uwagę różnorodną strukturę, kompetencje oraz system nadzoru nad podmiotami z obszaru bezpieczeństwa i służbami specjalnymi w poszczególnych państwach, stworzenie zunifikowanych reguł wydaje się być niemożliwe. Także uwzględniając charakter zadań z obszaru bezpieczeństwa i zmienność w czasie priorytetów – konsensus na poziomie ponadnarodowym może być niezwykle trudny. W takim przypadku krajowa – autonomiczna regulacja prawna uwzględniająca specyfikę środowiska prawnego, realiów krajowych oraz zadań w obszarze bezpieczeństwa może być salomonowym rozwiązaniem, w szczególności jeżeli standardy unijne dotyczące ochrony prywatności oraz etycznego rozwoju systemów AI potraktuje się jako standard minimalny, który będzie wdrożony do krajowych rozwiązań sektorowych. Pakiet unijnych regulacji może być z powodzeniem potraktowany jako środek prawny o charakterze zbliżonym do instrumentów minimalnej harmonizacji. W ramach instrumentów

krajowych poza kwestiami związanymi z nadzorem ogólnym nad modelami i systemami SI, autonomiczna regulacje dotyczące wykorzystywania systemów sztucznej inteligencji do celów bezpieczeństwa narodowego powinna obejmować co najmniej: 1) określenie zasad nadzoru nad stosowanymi modelami i systemami sztucznej inteligencji 2) wskazanie, czy dopuszczalne jest wykorzystywanie zakazanych systemów sztucznej inteligencji, na przykład z wykorzystaniem technik podprogowych, 3) określenie obowiązków podmiotów wykorzystujących systemy wysokiego ryzyka oraz 4) określenie ścieżki zgłaszania poważnych incydentów.

Bibliografia

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13.06.2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828.

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. L 119, 4.5.2016, p. 1–88).

Traktat o funkcjonowaniu Unii Europejskiej z 25.03.1957 (Dz.U.2004 Nr. 90 poz. 864 ze zm.).

Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. 1997 nr 78 poz. 483 ze zm.).

Konwencja Ramowa Rady Europy w sprawie sztucznej inteligencji https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f

Literatura

Drobny W., Źródła norm etycznych przy stosowaniu sztucznej inteligencji w służbie publicznej (zarys problemu z perspektywy teoretycznoprawnej) [w:] G. Sibiga (red.), Wpływ Aktu w sprawie sztucznej inteligencji na funkcjonowanie administracji publicznej. Warszawa 2025.

Działocha K., [w:] L. Garlicki (red.), Konstytucja RP. Komentarz, Warszawa 2007.

Florczak-Wątor F., [w:] M. Safjan, L. Bosek (red.), Konstytucja RP. Komentarz, t. 1, Warszawa 2016.

Garlicki L., Normy konstytucyjne relatywnie niezmieniane [w:] J. Trzciński (red.), Charakter i struktura norm Konstytucji, Warszawa 1997.

Grzelak A., [w:] A. Wróbel (red.) Traktat o Funkcjonowaniu Unii Europejskiej, Komentarz, Warszawa 2012.

Kaczmarczyk M., Quo vadis, sztuczna inteligencjo? Rozważania nad problematyką etyczną i prawną AI, Studia Prawnoustrojowe 2025, nr 68.

Kurek-Sobieraj J., [w:] P. Litwiński, ODO Compliance. Praktyczny komentarz z przykładami i orzecznictwem, Warszawa 2025.

Kurek J., Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big Data. Aspekty prawne, organizacyjne i systemowe, Warszawa 2021.

Kurek J., Bezpieczeństwo narodowe (państwa) – uwarunkowania traktatowe, Przegląd Prawa Konstytucyjnego 2022, nr 5(69).

Mednis A., Dotychczasowe obowiązki informacyjne z RODO a wymogi zapewnienia prejrzystości i wyjaśnialności przez podmioty stosujące systemy AI wysokiego ryzyka [w:] G. Sibiga (red.), Wpływ Aktu w sprawie sztucznej inteligencji na funkcjonowanie administracji publicznej, Warszawa 2025.

Szpunar M., [w:] M. Safjan, L. Bosek (red.), Konstytucja RP. Komentarz, t. 2, Warszawa 2016.

Szpyrka M., Uczenie maszynowe a prawa podstawowe.Czyli o obowiązkach organów administracji publicznej, które wdrażają systemy AI wysokiego ryzyka [w:] G. Sibiga (red.), Wpływ Aktu w sprawie sztucznej inteligencji na funkcjonowanie administracji publicznej, Warszawa 2025.

Wojtyczek K., Przekazywanie kompetencji państwa organizacjom międzynarodowym, Kraków 2007.

Wyszomirska M., AI Act as EU Legislator's Response to Challenges of Artificial Intelligence Development, Safty and Fire Technology SFT 2025, vol. 65, no. 1.