TOMASZ DĄBROWSKI

Nowe instrumenty administracyjnoprawne w ustawie o krajowym systemie cyberbezpieczeństwa po nowelizacji z 2026 roku[1]

New Administrative Law Instruments in the Polish Act on the National Cybersecurity System Following the 2026 Amendment

Abstract

This paper analyses the legal solutions introduced by the Act of 23 January 2026 amending the Polish Act on the National Cybersecurity System in order to determine whether they form a coherent administrative law model of cybersecurity compliance management. The analysis covers the classification of essential entities, self-registration, risk management, managerial accountability, supervision, administrative monetary penalties, and systemic security measures. The study primarily applies the doctrinal legal method, including linguistic, systemic, and purposive interpretation, analysis of legislative materials, and, subsidiarily, the historical legal method. It demonstrates that an entity's regulated status generally arises by operation of law, whereas entry in the statutory register is declaratory. The reconstructed model centres on continuous, proportionate risk management linked to the organisational accountability of management bodies. The effectiveness of supervision and sanctions depends on an individualised administrative response, compliance with the principle of proportionality, and effective judicial review by administrative courts. Separate consideration is given to high-risk supplier decisions, protective orders issued in response to critical incidents, supply-chain security, and the implications of the new framework for public procurement.

SŁOWA KLUCZOWE: cyberbezpieczeństwo, krajowy system cyberbezpieczeństwa, dyrektywa NIS2, zarządzanie zgodnością, nadzór administracyjny, administracyjne kary pieniężne

KEYWORDS: cybersecurity, national cybersecurity system, NIS2 Directive, compliance management, administrative supervision, administrative monetary penalties

TOMASZ DĄBROWSKI – doktor nauk prawnych, Uniwersytet Radomski im. Kazimierza Pułaskiego, e-mail: t.dabrowski@urad.edu.pl, ORCID – 0000-0001-6184-140X.

HTTPS://DOI.ORG/10.36128/0SGJ4995

1 Wprowadzenie

Pierwszym przekrojowym instrumentem prawa Unii Europejskiej służącym zapewnieniu wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych była dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.[2] Zobowiązywała ona państwa członkowskie do zapewnienia minimalnego poziomu krajowych zdolności w dziedzinie cyberbezpieczeństwa przez ustanowienie właściwych organów i pojedynczego punktu kontaktowego, powołanie zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz przyjęcie krajowych strategii cyberbezpieczeństwa[3]. Zgodnie z art. 25 ust. 1 dyrektywy NIS1 państwa członkowskie były zobowiązane do przyjęcia i opublikowania przepisów niezbędnych do jej wykonania do 9 maja 2018 r. Do prawa polskiego dyrektywę tę wdrożono ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, której zakres wykraczał częściowo poza wymagania prawa unijnego[4].

W warunkach postępującej cyfryzacji i rosnącej zależności społeczeństw od technologii informatycznych zapewnienie cyberbezpieczeństwa stało się jednym z podstawowych wyzwań organizacji publicznych i prywatnych. Rozwój usług cyfrowych i internetu rzeczy oraz wzrost skali i złożoności cyberzagrożeń sprawiły, że zarządzanie ryzykiem cyfrowym zyskało znaczenie strategiczne. W odpowiedzi Unia Europejska przyjęła dyrektywę

1 Artykuł jest rozszerzoną wersją wystąpienia na Zjeździe Katedr, Zakładów i Zespołów Badawczych Publicznego Prawa Gospodarczego „Prawo publiczne gospodarcze w dobie dynamicznych przemian", który odbył się w Olsztynie w dniach 10–12 czerwca 2026 r.

2 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, 1; dalej jako: dyrektywa NIS1). Akt ten został uchylony z dniem 18 października 2024 r.

3 Uzasadnienie projektu ustawy o krajowym systemie cyberbezpieczeństwa, druk sejmowy nr 2505, Sejm RP VIII kadencji, 2, https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2505 [dostęp: 26.07.2026].

4 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r., poz. 20; dalej jako: u.k.s.c.); Grażyna Szpor, „The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland" *Review of European and Comparative Law*, nr 3 (2021): 222.

Parlamentu Europejskiego i Rady (UE) 2022/2555[5] z dnia 14 grudnia 2022 r., która zastąpiła dyrektywę NIS1. Doświadczenia związane ze stosowaniem pierwszego z tych aktów prawnych wykazały, że model minimalnej harmonizacji nie zapewnił jednolitego poziomu odporności rynku wewnętrznego. Różnice w identyfikacji operatorów i egzekwowaniu obowiązków prowadziły do fragmentacji regulacyjnej, a dotychczasowy model nadzoru okazał się niewystarczający. Jednocześnie wzrost liczby incydentów transgranicznych, zależność infrastruktury krytycznej od technologii cyfrowych oraz trudności związane z przypisywaniem odpowiedzialności za cyberoperacje uczyniły cyberbezpieczeństwo istotnym elementem bezpieczeństwa państwa i zarządzania kryzysowego Unii Europejskiej[6].

Dyrektywa NIS2 stanowi element wielopoziomowego systemu regulacji cyberbezpieczeństwa Unii Europejskiej. System ten współtworzy rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r., które określa mandat ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa)[7] oraz ustanawia europejskie ramy certyfikacji cyberbezpieczeństwa ICT. Relację dyrektywy NIS2 z sektorowymi aktami prawa Unii precyzuje jej art. 4. W sektorze finansowym zasadnicze znaczenie ma także rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego, zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011[8]. Wyłączenie stosowania odpowiednich przepisów NIS2 jest dopuszczalne tylko wtedy, gdy sektorowe akty prawa Unii ustanawiają wymogi co najmniej równoważne pod względem skutku. Wytyczne Komisji 2023/C 328/02

5 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, 80; dalej jako: dyrektywa NIS2).

6 Krystian Mączka, „Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji" *Ochrona Ludności i Dziedzictwa Kulturowego*, nr 5 (2024): 111–112; Dominika Skoczylas, „Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń" *Europejski Przegląd Sądowy*, nr 12 (2024): 39.

7 Dz. Urz. UE L 151 z 7.06.2019, 15. Szpor, „The Evolution of Cybersecurity Regulation", 219–224.

8 Dz. Urz. UE L 333 z 27.12.2022, 1; dalej jako: DORA.

potwierdzają funkcjonalny charakter tego testu. Model zgodności wymaga zatem rozstrzygania relacji między reżimem horyzontalnym a sektorowym bez obniżania poziomu cyberodporności[9].

W art. 1 dyrektywy NIS2 prawodawca unijny określił jej cel jako osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii oraz poprawę funkcjonowania rynku wewnętrznego. Już z samej treści tego przepisu wynika, że cyberbezpieczeństwo nie stanowi wyłącznie zagadnienia technicznego, lecz jest również istotnym elementem ładu gospodarczego i administracyjnego Unii Europejskiej. Dyrektywę NIS2 transponowano do polskiego porządku prawnego ustawą z 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[10]. Akt ten, obowiązujący od 3 kwietnia 2026 r., zasadniczo przebudował model ustanowiony ustawą z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Potrzeba przeprowadzenia reformy wynikała nie tylko z obowiązku transpozycji dyrektywy, lecz także z nieadekwatności dotychczasowych instrumentów prawnych wobec ewolucji cyberzagrożeń. W uzasadnieniu projektu ustawy trafnie wskazano, że bardzo duża liczba podmiotów objętych dyrektywą NIS2 stanowi wyzwanie dla organów nadzoru, a podstawową trudnością jest ich prawidłowa identyfikacja. Podkreślono również, że samorejestracja ma ułatwić identyfikację podmiotów kluczowych i ważnych oraz zastąpić dotychczasowy wykaz operatorów usług kluczowych. W ocenie skutków regulacji wskazano przybliżoną liczbę 38 000 podmiotów kluczowych i ważnych, przy około 400 operatorach usług kluczowych i dostawcach usług cyfrowych w modelu dotychczasowym. Skala ta wyjaśnia, dlaczego ustawodawca sięgnął po mechanizmy samoidentyfikacji, deklaratoryjnego wpisu i następczego nadzoru. Ustawa zmieniająca nadała tym założeniom postać norm prawa krajowego, łącząc kwalifikację podmiotu, zarządzanie ryzykiem, odpowiedzialność kierownika, nadzór oraz sankcje w jeden spójny mechanizm zapewniania zgodności.

9 Rozporządzenie 2019/881, art. 3 ust. 1 i art. 46 ust. 1; Paweł Pelc, „DORA jako regulacja sektorowa w rozumieniu dyrektywy NIS2" *Cybersecurity and Law*, nr 1 (2026): 187; Komisja Europejska, Wytyczne dotyczące stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS2) (2023/C 328/02) (Dz. Urz. UE C 328, 2–10), pkt 4, 5 i 6.

10 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; dalej: ustawa nowelizująca).

Postawiony w niniejszym artykule problem badawczy dotyczy tego, czy nowe rozwiązania tworzą spójny administracyjnoprawny model zarządzania zgodnością. Główna teza zakłada, że model taki ma charakter zintegrowany – status adresata powstaje przede wszystkim z mocy prawa, samorejestracja zapewnia widoczność regulacyjną, system zarządzania bezpieczeństwem informacji organizuje ciągłą pracę z ryzykiem, odpowiedzialność kierownika wiąże cyberbezpieczeństwo z ładem organizacyjnym, a nadzór i sankcje służą wykonaniu obowiązków. Instrumenty dotyczące dostawcy wysokiego ryzyka, polecenia zabezpieczającego i łańcucha dostaw uzupełniają go na poziomie ryzyka systemowego.

Weryfikacja tezy została przeprowadzona z wykorzystaniem metody dogmatycznoprawnej, obejmującej wykładnię językową, systemową i funkcjonalną oraz analizę materiałów legislacyjnych, jak również metody historycznoprawnej.

Tak zrekonstruowany mechanizm wykazuje cechy regulacji opartej na zarządzaniu. W ujęciu Cary'ego Coglianese'a i Davida Lazera prawodawca nie przesądza wyczerpująco technologii ani jednostkowego rezultatu, lecz nakłada na organizację obowiązek ustanowienia wewnętrznego procesu planowania służącego realizacji celu publicznego. Do tej kategorii można odnieść art. 8 u.k.s.c., zgodnie z którym podmiot zachowuje elastyczność w doborze zabezpieczeń, ale ma obowiązek rozpoznać ryzyko, zaplanować reakcję, zapewnić zasoby, monitorować skuteczność i korygować przyjęte środki. Administracyjnoprawny model zgodności nie jest więc wyłącznie zbiorem nakazów technicznych, lecz publicznoprawnym obowiązkiem należytego zorganizowania procesu decyzyjnego[11]. Przez zarządzanie zgodnością należy w niniejszym opracowaniu rozumieć zorganizowany i podlegający dokumentowaniu proces rozpoznawania ryzyka, doboru środków bezpieczeństwa, zapewniania zasobów, monitorowania skuteczności zabezpieczeń oraz korygowania stwierdzonych nieprawidłowości w celu wykonania obowiązków publicznoprawnych.

11 Cary Coglianese, David Lazer, „Management-Based Regulation: Prescribing Private Management to Achieve Public Goals" *Law & Society Review*, nr 4 (2003): 691–696.

2 | Zakres podmiotowy i deklaratoryjna samorejestracja

Punktem wyjścia dla całego modelu jest rozróżnienie podmiotów kluczowych i ważnych[12]. Kryteria przewidziane w art. 5 ust. 1 i 2 u.k.s.c. łączą przynależność sektorową, wielkość podmiotu oraz przypadki, w których znaczenie działalności uzasadnia objęcie regulacją niezależnie od rozmiaru. Zbieg przesłanek rozstrzyga art. 5 ust. 4 u.k.s.c., nakazujący traktowanie podmiotu jako kluczowego. Wielkość ustala się co do zasady według stanu na dzień sporządzenia sprawozdania finansowego na podstawie art. 5 ust. 5 u.k.s.c. Rozwiązanie to ogranicza niepewność kwalifikacji i zastępuje wymóg nieustannego badania statusu oceną zakotwiczoną w okresowych danych finansowych[13]. Na szczególną uwagę zasługuje objęcie statusem podmiotów kluczowych również określonych podmiotów administracji publicznej, ponieważ ciągłość i cyberbezpieczeństwo świadczonych przez nie usług warunkują prawidłową realizację zadań publicznych[14].

Włączenie do systemu następuje zasadniczo z mocy prawa, a nie dopiero wskutek aktu organu. W uzasadnieniu projektu zmian wskazano, że rezygnacja z indywidualnego wyznaczania operatorów jest odpowiedzią na skalę nowego reżimu oraz trudność identyfikacji jego adresatów. Samorejestracja ma w tym ujęciu umożliwiać sprawną identyfikację podmiotów oraz dostarczać organom danych koniecznych do skutecznego nadzoru. Wpis do wykazu, o którym mowa w art. 7d ust. 5 u.k.s.c., jest czynnością materialno-techniczną o charakterze deklaratoryjnym, potwierdza

12 Emilia Chronowska-Sioła, „Unijna dyrektywa NIS2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych" *Cybersecurity and Law*, nr 2 (2025): 20.

13 Justyna Kurek-Sobieraj, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. Justyna Kurek-Sobieraj, Katarzyna Chałubińska-Jentkiewicz, Mirosław Karpiuk (Warszawa: C.H. Beck, 2026), Legalis, komentarz do art. 5, tezy 1, 17 i 19. Autorka podkreśla, że w razie jednoczesnego spełnienia przesłanek obu kategorii rozstrzygający jest status podmiotu kluczowego, a kryteria wielkościowe bada się według danych ze sprawozdania finansowego. Zob. Katarzyna Chałubińska-Jentkiewicz, Monika Nowikowska, „Entities Involved in the Policy of Ensuring the Security of Network and Information Systems in the Light of the NIS2 Directive (Part 1)" *Cybersecurity and Law*, nr 1 (2024): 7–8.

14 Dominika Skoczylas, „Dyrektywa NIS2 a cyberbezpieczeństwo administracji publicznej" *Dyskurs Prawniczy i Administracyjny*, nr 1 (2025): 233–234.

więc wcześniej powstały status, a nie go tworzy. Z tego względu brak wpisu nie może być utożsamiany z brakiem obowiązków materialnych.

Podmiot spełniający przesłanki po wejściu w życie nowelizacji jest obowiązany złożyć wniosek w terminie sześciu miesięcy, przewidzianym w art. 7c ust. 1 u.k.s.c. Podmioty spełniające przesłanki już w dniu jej wejścia w życie składają natomiast wnioski zgodnie z harmonogramem wynikającym z art. 33 ust. 3 w zw. z art. 34 ust. 3 pkt 1 ustawy nowelizującej. Zmiany danych zgłasza się w terminie czternastu dni na podstawie art. 7c ust. 3 u.k.s.c.[15]

Na tle polskiego rozwiązania uwagę zwraca § 33 ust. 1 niemieckiej ustawy o Federalnym Urzędzie Bezpieczeństwa Technologii Informacyjnych i bezpieczeństwie informatycznym podmiotów (BSI-Gesetz)[16], który nakłada na podmioty szczególnie ważne i ważne obowiązek przekazania danych rejestracyjnych Federalnemu Urzędowi Bezpieczeństwa Technologii Informacyjnych (BSI) najpóźniej w terminie trzech miesięcy od dnia, w którym po raz pierwszy albo ponownie spełniły przesłanki uznania ich za podmioty należące do jednej z tych kategorii. Niemiecki termin jest zatem krótszy od sześciomiesięcznego terminu przewidzianego w art. 7c ust. 1 u.k.s.c. Ponadto, zgodnie z § 33 ust. 3 BSIG, w razie niewykonania obowiązku rejestracyjnego BSI może, w porozumieniu z właściwymi organami nadzoru, dokonać rejestracji podmiotu z urzędu. Rozwiązanie niemieckie wyraźnie łączy zatem obowiązek samoidentyfikacji i samorejestracji z kompetencją organu do zastępczego dokonania rejestracji w przypadku bezczynności podmiotu.

Konstrukcja ta przesuwa ciężar prawidłowej kwalifikacji na adresata normy. Samorejestracja nie jest zatem prostą formalnością ewidencyjną, lecz elementem rozliczalności regulacyjnej. Jednocześnie deklaratoryjność wpisu wymaga ostrożności przy stosowaniu sankcji. Organ powinien odróżniać naruszenie obowiązku rejestracyjnego od niewykonania obowiązków materialnych oraz uwzględniać, że część podmiotów wpisuje się z urzędu. Wykładnia przeciwna prowadziłaby do nieuprawnionego uzależnienia stosowania ustawy od stanu rejestru, chociaż art. 5 u.k.s.c. wiąże status

15 Druk sejmowy nr 1955, uzasadnienie, 31; Kurek-Sobieraj, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 7c, tezy 2, 4 i 6 oraz art. 7d, teza 1. Wpis jest automatyczną czynnością materialno-techniczną o charakterze deklaratoryjnym. Zob. także art. 33 ust. 3 w zw. z art. 34 ust. 3 pkt 1 ustawy nowelizującej.

16 Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2. Dezember 2025, BGBl. 2025 I Nr. 301, art. 1, § 33 ust. 1 i 3 BSIG.

podmiotu z obiektywnymi cechami podmiotu i prowadzonej przez niego działalności.

Ustawodawca złagodził skutki przejścia na nowy model przez przepisy dostosowawcze. Przepis art. 33 ust. 1 ustawy nowelizującej przewiduje dwanaście miesięcy na realizację obowiązków rozdziału 3 u.k.s.c., a art. 33 ust. 2 wyznacza dwadzieścia cztery miesiące na pierwszy audyt podmiotu kluczowego. Pierwsze wpisy podmiotów objętych regulacją w dniu wejścia w życie nowelizacji następują według harmonogramu, do którego odsyła art. 33 ust. 3 w zw. z art. 34 ust. 3 pkt 1 ustawy nowelizującej. W uzasadnieniu projektu automatyczny wpis dotychczasowych operatorów usług kluczowych powiązano z potrzebą zachowania ciągłości obsługi incydentów oraz uniknięcia ich ponownej samoidentyfikacji. Terminy te nie odraczają powstania statusu, lecz wyznaczają okres organizacyjnego dostosowania. Ich funkcją jest umożliwienie wdrożenia rozwiązań wymagających zmian technicznych, kontraktowych i zarządczych bez rezygnacji z zasady odpowiedzialności podmiotu za rozpoznanie własnej pozycji prawnej[17].

Rozwiązanie to budzi jednakże pewne zastrzeżenia. Ustawodawca wyznaczył w art. 7c ust. 1 u.k.s.c. jednolity termin dla wszystkich nowych adresatów, mimo że uzasadnienie projektu wskazuje na około 38 000 podmiotów kluczowych i ważnych wobec zaledwie około 400 dotychczasowych operatorów usług kluczowych i dostawców usług cyfrowych. Możliwości organizacyjne dużego operatora infrastruktury krytycznej oraz małego podmiotu w zakresie samodzielnego ustalenia własnego statusu prawnego są nieporównywalne. Przemawia to za rozważeniem zróżnicowania terminu ze względu na sektor lub wielkość podmiotu, analogicznie do harmonogramu przewidzianego w art. 33 ust. 3 w zw. z art. 34 ust. 3 pkt 1 ustawy nowelizującej dla podmiotów objętych regulacją w dniu jej wejścia w życie. Deklaratoryjny charakter wpisu rodzi ponadto ryzyko dla podmiotu działającego w dobrej wierze, ponieważ ustawa nie przewiduje instrumentu umożliwiającego uzyskanie przed powstaniem odpowiedzialności wiążącego stanowiska organu co do statusu podmiotu. *De lege ferenda* należałoby rozważyć wprowadzenie fakultatywnego wniosku o wydanie wiążącej opinii kwalifikacyjnej, funkcjonalnie zbliżonej do interpretacji indywidualnej znanej

17 Druk sejmowy nr 1955, uzasadnienie, 168. W uzasadnieniu automatyczny wpis dotychczasowych operatorów usług kluczowych powiązano z zachowaniem ciągłości obsługi incydentów oraz uniknięciem ich ponownej samoidentyfikacji.

prawu podatkowemu, która chroniłaby wnioskodawcę do czasu istotnej zmiany stanu faktycznego lub prawnego.

3 | System zarządzania bezpieczeństwem informacji i odpowiedzialność kierownika

Rdzeń obowiązków materialnych stanowi system zarządzania bezpieczeństwem informacji uregulowany w art. 8 u.k.s.c. Nie jest on pojedynczym zabezpieczeniem technicznym, lecz trwałym procesem obejmującym identyfikację, analizę, ocenę, postępowanie z ryzykiem i monitorowanie skuteczności środków. Zakres wymaganych środków wyznacza zasada proporcjonalności, odnoszona do oszacowanego ryzyka oraz znaczenia i charakteru świadczonej usługi. Takie ujęcie odpowiada art. 21 ust. 1 dyrektywy NIS2, który wymaga właściwych i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych[18].

Katalog art. 8 ust. 1 u.k.s.c. należy odczytywać funkcjonalnie. Obejmuje on zarządzanie incydentami, ciągłość działania, bezpieczeństwo nabywania i rozwoju systemów, zarządzanie podatnościami, higienę cyberbezpieczeństwa, kryptografię, kontrolę dostępu i bezpieczeństwo zasobów ludzkich. Obowiązki te tworzą cykl zarządczy, a nie zbiór samodzielnych czynności[19]. W konsekwencji formalne przyjęcie polityk nie wystarcza, jeżeli podmiot nie potrafi wykazać, że środki odpowiadają aktualnemu ryzyku i podlegają okresowej ocenie[20].

Szczegółowe wymagania krajowe mogą zostać określone na podstawie art. 8a u.k.s.c., natomiast art. 8b u.k.s.c. wiąże krajowy model z unijnymi aktami wykonawczymi. W odniesieniu do kategorii dostawców objętych rozporządzeniem wykonawczym (UE) 2024/2690 oznacza to bezpośrednie stosowanie technicznych i metodycznych wymagań przyjętych przez Komisję.

---

18 Chałubińska-Jentkiewicz, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 8, teza 4; Mączka, „Dyrektywa NIS2", 122; Maciej Siwicki, „Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego" *Europejski Przegląd Sądowy*, nr 9 (2019): 17.

19 Agnieszka Baran, Klaudia Gierejko, „Zarządzanie bezpieczeństwem informacji w świetle dyrektywy NIS2 – obowiązki, wyzwania prawne i organizacyjne przedsiębiorstw" *Akademia Zarządzania*, nr 2 (2026): 367.

20 Chałubińska-Jentkiewicz, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 8, teza 4.

Normy techniczne oraz wytyczne ENISA pełnią funkcję konkretyzującą, lecz nie zastępują indywidualnej oceny ryzyka. Podmiot nie może powołać się na samo zastosowanie standardu, jeżeli charakter jego działalności wymaga środków dalej idących. Gdy wdrożenie szczegółowego wymagania jest obiektywnie niemożliwe, proporcjonalność może przemawiać za środkiem kompensującym, o ile zapewnia on równoważny poziom ochrony[21].

Krąg podmiotów objętych na podstawie art. 8b ust. 1 u.k.s.c. bezpośrednim stosowaniem wymogów technicznych rozporządzenia wykonawczego 2024/2690 został określony kazuistycznie. Obejmuje on w szczególności dostawców usług DNS, rejestry nazw domen najwyższego poziomu, dostawców usług chmurowych, dostawców usług centrum przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, a także dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych. Pozostałe podmioty kluczowe i ważne stosują na podstawie art. 8b ust. 2 u.k.s.c. środki określone w aktach wykonawczych wydawanych przez Komisję na podstawie art. 21 ust. 5 dyrektywy NIS2. Podmioty kluczowe lub ważne z podsektora energii elektrycznej, które na podstawie art. 52a ust. 2 u.k.s.c. zostały uznane za podmioty o dużym wpływie albo o krytycznym wpływie, dodatkowo stosują środki określone w rozporządzeniu delegowanym Komisji (UE) 2024/1366 – zgodnie z art. 8b ust. 3 u.k.s.c. Trójstopniowa struktura odesłań technicznych – obejmująca delegację krajową z art. 8a, bezpośrednie stosowanie unijnego rozporządzenia wykonawczego na podstawie art. 8b ust. 1 oraz odesłanie do przyszłych aktów wykonawczych Komisji w art. 8b ust. 2 – potwierdza zróżnicowany zakres elastyczności standardu ustawowego w zależności od kategorii adresata.

Analizę odpowiedzialności należy rozpocząć od legalnej definicji kierownika podmiotu zawartej w art. 2 pkt 8a u.k.s.c. Przepis ten odsyła do pojęcia kierownika jednostki w rozumieniu art. 3 ust. 1 pkt 6 ustawy o rachunkowości[22], a w przypadku jednostek sektora finansów publicznych –

21 Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodologicznych środków zarządzania ryzykiem w cyberbezpieczeństwie (Dz. Urz. UE L 2024/2690).

22 Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2026 r., poz. 522 ze zm.).

do kierownika jednostki, o którym mowa w art. 53 ust. 1 ustawy o finansach publicznych[23]. Odesłanie ma istotne znaczenie praktyczne, ponieważ krąg osób ponoszących odpowiedzialność w zakresie cyberbezpieczeństwa nie został ukształtowany autonomicznie na potrzeby ustawy o krajowym systemie cyberbezpieczeństwa. Może to prowadzić do wątpliwości interpretacyjnych, zwłaszcza w strukturach grupowych oraz w przypadku rozdzielenia funkcji zarządczych i nadzorczych.

Nowelizacja przenosi cyberbezpieczeństwo z poziomu wyłącznie technicznego na poziom ładu organizacyjnego. Zgodnie z art. 8c ust. 1 u.k.s.c. kierownik ponosi odpowiedzialność za wykonywanie przez podmiot wskazanych obowiązków ustawowych. Jeżeli kierownikiem jest organ wieloosobowy i nie wyznaczono osoby odpowiedzialnej, odpowiedzialność ponoszą wszyscy członkowie tego organu (art. 8c ust. 2 u.k.s.c.). Powierzenie wykonywania zadań innej osobie nie zwalnia kierownika z odpowiedzialności, co wyraźnie przesądza art. 8c ust. 3 u.k.s.c.[24]

Nie oznacza to zakazu delegowania czynności operacyjnych. Przepis art. 8d u.k.s.c. pozostawia kierownikowi decyzje dotyczące systemu zarządzania bezpieczeństwem informacji, zapewnienia środków finansowych, przydziału zadań i nadzoru nad ich wykonywaniem. Delegacja jest zatem dopuszczalna jako sposób organizacji pracy, lecz nie jako sposób przeniesienia publicznoprawnej odpowiedzialności. Coroczne szkolenie wymagane przez art. 8e ust. 1 u.k.s.c. wzmacnia założenie, że kierownik powinien posiadać zdolność do świadomego zatwierdzania ryzyka, a nie tylko otrzymywać informacje od personelu technicznego[25].

W perspektywie prawnoporównawczej uwagę zwraca niemiecka ustawa BSI-Gesetz, obowiązująca od 6 grudnia 2025 r., która w § 38 ust. 1 zobowiązuje kierownictwo podmiotów szczególnie ważnych i ważnych nie tylko do nadzorowania, lecz także do wdrożenia środków zarządzania ryzykiem wymaganych w § 30 BSIG. Rozwiązanie to wykracza poza literalne brzmienie art. 20 ust. 1 dyrektywy NIS2, zgodnie z którym organy zarządzające

23 Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2025 r., poz. 1483 ze zm.).

24 Michał Jaworski, Karol Witas, [w:] *Dyrektywa NIS2. Komentarz*, red. Mateusz Jakubik, Rafał Tomasz Prabucki (Warszawa: Wolters Kluwer, 2026), LEX, komentarz do art. 20, część 1 „Wprowadzenie".

25 Chałubińska-Jentkiewicz, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 8e, teza 1.

zatwierdzają środki zarządzania ryzykiem w cyberbezpieczeństwie i nadzorują ich wdrażanie. Ponadto § 38 ust. 2 BSIG przewiduje odpowiedzialność członków kierownictwa wobec podmiotu za szkodę wyrządzoną zawinionym naruszeniem tych obowiązków, w pierwszej kolejności według przepisów prawa spółek właściwych dla formy prawnej danego podmiotu. Odpowiedzialność bezpośrednio na podstawie BSIG znajduje zastosowanie, jeżeli właściwe przepisy prawa spółek nie zawierają odpowiedniej podstawy odpowiedzialności. Na tym tle art. 8c u.k.s.c. silniej eksponuje publicznoprawną odpowiedzialność kierownika za wykonywanie obowiązków przez podmiot, podczas gdy model niemiecki wyraźniej łączy odpowiedzialność kierownictwa za doprowadzenie do wdrożenia środków zarządzania ryzykiem z jego wewnętrzną odpowiedzialnością odszkodowawczą[26].

Konstrukcja ta nie jest jednak wolna od ryzyka nadmiernego automatyzmu. Artykuł 73a u.k.s.c. pozwala na nałożenie na kierownika kary do 300% wynagrodzenia, niezależnie od kary nałożonej na podmiot. Umyślny albo nieumyślny charakter naruszenia podlega jednak uwzględnieniu przy wymiarze kary na podstawie art. 76a ust. 1 w zw. z art. 53 ust. 12 pkt 5 u.k.s.c. Ustawa nie ustanawia natomiast odrębnej klauzuli wyłączającej odpowiedzialność kierownika, który wykazał należytą staranność, w szczególności wdrożył adekwatne środki, zapewnił szkolenie wymagane przez art. 8e ust. 1 u.k.s.c. oraz udokumentował proces decyzyjny prowadzący do wyboru zabezpieczeń. *De lege ferenda* należałoby rozważyć wyraźne wskazanie takich okoliczności jako przesłanek łagodzących odpowiedzialność. Postulat ten powinien być odnoszony do art. 76a ust. 9 u.k.s.c., który umożliwia odstąpienie od nałożenia kary zarówno wobec podmiotu, jak i wobec kierownika, jeżeli spełnione są określone w tym przepisie przesłanki.

4 Nadzór oparty na ryzyku i granice ingerencji

Zróżnicowanie modelu nadzoru znajduje bezpośrednie oparcie w prawie unijnym. Artykuł 32 dyrektywy NIS2 przewiduje wobec podmiotów kluczowych szeroki katalog środków nadzorczych, obejmujący działania zarówno wyprzedzające, w tym regularne audyty i kontrole wyrywkowe, jak i następcze. Przepis art. 33 dyrektywy NIS2 ogranicza natomiast nadzór nad

26 Art. 1, § 38 ust. 1–2 BSIG oraz art. 30; por. art. 20 ust. 1 dyrektywy NIS2.

podmiotami ważnymi do modelu następczego, uruchamianego po uzyskaniu dowodu lub informacji wskazujących na możliwość naruszenia. W doktrynie trafnie podkreśla się, że rozwiązanie to ogranicza ryzyko arbitralnej ingerencji wobec podmiotów ważnych, uzależniając ją od wystąpienia wiarygodnych przesłanek naruszenia. Stanowi ono podstawę zróżnicowania przyjętego w art. 53 ust. 3 u.k.s.c.[27]

Konstrukcja nadzoru z art. 53 u.k.s.c. różnicuje pozycję podmiotów według znaczenia ich działalności. Wobec podmiotów kluczowych nadzór ma charakter prewencyjny i następczy na podstawie art. 53 ust. 3 pkt 1 u.k.s.c. Wobec podmiotów ważnych art. 53 ust. 3 pkt 2 u.k.s.c. przyjmuje model następczy, uruchamiany w szczególności w razie uzasadnionego podejrzenia naruszenia. Rozróżnienie odpowiada art. 32 i 33 dyrektywy NIS2, a jego *ratio legis* polega na koncentracji zasobów nadzorczych tam, gdzie materializacja ryzyka może wywołać poważniejsze skutki. Projektodawca wyjaśnił zarazem, że metodyki i hierarchia priorytetów mają dostosować nadzór do sektora oraz sytuacji konkretnego podmiotu, uporządkować wykorzystanie zasobów i umożliwić wybór efektywnej formy ingerencji na podstawie analizy ryzyka[28].

Katalog działań z art. 53 ust. 2 u.k.s.c. obejmuje kontrolę, nakazanie audytu, ocenę bezpieczeństwa systemu oraz żądanie informacji, dokumentów i dowodów zgodności. Instrumenty egzekwowania przewidziane w art. 53 ust. 4 i 5 u.k.s.c. powinny tworzyć sekwencję narastającej ingerencji. Elektroniczne pismo z ostrzeżeniem wskazuje naruszenie, oczekiwane czynności i termin. Dopiero brak reakcji albo charakter zagrożenia uzasadnia sięgnięcie po środki bardziej dolegliwe. Gradacja nie ma jednak charakteru czysto mechanicznego. Organ powinien w każdym przypadku wykazać adekwatność środka do wagi naruszenia, czasu jego trwania, dotychczasowej postawy podmiotu i realnego ryzyka[29].

---

27 Monika Lasota, [w:] *Dyrektywa NIS2. Komentarz*, komentarz do art. 32, teza 4.2 oraz komentarz do art. 33, teza 4.1.

28 Druk sejmowy nr 1955, uzasadnienie, 121. Projektodawca przypisał metodykom nadzoru oraz hierarchii priorytetów funkcję sektorowego dostosowania działań, efektywniejszego wykorzystania zasobów i doboru formy nadzoru na podstawie analizy ryzyka. Zob. również Lasota, [w:] *Dyrektywa NIS2. Komentarz*, komentarz do art. 32, część 2.

29 Dominik Tyrawa, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 53, tezy 6 i 9. Autor akcentuje znaczenie uprzedniego ostrzeżenia oraz sądowoadministracyjnej kontroli środków nadzorczych.

Szczególną postacią ingerencji jest urzędnik monitorujący wyznaczany na podstawie art. 53 ust. 5 pkt 6 u.k.s.c. na okres nieprzekraczający miesiąca. Uprawnienia z art. 53d ust. 1 u.k.s.c. pozwalają mu obserwować działania naprawcze, żądać informacji i uczestniczyć w oględzinach. W uzasadnieniu projektu instytucję tę przedstawiono jako środek nadzoru prewencyjnego, odrębny od kontroli, służący wskazaniu obszarów wymagających poprawy jeszcze przed wystąpieniem incydentu. Projektodawca wykluczył przy tym ingerowanie przez urzędnika w technologie, infrastrukturę i bieżące zarządzanie podmiotem. Instytucja ta nie ustanawia zatem zarządu komisarycznego i nie przenosi kompetencji kierowniczych. Urzędnik nie może wydawać poleceń dotyczących bieżącej działalności ani zastępować organów podmiotu. Jednodniowe wcześniejsze zawiadomienie o oględzinach wymagane przez art. 53d ust. 4 u.k.s.c. pełni funkcję gwarancyjną i powinno być dokonane także wtedy, gdy potrzeba szybkiej reakcji wynika z dynamiki incydentu[30].

Zakres kompetencji urzędnika monitorującego określa art. 53d u.k.s.c. Urzędnik ten może swobodnie wstępować i poruszać się po terenie podmiotu kluczowego po uzyskaniu przepustki, uzyskiwać wgląd do dokumentów dotyczących działalności podmiotu, przetwarzać dane osobowe w zakresie niezbędnym do sprawowania nadzoru, żądać wyjaśnień oraz przeprowadzać oględziny urządzeń, nośników i systemów informacyjnych po uprzednim zawiadomieniu. Wymienione uprawnienia służą realizacji wymogów art. 32 ust. 2 lit. a dyrektywy NIS2, zobowiązującego państwa członkowskie do zapewnienia możliwości prowadzenia kontroli na miejscu przez przeszkolonych specjalistów. Ze względu na dostęp do dokumentów, danych osobowych i informacji technicznych dotyczących architektury bezpieczeństwa kompetencje te powinny być wykonywane z zachowaniem szczególnej ostrożności, zwłaszcza w celu ochrony tajemnicy przedsiębiorstwa i informacji o podatnościach systemu[31].

30 Druk sejmowy nr 1955, uzasadnienie, 120. Projektodawca określił urzędnika monitorującego jako prewencyjny środek nadzoru odrębny od kontroli oraz wykluczył ingerowanie przez niego w technologie, infrastrukturę i bieżące zarządzanie podmiotem.

31 Z literalnego brzmienia art. 53d ust. 4 u.k.s.c. wynika, że zawiadomienie przekazuje się na adres do doręczeń elektronicznych albo za pomocą systemu teleinformatycznego w terminie jednego dnia przed przeprowadzeniem oględzin; zob. też Lasota, [w:] *Dyrektywa NIS2. Komentarz*, komentarz do art. 32, teza 4.2 oraz do art. 33, teza 4.2.

Warto jednak zauważyć, że kluczowe ograniczenia kompetencji urzędnika monitorującego – zakaz ingerowania w technologię, infrastrukturę i bieżące zarządzanie podmiotem – wynikają wyłącznie z uzasadnienia projektu, nie z treści art. 53d u.k.s.c. Uzasadnienie nie wiąże organu ani sądu, ale to właśnie przepis, a nie intencja projektodawcy, wyznacza w praktyce granice dopuszczalnego działania. *De lege ferenda* należałoby przenieść te ograniczenia wprost do treści art. 53d u.k.s.c., nadając im rangę normatywną.

Najdalej idące środki z art. 53 ust. 9 u.k.s.c. obejmują czasowe wstrzymanie działalności oraz zakaz pełnienia funkcji zarządczych. Zgodnie z art. 53 ust. 10 u.k.s.c. nie stosuje się ich do podmiotów publicznych. Decyzja musi spełniać wymagania art. 53e ust. 1 u.k.s.c., a pojedynczy okres stosowania środka nie może przekroczyć czternastu dni. Możliwość ponawiania decyzji nie znosi obowiązku każdorazowego zbadania proporcjonalności. W przypadku wniesienia przez podmiot kluczowy skargi, o której mowa w art. 53 ust. 7 lub 8 u.k.s.c., środków z art. 53 ust. 9 nie stosuje się do czasu rozstrzygnięcia sprawy przez sąd administracyjny. Gwarancję tę ustanawia art. 53 ust. 11 u.k.s.c.[32]

Zasada skutecznego nadzoru nie uzasadnia automatyzmu. Motyw 123 dyrektywy NIS2 wymaga, aby wykonywanie uprawnień nadzorczych minimalizowało obciążenia adresatów. W prawie krajowym nakaz ten wzmacniają konstytucyjna zasada proporcjonalności oraz obowiązek należytego uzasadnienia aktu. Organ powinien więc wskazać nie tylko naruszoną normę, lecz także związek wybranego środka z ustalonym ryzykiem i przyczyny odrzucenia instrumentu mniej dolegliwego. Taka rekonstrukcja chroni model oparty na ryzyku przed przekształceniem w nadzór oparty wyłącznie na formalnym stwierdzeniu niezgodności[33].

5 | Administracyjne kary pieniężne jako element egzekwowania zgodności

Perspektywa historycznoprawna uwidacznia skalę zmiany. W stanie prawnym sprzed nowelizacji z 2026 r. kary pieniężne miały charakter

32 Tyrawa, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 53e, tezy 1 i 2.

33 Mirosław Karpiuk, „Normatywno-aksjologiczne aspekty bezpieczeństwa" *Cybersecurity and Law*, nr 1 (2025): 16. Na temat proporcjonalności obowiązków sektorowych zob. także Paweł Pelc, „Zasada proporcjonalności w DORA" *Cybersecurity and Law*, nr 2 (2024): 216.

kwotowy i były przypisane do określonych naruszeń. Jak wskazywał Wojciech Wąsowicz, wynosiły one od 1000 zł do 200 000 zł i mogły być nakładane m.in. za brak audytu lub niewykonanie zaleceń pokontrolnych. Pierwotne brzmienie ustawy o krajowym systemie cyberbezpieczeństwa nie zawierało regulacji ograniczającej stosowanie działu IVa Kodeksu postępowania administracyjnego[34], co zgodnie ze stanowiskiem tego autora oznaczało pełne zastosowanie dyrektyw wymiaru kary z art. 189d k.p.a., instytucji odstąpienia od kary z art. 189f k.p.a. oraz okoliczności wyłączającej odpowiedzialność określonej w art. 189e k.p.a. Nowelizacja z 2026 r. wielokrotnie podniosła górne granice kar, a zarazem przebudowała relację ustawy o krajowym systemie cyberbezpieczeństwa do działu IVa k.p.a., wprowadzając własny, częściowo autonomiczny katalog kryteriów wymiaru kary i selektywnie wyłączając stosowanie wybranych przepisów kodeksowych[35].

Sankcje z art. 73 u.k.s.c. dotyczą naruszeń obowiązków przez podmioty kluczowe i ważne. Odpowiedzialność ma co do zasady charakter formalny, ponieważ jej przesłanką jest niewykonanie obowiązku, a nie wystąpienie incydentu lub szkody. Brak skutku nie pozostaje jednak bez znaczenia, gdyż wpływa na ocenę wagi naruszenia i wymiar kary. Takie rozróżnienie pozwala pogodzić prewencyjną funkcję regulacji z wymogiem indywidualizacji reakcji administracyjnej[36].

Przepis art. 73 ust. 3 u.k.s.c. określa maksymalną karę dla podmiotu kluczowego jako wyższą z dwóch wartości: 10 mln euro albo 2% przychodów osiągniętych z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Ustawowe minimum wynosi 20 000 zł. Wobec podmiotu ważnego art. 73 ust. 4 u.k.s.c. przewiduje karę nieprzekraczającą 7 mln euro albo 1,4% przychodów, przy czym nie może być ona niższa niż 15 000 zł. Odrębny charakter ma kara do 100 mln zł określona w art. 73 ust. 5 u.k.s.c.

34 Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j. Dz. U. z 2025 r., poz. 1691; dalej jako: k.p.a.).

35 Wojciech Wąsowicz, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. Agnieszka Besiekierska (Warszawa: C.H. Beck, 2019), komentarz do art. 73, nb. 3, a także nb. 1 (charakter wyłącznie administracyjny odpowiedzialności), nb. 4 (znaczenie winy strony i stosowanie art. 189e k.p.a.), nb. 10 (pełne stosowanie dyrektyw wymiaru kary z art. 189d k.p.a.) oraz nb. 11 (obligatoryjne i fakultatywne odstąpienie od kary na podstawie art. 189f k.p.a.).

36 Monika Bartnik, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 73, tezy 7–9.

Jej nałożenie wymaga naruszenia powodującego bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi albo zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług.

Przesłanki kary kwalifikowanej pozostają niedookreślone – ustawa nie precyzuje progu „bezpośredniości" ani „powagi" cyberzagrożenia, chociaż jest to jedyna kara wyłączona z dwuletniego odroczenia przewidzianego w art. 35 ustawy nowelizującej, a jej wysokość może sięgać 100 mln zł. *De lege ferenda* należałoby rozważyć ustawowe doprecyzowanie tych przesłanek. Niezależnie od tego właściwe organy mogłyby publikować niewiążące wytyczne interpretacyjne służące ujednoliceniu praktyki decyzyjnej.

Nałożenie kary na kierownika na podstawie art. 73a u.k.s.c. jest niezależne od kary, którą nałożono na podmiot, nie ma jednak charakteru automatycznego. Organ może ją zastosować, jeżeli przemawiają za tym czas, zakres lub charakter naruszenia. Górna granica kary wynosi 300% wynagrodzenia, a w odniesieniu do kierownika podmiotu publicznego co do zasady 100% wynagrodzenia. Ograniczenie do 100% nie ma zastosowania, jeżeli podmiot publiczny podlega ustawie również na podstawie innego sektora wskazanego w załączniku nr 1 albo 2 do u.k.s.c. Powiązanie sankcji z art. 8c i 8d u.k.s.c. wymaga ustalenia, który obowiązek kierownika został naruszony oraz w jaki sposób zaniechanie wpłynęło na zdolność organizacji do zarządzania ryzykiem.

Indywidualizację zapewnia art. 76a u.k.s.c., odsyłający do kryteriów z art. 53 ust. 12 u.k.s.c. Nakazuje on uwzględniać m.in. wagę i czas trwania naruszenia, spowodowane szkody majątkowe i niemajątkowe oraz stopień współpracy podmiotu z organem, a niezależnie od tych kryteriów art. 76a ust. 1 u.k.s.c. nakazuje dodatkowo uwzględnić sytuację finansową kierownika. Przepis art. 76a ust. 9 u.k.s.c. pozwala organowi właściwemu do spraw cyberbezpieczeństwa odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów są znikome, a podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

W zakresie nieuregulowanym art. 76e u.k.s.c. nakazuje odpowiednie stosowanie działu IVa k.p.a. Ustawa zachowuje więc ogólne gwarancje prawa administracyjnego, lecz pierwszeństwo mają jej przepisy szczególne. Relacja ta wymaga dalszego doprecyzowania. Wyłączenie art. 189a § 2 k.p.a. na podstawie art. 76a ust. 1 u.k.s.c. ma charakter selektywny i obejmuje jedynie

mechanizm kolizyjny tego przepisu, nie rozciągając się na dział IVa k.p.a. jako całość – zgodnie z art. 76e u.k.s.c. przepisy tego działu znajdują odpowiednie zastosowanie w zakresie nieuregulowanym przez tę ustawę. W szczególności dotyczy to zasady *lex mitior* z art. 189c k.p.a., okoliczności wyłączającej odpowiedzialność z art. 189e k.p.a. oraz przepisów o przedawnieniu i ulgach w wykonaniu kary z art. 189g–189k k.p.a. Ustawodawca przewidział ponadto odesłania szczególne poza klauzulą generalną z art. 76e u.k.s.c. Na podstawie art. 76d ust. 1 u.k.s.c. kara za naruszenie określone w art. 73 ust. 1 pkt 3 u.k.s.c. może być nakładana w sposób przewidziany w art. 14 § 1b k.p.a. Chodzi o naruszenie polegające na niewdrożeniu systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi albo na tym, że system ten nie zapewnia funkcjonalności lub nie spełnia wymogów, o których mowa w art. 8 ust. 1 albo 3 u.k.s.c. Zgodnie natomiast z art. 76d ust. 2 u.k.s.c. do postępowania w sprawie nałożenia tej kary stosuje się przepisy działu II rozdziału 14 k.p.a., z wyjątkiem przepisów o milczącym załatwieniu sprawy. Rozwiązanie to potwierdza, że ustawodawca nie odsyła do Kodeksu postępowania administracyjnego *en bloc*, lecz dobiera konkretne instytucje procesowe do potrzeb danego trybu nakładania kary, co wzmacnia tezę o zintegrowanym, lecz wewnętrznie zróżnicowanym charakterze reżimu egzekwowania.

Unijny wymóg proporcjonalności administracyjnych kar pieniężnych ma charakter operacyjny, a nie wyłącznie programowy. W wyroku w sprawie C-205/20 Trybunał Sprawiedliwości uznał, że jednostka może powołać się na zakaz sankcji nieproporcjonalnych, a sąd krajowy powinien odstąpić od zastosowania regulacji krajowej jedynie w zakresie niezbędnym do umożliwienia wymierzenia sankcji proporcjonalnej. Chociaż orzeczenie dotyczyło innej dyrektywy, ustalony w nim standard zachowuje znaczenie interpretacyjne dla art. 34 ust. 1 dyrektywy NIS2 i przemawia przeciwko automatyzmowi przy wymierzaniu kar na podstawie u.k.s.c.[37].

Relację z ochroną danych osobowych porządkuje art. 76c u.k.s.c. Jeżeli za ten sam czyn Prezes Urzędu Ochrony Danych Osobowych prawomocnie nałożył karę, organ właściwy do spraw cyberbezpieczeństwa poprzestaje na pouczeniu, zachowując możliwość zastosowania środków nadzorczych.

37 Wyrok Trybunału Sprawiedliwości (wielka izba) z dnia 8 marca 2022 r., NE przeciwko Bezirkshauptmannschaft Hartberg-Fürstenfeld, C-205/20, ECLI:EU:C:2022:168, pkt 22–31 i 37–44.

Rozwiązanie urzeczywistnia zasadę *ne bis in idem* w wymiarze represyjnym, nie blokując działań służących usunięciu zagrożenia[38]. Nie przewiduje ono jednak żadnego mechanizmu współdziałania proceduralnego między obydwoma organami – choćby obowiązku wzajemnego informowania o wszczęciu postępowania dotyczącego tego samego czynu. Przy naruszeniach dotyczących jednocześnie danych osobowych i cyberbezpieczeństwa może to prowadzić do przewlekłości postępowań lub rozbieżnych ustaleń faktycznych. *De lege ferenda* należałoby więc uzupełnić art. 76c u.k.s.c. o taki obowiązek informacyjny.

Przepis przejściowy art. 35 ustawy nowelizującej odracza możliwość pierwszego nałożenia większości kar z art. 73 ust. 1–4, art. 73a–73c i 76b u.k.s.c. o dwa lata od 3 kwietnia 2026 r. Odroczenie nie obejmuje kwalifikowanej kary z art. 73 ust. 5 u.k.s.c. Nie jest to dwuletnie zwolnienie z obowiązków. Organy mogą prowadzić nadzór i stosować środki egzekwowania, a podmioty powinny wykorzystywać okres przejściowy do rzeczywistego wdrożenia systemu zarządzania bezpieczeństwem.

6 Bezpieczeństwo systemowe i łańcuch dostaw

Decyzja wobec dostawcy wysokiego ryzyka z art. 67b u.k.s.c. służy ochronie podstawowego interesu bezpieczeństwa państwa przez ograniczenie stosowania określonych produktów, usług i procesów ICT. Postępowanie ma szczególny charakter, ponieważ część ogólnych gwarancji Kodeksu postępowania administracyjnego została wyłączona, krąg stron określono autonomicznie, a decyzji nadano natychmiastową wykonalność na podstawie art. 67b ust. 18 u.k.s.c. Ograniczenia te powinny być wykładane ściśle, gdyż rozstrzygnięcie oddziałuje nie tylko na dostawcę, lecz także na licznych użytkowników jego rozwiązań[39].

Postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka ma charakter szczególny również pod względem procesowym. Ustawodawca w art. 67b ust. 2 u.k.s.c. wyłączył

38 Bartnik, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 76c, tezy 1–3; Dominika Nowak-Byrtek, „RODO i dyrektywa NIS2 – wpływ ochrony danych osobowych na regulacje dotyczące cyberbezpieczeństwa" *Monitor Prawniczy*, nr 11 (2024): 18–23.

39 Anna Możdżeń-Sypniewska, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 67b, tezy 1–5.

stosowanie art. 28, 31, 51, 66a oraz 79 k.p.a., a krąg stron ukształtował autonomicznie w art. 67b ust. 3 u.k.s.c., uznając za stronę każdego, wobec kogo postępowanie zostało wszczęte. Istotną gwarancją merytoryczną jest obowiązek zasięgnięcia przez ministra opinii Kolegium do Spraw Cyberbezpieczeństwa[40] przed wydaniem decyzji (przy czym termin na jej przekazanie – trzy miesiące – nie wlicza się do terminu załatwienia sprawy) z jednoczesnym wyłączeniem art. 106 § 5 k.p.a. (art. 67b ust. 10 u.k.s.c.). Szczególny charakter zachowuje również kontrola sądowa. Na podstawie art. 67e u.k.s.c. Wojewódzki Sąd Administracyjny rozpoznaje skargę na posiedzeniu niejawnym w składzie trzech sędziów, a skarżącemu doręcza się uzasadnienie wyroku wyłącznie w części niezawierającej informacji niejawnych – pełny odpis sentencji z uzasadnieniem otrzymuje jedynie minister właściwy do spraw informatyzacji. Konstrukcja ta, uzasadniona ochroną informacji niejawnych, siłą rzeczy ogranicza możliwość pełnej weryfikacji przez stronę zasadności rozstrzygnięcia.

Ochrona informacji niejawnych nie może zarazem pozbawić strony skuteczności środka zaskarżenia. W wyroku w sprawie C-300/11 Trybunał Sprawiedliwości przyjął, że sąd powinien niezależnie ocenić konieczność utajnienia, a zainteresowanemu należy w każdym przypadku przekazać zasadniczą treść ustaleń stanowiących podstawę rozstrzygnięcia. Wyrok ten nie przesądza oceny art. 67e u.k.s.c., lecz wyznacza istotny unijny standard interpretacyjny – ograniczenie dostępu do uzasadnienia nie może czynić kontroli sądowoadministracyjnej iluzoryczną[41].

Konsekwencje decyzji określa art. 67c u.k.s.c. Przepis ten nie ustanawia odrębnej oceny ryzyka, lecz wykonuje rozstrzygnięcie wydane na podstawie art. 67b ust. 15 u.k.s.c. Obejmuje on zakaz wprowadzania do użytkowania rozwiązań wskazanych w decyzji oraz obowiązek ich stopniowego wycofania. Termin zasadniczy wynosi siedem lat, a dla funkcji krytycznych przedsiębiorców telekomunikacyjnych – cztery lata. Dopuszczone w okresie

40 Zob. art. 64 u.k.s.c., zgodnie z którym przy Radzie Ministrów działa Kolegium do Spraw Cyberbezpieczeństwa jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych i organów właściwych do spraw cyberbezpieczeństwa.

41 Wyrok Trybunału Sprawiedliwości (wielka izba) z dnia 4 czerwca 2013 r., ZZ przeciwko Secretary of State for the Home Department, C-300/11, ECLI:EU:C:2013:363, pkt 53–65 i 68–69.

przejściowym korzystanie z wcześniej nabytych rozwiązań służy zachowaniu ciągłości usług i nie może prowadzić do rozszerzania zależności od dostawcy.

Brak ustawowego mechanizmu rekompensaty budzi przy tym wątpliwości z perspektywy proporcjonalności obciążeń, zwłaszcza wobec mniejszych podmiotów, dla których koszt wymiany infrastruktury jest proporcjonalnie najwyższy. *De lege ferenda* należałoby rozważyć wprowadzenie fakultatywnego mechanizmu wsparcia lub rozłożenia w czasie kosztów wycofania rozwiązań, przynajmniej dla mikro-, małych i średnich przedsiębiorców, bez tworzenia po stronie Skarbu Państwa roszczenia odszkodowawczego, co byłoby trudne do pogodzenia z racją stanu leżącą u podstaw decyzji.

Konstrukcja wycofania wyraża konieczność ważenia bezpieczeństwa państwa, ciągłości usług i kosztów transformacji technologicznej. Uzasadnienie projektu wskazuje, że okresy przejściowe mają umożliwić migrację bez wywoływania destabilizacji systemów. Nie tworzą jednak roszczenia o zachowanie dotychczasowego rozwiązania ani obowiązku kompensacji wynikającego z samej ustawy. Brak ustawowego mechanizmu rekompensaty wzmacnia potrzebę precyzyjnego ustalenia przesłanek decyzji, pełnego jej uzasadnienia i skutecznej kontroli sądowej przewidzianej w art. 67e u.k.s.c.[42].

Polecenie zabezpieczające z art. 67g ust. 1 u.k.s.c. jest nadzwyczajnym instrumentem stosowanym po wystąpieniu incydentu krytycznego. Decyzja może odnosić się do nieokreślonej liczby podmiotów należących do kategorii wskazanych w art. 67g ust. 2 u.k.s.c. W uzasadnieniu projektu określono ją jako decyzję generalną, kierowaną do kategorii podmiotów, co ma umożliwić reakcję również wtedy, gdy wszystkich indywidualnych adresatów nie można ustalić z góry. Kwalifikacja ta nie zwalnia jednak organu z obowiązku ścisłego określenia ustawowej kategorii adresatów i zakresu nakazu. Przed wydaniem polecenia minister właściwy do spraw informatyzacji powinien przeprowadzić analizę wymaganą przez art. 67g ust. 5 u.k.s.c., obejmującą cyberzagrożenie, ryzyko, przewidywane skutki, skuteczność nakazu, jego

42 Druk sejmowy nr 1955, uzasadnienie części dotyczącej art. 67c, 143; Możdżeń-Sypniewska, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 67c, teza 5. Uzasadnienie wyjaśnia funkcję okresów wycofania, natomiast komentatorka wskazuje na kontrowersje związane z brakiem ustawowej kompensacji kosztów wycofania infrastruktury.

dotkliwość i proporcjonalność. Zamknięty katalog zachowań możliwych do nakazania zawiera art. 67g ust. 10 u.k.s.c.[43].

Skala wyłączeń gwarancji procesowych w tym trybie jest szczególnie rozległa. Na podstawie art. 67g ust. 3 u.k.s.c. ustawodawca wyłączył stosowanie art. 10, 34, 79, 81, 81a, 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 k.p.a. oraz całego rozdziału 8 działu I k.p.a.; pozostałe przepisy Kodeksu stosuje się odpowiednio. Skumulowanie tych wyłączeń z generalnym charakterem decyzji, jej natychmiastową wykonalnością oraz doręczeniem przez obwieszczenie wzmacnia zastrzeżenia gwarancyjne i uzasadnia rozważenie dodatkowego mechanizmu informowania potencjalnych adresatów polecenia.

Natychmiastowa wykonalność i skutek doręczenia przez urzędowe ogłoszenie służą szybkości reakcji, lecz ograniczają możliwość wcześniejszej obrony adresatów. W uzasadnieniu projektu rygor natychmiastowej wykonalności powiązano z koniecznością szybkiego ograniczenia skutków incydentu krytycznego, wskazując zarazem na sądową ochronę adresata. Polecenie może obowiązywać przez czas koordynacji obsługi incydentu albo przez okres oznaczony, nieprzekraczający jednak dwóch lat. Termin dwóch miesięcy na wniesienie skargi wynikający z art. 67i ust. 1 u.k.s.c. nie podlega przywróceniu na podstawie art. 67i ust. 3 u.k.s.c. Z tego względu ogłoszenie powinno jednoznacznie określać krąg adresatów, nakazane zachowanie, termin wykonania i uzasadnienie proporcjonalności. Sądowa kontrola nie może ograniczać się do formalnej legalności, lecz powinna obejmować rzetelność analizy ryzyka, która stanowi materialną przesłankę ingerencji[44].

Konstrukcja ta budzi zastrzeżenia gwarancyjne. Łączne zastosowanie decyzji generalnej, natychmiastowej wykonalności, doręczenia przez

43 Druk sejmowy nr 1955, uzasadnienie, 149. Projektodawca określił polecenie zabezpieczające jako decyzję generalną skierowaną do ustawowo oznaczonej kategorii podmiotów, wskazując na możliwość nieustalenia z góry pełnego kręgu indywidualnych adresatów. Zob. również Możdżeń-Sypniewska, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, komentarz do art. 67g, tezy 2–3, 5 i 8.

44 Druk sejmowy nr 1955, uzasadnienie, 151. Projektodawca uzasadnia natychmiastową wykonalność potrzebą szybkiego ograniczenia skutków incydentu krytycznego, natomiast ochronę praw strony po wyłączeniu ponownego rozpatrzenia sprawy wiąże z możliwością wniesienia skargi do sądu administracyjnego. Zob. Martyna Wilbrandt-Gotowicz, „Transformacja regulacji krajowego systemu cyberbezpieczeństwa z perspektywy instytucji administracyjnego prawa procesowego" *Prawo i Więź*, nr 4 (2025): 198.

obwieszczenie oraz dwumiesięcznego terminu do wniesienia skargi, który nie podlega przywróceniu, istotnie ogranicza możliwość skutecznego skorzystania z prawa do sądu. Ocena zgodności tego rozwiązania z art. 45 ust. 1 Konstytucji RP[45] wymaga jednak pogłębionej analizy z wykorzystaniem orzecznictwa Trybunału Konstytucyjnego oraz sądów administracyjnych. *De lege ferenda* należałoby rozważyć obowiązek dodatkowego zawiadamiania właściwych organizacji branżowych lub izb gospodarczych równolegle do obwieszczenia, bez wstrzymywania wykonalności polecenia, oraz dopuścić przywrócenie terminu w wyjątkowych, ustawowo określonych przypadkach, np. w razie braku realnej możliwości powzięcia wiadomości o obwieszczeniu.

Chociaż, jak wspomniano, omawiana konstrukcja budzi zastrzeżenia gwarancyjne, sama nieprzywracalność terminu do wniesienia skargi nie przesądza o naruszeniu prawa do sądu. W wyroku z 4 grudnia 2006 r., P 35/05 Trybunał Konstytucyjny uznał za zgodny z art. 45 ust. 1 w zw. z art. 77 ust. 2 Konstytucji RP czternastodniowy, nieprzywracalny termin wniesienia sprzeciwu w innym szczególnym mechanizmie dostępu do sądu. Orzeczenie to nie rozstrzyga oceny art. 67i u.k.s.c., wskazuje jednak, że przedmiotem kontroli powinien być cały układ gwarancji proceduralnych. W analizowanym przypadku źródłem wątpliwości jest zatem kumulacja generalnego charakteru decyzji, doręczenia przez obwieszczenie, natychmiastowej wykonalności oraz terminu niepodlegającego przywróceniu. *De lege ferenda* powinno się wprowadzić obowiązek równoległego informowania właściwych organizacji branżowych lub izb gospodarczych, a także dopuścić przywrócenie terminu w ściśle określonych przypadkach braku realnej możliwości powzięcia wiadomości o obwieszczeniu[46].

Bezpieczeństwo łańcucha dostaw stanowi zwykły, a nie nadzwyczajny element systemu zarządzania. Przepis art. 8 ust. 1 pkt 2 lit. e u.k.s.c. wymaga uwzględnienia bezpieczeństwa i ciągłości łańcucha dostaw produktów, usług i procesów ICT oraz relacji z bezpośrednimi dostawcami. Podmiot musi ocenić podatności, praktyki bezpiecznego rozwoju, aktualizacje, obsługę incydentów, podwykonawstwo i możliwość audytu. Odpowiednie wymagania

45 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., Nr 78, poz. 483 ze zm.).

46 Wyrok Trybunału Konstytucyjnego z dnia 4 grudnia 2006 r., P 35/05, OTK-A 2006, nr 11, poz. 167, Dz. U. z 2006 r. Nr 227, poz. 1665.

powinny znaleźć odzwierciedlenie w umowach, ponieważ kontrola ryzyka bez instrumentów kontraktowych pozostaje niewykonalna[47].

W zamówieniach publicznych obowiązek zapewnienia cyberbezpieczeństwa nie wyłącza stosowania zasad uczciwej konkurencji, równego traktowania wykonawców i proporcjonalności. Wymagania dotyczące procesu lub etapu cyklu życia produktu albo usługi mogą zostać ujęte w opisie przedmiotu zamówienia zgodnie z art. 99 ust. 2 p.z.p.[48], jeżeli pozostają związane z przedmiotem zamówienia i są proporcjonalne do jego wartości oraz celów[49]. Przepis art. 99 ust. 4 p.z.p. zakazuje opisu utrudniającego uczciwą konkurencję[50]. Jeżeli ankieta cyberbezpieczeństwa, certyfikat lub raport z audytu stanowią przedmiotowy środek dowodowy, art. 106 ust. 1–3 p.z.p. wymaga, aby środek ten był niezbędny, związany z przedmiotem zamówienia i proporcjonalny, a zamawiający dopuszczał środki równoważne[51].

---

47 Karol Świtała, „Obowiązki organizacyjne administratorów danych osobowych i operatorów usług kluczowych. Wnioski de lege lata i postulaty de lege ferenda" *Przegląd Ustawodawstwa Gospodarczego*, nr 10 (2022): 34; Jarosław Greser, „Regulacja cyberbezpieczeństwa w sektorze energetycznym w świetle projektu dyrektywy NIS2" *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, nr 2 (2021): 95.

48 Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2026 r., poz. 793).

49 Zob. Michał Rogalski, „Cyberbezpieczeństwo w zamówieniach publicznych. Część druga" *Zamówienia publiczne Doradca*, nr 5 (2026): 59. Autor wskazuje, że obowiązek zarządzania bezpieczeństwem łańcucha dostaw z art. 8 ust. 1 pkt 2 lit. e u.k.s.c. oznacza w praktyce zamówieniowej konieczność żądania od wykonawcy informacji o podwykonawcach, w szczególności obsługujących systemy krytyczne.

50 Wymóg związku opisu przedmiotu zamówienia z rzeczywistymi potrzebami zamawiającego był wielokrotnie przedmiotem orzecznictwa Krajowej Izby Odwoławczej. Izba konsekwentnie akcentuje kryterium „uzasadnionych potrzeb zamawiającego" oraz „obiektywnych okoliczności" jako granicę dopuszczalności opisu ograniczającego krąg potencjalnych wykonawców. Zob. wyroki KIO: z 5.07.2011 r., KIO 1307/11, LEX nr 852642; z 8.07.2011 r., KIO 1344/11, LEX nr 862355; z 12.07.2012 r., KIO 1360/12, LEX nr 1212122. KIO dopuszcza przy tym żądanie rozwiązań nowoczesnych lub wyjątkowych, o ile jest to uzasadnione rzeczywistą potrzebą zamawiającego – zob. wyroki KIO: z 1.02.2011 r., KIO 79/11, KIO 89/11, KIO 90/11, LEX nr 784855; z 28.02.2012 r., KIO 229/12 i in., LEX nr 1125011; z 3.09.2014 r., KIO 1726/14, LEX nr 1538349.

51 Rogalski, „Cyberbezpieczeństwo w zamówieniach publicznych", 41. Autor zaleca różnicowanie kryteriów weryfikacji zdolności technicznej wykonawcy w zależności od tego, czy zamówienie dotyczy zamówień wrażliwych.

Zakaz nabywania rozwiązań objętych decyzją w sprawie uznania dostawcy za dostawcę wysokiego ryzyka wynika wprost z art. 67c ust. 4 u.k.s.c. Dodatkowo art. 226 ust. 1 pkt 19 p.z.p. nakazuje odrzucić ofertę obejmującą produkt ICT, którego typ określono w tej decyzji, albo wskazane w niej usługę lub proces ICT. Skutek ten nie stanowi kryterium oceny ofert, lecz ustawową konsekwencję decyzji wydanej na podstawie art. 67b ust. 15 u.k.s.c. Zamawiający powinien zatem uwzględnić obowiązującą decyzję w opisie potrzeb i wymagań, dokumentach zamówienia, badaniu ofert oraz zarządzaniu umową. Nie może jednak tworzyć własnej kategorii dostawcy wysokiego ryzyka ani rozszerzać ustawowego zakazu na podmioty lub rozwiązania nieobjęte decyzją. Wymagania wykraczające poza jej zakres muszą znajdować samodzielne uzasadnienie w analizie ryzyka i przepisach Prawa zamówień publicznych.

7 Zakończenie

Przeprowadzona analiza pozwala udzielić twierdzącej odpowiedzi na postawione pytanie badawcze, niepozbawionej jednakże kilku zastrzeżeń. Rozwiązania wprowadzone nowelizacją z 2026 r. mogą być postrzegane jako zintegrowany administracyjnoprawny model zarządzania zgodnością, w którym kwalifikacja adresata, samorejestracja, zarządzanie ryzykiem, odpowiedzialność kierownika, nadzór, sankcje oraz instrumenty bezpieczeństwa systemowego pozostają funkcjonalnie powiązane. Należy jednak wyraźnie podkreślić, że normatywnym spoiwem tej konstrukcji nie jest sam katalog obowiązków, lecz ryzyko – wyznacza ono treść zabezpieczeń po stronie podmiotu, a zarazem powinno ograniczać wybór i intensywność ingerencji po stronie organu.

Z ustalenia tego wynika podwójny obowiązek uzasadnienia. Podmiot regulowany powinien dokumentować nie tylko posiadanie procedur, lecz także tok rozpoznania ryzyka, kryteria wyboru zabezpieczeń, zapewnienie zasobów oraz sposób weryfikacji skuteczności środków. Organ nadzoru powinien natomiast wykazać, jakie ryzyko uzasadnia interwencję, dlaczego zastosowany instrument jest przydatny i konieczny oraz z jakich powodów środek mniej dolegliwy byłby niewystarczający. Dopiero symetria tych obowiązków pozwala odróżnić zarządzanie zgodnością od formalnego administrowania dokumentacją, a nadzór oparty na ryzyku od reakcji opierającej się jedynie na stwierdzeniu niezgodności.

Najpoważniejsze napięcia modelu ujawniają się w trzech obszarach. Po pierwsze, status powstający z mocy prawa nie może prowadzić do pomijania usprawiedliwionej niepewności kwalifikacyjnej przy indywidualizacji sankcji. Po drugie, osobista odpowiedzialność kierownika wymaga wskazania konkretnego obowiązku zarządczego i związku jego naruszenia z niezgodnością organizacji. Po trzecie, urzędnik monitorujący, decyzja wobec dostawcy wysokiego ryzyka i polecenie zabezpieczające wymagają wykładni gwarancyjnej, ponieważ skuteczność reakcji na cyberzagrożenie nie znosi obowiązku proporcjonalności ani prawa do efektywnej kontroli sądowoadministracyjnej.

De lege ferenda interwencja ustawodawcza powinna pozostać selektywna – należy doprecyzować granice kompetencji urzędnika monitorującego, wzmocnić sposób informowania o poleceniu zabezpieczającym, skoordynować postępowania sankcyjne z reżimem ochrony danych oraz ustanowić ustawową ewaluację funkcjonowania modelu po upływie trzech lat, nawiązując do mechanizmu przeglądowego z art. 40 dyrektywy NIS2.

O jakości reformy nie przesądzi intensywność administracyjnej represji, lecz zdolność podmiotów i organów do podejmowania sprawdzalnych, proporcjonalnych i podlegających kontroli decyzji opartych na ryzyku. Administracyjnoprawny model zarządzania zgodnością spełni swoją funkcję dopiero wtedy, gdy cyberodporność stanie się rezultatem tak rozumianej rozliczalności decyzyjnej, a nie jedynie skutkiem obawy przed sankcjami.

Bibliografia

Baran Agnieszka, Klaudia Gierejko, „Zarządzanie bezpieczeństwem informacji w świetle dyrektywy NIS2 – obowiązki, wyzwania prawne i organizacyjne przedsiębiorstw" *Akademia Zarządzania*, nr 2 (2026): 362–377.

Chałubińska-Jentkiewicz Katarzyna, Monika Nowikowska, „Entities Involved in the Policy of Ensuring the Security of Network and Information Systems in the Light of the NIS2 Directive (Part 1)" *Cybersecurity and Law*, nr 1 (2024): 5–20.

Chronowska-Sioła Emilia, „Unijna dyrektywa NIS2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych" *Cybersecurity and Law*, nr 2 (2025): 14–29.

Coglianese Cary, David Lazer, „Management-Based Regulation: Prescribing Private Management to Achieve Public Goals" *Law & Society Review*, nr 4 (2003): 691–730.

Dyrektywa NIS2. Komentarz, red. Mateusz Jakubik, Rafał Tomasz Prabucki. Warszawa: Wolters Kluwer, 2026. LEX.

Greser Jarosław, „Regulacja cyberbezpieczeństwa w sektorze energetycznym w świetle projektu dyrektywy NIS2" *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, nr 2 (2021): 87–101.

Karpiuk Mirosław, „Normatywno-aksjologiczne aspekty bezpieczeństwa" *Cybersecurity and Law*, nr 1 (2025): 14–24.

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

Nowak-Byrtek Dominika, „RODO i dyrektywa NIS2 – wpływ ochrony danych osobowych na regulacje dotyczące cyberbezpieczeństwa" *Monitor Prawniczy*, nr 11 (2024): 18–23.

Pelc Paweł, „DORA jako regulacja sektorowa w rozumieniu dyrektywy NIS2" *Cybersecurity and Law*, nr 1 (2026): 186–197.

Pelc Paweł, „Zasada proporcjonalności w DORA" *Cybersecurity and Law*, nr 2 (2024): 207–218.

Rogalski Michał, „Cyberbezpieczeństwo w zamówieniach publicznych. Część druga" *Zamówienia Publiczne Doradca*, nr 5 (2026).

Siwicki Maciej, „Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego" *Europejski Przegląd Sądowy*, nr 9 (2019): 13–20.

Skoczylas Dominika, „Dyrektywa NIS2 a cyberbezpieczeństwo administracji publicznej" *Dyskurs Prawniczy i Administracyjny*, nr 1 (2025): 227–236.

Skoczylas Dominika, „Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń" *Europejski Przegląd Sądowy*, nr 12 (2024): 39–44.

Szpor Grażyna, „The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland" *Review of European and Comparative Law*, nr 3 (2021): 219–235.

Świtała Karol, „Obowiązki organizacyjne administratorów danych osobowych i operatorów usług kluczowych. Wnioski de lege lata i postulaty de lege ferenda" *Przegląd Ustawodawstwa Gospodarczego*, nr 10 (2022): 29–35.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. Agnieszka Besiekierska. Warszawa: C.H. Beck, 2019.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. Justyna Kurek-Sobieraj, Katarzyna Chałubińska-Jentkiewicz, Mirosław Karpiuk. Warszawa: C.H. Beck, 2026. Legalis.

Wilbrandt-Gotowicz Martyna, „Transformacja regulacji krajowego systemu cyberbezpieczeństwa z perspektywy instytucji administracyjnego prawa procesowego" *Prawo i Więź*, nr 4 (2025): 173–204.



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