Pojęcia kluczowe: *tajemnica przedsiębiorstwa, big data, sztuczna inteligencja, ochrona danych, prawo porównawcze*

Maja Wojtyś

Ochrona tajemnic przedsiębiorstwa w erze sztucznej inteligencji i big data

Abstrakt

Publikacja analizuje wyzwania i nowe zagrożenia dla ochrony tajemnicy przedsiębiorstwa, wynikające z rozwoju sztucznej inteligencji i big data. Autor przedstawia problematykę w kontekście prawa polskiego, europejskiego i amerykańskiego, wskazując na potrzebę nowelizacji oraz stosowania nowoczesnych mechanizmów zabezpieczających.

I. Wstęp

W dobie czwartej rewolucji przemysłowej, której podstawą jest przetwarzanie ogromnych ilości danych oraz rozwój technologii opartych na sztucznej inteligencji, problematyka ochrony tajemnic przedsiębiorstwa nabiera zupełnie nowego wymiaru. Informacje o charakterze poufnym, obejmujące know-how, strategie rynkowe, algorytmy czy dane klientów, stają się kluczowym aktywem decydującym o pozycji konkurencyjnej podmiotów gospodarczych na rynku. Jednocześnie technologie AI i big data zwiększają ryzyko nieuprawnionego pozyskiwania, analizowania i rekonstruowania tych informacji, niejednokrotnie bez fizycznego naruszenia zabezpieczeń systemowych[1]. Tradycyjne ramy prawne, które przez dekady zapewniały względnie skuteczną ochronę tajemnic przedsiębiorstwa, okazują się niewystarczające wobec dynamicznie zmieniającego się otoczenia technologicznego. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943, choć stanowi istotny krok w kierunku ujednolicenia standardów ochrony poufnych informacji w krajach członkowskich Unii Europejskiej[2], nie

1 A. Sobusiak, *Ochrona tajemnicy przedsiębiorstwa a wspieranie innowacyjności małych i średnich przedsiębiorstw w Unii Europejskiej*, rozprawa doktorska, Uniwersytet Łódzki 2023, s. 118.

2 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.06.2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem, Dz.Urz. UE L 157.

 DOI: 10.54383/0031-0344.2026.01.5

uwzględnia specyfiki zagrożeń płynących z wykorzystania sztucznej inteligencji i zautomatyzowanego gromadzenia danych. Podobne problemy dostrzegane są również w orzecznictwie, m.in. amerykańskich sądów federalnych, które coraz częściej muszą rozstrzygać spory związane z naruszeniem tajemnic handlowych przy wykorzystaniu nowoczesnych technologii[3]. W świetle powyższego konieczne wydaje się ponowne zdefiniowanie granic pojęcia tajemnicy przedsiębiorstwa, uwzględniające specyfikę działania systemów AI oraz zdolność algorytmów do przetwarzania danych w sposób nieprzewidywalny dla ludzkiego użytkownika. Celem niniejszego opracowania jest analiza aktualnych regulacji prawnych w Polsce, Unii Europejskiej i Stanach Zjednoczonych, wskazanie niedoskonałości obowiązujących mechanizmów ochronnych oraz przedstawienie rekomendacji legislacyjnych i praktycznych. Szczególny nacisk położono na problematykę zgodności ochrony tajemnicy przedsiębiorstwa z rozwojem generatywnej sztucznej inteligencji oraz narzędzi przetwarzających big data. Niniejsza publikacja została oparta na metodzie dogmatycznoprawnej (analiza obowiązujących przepisów prawa krajowego i międzynarodowego) oraz metodzie prawnoporównawczej (zestawienie regulacji obowiązujących w Unii Europejskiej, Polsce oraz Stanach Zjednoczonych). W analizie uwzględniono także orzecznictwo sądów krajowych i unijnych, jak również stanowiska doktryny i opracowania naukowe poświęcone tajemnicy przedsiębiorstwa w kontekście nowoczesnych technologii, ze szczególnym uwzględnieniem sztucznej inteligencji i big data.

II. Pojęcie i zakres tajemnicy przedsiębiorstwa

Tajemnica przedsiębiorstwa stanowi jedną z kluczowych form ochrony interesów gospodarczych podmiotów działających na rynku. Jest to instytucja prawna o charakterze interdyscyplinarnym, funkcjonująca na styku prawa cywilnego, prawa gospodarczego, a także prawa konkurencji i prawa pracy. Jej głównym celem jest ochrona określonych informacji, których ujawnienie mogłoby narazić przedsiębiorcę na stratę majątkową lub utratę przewagi konkurencyjnej[4]. W prawie polskim podstawową regulację w tym zakresie stanowi ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[5]. Zgodnie z art. 11 ust. 2 tej ustawy przez tajemnicę przedsiębiorstwa rozumie się „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu

3 Epic Systems Corp. v. Tata Consultancy Services Ltd., No. 14-cv-748 (W.D. Wis. 2020); zob. także: M. Stechly, *Tajemnica przedsiębiorstwa w dobie cyfrowej transformacji*, „Przegląd Prawa Handlowego" 2022/5, s. 14.

4 M. Gawroński, *Definicja pojęcia „tajemnica przedsiębiorstwa" na gruncie polskiego porządku prawnego – zarys problematyki*, „Monitor Prawniczy" 2022/22, s. 1099.

5 Ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. 2022, poz. 1233.

DOI: 10.54383/0031-0344.2026.01.5

zachowania ich poufności"[6]. Konstrukcja ta zakłada spełnienie trzech warunków: poufności informacji, ich wartości gospodarczej oraz zachowania środków ostrożności w celu ich ochrony.

Podobne definicje funkcjonują w prawie międzynarodowym. Artykuł 39 Porozumienia w sprawie handlowych aspektów praw własności intelektualnej (TRIPS) zobowiązuje państwa członkowskie Światowej Organizacji Handlu do zapewnienia skutecznych środków ochrony informacji, które są poufne, mają wartość handlową i podlegają odpowiedniej ochronie przed ujawnieniem[7].

W prawie amerykańskim podstawową regulacją dotyczącą tajemnic handlowych jest Defend Trade Secrets Act z 2016 r. (DTSA), który definiuje je jako wszelkie informacje, które nie są powszechnie znane, mają wartość handlową i w odniesieniu do których podjęto rozsądne kroki zmierzające do zachowania ich w tajemnicy[8]. Przepis ten jest zbliżony do regulacji unijnej i stanowi podstawę do dochodzenia roszczeń cywilnoprawnych na szczeblu federalnym.

Wspólnym mianownikiem przyjętych definicji jest akcent położony na dwa elementy: wartość gospodarcza chronionej informacji oraz działania podmiotu zmierzające do jej ochrony. W dobie cyfryzacji coraz większego znaczenia nabiera jednak precyzyjne określenie, co może zostać uznane za informację poufną – w szczególności w kontekście danych przetwarzanych przez systemy sztucznej inteligencji. Dotyczy to zwłaszcza algorytmów, modeli predykcyjnych, danych treningowych oraz zestawów big data, które nierzadko zawierają kombinacje danych możliwych do odtworzenia przy użyciu narzędzi analitycznych AI[9]. W tym kontekście pojawia się pytanie, czy sama struktura algorytmu, sposób działania modelu językowego lub wynik jego działania może podlegać ochronie jako tajemnica przedsiębiorstwa. Odpowiedzi na to pytanie wymagają nie tylko analizy przepisów krajowych i międzynarodowych, ale również odniesienia się do praktyki sądowej oraz dynamicznie rozwijającego się piśmiennictwa prawniczego.

III. Wpływ sztucznej inteligencji i big data na ryzyko naruszeń tajemnicy przedsiębiorstwa

Rozwój sztucznej inteligencji (AI) oraz narzędzi analitycznych big data radykalnie przekształca sposób przetwarzania, gromadzenia i wykorzystywania informacji w obrocie gospodarczym. Technologie te – oparte na uczeniu maszynowym, głębokich

6 Art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji.

7 Porozumienie w sprawie handlowych aspektów praw własności intelektualnej (TRIPS), Dz.Urz. UE L 336/1994, art. 39.

8 Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(3).

9 C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, Generative *AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, „Computer Law & Security Review" 2024, vol. 55.

 DOI: 10.54383/0031-0344.2026.01.5

sieciach neuronowych czy modelach językowych – pozwalają na pozyskiwanie i przetwarzanie danych z niespotykaną dotąd precyzją i szybkością. Jednocześnie jednak otwierają zupełnie nowe obszary ryzyka dla ochrony informacji, które zgodnie z przepisami mogą stanowić tajemnicę przedsiębiorstwa. Algorytmy uczenia maszynowego mają zdolność rekonstrukcji danych poufnych na podstawie danych wejściowych, które nie muszą być bezpośrednio tajne. W praktyce oznacza to, że modele AI mogą „domyślać się" pewnych informacji, np. o strategiach cenowych, parametrach produkcyjnych czy schematach działania firmy, wyłącznie na podstawie publicznych lub łatwo dostępnych źródeł. Taka możliwość stawia pod znakiem zapytania dotychczasowy zakres ochrony prawnej, gdyż klasyczne podejście do tajemnicy przedsiębiorstwa zakłada istnienie „informacji nieujawnionej", a nie informacji pochodnej, wygenerowanej w sposób automatyczny[10].

W kontekście big data dodatkowym wyzwaniem jest ogromna skala danych, jakie są przetwarzane, oraz ich różnorodność. W środowisku opartym na analityce danych coraz trudniejsze staje się ustalenie, które dane są w ogóle objęte tajemnicą przedsiębiorstwa, a które – choć wcześniej poufne – poprzez wielokrotne użycie, analizę i krzyżowanie z innymi źródłami – zostały de facto ujawnione. Przykładowo, jeśli algorytm analizuje dane z publicznych rejestrów, profili społecznościowych pracowników i schematów zakupowych, może odtworzyć elementy strategii rynkowej przedsiębiorcy – mimo braku bezpośredniego dostępu do poufnych dokumentów.

W tym kontekście pojawiają się fundamentalne pytania:

- Czy dane wyjściowe (*output*) generowane przez AI mogą być uznane za tajemnicę przedsiębiorstwa, jeśli przedsiębiorca uznaje je za poufne i mają one wartość gospodarczą?
- Czy informacje pośrednio uzyskane z danych publicznych – ale prowadzące do ujawnienia elementów strategii konkurencji – stanowią naruszenie?
- Czy modele AI mogą stać się narzędziem naruszenia tajemnicy przedsiębiorstwa w sposób nieintencjonalny (np. przez tzw. hallucination modeli językowych)?

Prawo w obecnym kształcie nie daje jednoznacznych odpowiedzi. W nauce prawa podkreśla się, że przepisy ustawy o zwalczaniu nieuczciwej konkurencji oraz dyrektywy 2016/943 nie zostały stworzone z myślą o tak zaawansowanych formach przetwarzania informacji[11]. Dlatego konieczna staje się ich nowa wykładnia, uwzględniająca realia technologiczne XXI wieku.

Jednym z niewielu przykładów orzecznictwa, które dotyka tej tematyki, jest sprawa *Epic Systems Corp. v. Tata Consultancy Services Ltd.* W tej sprawie pracownicy spółki zależnej Tata uzyskali dostęp do portalu wewnętrznego firmy Epic, który zawierał

10 K. Czub, *Sztuczna inteligencja jako podmiot praw własności intelektualnej?,* „Państwo i Prawo" 2023/10, s. 3.

11 M. Stechly, *Tajemnica przedsiębiorstwa w dobie cyfrowej transformacji*, „Przegląd Prawa Handlowego" 2022/5, s. 12–19.

m.in. materiały szkoleniowe i dokumentację systemu informatycznego. Choć dostęp ten był pierwotnie przyznany w celach testowych, został przekroczony, a informacje wykorzystano do budowy konkurencyjnego produktu[12]. Sąd federalny uznał, że samo uzyskanie dostępu logicznego do systemu – nawet bez fizycznego kopiowania danych – może stanowić naruszenie tajemnicy handlowej, jeśli doszło do bezprawnego wykorzystania informacji o charakterze gospodarczym. Sprawa ta wskazuje, że granica między dostępem a naruszeniem zaciera się w kontekście cyfrowym, szczególnie gdy dane są analizowane automatycznie przez AI. Choć sąd nie oceniał bezpośrednio roli algorytmów w pozyskiwaniu informacji, literatura przedmiotu interpretuje to orzeczenie jako ostrzeżenie dla firm korzystających z AI: nawet niezamierzona rekonstrukcja danych konkurencji może prowadzić do odpowiedzialności cywilnoprawnej[13]. Dodatkowe zagrożenia płyną z rozwoju tzw. generatywnej AI, która – jak modele językowe (np. GPT) – potrafi generować teksty, kod, analizy czy symulacje na podstawie ogromnych zbiorów danych treningowych. Jeśli dane treningowe zawierały elementy wewnętrznej dokumentacji firmowej, nawet w sposób niezamierzony, istnieje ryzyko, że model wygeneruje treść zawierającą fragmenty tajemnicy przedsiębiorstwa. Tego typu zjawiska zostały już odnotowane w praktyce – m.in. pracownicy firm, korzystający z chatbotów AI do opracowania prezentacji lub analizy danych, przypadkowo ujawniali dane klientów, umowy handlowe czy schematy projektowe. W wielu przypadkach firmy nie miały świadomości, że dane te zostały wprowadzone do narzędzi trzecich – co rodzi pytania o odpowiedzialność za naruszenie tajemnicy przedsiębiorstwa nie tylko po stronie sprawcy, ale także użytkownika systemu. Szczególnie problematyczna staje się kwalifikacja prawna informacji wygenerowanych przez systemy sztucznej inteligencji, które nie istniały wcześniej w postaci autonomicznego zbioru danych, lecz powstały jako rezultat analizy danych wejściowych. Powstaje pytanie, czy taki „output algorytmiczny" może zostać objęty ochroną jako tajemnica przedsiębiorstwa, skoro nie posiada pierwotnego charakteru poufnego, lecz nabywa wartość gospodarczą dopiero na etapie jego wykorzystania przez przedsiębiorcę. W ujęciu funkcjonalnym należy jednak przyjąć, że decydujące znaczenie powinno mieć nie źródło informacji, lecz jej aktualna wartość gospodarcza oraz objęcie jej realnym reżimem poufności. Jeżeli wynik działania algorytmu stanowi element przewagi konkurencyjnej przedsiębiorcy (np. model predykcyjny, zoptymalizowany algorytm decyzyjny, syntetyczny zbiór danych) i został objęty odpowiednimi środkami ochronnymi, nie ma normatywnych podstaw do automatycznego wyłączenia go spod reżimu tajemnicy przedsiębiorstwa. Jednocześnie należy dostrzec ryzyko rozszerzającej interpretacji tej ochrony, która mogłaby prowadzić do monopolizacji informacji wytworzonych na bazie danych publicznych lub powszechnie dostępnych, co pozostawałoby w kolizji z zasadą

12 Epic Systems Corp. v. Tata Consultancy Services Ltd., No. 14-cv-748 (W.D. Wis. 2020).

13 C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, op. cit.

 DOI: 10.54383/0031-0344.2026.01.5

swobody konkurencji i dopuszczalności inżynierii odwrotnej. Wymaga to wyważenia interesu ochrony innowacyjności z interesem zachowania otwartego dostępu do informacji, co obecnie nie znajduje jednoznacznego odzwierciedlenia w obowiązujących regulacjach prawa krajowego i unijnego[14].

IV. Porównanie ochrony tajemnicy przedsiębiorstwa w Polsce, Unii Europejskiej i Stanach Zjednoczonych

Ochrona tajemnicy przedsiębiorstwa w systemach prawnych Polski, Unii Europejskiej oraz Stanów Zjednoczonych opiera się na zbliżonych założeniach konstrukcyjnych, jednak istotnie różni się w zakresie instrumentów prawnych, procedur dochodzenia roszczeń oraz podejścia do informacji generowanych przez nowe technologie. Wspólnym elementem jest uznanie, że ochrona tajemnicy przedsiębiorstwa dotyczy informacji, które mają wartość gospodarczą, nie są powszechnie znane i podlegają działaniom zmierzającym do ich utrzymania w poufności[15].

IV.I. Polska

W polskim porządku prawnym zasadniczą regulacją jest ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (UZNK). Art. 11 ust. 2 tej ustawy definiuje tajemnicę przedsiębiorstwa jako informacje nieujawnione do wiadomości publicznej, posiadające wartość gospodarczą, w odniesieniu do których przedsiębiorca podjął niezbędne działania zmierzające do zachowania ich poufności[16]. Przepis ten znajduje zastosowanie zarówno w relacjach B2B, jak i pracowniczych, co potwierdza orzecznictwo Sądu Najwyższego[17]. Polskie prawo nie przewiduje obecnie odrębnych przepisów odnoszących się bezpośrednio do ochrony danych przetwarzanych przez sztuczną inteligencję czy systemy big data jako tajemnicy przedsiębiorstwa. Niemniej w praktyce możliwe jest zastosowanie przepisów UZNK również do tego typu informacji, o ile spełniają one ustawowe przesłanki.

IV.II. Unia Europejska

Na poziomie unijnym kluczowym aktem jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z 8 czerwca 2016 r. w sprawie ochrony niejawnego

14 A. Sobusiak, *Ochrona tajemnicy przedsiębiorstwa a wspieranie innowacyjności małych i średnich przedsiębiorstw w Unii Europejskiej*, rozprawa doktorska, Uniwersytet Łódzki 2023, s. 210–218.

15 M. Gawroński, op. cit., s. 1099–1105.

16 Ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. 2022, poz. 1233.

17 Wyrok Sądu Najwyższego z 3.10.2000 r., I CKN 304/00, OSNC 2001/4/59.

know-how i informacji handlowych (tajemnic przedsiębiorstwa)[18]. Dyrektywa wprowadza jednolite definicje i standardy ochrony, pozostawiając jednak państwom członkowskim swobodę w implementacji. W art. 2 ust. 1 dyrektywy wskazano trzy elementy konieczne do uznania informacji za tajemnicę przedsiębiorstwa: poufność, wartość gospodarcza oraz podjęcie działań ochronnych. Mimo że akt ten nie odnosi się wprost do zagrożeń wynikających z AI i big data, pojawiają się głosy w literaturze postulujące jego nowelizację w celu dostosowania do wyzwań technologicznych[19].

IV.III. Stany Zjednoczone

W USA podstawowym instrumentem prawnym jest federalna ustawa *Defend Trade Secrets Act* z 2016 r. (DTSA), będąca uzupełnieniem wcześniejszego Uniform Trade Secrets Act (UTSA), przyjętego na poziomie stanowym. Zgodnie z definicją zawartą w 18 U.S.C. § 1839(3) tajemnica handlowa to każda informacja, która ma wartość gospodarczą, nie jest ogólnie znana, a której właściciel podjął rozsądne działania zmierzające do utrzymania jej w tajemnicy[20]. Ustawodawstwo amerykańskie oferuje szeroki wachlarz środków ochrony, w tym możliwość żądania zabezpieczenia dowodów, odszkodowania, a nawet środków karnych. W praktyce amerykańskie sądy coraz częściej mierzą się ze sprawami dotyczącymi wykorzystania technologii AI w kontekście naruszeń tajemnic handlowych, czego przykładem jest sprawa *Epic Systems Corp. v. Tata Consultancy Services Ltd*[21].

V. Case study i analiza orzecznictwa w kontekście ochrony tajemnic przedsiębiorstwa

Jednym z kluczowych elementów zrozumienia skuteczności mechanizmów ochrony tajemnic przedsiębiorstwa w erze nowych technologii jest analiza orzecznictwa – zarówno krajowego, jak i zagranicznego – w odniesieniu do przypadków, w których doszło do naruszeń tej ochrony. Praktyka sądowa pozwala nie tylko zweryfikować efektywność obowiązujących przepisów, lecz także unaocznia istniejące luki prawne, szczególnie w kontekście wykorzystania sztucznej inteligencji i big data.

Sprawa *Epic Systems v. Tata Consultancy Services* to jeden z najbardziej znanych przypadków sądowych dotyczących naruszenia tajemnic handlowych w kontekście użycia systemów informatycznych. Firma Epic Systems, dostawca oprogramowania

18 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.06.2016 r., Dz.Urz. UE L 157, s. 1.

19 A. Sobusiak, op. cit., s. 152.

20 Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(3).

21 Epic Systems Corp. v. Tata Consultancy Services Ltd., No. 14-cv-748 (W.D. Wis. 2020), 980 F.3d 1117 (7th Cir. 2020).

 DOI: 10.54383/0031-0344.2026.01.5

dla służby zdrowia, zarzuciła Tata Consultancy Services, że pracownicy indyjskiej spółki uzyskali nieuprawniony dostęp do wewnętrznego portalu Epic, kopiując dane i materiały szkoleniowe objęte ochroną handlową. Co istotne, nie doszło do klasycznego „wykradzenia danych", lecz raczej do ich pozyskania w ramach testowego dostępu, który następnie został przekroczony i wykorzystany do stworzenia konkurencyjnego systemu informatycznego. Sąd federalny w Wisconsin uznał to działanie za naruszenie tajemnic handlowych na podstawie ustawy *Defend Trade Secrets Act* (DTSA) i przyznał Epic Systems rekordowe odszkodowanie w wysokości 940 mln USD (ostatecznie zmniejszone przez sąd apelacyjny do 420 mln USD)[22]. Sprawa ta jest o tyle istotna, że pokazuje, iż nawet dostęp logiczny, bez fizycznego kopiowania danych, może zostać uznany za działanie sprzeczne z prawem, jeśli obejmuje informacje chronione jako tajemnica handlowa. W kontekście wykorzystania AI sprawa ta bywa przywoływana w literaturze jako przykład potencjalnych ryzyk związanych z automatyzacją analizy danych: modele AI mogą pozyskiwać informacje z dokumentacji firmowej nawet bez intencji naruszenia – co stawia pytania o odpowiedzialność prawną zarówno użytkownika, jak i twórcy technologii[23].

Na gruncie prawa polskiego warto wskazać na wyrok Sądu Najwyższego z 3 października 2000 r. (I CKN 304/00), w którym stwierdzono, że nieuprawnione wykorzystanie listy klientów uzyskanej od byłego pracownika stanowi czyn nieuczciwej konkurencji w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji[24]. Chociaż wyrok ten nie dotyczy bezpośrednio AI ani nowoczesnych form przetwarzania danych, jest nadal aktualny w kontekście interpretacji „wartości gospodarczej informacji" oraz obowiązku zachowania poufności.

W nowszym orzeczeniu z 28 listopada 2018 r. (I CSK 676/17) Sąd Najwyższy analizował, czy dane zapisane w systemach komputerowych przedsiębiorcy (plany finansowe, analizy, założenia strategiczne) mogą stanowić tajemnicę przedsiębiorstwa. SN jednoznacznie uznał, że tak – niezależnie od formy zapisu, jeżeli spełnione są przesłanki z art. 11 ust. 2 UZNK[25]. Tym samym sąd potwierdził, że również dane cyfrowe – w tym pliki, dokumenty, systemy CRM – mogą być objęte prawną ochroną jako tajemnice przedsiębiorstwa.

W kontekście prawa unijnego warto zauważyć brak ugruntowanego orzecznictwa Trybunału Sprawiedliwości UE dotyczącego bezpośrednio tajemnic przedsiębiorstwa w kontekście sztucznej inteligencji. Jednakże wyrok z 29 lipca 2019 r. w sprawie *Funke Medien NRW GmbH v. Bundesrepublik Deutschland* (C-469/17) może być interpretowany jako istotny z punktu widzenia ochrony informacji o charakterze

22 Epic Systems Corp. v. Tata Consultancy Services Ltd., No. 14-cv-748 (W.D. Wis. 2020), 980 F.3d 1117 (7th Cir. 2020).

23 C. Novelli, J. Guinchard, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, 2024, s. 21.

24 Wyrok SN z 3.10.2000 r., I CKN 304/00, OSNC 2001/4/59.

25 Wyrok SN z 28.11.2018 r., I CSK 676/17, LEX nr 2621997.

niejawnym[26]. Trybunał wskazał, że prawo dostępu do dokumentów publicznych nie ma pierwszeństwa przed ochroną informacji, które mają znaczenie dla bezpieczeństwa publicznego lub interesów gospodarczych państwa. To orzeczenie pokazuje, że nawet w kontekście prawa dostępu do informacji publicznej UE uznaje prymat ochrony określonych kategorii danych – co może być podstawą do szerszego rozumienia „interesu poufności" również na gruncie relacji gospodarczych.

Analiza wybranych orzeczeń pozwala zauważyć wyraźne przesunięcie akcentu w kierunku ochrony informacji w formie cyfrowej – zarówno w USA, jak i w Polsce. W systemie amerykańskim sądy są skłonne do interpretowania bardzo szeroko definicji „tajemnicy handlowej", obejmując nią nawet dane pośrednio wykorzystane przez AI. W Polsce orzecznictwo potwierdza, że dane zapisane cyfrowo – przy zachowaniu poufności – mogą podlegać ochronie ustawowej. W UE, mimo ograniczonej liczby spraw, widać tendencję do wzmacniania ochrony informacji o znaczeniu gospodarczym.

VI. Wnioski

Z przeprowadzonej analizy wynika jednoznacznie, że dotychczasowy model ochrony tajemnic przedsiębiorstwa, choć teoretycznie rozbudowany, nie nadąża za dynamiką zmian technologicznych, szczególnie w kontekście sztucznej inteligencji oraz analizy danych masowych (big data). Przepisy ustawowe – zarówno w Polsce, jak i w większości państw UE – nie zawierają odrębnych regulacji uwzględniających specyfikę informacji generowanych i przetwarzanych przez systemy AI, co prowadzi do licznych wątpliwości interpretacyjnych, a w konsekwencji także do luki w realnej ochronie danych przedsiębiorców[27].

Ustawa o zwalczaniu nieuczciwej konkurencji, podobnie jak Dyrektywa 2016/943, operuje klasycznymi pojęciami: „informacja nieujawniona", „wartość gospodarcza", „działania zabezpieczające". Brakuje natomiast precyzyjnych wskazówek dotyczących tego, w jaki sposób oceniać informacje powstałe w wyniku działania AI – np. parametry modelu predykcyjnego, dane treningowe, zestawy danych syntetycznych, które nie istniały wcześniej jako osobny byt informacyjny, ale powstały na skutek działania algorytmu[28]. Z prawnego punktu widzenia zasadniczym problemem jest określenie, czy takie dane mają „pierwotnie poufny charakter", czy też dopiero nabywają go wtórnie, w wyniku ich użycia lub przechowywania przez przedsiębiorcę. Co więcej, brakuje ugruntowanego stanowiska co do tego, czy wyciek informacji pochodzących z systemu AI, nawet bez fizycznego kopiowania pliku, ale np. na

26 Wyrok TSUE z 29.07.2019 r., C-469/17, ECLI:EU:C:2019:623.

27 M. Gawroński, op. cit., s. 20.

28 A. Sobusiak, op. cit., s. 142.

 DOI: 10.54383/0031-0344.2026.01.5

podstawie działania modelu generatywnego, może być traktowany jako naruszenie tajemnicy przedsiębiorstwa.

Chociaż dyrektywa 2016/943 stanowi istotny krok w kierunku harmonizacji ochrony tajemnicy przedsiębiorstwa w UE, nie zawiera ona przepisów uwzględniających AI i dane masowe. Nie zostały w niej również przewidziane standardy techniczne lub proceduralne dotyczące np. ochrony danych w chmurze, klasyfikacji danych wejściowych do systemów AI, czy zakresu dopuszczalnej inżynierii odwrotnej (*reverse engineering*)[29]. Brakuje również wskazówek interpretacyjnych co do relacji między tajemnicą przedsiębiorstwa a ochroną danych osobowych przetwarzanych przez AI, co ma znaczenie szczególnie w kontekście RODO. W publikacjach OECD także zauważono konieczność wprowadzenia wytycznych, które pozwoliłyby na ocenę, kiedy działanie technologiczne – np. „uczenie się" algorytmu oparte na danych konkurencyjnych – przekracza granicę uczciwego użytku i staje się naruszeniem tajemnicy[30].

Oprócz zmian legislacyjnych niezbędne są działania po stronie samych przedsiębiorców. Powinni oni wdrażać polityki compliance dotyczące korzystania z systemów AI i danych, w tym:

- precyzyjne klauzule NDA uwzględniające dane przetworzone przez AI,
- ograniczenia dostępu do danych treningowych modeli,
- wykorzystywanie szyfrowania, DLP i SIEM,
- audyty bezpieczeństwa systemów z dostępem do informacji poufnych,
- dokumentowanie klasyfikacji danych jako „tajemnica przedsiębiorstwa".

Tajemnica przedsiębiorstwa jako instytucja prawa gospodarczego znajduje się obecnie na rozdrożu – pomiędzy klasycznym rozumieniem informacji poufnej a rzeczywistością opartą na automatycznym przetwarzaniu danych, algorytmach i sztucznej inteligencji. Utrzymanie skuteczności tej instytucji wymaga zarówno rozwoju orzecznictwa, jak i konkretnych działań legislacyjnych. Bez zdefiniowania, czym są „informacje algorytmiczne", i bez jasnych zasad ich ochrony przedsiębiorcy nie będą w stanie skutecznie zabezpieczać swoich interesów w środowisku cyfrowym.

29 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943, Dz.Urz. UE L 157.

30 OECD, *Trade Secrets Protection and Enforcement*, 2023, s. 34.

mgr Maja Wojtyś

Magister prawa, doktorantka nauk prawnych w Szkole Doktorskiej Uniwersytetu w Białymstoku, absolwentka Wydziału Prawa Uniwersytetu w Białymstoku, studentka studiów magisterskich z zakresu zarządzania. Zainteresowania badawcze obejmują prawo nowych technologii, ochronę danych, prawo własności intelektualnej oraz wpływ sztucznej inteligencji na system prawa.

Master of Law, PhD student in legal sciences at the Doctoral School of the University of Białystok, graduate of the Faculty of Law at the University of Białystok, currently a Master's student in business management. Her research interests include new technologies law, data protection, intellectual property law, and the impact of artificial intelligence on legal sys-tems.

ORCID: 0009-0005-9876-1282

Abstract

Keywords: *trade secret, big data, artificial intelligence, data protection, comparative law*

Trade secret protection in the era of artificial intelligence and big data

This article explores the challenges and new threats to trade secret protection arising from the development of artificial intelligence and big data. The author examines the issue in the context of Polish, EU and US law, emphasizing the need for legal updates and modern protection mechanisms.

Bibligrafia

1. **Czub Krzysztof,** *Sztuczna inteligencja jako podmiot praw własności intelektualnej?*, Państwo i Prawo, 2023, nr 10
2. **Gawroński Maciej**, *Definicja pojęcia „tajemnica przedsiębiorstwa" na gruncie polskiego porządku prawnego – zarys problematyki*, Monitor Prawniczy, 2022, nr 22
3. **Novelli Claudio, Casolari Federico, Hacker Philipp, Spedicato Giorgio, Floridi Luciano,** *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*, Computer Law & Security Review, 2024, vol. 55
4. **Novelli Claudio, Guinchard J.** — *Generative AI in EU Law: Liability, Privacy,* Intellectual Property, and Cybersecurity, 2024
5. OECD, *Trade Secrets Protection and Enforcement*, 2023

 DOI: 10.54383/0031-0344.2026.01.5

6. **Sobusiak Agata,** *Ochrona tajemnicy przedsiębiorstwa a wspieranie innowacyjności małych i średnich przedsiębiorstw w Unii Europejskiej*, rozprawa doktorska, Uniwersytet Łódzki, 2023
7. **Stechly Michał,** *Tajemnica przedsiębiorstwa w dobie cyfrowej transformacji*", Przegląd Prawa Handlowego, 2022, nr 5