DOI: 10.52694/LES.127/2025.17

Joanna Kufel-Orłowska
Uniwersytet w Siedlcach
https://orcid.org/0000-0002-9247-0098
joanna.kufel-orlowska@uws.edu.pl

Agata Osińska
Międzynarodowa Akademia Nauk Stosowanych w Łomży
https://orcid.org/0009-0005-4166-9207
agataosinska@vp.pl

Krzysztof Konopka
Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej
w Warszawie
https://orcid.org/0000-0001-5528-3835
biegly@krzysztofkonopka.pl

Rola prawa cybernetycznego w cyberbezpieczeństwie

The role of cyber law in cybersecurity

Streszczenie

Dynamiczny charakter współczesnych zagrożeń cybernetycznych wymaga nieustannego dostosowywania zarówno technologicznych mechanizmów ochrony, jak i ram prawnych regulujących funkcjonowanie przestrzeni cyfrowej. Prawo cybernetyczne, obejmujące normy dotyczące korzystania z systemów informatycznych i urządzeń cyfrowych, odgrywa kluczową rolę w zwalczaniu cyberprzestępczości oraz ochronie własności intelektualnej podmiotów gospodarczych. Artykuł podejmuje analizę wzajemnych relacji pomiędzy cyberbezpieczeństwem a prawem cybernetycznym, wskazując na ich komplementarność w kontekście reagowania na zagrożenia oraz prewencji.

Słowa kluczowe: cyberbezpieczeństwo, prawo cybernetyczne, zagrożenia cyfrowe

Abstract

The dynamic nature of contemporary cyber threats necessitates the continuous adaptation of both technological protection mechanisms and the legal frameworks that govern the functioning of the digital environment. Cyber law, encompassing regulations related to the use of information systems and digital devices, plays a crucial role in combating cybercrime and protecting the intellectual property of economic entities. This article analyzes the interrelationship between cybersecurity and cyber law, highlighting their complementarity in the context of both threat response and prevention.

Keywords: cybersecurity, cyber law, digital threats

Wstęp

Postęp w dziedzinie technologii informatycznych zrewolucjonizował niemal wszystkie obszary życia ludzkiego. Internet stał się kluczową częścią współczesnego życia, kształtując sposób, w jaki się komunikujemy, pracujemy, spędzamy wolny czas. Wraz z tymi postępami pojawiły się nowe wyzwania prawne, od cyberprzestępstw po kwestie prywatności danych i ochrony własności intelektualnej, które doprowadziły do powstania złożonych ram regulacyjnych. Wykorzystywanie narzędzi teleinformatycznych oraz popularyzacja środków komunikacji elektronicznej sprawiły, że pojęcie bezpieczeństwa nabrało innego, cybernetycznego znaczenia[1].

Prawo nieustannie stara się nadążyć za zmieniającą się technologią. Coraz powszechniejsze wykorzystanie technologii stworzyło ludzkości ogromne możliwości wzrostu i rozwoju, jednocześnie stając się przestrzenią sprzyjającą występowaniu działań nieetycznych. Działania nieuczciwe i niezgodne z prawem nierzadko wyprzedzają mechanizmy reagowania opracowywane przez organy ścigania. W dobie społeczeństwa informacyjnego niemal każda jednostka pozostaje w różnym stopniu zależna od technologii komputerowej, wykorzystywanej do tworzenia, przesyłania, pobierania oraz przechowywania danych. Internet zapoczątkował nową erę komunikacji, znajdując szerokie zastosowanie zarówno w sektorze komercyjnym, jak i w usługach publicznych. Wraz z jego rozwojem

[1] D. Skoczylas, *Krajowy system cyberbezpieczeństwa*, Warszawa 2023, s. LVII.

pojawiła się konieczność stworzenia ram prawnych regulujących funkcjonowanie Internetu, co zaowocowało wyodrębnieniem się dziedziny określanej mianem cyberprawem.

W opracowaniu przyjęto metodologię badawczą, dostosowaną do specyfiki analizy prawa cybernetycznego, cyberbezpieczeństwa oraz regulacji dotyczących technologii blockchain i AI. Zasadniczą podstawę stanowi metoda dogmatyczno-prawna, polegająca na analizie obowiązujących aktów prawnych zarówno na poziomie krajowym, jak i unijnym, ze szczególnym uwzględnieniem rozporządzeń i dyrektyw UE (m.in. RODO, NIS2, DORA) oraz krajowych regulacji w zakresie bezpieczeństwa cyfrowego. Metoda ta pozwoliła na odtworzenie i systematyzację obowiązującego porządku prawnego, a także na wskazanie konsekwencji wynikających z jego stosowania.

Uzupełniająco zastosowano metodę komparatystyczną, umożliwiającą zestawienie i porównanie rozwiązań legislacyjnych przyjętych w Polsce, w Unii Europejskiej oraz w USA. Dzięki temu możliwe stało się zidentyfikowanie podobieństw, różnic oraz kierunków harmonizacji prawa, co jest szczególnie istotne wobec transgranicznego charakteru cyberprzestrzeni i globalnych wyzwań związanych z bezpieczeństwem cyfrowym.

Wykorzystano również metodą analityczno-systemową, której celem było umiejscowienie badanych regulacji w szerszym kontekście instytucjonalnym i społecznym. Pozwoliło to nie tylko na identyfikację luk prawnych i niejednoznaczności interpretacyjnych, lecz także na ocenę praktycznych skutków. W tym zakresie analiza miała również charakter prognostyczny, wskazując potencjalne kierunki dalszego rozwoju legislacji w obszarze cyberbezpieczeństwa, technologii blockchain i AI.

Istota cyberbezpieczeństwa

Słowo „cyberbezpieczeństwo" nie zostało jeszcze zdefiniowane w sposób kompleksowy ze względu na złożoną i zmieniającą się naturę technologii informatycznych i komunikacyjnych, zarówno na poziomie globalnym i krajowym. Jest nową dziedziną bezpieczeństwa państwa, która ma związek z cyberprzestępczością oraz cyberterroryzmem[2] Jedną

[2] T. Hoffmann, *Główni aktorzy cyberprzestrzeni i ich działalność*, [w:] T. Dębowski (red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku*, Łódź–Wrocław 2018, s. 27–28.

z najbardziej zwięzłych definicji można znaleźć na stronie internetowej *Techtarget* i stwierdza ono że: „Cyberbezpieczeństwo to zbiór technologii, procesów i praktyk mających na celu ochronę sieci, komputerów, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem[3]. Podobnie brzmiące definicje określa *National Research Council4* i *European Union Agency for Network and Information Security5* . Natomiast *Palo Alto Networks6* określa je jako ochronę informacji i systemów przed poważnymi cyberzagrożeniami, takimi jak cyberterroryzm, cyberwojna i cybernetyczne szpiegostwo.

Cyberbezpieczeństwo jest procesem zapewnienia bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni[7]. Ma ono na celu zapobieganie szkodom oraz ochronę, a także przywracanie integralności i dostępności systemów komputerowych, usług komunikacji elektronicznej, sieci przewodowych oraz bezprzewodowych[8]. Obejmuje ono zarówno sektor publiczny, jak i prywatny, uwzględniając również wzajemne relacje pomiędzy tymi podmiotami w zakresie tworzenia, wdrażania i egzekwowania norm dotyczących bezpieczeństwa informacyjnego[9]. Pojęcie to stanowi w istocie normatywną konstrukcję myślową oznaczającą bezpieczeństwo systemów i sieci (IT)[10]. Odnosi się do działań mających na celu zapewnienie bezpieczeństwa oraz przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni,

[3] Badruddin, A. Ahmad, *Cyber Security Challenges: Some Reflections on Law and Policy in India*, "The Haryana Police Journal" 2017, vol. 1, iss. 1, s. 78.

[4] Narodowa Rada ds. Badań Naukowych, organ operacyjny Narodowej Akademii Nauk, Inżynierii i Medycyny w Stanach Zjednoczonych.

[5] Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) była ośrodkiem wiedzy specjalistycznej w zakresie cyberbezpieczeństwa w UE, pomagając UE i jej państwom członkowskim w przygotowaniu się do problemów z bezpieczeństwem informacji i reagowaniu na nie. Rolą ENISA było opracowywanie porad i zaleceń dotyczących dobrych praktyk, pomoc państwom członkowskim we wdrażaniu odpowiednich przepisów UE oraz poprawa odporności krytycznej infrastruktury informacyjnej Europy.

[6] Palo Alto Networks – światowy lider w dziedzinie cyberbezpieczeństwa. Zob. https://www.paloaltonetworks.com/ [dostęp: 15 maja 2025].

[7] C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w]: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 31.

[8] Department of Homeland Security Authorization Act for Fiscal Year-2006, Part 3, 109th Congress First Session, Report, May 2005.

[9] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, vol. 2, s. 7.

[10] C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo*, Warszawa 2020, s. 16.

rozumianej jako przestrzeń komunikacji elektronicznej i przetwarzania danych.

Cyberbezpieczeństwo obejmuje zabezpieczanie wszystkich komponentów funkcjonujących w cyberprzestrzeni, w tym infrastruktury sieciowej, oprogramowania, informacji oraz operacji cyfrowych. Ponieważ te elementy mogą zawierać wrażliwe lub strategiczne dane, konieczne jest zapewnienie pięciu fundamentalnych atrybutów bezpieczeństwa informacji: poufności, integralności, dostępności, uwierzytelniania oraz niezaprzeczalności, które to stanowią podstawowe jego filary oraz zapewniają stabilność i odporność systemów informacyjnych[11]. Poufność odnosi się do ochrony informacji przed ujawnieniem osobom nieuprawnionym. Gwarantuje, że dane są dostępne wyłącznie dla wskazanych podmiotów. W kontekście RODO[12] (art. 5 ust. 1 lit. f) poufność jest ściśle związana z obowiązkiem ochrony danych osobowych przed nieautoryzowanym ujawnieniem. Również norma ISO/IEC 27001[13] uznaje poufność za jeden z trzech głównych celów systemu zarządzania bezpieczeństwem informacji (ISMS). Integralność zapewnia, że dane są dokładne, spójne oraz nie zostały nieautoryzowanie zmodyfikowane w trakcie przesyłu, przetwarzania lub przechowywania. Zgodnie z normą ISO/IEC 27001, integralność odnosi się do ochrony przed przypadkowymi lub celowymi zmianami danych. Również dyrektywa NIS2 nakłada na operatorów usług kluczowych obowiązek zapewnienia integralności systemów informatycznych. Dostępność oznacza zapewnienie, że dane i systemy są dostępne dla uprawnionych użytkowników w momencie, gdy są potrzebne. W ramach NIS2[14] dostępność infrastruktury krytycznej traktowana jest jako jeden z priorytetów bezpieczeństwa sieci i systemów informatycznych. Standardy ISO/IEC 27001 kładą szczególny nacisk na zapewnienie ciągłości

[11] I. Priyadarshini, *Introduction on cybersecurity*, [w:] L. DacNhuong, K. Raghvendra, B.K. Mishra, K. Manju (red.), *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies*, Beverly MA 2019, s. 6.

[12] Rozporządzenie Parlamnetu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

[13] ISO/ IEC 27001 to międzynarodowa, uznawana na całym świecie, norma dotycząca Systemu Zarządzania Bezpieczeństwem Informacji. Zwiera wskazówki, które pomagają Organizacjom ustanawiać, wdrażać, utrzymywać i stale doskonalić System Zarządzania Bezpieczeństwem Informacji. ISO/ IEC 27001 pomaga zidentyfikować zagrożenia związane z naruszeniami bezpieczeństwa informacji i wpływa na zmniejszenie prawdopodobieństwa wystąpienia naruszeń.

[14] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

działania jako elementu wspierającego dostępność. Uwierzytelnianie odnosi się do procesu potwierdzania tożsamości użytkownika, urządzenia lub systemu przed udzieleniem dostępu do określonych zasobów. Mechanizmy uwierzytelniające, takie jak hasła, certyfikaty cyfrowe czy biometria, są uznawane za kluczowy element systemów kontroli dostępu, wymagany zarówno przez RODO, jak i zalecany w ISO/IEC 27002 – zbiorze praktycznych wytycznych do ISO/IEC 27001.

Kluczowy z tego zakresu w Unii Europejskiej, oprócz wspomnianych wyżej rozporządzenia RODO, dyrektywy NIS2 i normy ISO/IEC 27002, jest również akt Unii Europejskiej w sprawie cyberbezpieczeństwa, który wzmacnia Agencję UE ds. Cyberbezpieczeństwa (ENISA) i ustanawia zakres certyfikacji dla produktów i usług[15].

Krajową implementację przepisów dyrektywy NIS stanowi Ustawa z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa[16], która oprócz ustanowienia zasad działania organów państwa, precyzuje, które podmioty wchodzą w skład krajowego systemu cyberbezpieczeństwa. Ze względów praktycznych wymogi ustawy nie są stosowane horyzontalnie wobec wszystkich przedsiębiorców, lecz – zgodnie z podejściem dyrektywy – kierowane są wyłącznie do podmiotów mających istotne znaczenie dla gospodarki i bezpieczeństwa[17]. Z pozostałych rozporządzeń i dyrektyw należy wskazać: rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19 października 2022r. w sprawie jednolitego rynku usług cyfrowych[18] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z 14 września 2022r. w sprawi kontestowalnych i uczciwych rynków w sektorze cyfrowym[19].

Warto wspomnieć również o Europejskich ramach certyfikacji EUCCF, który stanowi zestaw zasad i kryteriów opracowany przez Agencję UE ds.

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r., w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, link: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32019R0881 [dostęp: 15 maja 2025].

[16] Ustawa z 5 lipca 2018 r. – o Krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. 2018 poz. 1560)

[17] Sz. Ciach, *Prawo w IT. Praktycznie i po ludzku*, Gliwice 2024, s. 369.

[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), link: https://sip.lex.pl/akty-prawne/dzienniki-UE/rozporzadzenie-2022-2065-w-sprawie-jednolitego-rynku-uslug-cyfrowych-oraz-72067488 [dostęp: 15 maja 2025].

[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych).

Cyberbezpieczeństwa w celu zapewnienia poziomu cyberbezpieczeństwa produktów, usług i technologii informacyjno-komunikacyjnych[20].

Wśród organizacji i instytucji działających w tym obszarze w UE trzeba wyszczególnić: Europejskie centra wymiany i analizy informacji (ISAC), Europejską Organizację Cyberbezpieczeństwa (ESCO), zespoły reagowania na incydenty związane w bezpieczeństwem komputerowym CSIRT, zespoły reagowania na awarie komputerowe CERT, Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC), Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA[21]).

Omawiane zagadnienie stanowi obszar charakteryzujący się wyjątkowo wysoką dynamiką rozwoju, wynikającą bezpośrednio z ciągłego postępu technologicznego. Ewolucja środowiska cyfrowego prowadzi do powstawania coraz bardziej zaawansowanych narzędzi zarówno ofensywnych, jak i defensywnych. W rezultacie cyberprzestrzeń staje się nieustannym polem konfrontacji pomiędzy atakami a detekcją, reagowaniem i przeciwdziałaniem zagrożeniom, natomiast skala i złożoność prowadzonych działań wskazują na rosnące znaczenie tej interakcji w kontekście strategii zarządzania ryzykiem cybernetycznym zarówno w sektorze publicznym, jak i prywatnym.

W kontekście cyberprzestrzeni pojawia się zasadnicze pytanie dotyczące kwestii moralności oraz legalności. Współczesne społeczeństwo jest w dużej mierze zależne od Internetu, a cyberprzestrzeń, obejmująca sieci komputerowe, stanowi przestrzeń dostępną dla wszystkich użytkowników posiadających urządzenia łączące się z siecią. Brak rozróżnienia pod względem cech demograficznych, takich jak rasa czy wyznanie, implikuje konieczność uznania cyberprzestrzeni za środowisko o charakterze globalnym i inkluzywnym, co pociąga za sobą obowiązek etycznej i prawnej odpowiedzialności użytkowników. Istotne jest, aby zapewnić funkcjonowanie cyberprzestrzeni zgodnie z określonym kodeksem postępowania, promującym zasadę „żyj i pozwól żyć", która umożliwia harmonijne współistnienie użytkowników. Niemniej jednak obserwuje się liczne przypadki nadużywania cyberprzestrzeni oraz narzędzi i technik z nią związanych, zarówno w sposób zamierzony, jak i niezamierzony. Często osoby dotknięte skutkami takich działań nie zdają sobie sprawy

[20] B. Hołyst, *Kryminalistyka cyfrowa*, Warszawa 2025, s. 1121.
[21] B. Hołyst, *Kryminalistyka*…, s. 1122–1125.

z popełnionych naruszeń, co prowadzi do ich niesłusznego obarczania odpowiedzialnością za czyny nieświadome lub nieumyślne. Konieczne jest pogłębione zbadanie etycznych i prawnych wymiarów funkcjonowania w cyberprzestrzeni oraz identyfikacja ryzyk z nią związanych. Ponadto, istotne jest opracowanie kompleksowych polityk i regulacji, które pozwolą na minimalizację negatywnych skutków nadużyć oraz zagwarantują odpowiedzialne i zgodne z prawem korzystanie z tego globalnego środowiska cyfrowego[22].

Pojęcie prawa cybernetycznego

Dynamiczny wzrost wykorzystania Internetu w ostatniej dekadzie XX wieku i wszelkie zagrożenia związane z bezpieczeństwem jego użytkowania dało początek nowej dziedzinie prawa, określanej jako „prawo cybernetyczne", która zajmuje się regulacją zjawisk i relacji prawnych zachodzących w środowisku cyfrowym.

W miarę szybkiej ewolucji środowiska cyfrowego potrzebne były nowe przepisy, mających na celu ochronę praw i interesów zarówno jednostek, jak i podmiotów gospodarczych korzystających z zasobów Internetu. Celem tych regulacji jest również promowanie bezpiecznego oraz odpowiedzialnego korzystania z technologii umożliwiających komunikację elektroniczną. Obecnie prawo cybernetyczne zajmuje się szerokim zakresem zagadnień, od prywatności i własności intelektualnej po cyberbezpieczeństwo i wolność wypowiedzi w kontekście cyfrowym.

Prawo cybernetyczne ma za zadanie ustanowić normy postępowania w cyberprzestrzeni, zapewniając tym samym, że działalność użytkowników nie godzi w prawa innych uczestników środowiska cyfrowego. Jakiekolwiek naruszenie ustanowionych regulacji – niezależnie od jego formy – jest traktowane jako naruszenie zasad obowiązujących w cyberprzestrzeni i może skutkować odpowiedzialnością prawną na podstawie obowiązujących przepisów. Zasadniczym celem tej gałęzi prawa jest ochrona praw jednostek funkcjonujących w przestrzeni cyfrowej oraz zapobieganie działaniom naruszającym te prawa.

[22] I. Priyadarshini, Ch. Cotton, *Cybersecurity*. *Ethics, Legal, Risks, and Policies*, Floryda 2022, s. 54.

Prawo cybernetyczne[23] można zdefiniować jako ustawodawstwo, które stanowi podstawę akceptowalnego behawioralnego korzystania z technologii, takiej jak sprzęt komputerowy i oprogramowanie, Internet i sieci. Gwarantuje ono ochronę użytkowników przed wszelkimi szkodami poprzez umożliwienie prowadzenia dochodzeń i oskarżeń w sprawie przestępstw internetowych. Ponadto dotyczy ono działań ludzi, zgromadzeń, społeczeństwa ogólnego, rządu i stowarzyszeń prywatnych[24]. To gałąź prawa zajmująca się zagadnieniami prawnymi związanymi z użytkowaniem technologii informacyjno-komunikacyjnych połączonych w sieci. Reguluje ono aspekty związane z funkcjonowaniem komputerów oraz Internetu. Ma kluczowe znaczenie, ponieważ odnosi się do niemal wszystkich aspektów transakcji i aktywności realizowanych w Internecie, sieci *World Wide Web* oraz szeroko rozumianej cyberprzestrzeni. Każde działanie i reakcja w tym środowisku posiadają swoje implikacje prawne i cyberprawne. Zakres prawa cybernetycznego obejmuje regulacje dotyczące cyberprzestępczości, podpisów elektronicznych i cyfrowych, własności intelektualnej, ochrony danych osobowych oraz prywatności. Ponadto prawo to normuje globalną przestrzeń cyfrową, zapewniając ochronę przed cyberprzestępczością, naruszeniami bezpieczeństwa danych oraz cybernetycznym szpiegostwem.

Warto podkreślić, że cybernetyka jest nauką poświęconą kontroli, podczas gdy prawo jest jedną z metod kontroli społecznej. Zainteresowanie cybernetyków prawem, jak również zainteresowanie cybernetyką wykazywane przez prawników jest naturalne. Słowo cybernetyka pochodzi od greckiego *kybernetiken*, które oznacza umiejętność kierowania, sterowania. *Kybernetiken* pochodzi zaś od *kyberan*, co oznacza kierowanie, kontrolowanie[25].

Zasadniczym celem prawa cybernetycznego jest wymuszenie na organizacjach obowiązku zabezpieczenia informacji oraz systemów przed cyberatakami poprzez zastosowanie różnorodnych środków i metod prewencyjnych oraz reaktywnych.

Obowiązywanie prawa cybernetycznego w cyberprzestrzeni uzasadnione jest przez: (1) zakres regulacji – prawo to dotyczy niemal wszystkich aspektów transakcji oraz zachowań występujących w Internecie, sieci

[23] W artykule zamiennie używane są pojęcia prawo cybernetyczne, cyberprawo, prawo Internetu, prawo cyfrowe, prawo cyberprzestrzeni, prawo cyberbezpieczeństwa.
[24] I. Priyadarshini, Ch. Cotton, *Cybersecurity*. *Ethics, Legal…*, s. 136.
[25] M. Mazur, *Cybernetyczna teoria układów samodzielnych*, Warszawa 1966, s. 12.

World Wide Web oraz cyberprzestrzeni; (2) prawną skuteczność umów cyfrowych – zapewnia ono możliwość zawierania umów elektronicznych, umożliwiając legalne i skuteczne prowadzenie działalności w środowisku cyfrowym; (3) ochronę przed zagrożeniami – wobec rosnącej częstotliwości oraz potencjalnej szkodliwości cyberzagrożeń, takich jak malware, phishing, włamania, oszustwa komputerowe, nieautoryzowany dostęp, odmowa usługi (DoS) oraz rozpowszechnianie treści pornograficznych, prawo cybernetyczne stanowi fundament ochrony danych poufnych i systemów informatycznych; (4) dowody w postępowaniach karnych – w licznych sprawach karnych niezwiązanych bezpośrednio z cyberprzestępczością, takich jak zabójstwa, porwania, przestępstwa podatkowe czy sprawy rodzinne, istotne dowody często znajdują się w systemach komputerowych oraz urządzeniach mobilnych; oraz (5) ochronę gospodarki i reputacji – przyczynia się do ochrony interesów ekonomicznych oraz reputacji osób fizycznych i prawnych poprzez zapobieganie szkodom wynikającym z działań nielegalnych lub nieetycznych w cyberprzestrzeni[26]. Dodatkowo, ze względu na to, że niemal wszystkie transakcje odbywają się obecnie w formie elektronicznej, odpowiedzialność prawna w tym obszarze jest znacząca. Prawo cybernetyczne stanowi również integralną część kryminalistyki cyfrowej, a normy prawne, w tym przepisy odnoszące się do zasad legalności przeszukań oraz łańcucha dostaw, są niezbędne dla prawidłowego zabezpieczenia i wykorzystania dowodów cyfrowych w postępowaniach sądowych.

W miarę rozwoju technologii i komunikacji elektronicznej stało się jasne, że ramy prawne istniejące na początku ery cyfrowej nie będą wystarczające, aby zapewnić bezpieczny, uczciwy i inkluzywny Internet dla wszystkich użytkowników. Przepisy i regulacje, które obejmują to, co obecnie nazywa się prawem cybernetycznym, mają na celu uregulowanie następujących kwestii: (1) prywatność i ochronę danych wraz z rozwojem handlu internetowego, w którym osoby i organizacje zaczęły udostępniać ogromne ilości danych osobowych i poufnych, konieczne stało się wprowadzenie przepisów chroniących prywatność i regulujących gromadzenie, przechowywanie i wykorzystywanie danych; (2) ochronę własności intelektualnej – Internet ułatwił odtwarzanie i dystrybucję

[26] I. Priyadarshini, H. Wang, C. Cotton, *Some cyberpsychology techniques to distinguish humans and bots for authentication*, "Proceedings of the Future Technologies Conference" 2019, nr 2, s. 306; H. Saini, Y. Rao, T.C. Panda, *Cyber-crimes and their* impacts: A review, "International Journal of Engineering Research and Applications" 2012, nr 2, s. 202–209.

własności intelektualnej, takiej jak muzyka, filmy, oprogramowanie i treści pisemne. W rezultacie przepisy dotyczące naruszenia praw autorskich, piractwa i ochrony własności intelektualnej online musiały zostać zaktualizowane, aby odzwierciedlały nową rzeczywistość; (3) cyberbezpieczeństwo i cyberprzestępczość – wraz ze wzrostem liczby cyberataków, hakowania i oszustw internetowych, prawo cybernetyczne pomogło zdefiniować i egzekwować zasady dotyczące cyberbezpieczeństwa oraz ścigać cyberprzestępców.; (4) handel elektroniczny i umowy online – wraz z rozwojem handlu internetowego, kluczowe stało się ustanowienie nowych zasad dotyczących umów online, podpisów elektronicznych, ochrony konsumentów i rozstrzygania sporów w transakcjach e-commerce, (5) wolność wypowiedzi i słowa – Internet rozszerzył możliwości jednostek do wyrażania swoich poglądów, ale podniósł również kwestie dotyczące granic wolności słowa i regulacji mowy nienawiści, zniesławienia i innych szkodliwych treści online; (6) zarządzanie Internetem – prawo cybernetyczne odegrało kluczową rolę w ustanowieniu ram zarządzania Internetem, w tym zarządzania nazwami domen, standardów internetowych i regulacji dostawców usług internetowych; (7) odpowiedzialność – prawo cybernetyczne odegrało kluczową rolę w określeniu odpowiedzialności i zobowiązań różnych podmiotów, w tym platform internetowych, twórców treści i użytkowników; (8) działalność organów ścigania i współpraca międzynarodowa – prawo cybernetyczne odegrało rolę w ułatwianiu współpracy między organami ścigania ponad granicami w celu zwalczania cyberprzestępczości i egzekwowania przepisów dotyczących cyberprzestrzeni[27].

Współczesne prawo cyberbezpieczeństwa w znacznym stopniu opiera się na paradygmacie zarządzania ryzykiem informacyjnym, którego integralnymi elementami są: identyfikacja i analiza zagrożeń, oceny ryzyka, przeprowadzanie regularnych audytów bezpieczeństwa oraz projektowanie i wdrażanie procedur reagowania na incydenty. Tego rodzaju podejście umożliwia systematyczne minimalizowanie potencjalnych szkód wynikających z naruszeń bezpieczeństwa cyfrowego. Nadrzędnym celem cyberprawa jest zapewnienie ochrony poufności, integralności i dostępności informacji – zarówno danych osobowych, jak i zasobów o charakterze strategicznym, takich jak własność intelektualna czy infrastruktura

[27] *Cyber Law: What You Need to Know*, „AXIOM", link: https://www.axiomlaw.com/guides/cyber-law [dostęp: 12.04.2025].

krytyczna. System prawny w tym zakresie dąży do stworzenia bezpiecznego środowiska cyfrowego poprzez ustanowienie norm zapobiegających zagrożeniom oraz umożliwiających skuteczne przeciwdziałanie incydentom naruszającym bezpieczeństwo cyberprzestrzeni.

Prawo Internetu nie ogranicza się do bezpieczeństwa IT i wykracza poza ochronę danych[28], koncentrując się na integralności technologii operacyjnej, która kontroluje procesy fizyczne. Ma ono również zastosowanie do każdej organizacji, która przetwarza dane osobowe lub utrzymuje systemy cyfrowe, niezależnie od wielkości lub branży. W zakresie cybeprzestępczości, skupia się również na środkach zapobiegawczych, odpowiedzialności organizacyjnej i reagowania na incydenty.

Elementy polityki cyberbezpieczeństwa

Pomimo że przepisy prawne i regulacje stanowią istotny mechanizm prewencyjny wobec cyberprzestępczości, nie gwarantują one całkowitej eliminacji incydentów, takich jak ataki hakerskie czy ransomware. Wobec tego kluczowym aspektem strategii ochrony zasobów cyfrowych jest wdrożenie przez przedsiębiorstwa i organizacje kompleksowych polityk cyberbezpieczeństwa. Polityki te powinny być ukierunkowane na zapewnienie triady bezpieczeństwa informacji – poufności, integralności oraz dostępności danych i systemów – stanowiąc fundament odporności na zagrożenia i minimalizując potencjalne skutki naruszeń.

Prawo cybernetyczne obejmuje zestaw norm mających na celu ochronę danych oraz zapewnienie bezpiecznego funkcjonowania systemów i sieci informatycznych. Kluczowe elementy tych regulacji zostały opisane we wcześniejszej części artykułu.

Prawo cybernetyczne obejmuje normy mające na celu ochronę danych i zapewnienie bezpiecznego działania systemów i sieci. Są to: (1) – przepisy prawa karnego – które karze osoby atakujące sieci komputerowe i dane komputerowe; (2) wymagania dotyczące wdrożenia środków organizacyjnych i technicznych w celu ochrony sieci i informacji przed nieautoryzowanym dostępem, naruszeniami i cyberprzestępczością. Obowiązki powierników danych w zakresie ochrony danych osobowych przed utratą

[28] J. Dempsey, Ch. Saniuk-Heing, *Cybersecurity Law Basics*, „IAPP", styczeń 2025 r., link: https://iapp.org/resources/article/cybersecurity-law-basics/ [dostęp: 25 maja 2025 r.].

lub niewłaściwym wykorzystaniem; (3) przepisy nakazujące powiadamianie o naruszeniach i incydentach władzom i/lub osobom dotkniętym, aby umożliwić szybką reakcję na cyberzagrożenia, oraz (4) środki ułatwiające międzynarodową współpracę między organizacjami i rządami w zakresie cyberzagrożeń, nieograniczone tradycyjnymi granicami.

Pomimo, że cyberprzestrzeń ma charakter globalny, regulacje prawne dotyczące cybernetyki wykazują istotne zróżnicowanie pomiędzy poszczególnymi państwami a wdrażanie krajowych ustawodawstw antycyberprzestępczych przebiega w różnym tempie i formie.

Obecnie liderem w dziedzinie cyberbezpieczeństwa pozostają Stany Zjednoczone. Wynika to z wielowymiarowych działań, w których sektor publiczny odgrywa kluczową rolę, zarówno poprzez ustanawianie sprzyjających regulacji dla przedsiębiorstw z sektora cyberbezpieczeństwa, jak i poprzez aktywne wspieranie rozwoju branży we współpracy z podmiotami prywatnymi Większość państw posiada uregulowania prawne w zakresie cybernetyki, część natomiast pracuje nad projektami ustaw, a niektóre nadal nie mają formalnych regulacji w tym obszarze. Wiele jurysdykcji podejmuje inicjatywy legislacyjne polegające na tworzeniu nowych aktów prawnych bądź rozszerzaniu istniejących kodeksów o przepisy odnoszące się do cyberprzestępczości. Dotychczasowe regulacje prawne uwzględniały specyfikę lokalnych uwarunkowań oraz priorytetów bezpieczeństwa. Znaczne różnice istnieją także w zakresie zdolności państw do prowadzenia skutecznych dochodzeń oraz egzekwowania kar za przestępstwa popełniane w cyberprzestrzeni. Dodatkowo zróżnicowane poziomy zagrożeń w poszczególnych krajach komplikują próby ustanowienia uniwersalnych, globalnych norm prawnych dotyczących tego zagadnienia. Np. prawo cybernetyczne rozwija się w odmienny sposób w Stanach Zjednoczonych i w Unii Europejskiej. Unia Europejska buduje prawo cybernetyczne w sposób bardziej scentralizowany i jednolity, akcentując prawa jednostki oraz bezpieczeństwo rynku wewnętrznego, podczas gdy Stany Zjednoczone stawiają na pragmatyzm i elastyczność, kosztem fragmentaryczności i zróżnicowanego poziomu ochrony.

Unia Europejska stara się tworzyć regulacje obejmujące jak najszerszy zakres technologii cyfrowych – od zagadnień związanych z ochroną danych osobowych, przez kwestie cyberbezpieczeństwa, aż po rozwój tokenizacji i sztucznej inteligencji[29]. Z kolei Stany Zjednoczone sku-

[29] Zob. European Union Agency for Cybersecurity, *ENISA Threat Landscape 2023*, Luxembourg 2023.

piają się przede wszystkim na zabezpieczaniu interesów gospodarczych oraz ochronie bezpieczeństwa narodowego, wprowadzając regulacje dostosowane do specyficznych sektorów i aktualnych wyzwań[30]. Unia Europejska stosuje podejście prewencyjne i dąży do ujednolicenia ram prawnych dla wszystkich państw członkowskich. Stąd tak ważne akty jak Ogólne rozporządzenie o ochronie danych (RODO), dyrektywa NIS2 czy niedawno przyjęty AI Akt o sztucznej inteligencji, które mają charakter kompleksowy i obejmują szeroki zakres zastosowań technologii cyfrowych. Z kolei w Stanach Zjednoczonych system jest bardziej sektorowy i reaktywny. Brak tu jest jednego, całościowego aktu odpowiadającego np. RODO, a regulacje powstają w odniesieniu do określonych branż, jak *Health Insurance Portability and Accountability Act* (HIPAA) dla danych medycznych czy *Gramm–Leach–Bliley Act* (GLBA) dla sektora finansowego, lub na poziomie stanowym jak np. *California Consumer Privacy Act* (CCPA)[31]. Co więcej, w Europie ochrona danych uznawana jest za prawo podstawowe, co przekłada się na rygorystyczne obowiązki nałożone na pracodawców, instytucje i przedsiębiorstw. Stany Zjednoczone nie posiadają jednego, spójnego systemu, a poziom ochrony danych zależy od branży i jurysdykcji stanowej[32]. Widać również różnicę w zakresie egzekwowania prawa i nakładania sankcji. W UE kary za naruszenia mogą sięgać do 4% globalnego obrotu przedsiębiorstwa, co czyni system bardziej restrykcyjnym i odstraszającym[33] W USA kary mają charakter sektorowy, a egzekwowanie przepisów spoczywa na różnych instytucjach, takich jak Federalna Komisja Handlu (FTC), Departament Sprawiedliwości czy wyspecjalizowane agencje branżowe[34]. Unia Europejska tworzy akty kompleksowe i spójne, co zwiększa bezpieczeństwo prawne, ale jednocześnie czyni proces legislacyjny powolnym i trudnym do adaptacji w obliczu dynamicznych zmian technologicznych. Stany Zjednoczone,

[30] Raport National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018, link: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf [dostęp: 24.09.2025]

[31] Ustawa o ochronie prywatności konsumentów w Kalifornii (CCPA) to ustawa o ochronie danych osobowych, która zapewnia mieszkańcom Kalifornii większą kontrolę nad swoimi danymi osobowymi.

[32] S.S. Bakare, A.O. Adeniyi, Ch.U. Akpuokwe, N.E. Eneh, *Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations*, "Computer Science & IT Research Journal", 2024, vol. 5, iss.3., s. 528.

[33] P. Voigt., A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (2nd ed.), Cham 2024, s. 289.

[34] Zob. *The Federal Trade Commission 2023 Privacy and Data Security Update*, link: https://www.ftc.gov/system/files/ftc_gov/pdf/2024.03.21-PrivacyandDataSecurityUpdate-508.pdf [dostęp: 24.09.2025].

dzięki miękkim regulacjom i sektorowemu podejściu, reagują szybciej, lecz kosztem spójności i równego poziomu ochrony obywateli.

Podejście USA charakteryzuje się większą elastycznością i szybkością reakcji, co umożliwia natychmiastowe wdrażanie nowych standardów w odpowiedzi na dynamiczne zagrożenia. Jednak sektorowy model powoduje brak spójności. UE natomiast tworzy przepisy bardziej spójne i przewidywalne, ale proces legislacyjny jest długotrwały, co utrudnia szybkie dostosowanie prawa do szybko rozwijających się technologii.

Cyberbezpieczeństwo a cyberprawo

Rolą prawa cybernetycznego jest zatem prawne regulowanie kwestii związanych z bezpieczeństwem w cyberprzestrzeni, natomiast cyberbezpieczeństwo to działania i środki mające na celu ochronę przed cyberzagrożeniami. Jedno określa zasady, drugie – metody działania. Prawo cybernetyczne tworzy ramy prawne, zaś cyberbezpieczeństwo to praktyczne działania mające na celu przestrzeganie tych przepisów i ochronę przed cyberzagrożeniami. Oznacza to, że przepisy określają, jakie działania są dozwolone, a jakie są zabronione w cyberprzestrzeni. Cyberbezpieczeństwo to natomiast praktyczne działania, które mają na celu przestrzeganie tych przepisów i minimalizowanie ryzyka związanych z cyberzagrożeniami[35]. Na przykład: prawo cybernetyczne wskazuje w RODO – Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679) – jak chronić dane osobowe, cybeberzpieczeństwo zaś to podjęcie działań, mających na celu zapewnienie, że przetwarzanie danych osobowych następuje zgodnie z tymi przepisami. Inny przykład dotyczy cyberprawa jako instrumentu normotwórczego, który definiując, które działania w środowisku cyfrowym stanowią przestępstwa komputerowe (np. hacking), naruszenie integralności danych lub sabotaż cyfrowy, ustanawia ramy odpowiedzialności prawnej, zarówno karnej, jak i cywilnej, dla sprawców naruszeń w cyberprzestrzeni. W tym przypadku cybebezpieczeństwo obejmuje zbiór środków technicznych, organizacyjnych i proceduralnych, mających na celu zapobieganie tego rodzaju incydentom.

[35] *Difference Between Cyber Security and Cyber Law*, „CyberSapiens The Cyber Seciurity Experts", 28 grudnia 2024 r., link: https://cybersapiens.com.au/cyber-awareness/difference-between-cyber-security-and-cyber-law/ [dostęp: 15 maja 2025 r.].

W praktyce oznacza to wdrażanie mechanizmów ochronnych, takich jak silne metody uwierzytelniania, systemy antywirusowe, firewalle, segmentacja sieci oraz regularna aktualizacja i utrzymanie oprogramowania. Cyberprzepisy ograniczają lub zapobiegają szkodom wyrządzonym przez działalność przestępczą w Internecie, chroniąc prywatność, dostęp do informacji, własność intelektualną (IP), komunikację i wolność słowa związaną z korzystaniem ze stron internetowych, telefonów komórkowych, poczty e-mail, komputerów, Internetu, oprogramowania i sprzętu, takiego jak urządzenia do przechowywania danych.

Prawo cyberbezpieczeństwa odgrywa kluczową rolę w regulacji funkcjonowania cyberprzestrzeni, stanowiąc podstawę ładu normatywnego w środowisku cyfrowym. Jako element globalnej infrastruktury prawnej, obejmuje swoim zakresem zarówno podmioty indywidualne, organizacje, jak i instytucje rządowe. Obszary objęte regulacjami prawa cyberbezpieczeństwa obejmują m.in. przeciwdziałanie cyberprzestępczości, ochronę własności intelektualnej w środowisku cyfrowym, regulacje handlu elektronicznego, prawo do prywatności oraz zarządzanie ochroną danych osobowych.

W kontekście działalności gospodarczej, prawo cyberbezpieczeństwa ma istotne znaczenie strategiczne. Umożliwia przedsiębiorstwom wdrażanie ram zgodności z przepisami prawnymi, wzmacniając tym samym ich odporność na zagrożenia cyfrowe. Ponadto stanowi podstawę do tworzenia polityk wewnętrznych dotyczących zarządzania ryzykiem informacyjnym, zapobiegania incydentom naruszenia danych oraz zapewnienia zgodności operacyjnej z krajowymi i międzynarodowymi standardami ochrony informacji.

Efektywne zarządzanie zagrożeniami w środowisku cyfrowym wymaga zintegrowanego podejścia, w którym cyberbezpieczeństwo i prawo cybernetyczne odgrywają komplementarne, lecz odrębne funkcje. Jedno stanowi technologiczną infrastrukturę pierwszej reakcji – jego zadaniem jest zapobieganie atakom, detekcja incydentów w czasie rzeczywistym oraz minimalizowanie skutków naruszeń. W przypadku, gdy mechanizmy prewencyjne zawodzą, aktywizuje się komponent normatywny, tj. prawo cybernetyczne, którego celem jest uregulowanie odpowiedzialności, ochrona interesów podmiotów poszkodowanych oraz wdrożenie procedur sankcyjnych i naprawczych.

Tabela 1. Różnica między cyberbezpieczeństwem a prawem cybernetycznym

	Cyberbezpieczeńswo	**Prawo cybernetyczne**
Cel	Ochrona systemów teleinformatycznych, sieci, danych i użytkowników przed zagrożeniami cyfrowymi. Zwiększanie odporności organizacyjnej i technicznej państwa oraz podmiotów prywatnych	Egzekwowanie zasad prawnych w cyberprzestrzeni, zapewnienie zgodności działań z obowiązującymi normami oraz nakładanie sankcji na sprawców naruszeń.
Przedmiot działania	Zapobieganie, wykrywanie i neutralizacja zagrożeń: ataków hakerskich, wirusów, ransomware, phishingu. Ochrona infrastruktury krytycznej i usług cyfrowych.	Regulacja odpowiedzialności i praw w sieci. Obejmuje m.in. ochronę danych osobowych (RODO), odpowiedzialność za cyberprzestępstwa, regulacje dot. usług cyfrowych, prawa autorskie online, handel elektroniczny.
Odpowiedzialne podmioty	Zapobieganie, wykrywanie i neutralizacja zagrożeń: ataków hakerskich, wirusów, ransomware, phishingu. Ochrona infrastruktury krytycznej i usług cyfrowych	Regulacja odpowiedzialności i praw w sieci. Obejmuje m.in. ochronę danych osobowych (RODO), odpowiedzialność za cyberprzestępstwa, regulacje dotyczące usług cyfrowych, prawa autorskie online, handel elektroniczny.
Charakter	Proaktywny – działania wyprzedzające, prewencja, stosowanie systemów wczesnego ostrzegania, testy penetracyjne, szkolenia użytkowników.	Reaktywny – uruchamiany w sytuacji naruszenia prawa, ukierunkowany na ściganie przestępstw, rozliczalność i stosowanie sankcji.
Metody	Narzędzia techniczne: firewalle, szyfrowanie, systemy SIEM, sztuczna inteligencja w monitoringu zagrożeń, procedury reagowania kryzysowego.	Narzędzia prawne: ustawy, dyrektywy i rozporządzenia (np. NIS2, DORA, RODO), postępowania sądowe, normy międzynarodowe
Zakres oddziaływania	Bezpośrednia ochrona systemów, sieci i danych. Skutki widoczne na poziomie technicznym i operacyjnym.	Regulacja całego ekosystemu cyfrowego – od indywidualnych użytkowników, przez przedsiębiorstwa, po administrację publiczną
Wynik końcowy	Zmniejszenie ryzyka incydentów	Zapewnienie odpowiedzialności prawnej, porządku prawnego w cyberprzestrzeni i odstraszanie potencjalnych sprawców

Źródło: https://cybersapiens.com.au/cyber-awareness/difference-between-cyber-security-and-cyber-law/ [dostęp: 16 kwietnia 2025 r.].

Model współdziałania tych dwóch obszarów doskonale ilustruje przypadek naruszenia danych osobowych w firmie Equifax i Dow Jones w 2017 roku, uznawane za jedne z największych incydentów tego typu w historii. Pomimo istnienia zabezpieczeń technologicznych, doszło do ujawnienia danych ponad 140 milionów osób. W odpowiedzi, na poziomie prawnym uruchomiono szereg działań: wszczęto postępowania sądowe, nałożono wielomilionowe grzywny, a incydent ten przyczynił się do intensyfikacji debaty na temat zaostrzenia przepisów dotyczących ochrony danych osobowych i odpowiedzialności korporacyjnej[36].

Tym samym, dopiero koordynacja działań w zakresie prewencji technologicznej oraz egzekucji prawnej umożliwia budowę spójnego, holistycznego systemu bezpieczeństwa cyfrowego, który nie tylko reaguje na istniejące zagrożenia, lecz także kształtuje normy zapobiegające ich eskalacji w przyszłości.

Prawo cybernetyczne a aktualne wyzwania technologiczne

Postęp technologiczny, obejmujący między innymi rozwój sztucznej inteligencji, technologii blockchain oraz komputerów kwantowych, generuje szereg nowych wyzwań prawnych w obszarze cyberbezpieczeństwa i regulacji cyfrowych. Zjawiska te wymuszają konieczność adaptacji i rozbudowy istniejących ram normatywnych.

Sztuczna inteligencja wprowadza istotną złożoność w zakresie odpowiedzialności prawnej, ochrony danych osobowych oraz zarządzania własnością intelektualną. Autonomiczne systemy decyzyjne generują nowe dylematy związane z rozdzieleniem odpowiedzialności między twórców, użytkowników oraz same algorytmy. W konsekwencji, istnieje zaistniała pilna potrzeba aktualizacji i harmonizacji regulacji prawnych, które uwzględniałyby zarówno aspekty etyczne, jak i bezpieczeństwo operacyjne systemów AI. Zgodnie z raportem *Global Cybersecurity Outlook 2024* Światowego Forum Ekonomicznego, rośnie zapotrzebowanie na kompleksowe ramy prawne regulacje jurydyczne, maj na celu efektywne zarządzanie ryzykiem związanym z wdrażaniem sztucznej inteligencji. Odpowiedzią na to jest wprowadzenie na obszarze Unii Europejskiej AI

[36] L. Grustniy, *5 największych wycieków danych w 2017 r. (jak dotąd)*, „Kasperski daily", 13 października 2017 r., link: https://plblog.kaspersky.com/data-leaks-2017/8320/ [dostęp: 20 maja 2025 r.].

Act[37], który ustanawia jednolite ramy prawne, w szczególności w zakresie rozwoju, wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji. Przesłanką zastosowania poszczególnych regulacji przewidzianych w AI Act wobec produktów mieszczących się w definicji „systemu AI" jest dokonanie szczegółowej analizy ryzyka, związanego z potencjalnym oddziaływaniem danego rozwiązania na prawa podstawowe oraz bezpieczeństwo osób korzystających z technologii sztucznej inteligencji. Trzeba zaznaczyć, że już sama definicja „systemu AI" jest bardzo szeroka i nie precyzuje dokładnie, które technologie są wyłączone lub włączone. Nie ma też dokładnie określonych wymogów dla szerokiego użytku konsumenckiego co umożliwiać może tworzenie i rozpowszechnianie treści szkodliwych bez formalnej odpowiedzialności producenta AI. Ponadto AI Act wymaga zgodności z innymi regulacjami UE (ochrona danych, prawo pracy, bezpieczeństwo produktów), ale nie rozstrzyga rozbieżności między nimi a to skutkować może m.in. kolizyjnymi wymaganiami pomiędzy AI Act a RODO[38]. AI Act obowiązuje w UE, ale nie reguluje systemów AI używanych poza UE, które wpływają na rynek UE w sposób pośredni lub online a to powodować może, że firmy międzynarodowe mogą pomijać regulacje UE i stosować różne stadardy w zależności od regionu[39].

W odróżnieniu od Unii Europejskiej, państwa trzecie – w szczególności Stany Zjednoczone – przyjęły bardziej powściągliwe podejście do kwestii regulacji prawnych w obszarze sztucznej inteligencji. Działania legislacyjne były i są podejmowane tutaj z dużą ostrożnością, przy czym zasadniczym motywem jest niedopuszczenie do nadmiernej normalizacji, która mogłaby zahamować dynamikę innowacyjną oraz osłabić pozycję konkurencyjną tych państw w globalnym wyścigu technologicznym. W Stanach Zjednoczonych brak jest obecnie aktu prawnego odpowiadającego zakresem regulacyjnym unijnemu AI Act. Zamiast tego dominują instrumenty o charakterze niewiążącym, w szczególności rekomendacje i regulacje typu *soft law*. Wypracowywanie norm wiążących pozostaje domeną wyspecjalizowanych organów sektorowych oraz legislatur stanowych. Ponadto podejmowane są prace nad kodeksami postępowania

[37] Rozporządzenie 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 (akt w sprawie sztucznej inteligencji).

[38] R. Schwartmann, T. O. Keber, K.Zenner, *AI Act: A practical guide*, Heidelberg 2025, s. 204 i n.

[39] P. Voight, N. Hullen, *The EU AI Act. Answers to Frequently Asked Questions*, Berlin 2025, s. 190 i n.

w zakresie sztucznej inteligencji, których stosowanie miałoby charakter dobrowolny. Przykładem jest tu *America's AI Action Plan*, amerykański dokument 90 działań federalnych, który zakłada wykorzystanie wszelkich dostępnych instrumentów w sferze zasobów publicznych, jak również wprowadzenie mechanizmów deregulacyjnych, celem zagwarantowania utrzymania globalnej przewagi Stanów Zjednoczonych w dziedzinie sztucznej inteligencji[40].

Nowym. amerykańskim regulacjom zarzucić można nadmierną ingerencję w obszar gospodarki znajdującej się na początkowym etapie rozwoju. Uznaje się, że wprowadzenie zbyt restrykcyjnych rozwiązań prawnych może prowadzić do ograniczenia ilości danych podlegających przetwarzaniu, co w konsekwencji utrudni proces doskonalenia systemów sztucznej inteligencji. Wskazać można również to, że państwa stosujące mniej rygorystyczne podejście w tym zakresie, w szczególności Chiny, w których nie funkcjonują takie ograniczenia, uzyskują przewagę w zakresie rozwoju technologii uznawanej za strategiczną dla przyszłej gospodarki światowej.

Kolejnym wyzwaniem dla tradycyjnych mechanizmów egzekwowania prawa, ze względu na swój zdecentralizowny i niezmienny charakter stanowi technologia blockchain Jej zakres jest niezwykle szeroki i obejmuje nie tylko zagadnienia z zakresu prawa cywilnego, prawa autorskiego, regulacji dotyczących treści cyfrowych oraz ochrony danych osobowych i innych danych, lecz także kwestie prawa konsumenckiego, prawa konkurencji, zasad praworządności, praw człowieka[41] oraz praw podstawowych[42].

Unia Europejska tworzy jeden z najbardziej rozbudowanych na świecie systemów regulacji dotyczących technologii blockchain i kryptoaktywów. Kluczowe akty prawne to: *Markets in Crypto-Assets Regulation* (MiCA – regulacje rynku kryptoaktywów), DLT Pilot Regime (tokenizacja i rynki finansowe), *Digital Operational Resilience Act* (DORA – cyfrowa

[40] Autor, *nazwa*, „Publikator", link: https://ai-ei.org/the-u-s-ai-action-plan-a-path-to-ethical-and-responsible-use-of-ai/?gad_source=1&gad_campaignid=22979320730&gbraid=0AAAAA_P7btoBQSRAWYtIQ6pIr_kq_5g5Y&gclid=EAIaIQobChMIlpH09KzkjwMVRMl5BB3RBDAAEAAYAyAAEgJ1CPD_BwE [dostęp: 19 września 2025 r.].

[41] K. Lee, *AI Super-Powers China. Silicon valley and the new world order*, Boston 2018, s. 1.

[42] K. Lee, *AI 2041. The vision for our future*, New York 2024, s. xxi.

odporność operacyjna) oraz pakiet AML[43] (przeciwdziałanie praniu pieniędzy). Pomimo bardzo rozbudowanego systemu jurydycznego w tej kwestii, również dopatrzeć się można pewnych luk[44], jak np. problemy z egzekwowaniem wobec podmiotów działających poza UE gdy chodzi o MiCA, brak wytycznych dotyczących interoperacyjności systemów DLT między krajami UE czy też brak pewności co do ciągłości rozwiązań po zakończeniu okresu testowego w przypadku DLT Pilot Regime, brak dedykowanych zapisów dla specyfiki blockchaina w przypadku DORA.

Natomiast w Stanach Zjednoczonych regulacje dotyczące technologii blockchain są wciąż w fazie kształtowania. Niedawno uchwalona *Genius Act45 wprowadza ramy prawne dla płatniczych stablecoinów, nakładając obowiązek pełnego zabezpieczenia rezerwowego, comiesięcznych audytów oraz przestrzegania przepisów przeciwdziałających praniu pieniędzy – Anti-Money Laundering* (AML). Wśród inicjatyw federalnych znajdują się także *Clarity Act*, mająca jednoznacznie określić status aktywów cyfrowych w kontekście papierów wartościowych i towarów, oraz *Anti-CBDC Surveillance State Act*, blokująca emisję publicznej cyfrowej waluty banku centralnego (CBDC) bez zgody Kongresu. Na poziomie stanowym, np. w Kalifornii, obowiązują przepisy wymagające licencji dla podmiotów działających w obszarze cyfrowych aktywów finansowych, podczas gdy inne stany tworzą własne regulacje, generując zróżnicowany krajobraz prawny. Kluczowymi organami nadzoru pozostają *United States Securities and Exchange Commission* (SEC – aktywa cyfrowe jako papiery wartościowe), *Commodity Futures Trading Commission* (CFTC – aktywa cyfrowe jako towary i instrumenty pochodne) oraz Departament Skarbu, odpowiedzialny m.in. za regulację stablecoinów i egzekwowanie przepisów AML.

---

[43] Pakiet AML/CFT to regulacje, których celem jest przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. W skład Pakietu AML/CFT wchodzą: rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1620 z dnia 31 maja 2024 r. w sprawie ustanowienia Urzędu ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010 (rozporządzenie AMLA), dyrektywę Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca dyrektywę (UE) 2019/1937 oraz zmieniająca i uchylająca dyrektywę (UE) 2015/849 (dyrektywa AML) oraz Rozporządzenie Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (rozporządzenie AML). Zob. Organ, *nazwa*, „Publikator", link: https://poir.parp.gov.pl/component/content/article/88035:pakiet-aml-cft-kogo-dotyczy-i-jakie-procedury-ustanawia [dostęp: 24.09.2025].

[44] Wybrane przykładowe luki najczęściej poruszane w dyskursie naukowym.

[45] Guiding and Establishing National Innovation for U.S. Stablecoins, "Public Law" 119-27, s. 1582, 119th Cong. (2025), or in U.S. Code format, as 12 U.S.C. §§ 5901-5916.

W Polsce już od kilku obserwuje się również działania instytucjonalne ukierunkowane na wspieranie rozwoju technologii blockchain oraz zwiększanie jej zastosowań w sektorze gospodarczym. Ministerstwo Cyfryzacji, w ramach programu strategicznego „Od papierowej do cyfrowej Polski", powołało szereg tzw. strumieni tematycznych, których celem jest intensyfikacja procesów depapieryzacji w administracji publicznej oraz w obrocie gospodarczym. Do kluczowych obszarów zaliczono m.in. Cyfrowe Usługi Publiczne, Cyfrową Tożsamość, rozwój obrotu bezgotówkowego, Schemat Krajowy, eFakturę i eParagon, eDaniny i eŚwiadczenia, eZdrowie, eTransport, Cyberbezpieczeństwo, a także dedykowany Strumień Blockchain/DLT oraz waluty cyfrowe[46]. Brak jest jednak jednolitej ustawy regulującej kwestie związane z tą technologią co w konsekwencji prowadzi do niepewności prawnej w zakresie tokenizacji aktywów, obrotu kryptowalutami oraz implementacji rozwiązań opartych na blockchain w administracji publicznej. Podobnie Unia Europejska nie dysponuje jednym, spójnym systemem obejmującym wszystkie technologie cyfrowe a to spowodować może luki regulacyjne, zróżnicowanie standardów między państwami członkowskimi oraz zwiększoną podatność na nadużycia i cyberzagrożenia.

Technologia blockchain charakteryzuje się znacznym potencjałem w zakresie wzmacniania bezpieczeństwa systemów cyfrowych, wynikającym m.in. z jej rozproszonej architektury, niezmienności zapisów oraz mechanizmów pseudonimizacji. Jednocześnie właściwości te generują istotne wyzwania z perspektywy prawa cybernetycznego, w szczególności w obszarze ochrony danych osobowych, odpowiedzialności prawnej oraz nadzoru regulacyjnego. Może ona stanowić istotne narzędzie wzmacniające bezpieczeństwo systemów cyfrowych, znajdując zastosowanie w m.in. rejestrach medycznych, łańcuchach dostaw oraz mechanizmach ochrony dokumentacji cyfrowej. Jednocześnie charakterystyczne właściwości tej technologii, takie jak decentralizacja, niezmienność zapisów oraz trudność w modyfikacji danych, generują istotne wyzwania w zakresie obowiązujących przepisów prawa, w szczególności dotyczących ochrony danych osobowych, odpowiedzialności prawnej oraz mechanizmów audytu.

Wreszcie kwestia komputerów kwantowych, które stwarzają zagrożenia dla aktualnych standardów kryptograficznych, co może prowadzić do kompromitacji systemów zabezpieczających integralność i poufność

[46] D. Szostek, *Blockchain a prawo*, Warszawa 2018, s. 4–5.

danych. Komputery kwantowe nie zastępują klasycznych maszyn, lecz pozwalają znacząco rozszerzyć zakres problemów obliczeniowych możliwych do rozwiązania. Istnieją zadania, które dla tradycyjnych komputerów są praktycznie nieosiągalne, natomiast systemy kwantowe mogą je efektywnie realizować, otwierając nowe możliwości w informatyce i naukach ścisłych[47]. W Polsce od czerwca 2025 uruchomiono pierwszy taki komputer[48] działający w oparciu o technologię spułapkowanych jonów[49].

W odpowiedzi i na to wyzwanie, konieczne jest opracowanie i wdrożenie nowych technologii kryptograficznych odpornych na ataki kwantowe. To jednak wymaga to intensyfikacji międzynarodowej współpracy regulacyjnej i technicznej, mającej na celu utrzymanie globalnej odporności cyberbezpieczeństwa Z uwagi na *novum*, jakim jest techologia kwantowa, na chwilę obecną ani w Polsce, ani w Unii Europejskiej, nie ma prawnych uregulowań chroniących niezależność i suwerenność cyfrową, jakkolwiek „kraje powinny jednak sklasyfikować potencjalne zagrożenia i przygotować plany na przyszłość oraz przestawić szyfrowanie ze starego na nowe"[50], mając na względzie to, aby prawne ograniczenia nie wpłynęły negatywnie na rozwój tej technologii. Jak wskazują niektórzy naukowcy „Niebezpieczne jest regulowanie samej technologii. Należy regulować jej użycie". W chwili obecnej kwestię regulowania technologii kwantowych porównuje się z wdrożeniem AI Act.

Jeśli chodzi o USA to od 2022 roku obowiązuje *Quantum Computing Cybersecurity Preparedness Act* – Ustawa o gotowości na cyberbezpieczeństwo komputerów kwantowych (H.R.7535)[51], która nakłada na agencje federalne obowiązek migracji systemów do kryptografii postkwantowej, która jest odporna na ataki ze strony komputerów kwantowych i standardowych[52]. Obecnie przygotowany został kolejny projekt ustawy *National Quantum Cybersecurity Migration Strategy Act* – Ustawa o krajowej strategii

[47] E.R. Johnston, H. Harrigan, M. Gimeno-Segovia, *Komputer kwatowy. Programowanie, algorytmy, kod*, Gliwice 2021, s. 14.

[48] Autor, tytuł, „Publikator", link: https://www.gov.pl/web/cyfryzacja/otwarcie-pierwszego-europejskiego--komputera-kwantowego-w-polsce [dostęp: 20 września 2025 r.].

[49] Polska jest jednym z 6 krajów europejskich (pozostałe to: Czechy, Niemcy, Hiszpania, Francja, Włochy), który został wybrany przez Europejskie partnerstwo EuroHPC (*European High-Performance Computing Joint Undertaking*) jako jedna z sześciu lokalizacji, w których znajdą się pierwsze europejskie komputery kwantowe.

[50] *Technologie kwantowe a ochrona danych osobowych – konferencja*, 13 czerwca link: https://uodo.gov.pl/pl/138/3741 [dostęp: 20 września 2025 r.].

[51] H.R.7535 – 117th Congress (2021-2022): *Quantum Computing Cybersecurity Preparedness Act*

[52] Organ, *Nazwa*, „Publikator", link: https://www.congress.gov/bill/117th-congress/house-bill/7535 [dostęp: 24.09.2025].

migracji w zakresie cyberbezpieczeństwa kwantowego, której celem jest zapewnienie, że rząd federalny przygotuje się na komputery kwantowe łamiące szyfrowanie. Ustawa ta nakazuje Białemu Domowi opracowanie kompleksowej krajowej strategii cyberbezpieczeństwa postkwantowego i nakazuje agencjom federalnym rozpoczęcie programów pilotażowych wdrażających szyfrowanie bezpieczne dla komputerów kwantowych. Celem jest wyprzedzenie „szybko rozwijających się komputerów kwantowych", które mogłyby pewnego dnia ominąć nowoczesne szyfrowanie i narazić wrażliwe dane na ujawnienie. Kluczowa jest tu przede wszystkim ochrona danych wrażliwych i bezpieczeństwa narodowego przed pojawiającymi się zagrożeniami bezpieczeństwa danych, napędzanymi przez komputery kwantowe.

Zakończenie

Cyberbezpieczeństwo i prawo cybernetyczne, choć funkcjonują w odmiennych sferach, stanowią wzajemnie uzupełniające się elementy systemu ochrony w erze cyfrowej. Podczas gdy cyberbezpieczeństwo koncentruje się na działaniach prewencyjnych oraz ochronnych, takich jak identyfikacja zagrożeń, zapobieganie atakom i reagowanie na incydenty w czasie rzeczywistym, prawo cybernetyczne pełni rolę normatywną i represyjną – zajmuje się kwalifikacją naruszeń, egzekwowaniem odpowiedzialności oraz zapewnieniem sprawiedliwości po wystąpieniu incydentów.

Samo prawo, operujące *post factum*, nie jest wystarczające do zapewnienia pełnej ochrony przed zagrożeniami w cyberprzestrzeni. Skuteczne przeciwdziałanie wymaga bowiem synergii pomiędzy regulacjami prawnymi a zaawansowanymi technologiami zabezpieczającymi. Dopiero integracja tych dwóch podejść – prewencyjnego (technicznego) i normatywnego (prawnego) – tworzy kompleksowy system ochrony, zdolny do efektywnego przeciwdziałania zagrożeniom oraz zarządzania ich skutkami.

W odpowiedzi na rosnącą złożoność cyberzagrożeń, organizacje wdrażają dynamiczne i adaptacyjne oprogramowanie bezpieczeństwa, zdolne do samoczynnego aktualizowania się w reakcji na wykrycie nowych ataków. W tym celu powoływane są specjalistyczne zespoły ds.

cyberbezpieczeństwa, których zadaniem jest monitorowanie, analiza i szybkie reagowanie na zmieniające się warunki zagrożenia.

Jednocześnie nie można pomijać roli użytkownika końcowego w zapewnieniu cyberbezpieczeństwa. Odpowiedzialność za bezpieczeństwo cyfrowe nie spoczywa wyłącznie na rządach i instytucjach – również użytkownicy indywidualni muszą wykazywać się świadomością zagrożeń, stosować się do zasad cyberhigieny oraz dbać o aktualność oprogramowania i praktyk zabezpieczających.

Zatem efektywna współpraca trzech głównych podmiotów – organów regulacyjnych, organizacji technologicznych oraz samych użytkowników – stanowi kluczowy warunek budowy bezpiecznego, zaufanego i zrównoważonego ekosystemu cyfrowego. Tylko dzięki takiej współpracy możliwe jest skuteczne poruszanie się w realiach dynamicznie rozwijającej się przestrzeni cyfrowej, jaką stanowi współczesny Internet.

Bibliografia

Badruddin, Ahmad A., *Cyber Security Challenges: Some Reflections on Law and Policy in India*, "The Haryana Police Journal" 2017, vol. 1, iss. 1

Bakare S.S., Adeniyi A.O., Akpuokwe Ch.U., N.E. Eneh, *Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations*, "Computer Science & IT Research Journal" 2024, vol. 5, iss. 3

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w]: Banasiński C.(red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018

Banasiński C., Rojszczak M. (red.), *Cyberbezpieczeństwo*, Warszawa 2020

Ciach Sz., *Prawo w IT. Praktycznie i po ludzku*, Gliwice 2024

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, vol 2

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2025, vol 1

Department of Homeland Security Authorization Act for Fiscal Year-2006, Part 3, 109th Congress First Session, Report, May 2005

Hoffmann T., *Główni aktorzy cyberprzestrzeni i ich działalność*, [w:] T. Dębowski (red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku*, Łódź–Wrocław 2018

Hołyst B., *Kryminalistyka cyfrowa*, Warszawa 2025

Johnston E.R., Harrigan H., Gimeno-Segovia M., *Komputer kwatowy. Programowanie, algorytmy, kod*, Gliwice 2021

Lee K., *AI Super-Powers China. Silicon valley and the new world order*, Boston 2018

Lee K, *AI 2041. The vision for our future*, New York, 2024

Mazur M., *Cybernetyczna teoria układów samodzielnych*, Warszawa 1966

Priyadarshini I., *Introduction on cybersecurity*, [w:] L. DacNhuong, K. Raghvendra, B.K. Mishra, K. Manju (red.) *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies*, Beverly MA 2019

Priyadarshini I., Cotton Ch., *Cybersecurity. Ethics, Legal, Risks, and Policies*, Floryda 2022

Priyadarshini I., Wang H., Cotton Ch., *Some cyberpsychology techniques to distinguish humans and bots for authentication*, "Proceedings of the Future Technologies Conference" 2019, vol. 2

Saini H., Rao Y., Panda T.C., *Cyber-crimes and their* impacts: A review, "International Journal of Engineering Research and Applications" 2012, vol. 2

Schwartmann R., Keber T.O, Zenner K., *AI Act: A practical guide*, Heidelberg 2025

Skoczylas D., *Krajowy system cyberbezpieczeństwa*, Warszawa 2023

Szostek D., *Blockchain a prawo*, Warszawa 2018

Voigt P., von dem Bussche A., *The EU General Data Protection Regulation (GDPR): A Practical Guide* (2nd ed.), Cham 2024

Voight P., N. Hullen, *The EU AI Act. Answers to Frequently Asked Questions*, Berlin 2025

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r., w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)

Ustawa z 5 lipca 2018 r. – o Krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. 2018 poz. 1560)

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

Źródła internetowe

Cyber Law: What You Need to Know, „AXIOM", https://www.axiomlaw.com/guides/cyber-law.

Grustniy L., *5 największych wycieków danych w 2017 r. (jak dotąd)*, „Kasperski daily", 13 października 2017 r., link: https://plblog.kaspersky.com/data-leaks-2017/8320/

Dempsey J., Saniuk-Heing Ch., *Cybersecurity Law Basics*, „IAPP", styczeń 2025 r., link: https://iapp.org/resources/article/cybersecurity-law-basics

Difference Between Cyber Security and Cyber Law, „CyberSapiens The Cyber Seciurity Experts", 28 grudnia 2024 r., link:

https://cybersapiens.com.au/difference-between-cyber-security-and-cyber-law/

H.R.7535 – 117th Congress (2021-2022): *Quantum Computing Cybersecurity Preparedness Act*, link: https://www.congress.gov/bill/117th-congress/house-bill/7535

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 16 kwietnia, 2018, link: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Otwarcie pierwszego komputera kwantowego w ramach europejskiej sieci EuroHPC w Polsce, 23 czerwca 2025, link: https://www.gov.pl/web/cyfryzacja/otwarcie-pierwszego-europejskiego-komputera-kwantowego-w-polsce

Pakiet AML/CFT – kogo dotyczy i jakie procedury ustanawia, 4 lutego 2025 r., link: https://poir.parp.gov.pl/component/content/article/88035:pakiet-aml-cft-kogo-dotyczy-i-jakie-procedury-ustanawia

Raport National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018, link: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Technologie kwantowe a ochrona danych osobowych – konferencja, 13 czerwca 2025, link: https://uodo.gov.pl/pl/138/3741

The Federal Trade Commission 2023 Privacy and Data Security Update, link: https://www.ftc.gov/system/files/ftc_gov/pdf/2024.03.21-PrivacyandDataSecurityUpdate-508.pdf