MAREK PORZEŻYŃSKI

Między technologią a regulacją. Rola prawa w kształtowaniu systemu cyberbezpieczeństwa

Between Technology and Regulation: The Role of Law in Shaping the Cybersecurity System

Abstract

This paper examines the role of law, in particular European Union law and its national implementation, in shaping the cybersecurity system. It defends the thesis that law is not merely an external constraint but functions as the basis and axis integrating the three pillars of security: technological, organisational and regulatory. The analysis covers the basic legal acts such as the NIS2 Directive, the DORA Regulation and the CER Directive, as well as other regulations that influence the information security system, in order to verify their effects on cybersecurity requirements. The paper concludes with *de lege lata* and *de lege ferenda* proposals concerning competence standards, the coordination of reporting obligations, procedural safeguards in high-risk vendor proceedings, support for entities with limited resources, and the role of certification and education.

SŁOWA KLUCZOWE: cyberbezpieczeństwo, dyrektywa NIS2, krajowy system cyberbezpieczeństwa, edukacja

KEYWORDS: cybersecurity, NIS2 Directive, national cybersecurity system, education

MAREK PORZEŻYŃSKI – doktor habilitowany nauk prawnych, Politechnika Warszawska, e-mail: marek.porzezynski@pw.edu.pl, ORCID – 0000-0002-4709-2788.

HTTPS://DOI.ORG/10.36128/XWTQ8A43

1 Wprowadzenie

Współczesne cyberbezpieczeństwo nie jest jedynie (a nawet głównie) zagadnieniem natury technicznej. Rozwój internetu, internetu rzeczy, różnego rodzaju usług z nim związanych oraz pracy zdalnej poszerzył możliwe zakresy ataków i zwiększył skalę incydentów o charakterze społeczno-technicznym. Skalę zjawiska ilustrują szacunki branżowe, według których globalne straty powodowane cyberprzestępczością przekroczyły w 2025 r. 10 bilionów dolarów rocznie[1].

Ważniejsze od samej skali jest jednak źródło ryzyka. Według najświeższych doniesień, np. raportu Verizon za 2025 r., około 60% potwierdzonych naruszeń wiązało się z udziałem człowieka, w tym kliknięciem w złośliwy odnośnik, uleganiem manipulacji albo błędem przy przetwarzaniu danych[2]. Zbliżony obraz wynika z raportu ENISA, gdzie w próbie blisko pięciu tysięcy incydentów przeanalizowanych przez agencję za okres od lipca 2024 r. do czerwca 2025 r. phishing i pokrewne techniki socjotechniczne stanowiły około 60% zaobserwowanych wektorów pierwotnego dostępu[3]. Sięgając jednak głębiej, można również dotrzeć do raportów wskazujących, że ponad 90%[4] lub nawet 99%[5] incydentów jest związanych z wykorzystaniem błędów człowieka. Dane te wyznaczają granice rozwiązań czysto technologicznych, albowiem żadne zabezpieczenie lub konfiguracja zabezpieczeń nie wyłączy

1 David Braue, „Cybercrime to Cost the World $12.2 Trillion Annually by 2031" *Cybercrime Magazine*, 2025, https://cybersecurityventures.com/official-cybercrime-report-2025/ [dostęp: 9.07.2026]. Szacunki Cybersecurity Ventures mają charakter prognozy komercyjnej i bywają kwestionowane co do metodologii; przywołuję je wyłącznie jako ilustrację rzędu wielkości zjawiska.

2 Verizon, *2025 Data Breach Investigations Report* (Verizon Business, 2025), https://www.verizon.com/business/resources/reports/dbir/ [dostęp: 9.07.2026].

3 European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025* (ENISA, 2025), https://www.enisa.europa.eu [dostęp: 11.05.2026]. Raport obejmuje 4875 incydentów z okresu od lipca 2024 r. do czerwca 2025 r.; odsetek odnosi się do przypadków, w których wektor wejścia udało się ustalić.

4 Microsoft, *Microsoft Digital Defense Report 2024* (Microsoft, 2024), https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024 [dostęp: 13.05.2026].

5 Proofpoint, *Human Factor Report 2019* (Proofpoint, 2019), https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more [dostęp: 18.02.2026].

ryzyka, którego istotnym ogniwem pozostaje zachowanie poszczególnych osób.

Prawodawca unijny odpowiedział na tę diagnozę zmianą paradygmatu, odchodząc od bezpieczeństwa rozumianego jako dołożenie najwyższej staranności, w kierunku odporności opartej na analizie ryzyka. Poddane analizie akty prawne w postaci dyrektywy NIS2, rozporządzenia DORA oraz dyrektywy CER nakładają obowiązki w zakresie rozliczalności kierownictwa, zgłaszania incydentów, testowania odporności i systematycznego zarządzania ryzykiem[6]. Prawo przestaje być jedynie tłem dla techniki i samo staje się czynnikiem kształtującym system cyberbezpieczeństwa, co oddaje tytuł niniejszego artykułu.

Bezpośrednią inspiracją do podjęcia tematu jest studium przypadku programu kształcenia zrealizowanego na Politechnice Warszawskiej, którego kierownikiem jest autor niniejszego artykułu, a którego przebieg i wstępne wyniki zostały opisane i zaprezentowane przez członków zespołu projektowego na prestiżowych międzynarodowych i polskich konferencjach naukowych[7]. Autorzy ujęli w nim cyberbezpieczeństwo jako integrację trzech domen kompetencji: technicznej, organizacyjnej i regulacyjnej, proponując traktowanie regulacji jako swoistego rusztowania kompetencyjnego. Obserwacja ta koresponduje z ustaleniami literatury poświęconej kształceniu w dziedzinie cyberbezpieczeństwa, która od dawna

6 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 (Dz. Urz. UE L 333 z 27.12.2022, s. 80), dalej: dyrektywa NIS2; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, s. 1), dalej: rozporządzenie DORA; dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, s. 164), dalej: dyrektywa CER.

7 M.in.: Krzysztof Ejsmont, Jerzy Krawiec, Sebastian Zielinski, Marek Porzezyński, Michal Wisniewski, Pawel Gepner, Mieczyslaw Morawski, „Reframing Cybersecurity Education Through Technical, Organisational, and Regulatory Integration: Google Grant Implementation Case Study at WUT", [w:] *Computational Science – ICCS 2026 Workshops*, red. Maciej Paszynski, Amanda S. Barnard, Yongjie Jessica Zhang, Lecture Notes in Computer Science 16789 (Cham: Springer, 2026), 464–478.

odnotowuje rosnące znaczenie obszarów pozatechnicznych w programach studiów[8]. Niniejszy artykuł pokazuje rolę nauk prawnych w kształtowaniu systemów bezpieczeństwa informacji.

Celem artykułu jest ustalenie, jaką rolę odgrywa prawo w kształtowaniu systemu cyberbezpieczeństwa, oraz zbadanie relacji między wymiarem regulacyjnym a filarami technologicznym i organizacyjnym. Teza główna zakłada, że prawo pełni funkcję podstawy oraz osi integrującej wszystkie trzy aspekty cyberbezpieczeństwa. Wymagania regulacyjne nie tylko nakazują wdrożenie środków technicznych i organizacyjnych, lecz wyznaczają ich zakres i strukturę. Tezy szczegółowe wskazują, że obowiązki te mają charakter ciągły oraz że wymiar regulacyjny stanowi odrębną, niezbędną domenę kompetencji w obszarze cyberbezpieczeństwa.

Realizacji celu służą cztery pytania badawcze: (1) czy prawo samodzielnie kształtuje strukturę systemu cyberbezpieczeństwa? (2) jak rozkłada odpowiedzialność wewnątrz organizacji? (3) czy prawidłowa realizacja obowiązków wymaga integracji trzech wymiarów? (4) jak polska ustawa odwzorowuje rozwiązania unijne na tle innych państw członkowskich? Podstawową metodą jest analiza dogmatycznoprawna. Uzupełniają ją elementy analizy prawnoporównawczej ograniczone do sposobu i tempa transpozycji NIS2 w Belgii i w Niemczech oraz ilustracyjne studium przypadku. Dane statystyczne pełnią funkcję wyłącznie kontekstową i są interpretowane ostrożnie. Wywód prowadzi od diagnozy zjawiska (rozdział 2), przez konstrukcję trzech filarów (rozdział 3), analizę prawa unijnego (rozdział 4) i implementacji krajowej (rozdział 5), po operacjonalizację wymagań (rozdział 6) i wnioski (rozdział 6).

2 | Cyberbezpieczeństwo jako zjawisko społeczno-techniczne

Punktem wyjścia dla analizy cyberbezpieczeństwa jako szerszego zjawiska powinna być odpowiednia diagnoza źródeł ryzyka. Bezpieczeństwo sieci i systemów informatycznych oznacza ich odporność na działania naruszające

8 Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respício, „Cybersecurity Education: Evolution of the Discipline and Analysis of Master Programs" *Computers & Security*, 75 (2018): 24–35.

poufność, integralność i dostępność[9] danych oraz usług. Współczesne incydenty rzadko mają jednak charakter czysto techniczny, tj. wyłącznie wykorzystujący luki danego programu. Przytoczone we wprowadzeniu dane o udziale czynnika ludzkiego w naruszeniach i o dominacji socjotechniki jako ich początku[10] pokazują, że najsłabszym ogniwem pozostaje człowiek osadzony w organizacji, a nie sama technologia. Zwrócić należy jednak uwagę, że udział czynnika ludzkiego może mieć różny charakter. Może on obejmować różne zachowania: od przekazania informacji niezbędnych do uzyskania dostępu do danego systemu lub kliknięcia w link prowadzący do pobrania lub uruchomienia złośliwego oprogramowania, przez udzielenie potencjalnie nieszkodliwej informacji składowej, stanowiącej część szerszego ich zestawu niezbędny do przeprowadzenia ataku, aż po brak niezwłocznej aktualizacji systemów po udostępnieniu tzw. łatki.

Konsekwencja tej diagnozy jest dla prawodawcy doniosła. Skoro ryzyko ma w głównej mierze charakter społeczny, odpowiedni system nie może pozostawać domeną wyłącznie techniczną, a skuteczna regulacja nie może ograniczać się do nakazu stosowania określonych narzędzi. Niezbędne jest sięganie po instrumenty oddziałujące na ludzi, procesy i odpowiedzialność w organizacji, w tym po obowiązki szkoleniowe oraz wymagania dotyczące ładu korporacyjnego i rozliczalności. Prawo Unii Europejskiej przeszło tę drogę stopniowo od trudnych początków wyznaczanych przez pierwszą dyrektywę NIS z 2016 r., wzmocnioną aktem o cyberbezpieczeństwie i powiązaną z RODO[11], a zasadnicza zmiana jakościowa nastąpiła wraz z pakietem odporności z grudnia 2022 r., w którym wymagania stały

9 Jest to tzw. triada cyberbezpieczeństwa, stanowiąca jeden z podstawowych elementów np. normy ISO/IEC 27001.

10 Verizon, *2025 Data Breach Investigations Report*; ENISA, *ENISA Threat Landscape 2025*.

11 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, s. 1), dalej: dyrektywa NIS; 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1), dalej: RODO; zob. Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, „The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation" *Computer Law & Security Review*, nr 6 (2019): 105336.

się mierzalne i egzekwowalne[12]. Wzmiankowane powyżej akty prawne stanowią zasadniczą część regulacji odnoszących się do szeroko rozumianej sfery cyberbezpieczeństwa. Należą do nich regulacje przekrojowe, mające znaczenie dla możliwie szerokiego zakresu branż, jak również sektorowe, które są dedykowane tylko do konkretnego zakresu podmiotów ze względu na ich szczególny charakter lub rolę. Każdy z nich odnosi się jednak zarówno do sfery technicznej (wymagania w zakresie stosowania odpowiednich narzędzi), organizacyjnej (odpowiednie zarządzanie oraz procedury), jak i prawnej (odpowiedzialność, rozliczalność i nadzór).

3 | Trzy filary systemu cyberbezpieczeństwa: technologia, organizacja, prawo

Incydenty najczęściej wynikają ze splotu wielu czynników, w tym eksploatacji warstwy technologicznej, wykorzystania zachowań ludzi oraz luk w systemach organizacyjnych w postaci braku lub błędnych procedur[13]. Z tej perspektywy bezpieczeństwa nie da się sprowadzić do jednego wymiaru. Wymaga ono jednoczesnego oddziaływania na technologię, organizację i regulacje. Podział na trzy odpowiadające tym wymiarom domeny kompetencji nie jest przy tym pomysłem jednego zespołu badawczego. Ma on umocowanie w międzynarodowych wytycznych programowych – np. wytyczne ACM i IEEE z 2017 r. obok obszarów ściśle technicznych wyodrębniają bezpieczeństwo organizacyjne i społeczne[14]. Jednocześnie należy wskazać, że analiza dwudziestu jeden programów magisterskich prowadzonych przez czołowe ośrodki naukowe wykazała systematyczny wzrost znaczenia obszarów pozatechnicznych w programach związanych z cyberbezpieczeństwem[15]. Wydaje się jednak, że sfera cyberbezpieczeństwa, pomimo tych faktów, nadal traktowana jest jako wyłącznie techniczna, o czym może świadczyć chociażby dominujący model umiejscowienia działu odpowiedzialnego za cyberbezpieczeństwo w pionach IT czy prowadzenie dydaktyki w tym obszarze (obejmujące również sfery regulacyjne i organizacyjne) na wydziałach

12 Niels Vandezande, „Cybersecurity in the EU: How the NIS2-Directive Stacks Up against Its Predecessor" *Computer Law & Security Review*, 52 (2024): 105890.

13 Tak również: Ejsmont i in., „Reframing Cybersecurity Education", 465–467.

14 *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* (Nowy Jork: ACM, 2017).

15 Cabaj i in., „Cybersecurity Education", 30–34.

technicznych i częstokroć jedynie przez osoby o wykształceniu inżynierskim. Kluczowe jest założenie, że domen tych nie należy traktować rozłącznie, ponieważ dopiero razem mają szansę stworzyć w pełni działający system.

Sfera techniczna nadal pozostaje nieodzownym elementem dobrze funkcjonującego systemu bezpieczeństwa informacji i obejmuje inżynierię oraz walidację zabezpieczeń, w tym w szczególności architekturę bezpiecznych systemów, wykrywanie podatności i zarządzanie nimi, wykonywanie okresowych testów. Jej rdzeniem jest podejście systemowe oparte na normie ISO/IEC 27001, spinające kontrole techniczne z odpowiednio opracowanymi politykami[16]. Warstwę metodyczną uzupełniają standardy OWASP oraz baza technik MITRE ATT&CK[17]. Filar ten ma jednak wyraźne granice. Systematyczny przegląd metod szkoleniowych pokazuje, że samo opracowanie i dostarczenie narzędzi lub wiedzy nie przekłada się automatycznie na trwałą zmianę zachowań[18], dlatego rozwiązania techniczne muszą być osadzone w ramach organizacyjnych i skorelowane z wymaganiami prawnymi.

Filar organizacyjny obejmuje ład wewnętrzny oraz działania związane z analizą ryzyka – jego ocenę, analizę wpływu na działalność, ciągłość działania i wskaźniki skuteczności. Badania nad ładem cyberbezpieczeństwa dokumentują rosnącą rolę organów zarządzających, a zarazem trudności, jakie sprawia im nadzór nad materią techniczną[19]. Praktycznym wzorcem podziału odpowiedzialności pozostaje model trzech linii[20], którego zastosowania w cyberbezpieczeństwie podsumowuje przegląd systematyczny Valkenburga i Bongiovanniego[21].

---

16 PN-EN ISO/IEC 27001:2023 (ISO/IEC 27001:2022); por. Krystian Mączka, „Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji" *Ochrona Ludności i Dziedzictwa Kulturowego*, nr 5 (2024): 111–124.

17 OWASP Foundation, *OWASP Top 10:2025* (OWASP, 2025), https://owasp.org/Top10/2025/ [dostęp: 9.07.2026]; MITRE Corporation, *MITRE ATT&CK: Enterprise Techniques*, https://attack.mitre.org/ [dostęp: 9.07.2026].

18 Jan Prümmer, Tommy van Steen, Bibi van den Berg, „A Systematic Review of Current Cybersecurity Training Methods" *Computers & Security*, 136 (2024): 103585.

19 Megan Gale, Ivano Bongiovanni, Sergeja Slapničar, „Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead" *Computers & Security*, 121 (2022): 102840.

20 Tłumaczenie własne.

21 Bert Valkenburg, Ivano Bongiovanni, „Unravelling the Three Lines Model in Cybersecurity: A Systematic Literature Review" *Computers & Security*, 139 (2024): 103708.

Zakres regulacyjny, w opinii autora, jest jednak absolutną podstawą niezbędną do rozpoczęcia[22] wprowadzania zmian w organizacjach, które mają zapewnić wyższy poziom bezpieczeństwa informacji, w tym cyberbezpieczeństwa, o czym szerzej w kolejnym rozdziale. Regulacje wpływają na ocenę zgodności i wprowadzają ramy rozliczalności w obszarze cyberbezpieczeństwa. Istota jego integrującej roli polega na tym, że wymóg prawny nie pozostaje obojętny dla pozostałych filarów. Obowiązki przewidziane w regulacjach wyznaczają zakres polityk i procedur organizacyjnych, które zaś ograniczają projekt techniczny i określają, co należy przetestować i udokumentować[23]. Prawo działa więc zarazem jako inicjator oraz oś porządkująca. Można stąd wywieść, że od przepisu prowadzi łańcuch do procedury, od procedury do rozwiązania technicznego, a od niego do dowodu, który można przedstawić organowi nadzoru działającemu na podstawie przepisów prawa. Weryfikacji tej konstrukcji na materiale normatywnym służy kolejny rozdział. Jednocześnie zaznaczyć należy, że same przepisy wyznaczają również katalog podmiotów zobowiązanych do aplikowania danych zasad. Na gruncie prawa polskiego katalog podmiotów i rozkład zadań szczegółowo analizują chociażby Katarzyna Chałubińska-Jentkiewicz i Monika Nowikowska[24].

4 | Rola prawa Unii Europejskiej w kształtowaniu systemu cyberbezpieczeństwa

Prawo Unii Europejskiej tworzy w obszarze cyberbezpieczeństwa wielowarstwową architekturę, w której instrumenty horyzontalne, sektorowe i wspierające wzajemnie się przenikają. Akty prawa Unii Europejskiej wyznaczyły[25] jednocześnie standardy cyberbezpieczeństwa, które są

22 A czasem wymuszenia.

23 Ejsmont i in., „Reframing Cybersecurity Education", 467 (w oryginale: „regulatory requirements motivate organisational policies and procedures; these, in turn, constrain technical design and define what must be tested and evidenced"; tłum. własne).

24 Katarzyna Chałubińska-Jentkiewicz, Monika Nowikowska, „Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS2 (cz. 2)" *Cybersecurity and Law*, nr 2 (2024): 5–24.

25 Wydaje się, że odpowiedniejszym sformułowaniem byłoby „zunifikowały", ale to dzięki ich wprowadzeniu w formie aktów prawnych podejście wielu podmiotów zasadniczo się zmieniło.

niezbędne do spełnienia przez szereg podmiotów zobowiązanych. Aby uchwycić fundamentalną rolę regulacji dla kreowania tego systemu, pokrótce omówione zostaną trzy zasadnicze akty z „pakietu cyberbezpieczeństwa", a następnie ich relacje z instrumentami powiązanymi, które również odgrywają zasadniczą rolę w całościowo pojmowanym systemie bezpieczeństwa informacji, jak np. RODO.

4.1. Akty prawne o podstawowym znaczeniu dla systemu cyberbezpieczeństwa

Na wstępie należy podkreślić absolutnie zasadnicze znaczenie dyrektywy NIS, jak również jej następcy – dyrektywy NIS2 – w zapoczątkowaniu pojmowania systemu cyberbezpieczeństwa jako elementu wymagań prawnych i obszaru niezbędnego do włączenia do całokształtu ładu korporacyjnego. Dyrektywa NIS i zastępujący ją akt są pierwszymi instrumentami horyzontalnymi ustanawiającymi wspólny wysoki poziom cyberbezpieczeństwa w całej Unii Europejskiej. Choć w tytule wskazuje się na wysoki poziom cyberbezpieczeństwa, to w opinii autora są to raczej podstawowe zasady, które powinny być wdrażane w jeszcze szerszym zakresie podmiotowym[26]. Dyrektywa NIS2 wprowadza podział na podmioty kluczowe i ważne (zastępujący wcześniejszy podział proponowany w ramach jej poprzednika) i obejmuje łańcuch dostaw, a dodatkowo, w porównaniu z dyrektywą NIS, zaostrza wymagania i wzmacnia nadzór[27]. Trzon obowiązków tworzą środki zarządzania ryzykiem wymienione w art. 21 ust. 2 (od polityk analizy ryzyka, przez bezpieczeństwo łańcucha dostaw, po kryptografię i higienę cyfrową) oraz wieloetapowe zgłaszanie poważnych incydentów na podstawie art. 23: wczesne ostrzeżenie w ciągu 24 godzin, pełne zgłoszenie w ciągu 72 godzin i sprawozdanie końcowe w terminie miesiąca[28].

Największą nowością konstrukcyjną jest jednak art. 20, który czyni z cyberbezpieczeństwa materię zarządu. Organy zarządzające podmiotów kluczowych i ważnych zatwierdzają środki zarządzania ryzykiem, nadzorują ich wdrażanie i ponoszą odpowiedzialność za naruszenia, a ponadto mają

26 Tak np. Marek Porzeżyński, Łukasz Kulicki, „Changes Introduced by the NIS Directive 2.0 and Their Potential Effects on the Cybersecurity Labour Market" *Cybersecurity and Law*, nr 1 (2024).

27 Vandezande, „Cybersecurity in the EU", 105890.

28 Dyrektywa NIS2, art. 21 i 23.

obowiązek odbywania regularnych szkoleń i oferowania analogicznych szkoleń pracownikom. Kary pieniężne zaproponowane w ramach nowelizacji bezpośrednio nawiązują do wzorca wypracowanego w RODO, który został już zweryfikowany w praktyce, i sięgają co najmniej 10 mln euro lub 2% światowego obrotu w przypadku podmiotów kluczowych oraz 7 mln euro lub 1,4% obrotu w przypadku podmiotów ważnych, a wśród środków nadzorczych przewidziano nawet możliwość wystąpienia o czasowy zakaz pełnienia funkcji kierowniczych w podmiocie kluczowym (art. 32 ust. 5)[29].

Powyższe jasno wskazuje, że regulacje wyznaczają ramy, które muszą następnie być wdrożone nie tylko w dziale prawnym czy dziale technicznym (IT) danego przedsiębiorstwa, ale muszą się przekładać na całościowe podejście, w szczególności w formie wypracowywanych polityk i procedur, które następnie wypełniane są i weryfikowane w sposób skoordynowany w ramach całego przedsiębiorstwa. Ponadto w literaturze zwraca się uwagę, że tak ukształtowana rozliczalność wpisuje się w szerszy trend przenoszenia nadzoru nad cyberbezpieczeństwem na poziom organów spółek, obserwowany także poza Europą, co nie powinno obecnie dziwić w związku ze stale rosnącymi zagrożeniami sieciowymi[30].

Oprócz aktów o charakterze przekrojowym istnieje szereg regulacji sektorowych, do których w szczególności należy rozporządzenie DORA czy dyrektywa CER. Pierwszy ze wskazanych aktów prawnych jest aktem sektorowym odnoszącym się do sfery finansowej, opartym na pięciu filarach, znanych już wcześniej z innych obszarów, tj. zarządzaniu ryzykiem, zgłaszaniu incydentów, testowaniu operacyjnej odporności cyfrowej, nadzorze nad zewnętrznymi dostawcami usług ICT oraz wymianie informacji[31]. Choć wymagania te są rozpoznawane w systemie cyberbezpieczeństwa, nie powstaje ryzyko superfluum ustawowego. Relację obu reżimów rozstrzyga sama NIS2, zgodnie z którą przepisy sektorowych aktów unijnych o skutku co najmniej równoważnym mają pierwszeństwo,

29 Ibidem, art. 20, 32 i 34.

30 Gale, Bongiovanni, Slapničar, „Governing Cybersecurity from the Boardroom", 102840.

31 Christopher P. Buttigieg, Beatriz Brunelli Zimmermann, „The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision" *ERA Forum*, 25 (2024): 11–28; Dirk Clausmeier, „Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)" *International Cybersecurity Law Review*, nr 1 (2023): 79–90.

a motyw 28 tej dyrektywy wprost wskazuje DORA jako taki akt w odniesieniu do podmiotów finansowych. W praktyce oznacza to, że instytucja finansowa stosuje DORA jako regulację szczegółową zamiast odpowiednich przepisów NIS2. To modelowy przykład reguły lex specialis użytej świadomie jako narzędzie architektury systemu, a nie tylko jako reguła kolizyjna stosowana *ex post*.

Dyrektywa CER natomiast uzupełnia perspektywę cyfrową o wymiar odporności fizycznej. Opiera się na podejściu uwzględniającym wszystkie zagrożenia i nakłada na podmioty krytyczne obowiązki oceny ryzyka i zapewnienia ciągłości działania[32]. Oba reżimy (tj. wyznaczone w NIS2 i CER) są sprzężone także podmiotowo. Podmiot uznany za krytyczny na podstawie CER jest z mocy prawa traktowany jako podmiot kluczowy w rozumieniu NIS2, a więc podlega również obowiązkom tam wyrażonym. Jest to dobrze widoczny przykład funkcjonowania prawa w tym obszarze, które nie wyznacza równolegle funkcjonujących mechanizmów, ale tworzy jeden spójny system.

4.2. Relacje i współzależności regulacyjne

Systemowa rola prawa najwyraźniej ujawnia się na styku poszczególnych regulacji. W momencie opracowywania i uchwalania dyrektywy NIS ten sam los dzieliło RODO. Choć akty te dotyczą odrębnej materii, to jednak są ze sobą powiązane w znaczącym stopniu. RODO reguluje materię ochrony danych osobowych, która jest jednym z kluczowych elementów dla systemu bezpieczeństwa informacji różnego rodzaju podmiotów. Bez wątpienia musi być zatem również uwzględniona przy okazji tworzenia procedur i polityk związanych z zagrożeniami sieciowymi. Zauważyć należy, że w obu przypadkach pierwowzorem są normy, w tym w szczególności z rodziny ISO 27001, i w obu przypadkach występują podobne obowiązki jak np. obowiązek zapewnienia bezpieczeństwa informacji/systemów oraz zgłaszania naruszeń organowi nadzorczemu/odpowiedniemu CSIRT. Takie zależności występowały i zwracano na nie uwagę już w momencie uchwalania obu wskazanych aktów prawnych[33], co trwa nadal. Dla porządku i klaryfikacji należy jednak podkreślić, że nie należy z powyższego wyciągać wniosku, jakoby każdy incydent cyberbezpieczeństwa był jednocześnie automatycznie

32 Dyrektywa CER.

33 Markopoulou, Papakonstantinou, de Hert, „The New EU Cybersecurity Framework", 105336.

incydentem ochrony danych osobowych i odwrotnie. Doświadczenie wskazuje jednak, że jest to bardzo częsta sytuacja.

W sektorze płatniczym dyrektywa PSD2[34] wprowadziła wyższe poziomy zabezpieczeń z uwagi na jego narażenie na intensywniejsze zainteresowanie cyberprzestępców, wprowadzając wymóg silnego uwierzytelniania klienta (art. 97), doprecyzowany następnie w odpowiednich regulacyjnych standardach technicznych[35]. Jest to zatem jeden ze sztandarowych przykładów obowiązku wprowadzonego w postaci normy prawnej, która bezpośrednio kształtuje rozwiązanie techniczne. Z kolei akt o usługach cyfrowych[36] nakłada na bardzo duże platformy internetowe obowiązek oceny i ograniczania ryzyk systemowych (art. 34–35), przenosząc logikę zarządzania ryzykiem na grunt bezpieczeństwa usług cyfrowych[37].

Są to niektóre przykłady współzależności i współfunkcjonowania różnych rozwiązań regulacyjnych w obszarze cyberbezpieczeństwa. Funkcję spajającą w tym systemie pełni akt o cyberbezpieczeństwie, który nadał Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) stały (i jednocześnie szerszy niż do tej pory) mandat i ustanowił europejskie ramy certyfikacji[38]. Sektor

34 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337 z 23.12.2015, s. 35), dalej: dyrektywa PSD2; rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Dz. Urz. UE L 69 z 13.03.2018, s. 23).

35 Zob. Mary Donnelly, „Payments in the Digital Market: Evaluating the Contribution of Payment Services Directive II" *Computer Law & Security Review*, nr 6 (2016): 827–839.

36 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) (Dz. Urz. UE L 277 z 27.10.2022, s. 1), art. 34–35.

37 Zob. Caroline Cauffman, Catalina Goanta, „A New Order: The Digital Services Act and Consumer Protection" *European Journal of Risk Regulation*, nr 4 (2021): 758–774.

38 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 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 7.06.2019, s. 15).

nowych technologii rozwija się jednak niezwykle dynamicznie i podobnie dzieje się w związku z tym w obszarze regulacyjnym. W styczniu 2026 r. Komisja przedstawiła projekt nowego rozporządzenia, określanego jako akt o cyberbezpieczeństwie 2[39], który ma zreformować ramy certyfikacji i silniej objąć bezpieczeństwo łańcucha dostaw ICT. Całość tworzy wzajemnie powiązany i przenikający się system, w którym zbiegi obowiązków porządkują reguły kolizyjne naturalne dla praktyki prawnej.

5 | Implementacja krajowa dyrektywy NIS2 na przykładzie Polski jako przykład potrzeby dalszej integracji systemu cyberbezpieczeństwa

Podstawą krajowego systemu do niedawna była ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, uchwalona jako transpozycja dyrektywy NIS[40]. W związku z uchwaleniem dyrektywy NIS2 niezbędna stała się jej gruntowna zmiana, która ostatecznie udała się dopiero w styczniu 2026 r.[41].

5.1. Trudna droga implementacji dyrektywy NIS2 w Polsce

Droga do implementacji była zatem wyjątkowo długa i trudna, a termin transpozycji dyrektywy NIS2 upłynął 17 października 2024 r. Wobec niedotrzymania tego terminu, w listopadzie 2024 r. Komisja Europejska wszczęła postępowania wobec dwudziestu trzech państw członkowskich, a 7 maja 2025 r. skierowała uzasadnione opinie do dziewiętnastu z nich, w tym do Polski. Równoległe postępowanie dotyczyło braku transpozycji dyrektywy CER[42].

Ministerstwo Cyfryzacji przedstawiało kolejne wersje projektu, jednak żadna z nich nie została uchwalona. Dopiero po wytężonych pracach pod

39 Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ENISA, europejskich ram certyfikacji cyberbezpieczeństwa oraz bezpieczeństwa łańcucha dostaw ICT, COM(2026) 11 final z 20.01.2026 r.

40 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r., poz. 20 ze zm.).

41 Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r., poz. 252).

42 Komisja Europejska, „Commission Calls on 19 Member States to Fully Transpose the NIS2 Directive", 7.05.2025, https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive [dostęp: 9.07.2026].

koniec 2025 r., których kulminacyjnym momentem były prace w komisjach sejmowych w grudniu 2025 r., Sejm uchwalił ustawę dnia 23 stycznia 2026 r., a Prezydent RP podpisał ją 19 lutego 2026 r. Zaznaczenia wymaga, że Prezydent RP jednocześnie skierował ją do Trybunału Konstytucyjnego w ramach wniosku o następczą kontrolę w zakresie przepisów dotyczących procedury dostawcy wysokiego ryzyka, która była jednym z najszerzej komentowanych i krytykowanych mechanizmów podczas prac legislacyjnych[43]. Ustawa weszła w życie po upływie miesiąca od ogłoszenia, to jest 3 kwietnia 2026 r. Od tej daty biegną okresy na dostosowanie – sześć miesięcy na rejestrację podmiotów kluczowych i ważnych, dwanaście miesięcy na wdrożenie środków zarządzania ryzykiem i dwadzieścia cztery miesiące na przeprowadzenie pierwszego audytu bezpieczeństwa[44].

Ustawa wdraża NIS2, a w odniesieniu do sieci telekomunikacyjnych również zalecenia unijnego zestawu środków dla bezpieczeństwa 5G. Wprowadza podział na podmioty kluczowe i ważne, istotnie rozszerza katalog sektorów objętych systemem oraz wprowadza nowe mechanizmy, takie jak obowiązek samoidentyfikacji. W warstwie technicznej praktycznym punktem odniesienia pozostaje jednak ten sam system zarządzania bezpieczeństwem informacji zbudowany zgodnie z normą ISO/IEC 27001[45]. Zmianą o największym ciężarze w odniesieniu do budowania systemów cyberbezpieczeństwa w poszczególnych firmach jest bezpośrednia odpowiedzialność kadry kierowniczej, odwzorowująca logikę art. 20 NIS2 i sprzężona z rozbudowanym nadzorem oraz karami pieniężnymi.

Najbardziej sporna pozostaje procedura dostawcy wysokiego ryzyka. Minister właściwy do spraw informatyzacji, po zasięgnięciu opinii Kolegium

43 Kancelaria Prezydenta RP, „Informacja w sprawie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa", 19.02.2026, https://www.prezydent.pl [dostęp: 9.07.2026].

44 Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r., poz. 252); zob. też komunikat Ministerstwa Cyfryzacji z dnia 23.01.2026 r., https://www.gov.pl/web/cyfryzacja/sejm-uchwalil-nowelizacje-ustawy-o-krajowym-systemie-cyberbezpieczenstwa [dostęp: 9.07.2026].

45 Mączka, „Dyrektywa NIS2 jako wytyczna", 115–121; szerzej o wymaganiach bezpieczeństwa sieci i usług: Maciej Rogalski, *Bezpieczeństwo sieci i usług łączności elektronicznej w prawie Unii Europejskiej oraz w prawie polskim* (Warszawa: Oficyna Wydawnicza Uczelni Łazarskiego, 2024), 141–189, https://www.lazarski.pl/sites/default/files/2024-03/bezpieczenstwo-sieci_www_ISBN978-83-66723-71-9.pdf.

do Spraw Cyberbezpieczeństwa, może w drodze decyzji administracyjnej uznać dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, co wiąże się z daleko idącymi konsekwencjami. Skutkiem decyzji jest bowiem zakaz wprowadzania objętych nią produktów do systemów oraz, co więcej, obowiązek wycofania już używanych. Co prawda, przewidziano w tym przypadku długi okres na dostosowanie się, bowiem podmiot, który posiada komponenty oznaczone jako dostarczone przez dostawcę wysokiego ryzyka, ma na ich wycofanie co do zasady siedem lat, a w odniesieniu do sprzętu realizującego funkcje krytyczne dla bezpieczeństwa sieci okres ten skraca się do czterech lat. Rozwiązanie to, obejmujące potencjalnie wszystkie podmioty kluczowe i ważne, a nie tylko operatorów telekomunikacyjnych, spotkało się z zarzutami nadmiernej ingerencji w swobodę działalności gospodarczej i stało się przedmiotem wspomnianego wniosku do Trybunału Konstytucyjnego. Dla niektórych branż cykl życia rozwiązań technologicznych jest kalkulowany w dłuższym okresie niż najdłuższy możliwy wynikający z tego rozwiązania, co oznacza, że skorzystanie z niego może mieć potencjalnie negatywne skutki dla całych obszarów gospodarki. Rozstrzygnięcie Trybunału zdeterminuje kształt jednego z najdalej idących instrumentów całego systemu.

5.2. Polska implementacja na tle innych państw członkowskich

Prawidłowa ocena polskiej drogi legislacyjnej wymaga tła porównawczego, co wynika bezpośrednio z faktu, że ustawodawca unijny przyjął formę dyrektywy dla tak newralgicznego elementu kształtującego system cyberbezpieczeństwa w UE, jakim jest dyrektywa NIS2. Z uwagi na ograniczenia objętości przedstawione zostaną wyniki analizy jedynie dla najciekawszych rozwiązań przyjmowanych w innych państwach.

Belgia transponowała ten akt prawny jako jedno z pierwszych państw. Ustawa implementująca weszła tam w życie 18 października 2024 r., a więc w unijnym terminie[46]. Model belgijski został przedstawiony ze względu na ciekawy rodzaj mechanizmu, który może się przełożyć na podwyższenie poziomu cyberbezpieczeństwa. Krajowe ramy „CyberFundamentals" przypisują obowiązkom ustawowym konkretne, stopniowalne zestawy

46 Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (Moniteur belge z 17.05.2024). Zob. Komisja Europejska, „NIS2 Directive: Transposition in EU Countries", https://digital-strategy.ec.europa.eu/en/policies/nis-transposition [dostęp: 9.07.2026].

zabezpieczeń. Oznacza to, że uproszczono zasadniczo jeden z pierwszych kroków, który jest niezbędny do podjęcia, aby móc zastosować odpowiednie rodzaje zabezpieczeń. Co więcej, w tym przypadku zgodność można wykazywać przez certyfikację, z którą wiąże się domniemanie spełnienia wymagań prawnych. Niemcy znalazły się na przeciwnym biegunie, gdyż ustawa implementacyjna, oparta na gruntownej nowelizacji już istniejącego aktu prawnego, została ogłoszona dopiero 5 grudnia 2025 r., po długich sporach o zakres wyłączeń administracji publicznej i koszty wdrożenia[47]. Istotne jest jednak, aby podkreślić, że w państwie tym już wcześniej istniał odpowiednik mechanizmu dostawcy wysokiego ryzyka[48], a obecnie został nieznacznie uproszczony.

Na tym tle Polska niestety należy do niechlubnej czołówki państw, które spóźniały się z implementacją dyrektywy NIS2. Z drugiej jednak strony, przyjęte rozwiązania należy uznać za jedne z bardziej rozbudowanych względem treści samej dyrektywy. Porównanie zakresów różnych rodzajów i sposobów wdrożeń może prowadzić do dwóch zasadniczych wniosków. Po pierwsze, opóźnienia transpozycji nie były polską specyfiką, ponieważ dotknęły większość państw członkowskich niezależnie od ich dojrzałości technologicznej, stopnia ryzyka czy wielkości. Po drugie, wdrożenia w różnych państwach różnią się między sobą nie tyle katalogiem obowiązków, co mechanizmami wprowadzanymi dla ułatwienia ich wykonania. Najlepszym tego przykładem jest przywołane belgijskie połączenie aktu wdrażającego z gotowymi ramami zgodności, co kontrastuje z modelem przyjętym w większości państw, w tym w Polsce, w którym podmiot zobowiązany otrzymuje czystą normę bez narzędzi, które mogą ułatwić lub przyspieszyć jej zrozumienie i wdrożenie w praktyce.

47 Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Stärkung der Cybersicherheit (NIS-2-Umsetzungs-und Cybersicherheitsstärkungsgesetz), ogłoszona 5.12.2025 r.; zob. Komisja Europejska, „NIS2 Directive Implementation in Germany". https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-germany [dostęp: 9.07.2026].

48 Na tej podstawie prowadzono między innymi postępowania wobec Huawei i ZTE, a usunięcie urządzeń tych producentów ma zostać dokonane do końca 2026 r.; zob. Reuters, „Germany to Phase Out Huawei, ZTE Components from Its 5G Core Network", 11.07.2024. https://www.reuters.com/business/media-telecom/germany-agrees-phaseout-huawei-zte-components-5g-core-network-2024-07-11/ [dostęp: 2.06.2026].

6 Studium przypadku

Nie od dziś wiadomo, że od teorii do praktyki wiedzie długa i wyboista droga. W omawianej tematyce podobna odległość dzieli czystą normę wyrażoną w danym akcie prawnym od zastosowania się do wywiedzionego z niej obowiązku w praktyce. Z tego powodu, a również włączając w to potrzebę przeobrażenia modelu dydaktyki w zakresie cyberbezpieczeństwa dla odpowiedniego wypełnienia luki kompetencyjnej, zaproponowano projekt dydaktyczny i naukowy wraz z komponentami organizacyjnymi realizowany na Politechnice Warszawskiej[49].

W ramach tego projektu zaproponowano m.in. mechanizm, w którym regulacja jest punktem wyjścia dla kompetencji i artefaktów zgodności, czego efektem ma być umiejętność przełożenia wymagań regulacyjnych na mechanizmy kontrolne organizacji, wdrożenie i zwalidowanie zabezpieczeń technicznych oraz komunikacja w tym zakresie z decydentami i organami nadzoru i kontroli[50].

Rdzeniem operacjonalizacji jest warstwa pośrednicząca, która każdemu obowiązkowi przyporządkowuje rodzaj dowodu i konkretny artefakt. Tabela 1 przedstawia takie przyporządkowanie dla wybranych obowiązków pakietu odporności; zestawienie jest opracowaniem własnym nawiązującym do koncepcji zaproponowanej w studium przypadku[51].

Należy zauważyć, że większość obowiązków angażuje co najmniej dwa filary, co potwierdza tezę o ich systemowym powiązaniu. Zestawienie nie stanowi wykładni prawa, a jedynie pokazuje, że obowiązki da się powiązać z wymaganiami, które są możliwe do weryfikacji.

Podejście to sprawdzono w praktyce w programie prowadzonym w latach 2024–2026 na trzech wydziałach Politechniki Warszawskiej, tj. Wydziale Administracji i Nauk Społecznych będącym liderem projektu, Wydziale Zarządzania i Wydziale Mechanicznym Technologicznym.

49 Niniejszy artykuł nie został przygotowany ani sfinansowany w ramach tego projektu; jedynie częściowo odwołuje się do doświadczeń autora z jego realizacji oraz do wyników przedstawionych w artykule przygotowanym w jego ramach.

50 Ejsmont i in., „Reframing Cybersecurity Education", 468 (w oryginale: „translate regulatory requirements into organisational controls, implement and validate technical safeguards, and communicate evidence to decision-makers and authorities"; tłum. własne).

51 Por. tabela 1 w: Ejsmont i in., „Reframing Cybersecurity Education", 469.

Tabela 1. Przykładowe przyporządkowanie obowiązków prawnych do filarów systemu i artefaktów zgodności

Podstawa prawna	Typowy obowiązek	Filary	Przykładowy artefakt zgodności
NIS2, art. 21 ust. 2	Polityki analizy ryzyka i oceny skuteczności zabezpieczeń	Org + Tech	Rejestr ryzyka; plan postępowania z ryzykiem; raport z przeglądu zabezpieczeń
NIS2, art. 23	Wieloetapowe zgłaszanie poważnych incydentów (24 godz. / 72 godz. / miesiąc)	Reg + Org	Procedura klasyfikacji incydentu; szablon wczesnego ostrzeżenia; rejestr dowodów
DORA, art. 24–27	Testowanie operacyjnej odporności cyfrowej i wnioski z wyników	Tech	Plan testów; raport z testu scenariuszowego wraz z omówieniem wyników
DORA, art. 28	Zarządzanie ryzykiem zewnętrznych dostawców usług ICT	Reg + Org	Rejestr informacji o umowach ICT; macierz oceny i zapewnienia dostawcy
CER	Ocena ryzyka, ciągłość działania, ćwiczenia	Org	Analiza wpływu na działalność; cele odtworzeniowe; scenariusz ćwiczenia
RODO, art. 33–34; NIS2, art. 23	Równoległe obowiązki zgłoszeniowe wobec różnych organów	Reg	Mapa obowiązków: co, komu i w jakim terminie należy zgłosić

Źródło: opracowanie własne z wykorzystaniem koncepcji warstwy tłumaczącej według: Ejsmont i in., „Reframing Cybersecurity Education", 469.

Ścieżka dydaktyczna dla studentów obejmowała 135 godzin w blokach technicznym, prawno-regulacyjnym i organizacyjnym, wspieranych przez laboratorium, klinikę cyberbezpieczeństwa i platformę e-learningową, a jej uzupełnieniem były prowadzone przez studentów zajęcia z zakresu podstaw cyberbezpieczeństwa m.in. w szkołach. W pierwszym roku do programu zapisało się 271 studentów, 137 ukończyło pełną ścieżkę, a 73 uzyskało certyfikaty specjalistyczne. Ankieta przeprowadzona na początku 2026 r. wykazała wysokie deklarowane przyrosty wiedzy i zmiany zachowań[52]. Choć są to wstępne wyniki z badań pilotażowych, to należy podkreślić, że badania te są nadal w toku. Zaznaczyć również należy, że istotne jest nie tyle mierzenie efektów dydaktycznych, ile wykazanie wykonalności

52 Ejsmont i in., „Reframing Cybersecurity Education", 470–476. Wyniki ankiety (n = 40) są samodeklarowane, oparte na małej próbie i pozbawione grupy kontrolnej, co autorzy wyraźnie zastrzegają.

zaprojektowanego i zaproponowanego modelu, w którym obowiązki prawne są możliwe do jasnego przekazania w formie ich przetłumaczenia na sprawdzalne artefakty i kompetencje, a regulacja pełni funkcję podstawy konstrukcyjnej i porządkującej program kształcenia.

Studium wpisuje się przy tym w szerszy kontekst prawny i faktyczny. Artykuł 20 ust. 2 NIS2 przekształca szkolenie z dobrej praktyki w obowiązek prawny organów zarządzających, nie określa jednak jego treści ani miary. Punktem odniesienia mogą być europejskie ramy kompetencji ENISA, które przypisują rolom zawodowym w cyberbezpieczeństwie konkretne zestawy wiedzy i umiejętności[53]. Potrzebę skalowalnych modeli kształcenia uzasadnia dodatkowo utrzymująca się luka kadrowa, szacowana w Unii na 260–500 tysięcy specjalistów[54]. Literatura dydaktyczna podpowiada zarazem, że formaty praktyczne, takie jak zawody typu „*capture the flag*", dobrze rozwijają umiejętności techniczne, słabiej zaś kompetencje organizacyjne i regulacyjne[55], a samo przekazanie wiedzy nie gwarantuje zmiany zachowań[56]. Zaproponowany model integrujący trzy filary, z prawem jako podstawą i osią, odpowiada na te ograniczenia.

7 Podsumowanie i postulaty

Cyberbezpieczeństwo przestało być domeną działu IT. Przeprowadzona analiza potwierdza tezę główną, zgodnie z którą należy uznać co najmniej trójfilarową strukturę systemu cyberbezpieczeństwa, w której regulacje pełnią funkcję podstawy oraz osi integrującej dla tego systemu. Wymagania regulacyjne nie tylko nakazują wdrożenie środków technicznych i organizacyjnych, ale również wyznaczają ich zakres, strukturę i rozkład

53 European Union Agency for Cybersecurity (ENISA), *European Cybersecurity Skills Framework (ECSF)* (ENISA, 2022), https://www.enisa.europa.eu [dostęp: 9.07.2026].

54 Borka Jerman Blažič, „Changing the Landscape of Cybersecurity Education in the EU: Will the New Approach Produce the Required Cybersecurity Skills?" *Education and Information Technologies*, 27 (2022): 3011–3036; taż, „The Cybersecurity Labour Shortage in Europe: Moving to a New Concept for Education and Training" *Technology in Society*, 67 (2021): 101769.

55 Valdemar Švábenský, Pavel Čeleda, Jan Vykopal, Silvia Brišáková, „Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges" *Computers & Security*, 102 (2021): 102154.

56 Prümmer, van Steen, van den Berg, „A Systematic Review of Current Cybersecurity Training Methods", 103585.

odpowiedzialności, a trzy wspomniane filary działają wyłącznie jako powiązany system.

W obecnym stanie prawnym dyrektywa NIS2, rozporządzenie DORA i dyrektywa CER, wraz z RODO, PSD2, aktem o usługach cyfrowych i aktem o cyberbezpieczeństwie, tworzą spójny, choć złożony system obowiązków, który zakłada jednoczesne dysponowanie kompetencjami technicznymi, organizacyjnymi i prawnymi dla zapewnienia jego odpowiedniego zaimplementowania w organizacji. Obowiązki te mają charakter ciągły i procesowy, co wymusza potrzebę stałego podnoszenia kompetencji we wszystkich wskazanych zakresach. Złożoność tego systemu dodatkowo realnie podnosi ryzyko nakładania się obowiązków w jego ramach np. w zakresie raportowania[57]. Jednocześnie, jak się wydaje, niekorzystnym czynnikiem wynikającym z wybrania przez ustawodawcę unijnego formy dyrektywy dla kluczowego aktu w obszarze cyberbezpieczeństwa, tj. dyrektywy NIS2 był przedłużający się proces implementacyjny w skali niemalże całej Unii Europejskiej, a także wątpliwości, jakie wiążą się z dodatkowymi mechanizmami wprowadzanymi wraz z implementacją danego aktu[58]. Przedstawione studium przypadku dowodzi natomiast, że obowiązki te da się zoperacjonalizować w pełnym cyklu, co przemawia za traktowaniem regulacji jako konstrukcji porządkującej, a nie wyłącznie bariery.

W świetle powyższego można sformułować kilka postulatów, których wdrożenie zdecydowanie wzmocniłoby minimalny poziom cyberbezpieczeństwa. Po pierwsze, co autor wskazywał już dla dyrektywy NIS2 na etapie zapowiadania nowelizacji dyrektywy NIS, akt ten powinien mieć formę rozporządzenia, ze względu na jego kluczową rolę w obszarze cyberbezpieczeństwa. Wydaje się, że przy wielości aktów prawnych odnoszących się do tego sektora, dobrym pomysłem byłoby odpowiednie skoordynowanie podobnych obowiązków nakładanych na podmioty na gruncie różnych aktów. Dobrym przykładem w tym zakresie są obowiązki raportowania, które występują w różnych aktach (np. RODO i NIS2), które mogłyby zostać zharmonizowane do jednego formatu i przekazywane w ramach jednego systemu, który rozdysponowywałby je pomiędzy odpowiednie organy. Wdrożenie powyższych postulatów powinno być

57 Markopoulou, Papakonstantinou, de Hert, „The New EU Cybersecurity Framework", 105336.

58 Rogalski, *Bezpieczeństwo sieci i usług łączności elektronicznej*, 233–268.

potraktowane jako priorytetowe ze względu na ich podstawowy charakter dla spójnego systemu cyberbezpieczeństwa w skali całej Unii Europejskiej.

Jednocześnie należałoby sformułować postulaty o bardziej technicznym charakterze, które ułatwiłyby wykonywanie obowiązków w odpowiedni i zharmonizowany sposób, co z pewnością mogłoby się przełożyć na cele dyrektywy NIS2. Pierwszym z nich byłoby wsparcie mniejszych podmiotów zobowiązanych oraz urzędów administracji publicznej poprzez udostępnienie ram, wzorów i standardów wraz z odpowiednią wiedzą w każdym z opisywanych trzech filarów cyberbezpieczeństwa. W tym przypadku dobrym wzorcem jest przywołany model belgijski. Dobrym pomysłem byłoby również powiązanie uzyskania odpowiedniej i uznanej certyfikacji cyberbezpieczeństwa z domniemaniem zgodności z przepisami prawa w tym obszarze.

Nade wszystko jednak podkreślić należy ponownie i nieustannie podstawowe znaczenie edukacji w zapewnieniu odpowiedniego poziomu cyberbezpieczeństwa. Statystyki pokazują jasno, że to ten obszar może pozwolić na osiągnięcie najlepszych efektów w zamian za relatywnie najniższe nakłady. Powyższe ma znaczenie zarówno na poziomie eksperckim, w którym zmagamy się z tzw. luką kompetencyjną i niedoborem kadr[59], jak i na poziomie podstawowym w odniesieniu do każdego pracownika danego podmiotu. Integracja wszystkich trzech filarów w ramach edukacji cyberbezpieczeństwa powinna być zatem uznana za standard.

Tytułowe napięcie między technologią a regulacją okazuje się ostatecznie pozorne, choć w wielu organizacjach nadal jest w ten sposób postrzegane. Prawo nie jest zatem przeciw rozwojowi technologii i nie zmierza do jego ograniczenia, ale porządkuje ją (i daną organizację) w jeden sprawdzalny system, pełniąc rolę podstawy, na której i w ramach której podmioty zobowiązane kształtują własne procedury. Ocena skuteczności przyjętych rozwiązań, w tym wpływu polskiej ustawy na praktykę podmiotów zobowiązanych po upływie okresów przejściowych, wymagać będzie dalszych badań.

59 Jerman Blažič, „The Cybersecurity Labour Shortage in Europe", 101769; Ejsmont i in., „Reframing Cybersecurity Education", 476–477.

Bibliografia

Braue David, „Cybercrime to Cost the World $12.2 Trillion Annually by 2031" *Cybercrime Magazine*, 2025. https://cybersecurityventures.com/official-cybercrime-report-2025/.

Buttigieg Christopher P., Beatriz Brunelli Zimmermann, „The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision" *ERA Forum*, 25 (2024): 11–28. https://doi.org/10.1007/s12027-024-00793-w.

Cabaj Krzysztof, Dulce Domingos, Zbigniew Kotulski, Ana Respício, „Cybersecurity Education: Evolution of the Discipline and Analysis of Master Programs" *Computers & Security*, 75 (2018): 24–35. https://doi.org/10.1016/j.cose.2018.01.015.

Cauffman Caroline, Catalina Goanta, „A New Order: The Digital Services Act and Consumer Protection" *European Journal of Risk Regulation*, nr 4 (2021): 758–774. https://doi.org/10.1017/err.2021.8.

Chałubińska-Jentkiewicz Katarzyna, Monika Nowikowska, „Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS2 (cz. 2)" *Cybersecurity and Law*, nr 2 (2024): 5–24. https://doi.org/10.35467/cal/188555.

Clausmeier Dirk, „Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)" *International Cybersecurity Law Review*, nr 1 (2023): 79–90. https://doi.org/10.1365/s43439-022-00076-5.

Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Nowy Jork: ACM, 2017.

Donnelly Mary, „Payments in the Digital Market: Evaluating the Contribution of Payment Services Directive II" *Computer Law & Security Review*, nr 6 (2016): 827–839. https://doi.org/10.1016/j.clsr.2016.07.003.

Ejsmont Krzysztof, Jerzy Krawiec, Sebastian Zielinski, Marek Porzezyński, Michal Wisniewski, Pawel Gepner, Mieczyslaw Morawski, „Reframing Cybersecurity Education Through Technical, Organisational, and Regulatory Integration: Google Grant Implementation Case Study at WUT", [w:] *Computational Science – ICCS 2026 Workshops*, red. Maciej Paszynski, Amanda S. Barnard, Yongjie Jessica Zhang, Lecture Notes in Computer Science 16789. Cham: Springer, 2026. https://doi.org/10.1007/978-3-032-29918-5_33.

European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025*. ENISA, 2025. https://www.enisa.europa.eu.

European Union Agency for Cybersecurity (ENISA), *European Cybersecurity Skills Framework (ECSF)*. ENISA, 2022. https://www.enisa.europa.eu.

Gale Megan, Ivano Bongiovanni, Sergeja Slapničar, „Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead" *Computers & Security*, 121 (2022): 102840. https://doi.org/10.1016/j.cose.2022.102840.

Jerman Blažič Borka, „Changing the Landscape of Cybersecurity Education in the EU: Will the New Approach Produce the Required Cybersecurity Skills?" *Education and Information Technologies*, 27 (2022): 3011–3036. https://doi.org/10.1007/s10639-021-10704-y.

Jerman Blažič Borka, „The Cybersecurity Labour Shortage in Europe: Moving to a New Concept for Education and Training" *Technology in Society*, 67 (2021): 101769. https://doi.org/10.1016/j.techsoc.2021.101769.

Komisja Europejska, „Commission Calls on 19 Member States to Fully Transpose the NIS2 Directive", 7.05.2025. https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive.

Komisja Europejska, „NIS2 Directive: Transposition in EU Countries". https://digital-strategy.ec.europa.eu/en/policies/nis-transposition.

Mączka Krystian, „Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji" *Ochrona Ludności i Dziedzictwa Kulturowego*, nr 5 (2024): 111–124. https://doi.org/10.4467/29563763.OLDK.24.014.21363.

Markopoulou Dimitra, Vagelis Papakonstantinou, Paul de Hert, „The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation" *Computer Law & Security Review*, nr 6 (2019): 105336. https://doi.org/10.1016/j.clsr.2019.06.007.

Microsoft, *Microsoft Digital Defense Report 2024*. Microsoft, 2024. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024.

MITRE Corporation, *MITRE ATT&CK: Enterprise Techniques*. https://attack.mitre.org/.

OWASP Foundation, *OWASP Top 10:2025*. OWASP, 2025. https://owasp.org/Top10/2025/.

Porzeżyński Marek, Łukasz Kulicki, „Changes Introduced by the NIS Directive 2.0 and Their Potential Effects on the Cybersecurity Labour Market" *Cybersecurity and Law*, nr 1 (2024).

Proofpoint, *Human Factor Report 2019*. Proofpoint, 2019. https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more.

Prümmer Jan, Tommy van Steen, Bibi van den Berg, „A Systematic Review of Current Cybersecurity Training Methods" *Computers & Security*, 136 (2024): 103585. https://doi.org/10.1016/j.cose.2023.103585.

Rogalski Maciej, *Bezpieczeństwo sieci i usług łączności elektronicznej w prawie Unii Europejskiej oraz w prawie polskim*. Warszawa: Oficyna Wydawnicza Uczelni Łazarskiego, 2024. https://www.lazarski.pl/sites/default/files/2024-03/bezpieczenstwo-sieci_www_ISBN978-83-66723-71-9.pdf.

Švábenský Valdemar, Pavel Čeleda, Jan Vykopal, Silvia Brišáková, „Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges" *Computers & Security*, 102 (2021): 102154. https://doi.org/10.1016/j.cose.2020.102154.

Valkenburg Bert, Ivano Bongiovanni, „Unravelling the Three Lines Model in Cybersecurity: A Systematic Literature Review" *Computers & Security*, 139 (2024): 103708. https://doi.org/10.1016/j.cose.2024.103708.

Vandezande Niels, „Cybersecurity in the EU: How the NIS2-Directive Stacks Up against Its Predecessor" *Computer Law & Security Review*, 52 (2024): 105890. https://doi.org/10.1016/j.clsr.2023.105890.

Verizon, *2025 Data Breach Investigations Report*. Verizon Business, 2025. https://www.verizon.com/business/resources/reports/dbir/.

This article is published under a Creative Commons Attribution 4.0 International license.
For guidelines on the permitted uses refer to
https://creativecommons.org/licenses/by/4.0/legalcode