ZESZYT PRAWNICZY UAM
NR 14/2024
https://doi.org/10.14746/zpuam.2024.14.12

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

ALEKSANDRA SZULC

Uniwersytet Ekonomiczny w Krakowie
https://orcid.org/0000-0002-1578-8262
1002115@student.uek.krakow.pl

Obowiązki podmiotów finansowych w obszarze cyberbezpieczeństwa w świetle prawodawstwa Unii Europejskiej

Obligations of Financial Entities in the Area of Cybersecurity in Light of European Union Legislation

Abstract: The choice of subject matter for this article is justified by the process of updating the legal framework for the financial sector in fields of digital resilience processes and standards as part of the EU digital single market policy. The aim of the article is to explain changes in the legal environment of financial entities and the community approach to the issue of information security as a result of the transformation of the digital environment. Another goal is to review the cybersecurity requirements of these institutions. Using theoretical studies, the legal-dogmatic method and document analysis, the requirements imposed on financial institutions in terms of ensuring protection and counteracting cyber threats are analysed.

Keywords: cybersecurity, cyber risk, digital operational resilience, ICT risk, DORA

Wprowadzenie

Kwestia bezpieczeństwa informacyjnego znalazła się w kręgu zainteresowania instytucji Unii Europejskiej (dalej: UE) już w 2004 r., na co wskazuje choćby powołanie specjalnego podmiotu – Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (dalej: ENISA) koncentrującego swoje działania na zapewnieniu wysokiego poziomu odporności unijnej infrastruktury na zagrożenia ze środowiska cyfrowego. Za kolejny milowy krok należy uznać komunikat Komisji Europejskiej z 2009 r. dotyczący problematyki zaufania do cyfrowego bezpieczeństwa społeczeństwa, efektem którego cztery lata później stała się Strategia Cyberbezpieczeństwa UE przedstawiona decyzyjnym organom Wspólnoty przez Wysokiego Przedstawiciela Unii do spraw Zagranicznych i Polityki Bezpieczeństwa[1]. Postęp technologiczny i wymuszone przez pandemię COVID-19 przeniesienie znaczących obszarów aktywności podmiotów gospodarczych do przestrzeni Internetu wzmocniły potrzebę implementacji narzędzi ograniczających rosnące ryzyko przestępczości cyfrowej. Szczególnie rozwój infrastruktury informatycznej, bankowości elektronicznej i rozwiązań automatyzujących procesy w instytucjach uświadomił, jak wrażliwy i podatny na zagrożenia pochodzące z cyberprzestrzeni stał się obecnie sektor finansowy. Rozwój techno-

[1] D. Markopoulou, V. Papakonstantinou, P. De Hert, *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, „Computer Law & Security Review" 2019, t. 35, nr 6, s. 2.

logiczny spowodował także pojawienie się nowych aktorów na rynku – dostawców usług informatycznych, w tym oferujących technologie oparte na rozwiązaniach ICT[2] i wykorzystywanych do świadczenia usług finansowych (*fintech*).

Analiza zagadnień została w niniejszym artykule zawężona do otoczenia prawnego podmiotów finansowych – kategorii podmiotów, które ze względu na złożoności definicyjne w regulacjach UE należy na poczet opracowania rozumieć w sposób rozszerzający (art. 4 Rozporządzenia 575/2013)[3]. W stosunku do tej kategorii będzie zamiennie stosowane pojęcie „instytucje finansowe".

1. Cyberbezpieczeństwo sektora finansowego

Pomimo szerokiego zastosowania terminu „cyberbezpieczeństwo" dotąd nie skonstruowano w doktrynie i w prawodawstwie unijnym jego jednolitej definicji. Znaczenie pojęcia jest skorelowane z konceptem bezpieczeństwa informacyjnego i zagrożeniami związanymi z aktywnością w cyberprzestrzeni. W analizie tej problematyki używa się zamiennie terminów: cyberbezpieczeństwo, bezpieczeństwo informacyjne, bezpieczeństwo ICT, operacyjna odporność cyfrowa. Dyrektywa nr 2016/1148[4], uznana jako pierwszy akt unijny regulujący ten obszar, posługuje się pojęciem „bezpieczeństwo sieci i systemów informatycznych", oznaczającym „odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne"(art. 4 pkt 2 NIS).

Wspomniane w przytoczonej definicji dostępność, autentyczność, integralność lub poufność danych składają się na obszar bezpieczeństwa informacji. Działania, których skutkiem jest naruszenie chociażby jednego z tych czterech elementów, określane są mianem cyberataków, a prawdopodobieństwo materializacji tych zagrożeń – cyberryzykiem (ryzykiem cybernetycznym). Do zdarzenia, które doprowadziło do wskazanych zakłóceń infrastruktury, stosuje się pojęcie incydentu. Cyberryzyko, jako jedne z rodzajów ryzyka występującego w działalności przedsiębiorstwa, może być definiowane w zależności od typu szkody czy formy zagrożenia, które może spowodować. Koncentrując się na obszarze operacyjnym, może ono

[2] Technologia informacyjno-komunikacyjna.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych oraz zmieniające rozporządzenie (UE) nr 648/2012 (Dz.Urz. UE L 176 z 2013 r., s. 1).

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 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 2016 r., s. 1), dalej: NIS.

stanowić rezultat aktywności ludzkiej, zakłóceń pracy systemu i technologii, nieprawidłowości procesów wewnętrznych oraz zdarzeń zewnętrznych[5]. Pokrewnym pojęciem z podobnym zakresem znaczeniowym jest ryzyko ICT, rozumiane, zgodnie z rozporządzeniem DORA[6], jako okoliczność w środowisku informatycznym, której materializacja ma potencjał zakłócenia bezpieczeństwa sieci, systemów informatycznych, urządzeń i procesów oraz wywołania negatywnych skutków w ich otoczeniu (art. 3 pkt 5 DORA). Termin „cyberbezpieczeństwo" odnajdziemy w Rozporządzeniu (UE) 2019/881 z dnia 17 kwietnia 2019 r.[7], gdzie jest rozumiane jest jako: „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami" (art. 2 pkt 1 aktu o cyberbezpieczeństwie).

Bezpieczeństwo cybernetyczne stanowi pojęcie dynamiczne i zyskuje znaczenie zależnie od kontekstu i przedmiotu tekstu prawnego, w którym zostało użyte[8]. W próbach określenia jego zakresu znaczeniowego warto posłużyć się wykładnią celowościową i kierować się *ratio legis* danej regulacji. Występujące w powyższych definicjach łączniki, takie jak odporność i ochrona przed zagrożeniami dla sieci, systemów informatycznych i danych, wystarczą dla wskazania ogólnej, elastycznej i wystarczającej na potrzeby dyskursu definicji cyberbezpieczeństwa.

Dane pozyskiwane i przetwarzane przez instytucje finansowe opierają się na prawidłowym i niezawodnym funkcjonowaniu systemów informatycznych. Wzajemne powiązania pomiędzy tymi systemami i kanałami przekazywania danych wzmacniają potrzebę wdrożenia odpowiednich zabezpieczeń. Wspomniana korelacja generuje ryzyko podatności na cyberzagrożenia także o charakterze systemowym. Lokalne naruszenia infrastruktury przy obecnej prędkości przepływu informacji mogą doprowadzić do incydentu obejmującego szereg podmiotów powiązanych z instytucją finansową. Powstałe skutki mogą negatywnie wpłynąć nie tylko na płynność finansową i wiarygodność podmiotu na rynku, lecz także na stabilność krajowego, a nawet unijnego systemu finansowego (art. 3 DORA). Początkowo pierwsze horyzontalne ramy dla bezpieczeństwa cybernetycznego objęły wyłącznie, uznaną za kluczową, część sektora finansowego, przede wszystkim instytucje kredytowe i operatorów na rynku regulowanym. Znaczenie zarządzania cyberryzykiem

[5] J.J. Cebula, M.E. Popeck, L.R. Young, *A Taxonomy of Operational Cyber Security Risks Version 2*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2014, s. 1.

[6] Rozporządzenie Parlamentu Europejskiego i Rady nr 2022/2554 z dnia 14 grudnia 2022 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 2022 r., s. 1), dalej: DORA.

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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 2019 r., s. 15), dalej: akt o cyberbezpieczeństwie.

[8] C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023, s. 36.

i ochrony infrastruktury finansowej przez cyberzagrożeniami wzrosło na tyle, że prawodawca unijny w DORA wskazał przez enumerację szeroką gamę czynnych uczestników jednolitego rynku finansowego zobowiązanych do stosowania nowych wymogów, określając ich zbiorczo mianem „podmiotów finansowych"[9].

2. Aktywność legislacyjna UE w obszarze cyberbezpieczeństwa

Działalność instytucji finansowych jest silnie unormowana, a przepisy dotyczące odporności cyfrowej i zawierające wymogi w zakresie zarządzania ryzykiem ICT są rozproszone w różnych regulacjach krajowych i unijnych. W kontekście niniejszego opracowania należy dokonać rozróżnienia aktów prawnych z zakresu cyberbezpieczeństwa na te dotyczące wszystkich podmiotów (generalne) i na sektorowe, których zakres stosowania obejmuje wyłącznie usługodawców na rynku finansowym czy podmioty sektora bankowego. Dodatkowo, część przepisów stanowiących normy w zakresie ochrony infrastruktury informatycznej znajduje się w regulacjach związanych bezpośrednio ze sferą finansów, przykładowo w obszarze usług płatniczych i obrotu instrumentami finansowymi czy w obszarze ochrony i dostępu do danych. Kompleksowość i fragmentację otoczenia prawnego dla cyberbezpieczeństwa rynku finansowego pogłębia zdecydowana przewaga regulacji wymagających najpierw transponowania do krajowych systemów prawnych[10]. Dodatkowo pozostawienie dużej swobody państwom członkowskich w projektowaniu krajowych strategii i polityk oraz zróżnicowane podejścia krajowych nadzorców doprowadziły do powstania istotnych rozbieżności. Brak wymogu bezpośredniego stosowania przepisów i ograniczenie ram prawnych do minimum wymaganego dyrektywą sprawił, że UE przez lata nie poczyniła istotnych postępów w kierunku przyjęcia zunifikowanego podejścia do kwestii cyberbezpieczeństwa sektora finansowego.

Mnogość i rozdrobnienie przepisów dotyczących ryzyka cybernetycznego zwiększają niepewność prawną, która przekłada się na koszty i obciążenia administracyjne związane z dostosowaniem do zasad panujących w różnych jurysdykcjach[11]. Zważywszy na transgraniczny charakter usług cyfrowych i postępującą digitalizację sektora finansowego rozwiązanie tego problemu stało się kwestią priorytetową. Innym dylematem jest rozbieżność w podejściu regulatorów krajowych do kwestii zarządzania ryzykiem ICT, w tym szczególnie do raportowania incydentów i prze-

[9] A. Lichosik, *DORA jako prawny instrument ochrony cyfrowego bezpieczeństwa rynku finansowego*, „Studia Prawnoustrojowe" 2023, nr 62, s. 371.

[10] P.S. Krüger, J.-P. Brauchle, *The European Union, Cybersecurity, and the Financial Sector*: *A Primer*, Washington, DC 2021, s. 3.

[11] G. Pavlidis, *Europe in the Digital Age: Regulating Digital Finance without Suffocating Innovation*, „Law, Innovation and Technology" 2021, t. 13, nr 2, s. 474.

prowadzania testów bezpieczeństwa, jak również częste nakładanie się przepisów i obowiązków podmiotów finansowych (motyw 10 DORA).

W obszarze cyberbezpieczeństwa szczególne znaczenie należy przypisać NIS. Prymarnym celem uchwalenia regulacji było zobligowanie państw członkowskich do opracowania własnych strategii w zakresie cyberbezpieczeństwa[12], a tym samym włączenia przez nie sieci i systemów informatycznych do grupy obszarów podatnych na zagrożenia. W stosunku do podmiotów finansowych dyrektywa wskazuje w załączniku II trzy rodzaje podmiotów: instytucje kredytowe, operatorów na rynku regulowanym, OTF i MTF[13] oraz kontrahentów centralnych. W gestii krajowego prawodawcy pozostawia się dokonanie wyboru operatorów kluczowych, do których mają znaleźć zastosowanie szczególne wymogi w zakresie bezpieczeństwa sieci i systemów informatycznych. Do tej samej kategorii generalnych aktów prawnych należy zaliczyć rozporządzenie (UE) 2016/679[14] koncentrujące się na przetwarzaniu i naruszeniach danych osobowych. Sama dyrektywa NIS sporadycznie i w sposób ograniczony odnosi się do kwestii związanych z unijnym reżimem ochrony danych, co wynika z niezależnego od siebie procedowania obu aktów prawa UE[15].

Jako kolejny akt prawny należy wskazać akt o cyberbezpieczeństwie, który wprowadza do wspólnotowego systemu prawnego ramy dla funkcjonowania ENISA i certyfikacji bezpieczeństwa cyfrowego. Certyfikat stanowi potwierdzenie zapewnienia przez podmiot odpowiedniego poziomu cyberbezpieczeństwa narzędzi, rozwiązań, procedur i infrastruktury ICT (art. 1 ust. 1 pkt 1 aktu o cyberbezpieczeństwie). Rozporządzenie zawiera szereg definicji związanych z bezpieczeństwem sieci i systemów informatycznych, do których odwołują się później uchwalone i procedowane regulacje unijne.

Nowelizacja dyrektywy NIS z 14 grudnia 2022 r.[16] przyniosła szereg zmian, uzupełniając luki poprzedniczki, szczególnie w obszarze mechanizmów współpracy, kryteriów podmiotowych stosowania ram regulacyjnych i środków ich skutecznego egzekwowania (motyw 5 NIS2). Wprowadziła zaostrzenie obowiązków w obszarze

[12] N. Vandezande, *Cybersecurity in the EU: How the NIS2-directive Stacks up against Its Predecessor*, „Computer Law & Security Review" 2024, t. 52, artykuł 105890, s. 2.

[13] Organised Trading Facility (OTF, zorganizowana platforma obrotu), Multilateral Trading Facilitiy (MTF, alternatywna platforma obrotu), zgodnie z Dyrektywą Parlamentu Europejskiego i Rady nr 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniającą dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.Urz. UE L 173 z 2014 r., s. 349 z późn. zm.), dalej: MIFIDII.

[14] 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 2016 r., s. 1 z późn. zm.).

[15] D. Markopoulou, V. Papakonstantinou, P. De Hert, op. cit., s. 9.

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 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 2022 r., s. 80), dalej: NIS2.

obligatoryjnie prowadzonej polityki zarządzania ryzykiem ICT poprzez introdukcję katalogu minimalnego wymogów cyberbezpieczeństwa i doprecyzowanie wymogów w zakresie zgłaszania przeprowadzonych czynności w odpowiedzi na ujawnione incydenty[17]. Nowa odsłona dyrektywy miała zaradzić powstałej po wejściu w życie NIS znaczącej dysproporcji pomiędzy poziomami ochrony w różnych państwach członkowskich i arbitralnemu kreowaniu przez krajowych regulatorów ram zarządzania cyberryzykiem.

Uzupełnienie NIS2 w zakresie, w którym w sposób niewystarczający normuje pewne aspekty związane z ochroną infrastruktury cyfrowej, zapewnia dyrektywa (UE) 2022/2557[18]. Regulacja podkreśla potrzebę nadania przez państwa członkowskie instytucjom rynku finansowego statusu podmiotów krytycznych, co implikuje stosowanie wobec nich wymogów dyrektywy z zakresu strategii, oceny ryzyka i narzędzi wsparcia (motyw 20 NIS2).

Drugą kategorię źródeł prawa dla cyberbezpieczeństwa sektora finansowego stanowią przepisy aktów prawnych, których zakres stosowania zamyka się na podmiotach finansowych. Mimo że punkt koncentracji w tych regulacjach opiera się na kreowaniu zasad prowadzenia poszczególnych obszarów działalności, szereg normatywnych wymogów i obowiązków dotyczy kwestii ryzyka cybernetycznego i ochrony infrastruktury ICT. Do tej grupy można zaliczyć dyrektywy 2014/65/UE i 2015/2366[19]. Druga odsłona PSD, obowiązująca od 13 stycznia 2018 r., stanowi fundament dla otoczenia prawnego elektronicznych usług płatniczych, prowadzenia rachunków płatniczych w sieci i środowiska otwartej bankowości. Za przełomowe należy uznać wprowadzenie przez regulację wymogu stosowania dwuetapowego silnego uwierzytelniania klienta (SCA) przy inicjowaniu elektronicznych transakcji płatniczych i dostępie do rachunku (art. 97 PSD2). W przedmiocie cyberbezpieczeństwa, obowiązki w tym zakresie można odnaleźć choćby w katalogu wymogów wniosku o udzielenie zezwolenia na prowadzenia działalności. Zgodnie z art. 5 ust. 1 PSD2 instytucja powinna przedstawić dokumentację dotyczącą również wdrożonych środków kontroli bezpieczeństwa i ograniczania ryzyka uwzględniających „sposób zapewniania wysokiego poziomu bezpieczeństwa technicznego i ochrony danych, w tym w odniesieniu do oprogramowania i systemów informatycznych". Większość standardów w przedmiocie ochrony przed cyberzagrożeniami została ulokowana w sekcjach przepisów dotyczących ram zarządzania ryzykiem operacyjnym

[17] W. Szpringer, *Platformizacja gospodarki cyfrowej 5.0. Nowe wyzwania dla regulacji*, Warszawa 2022, s. 163.

[18] Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 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 2022 r., s. 164).

[19] 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.U. UE L 337 z 2015 r., s. 35 z późn. zm.), dalej: PSD2.

i ryzykiem bezpieczeństwa oraz wśród obowiązków związanych ze zgłaszaniem poważnych incydentów[20].

Podobny przykład można odnaleźć w dyrektywie w sprawie rynków instrumentów finansowych. Zgodnie z art. 16 ust. 5 MIFIDII firma inwestycyjna powinna wdrożyć „skuteczne mechanizmy kontroli i zabezpieczenia dotyczące systemów przetwarzania informacji" i „należyte mechanizmy bezpieczeństwa służące zagwarantowaniu bezpieczeństwa środków przekazu informacji i ich uwierzytelnianiu, minimalizowaniu ryzyka uszkodzenia danych oraz nieuprawnionego dostępu i zapobieganiu wyciekowi informacji".

Inną kategorią źródła prawa, o której należy wspomnieć, są regulacje normujące wąskie obszary aktywności korzystające z innowacji i wprowadzające dostosowane do tych rozwiązań technologicznych zasady w zakresie bezpieczeństwa cyfrowego. Przykładem w tej grupie jest rozporządzenie 2023/1114[21] regulujące aktywność instytucji finansowych prowadzoną z wykorzystaniem technologii rozproszonego rejestru (DLT) i rozporządzenie 910/2014[22].

Rozporządzenie eiDAS reguluje zagadnienia związane z identyfikacją elektroniczną i usługami zaufania w obszarze transakcji elektronicznych. W dobie cyfryzacji usług płatniczych na rynku finansowym za szczególnie ważne uznano wdrożenie skutecznych norm bezpieczeństwa informacyjnego i minimalizacji zagrożeń, w tym cyberzagrożeń, związanych z kradzieżą tożsamości i nieautoryzowanym dostępem.

3. Rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego

W procesie budowania jednolitego rynku cyfrowego UE kwestią priorytetową stała się aktualizacja ram prawnych dla sektora finansowego, w szczególności w zakresie procesów i standardów odporności cyfrowej. Aktywność legislacyjną w tym obszarze zainaugurowała we wrześniu 2020 r. Komisja Europejska w strategii w obszarze finansów cyfrowych, wskazującej cztery obszary priorytetowe dla przekształcenia cyfrowego otoczenia rynku finansowego:

a) zniwelowanie fragmentaryzacji sektora finansowego, stanowiącej barierę dla rozwoju transgranicznego rynku,

---

[20] C. Calliess, A. Baumgarten, *Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective*, „German Law Journal" 2020, t. 21, nr 6, s. 1169.

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.Urz. UE L 150 z 2023 r., s. 40 z późn. zm.).

[22] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z 2014 r., s. 73), dalej: eIDAS.

b) wprowadzanie reżimów prawnych sprzyjających innowacjom,

c) budowa europejskiego obszaru danych finansowych,

d) odpowiednie przygotowanie sektora finansowego na wyzwania i zagrożenia związane z procesem digitalizacji[23].

Istotnym narzędziem w realizacji tych planów stało się Rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA), opublikowane 27 grudnia 2022 r. w Dzienniku Urzędowym UE. Celem przyświecającym regulacji jest wprowadzenie zbioru jednolitych standardów zarządzania ryzykiem ICT dla unijnego rynku finansowego. Intencją unijnego ustawodawcy była również harmonizacja zasad sprawowania nadzoru, testowania operacyjnej odporności cyfrowej i uzupełnienie dotychczasowej luki w zakresie monitorowania ryzyka związanego z korzystaniem z usług zewnętrznych dostawców technologii (motyw 9 DORA). Swoim zakresem stosowania obejmuje zakłady ubezpieczeń i reasekuracji, firmy inwestycyjne, instytucje kredytowe, płatnicze i pieniądza elektronicznego, dostawców usług w zakresie kryptoaktywów, firmy audytorskie, agencje ratingowe oraz inne podmioty finansowe. Wymogi wynikające z Rozporządzenia dotyczą bezpośrednio także dostawców usług ze spektrum technologii informacyjno-komunikacyjnych kluczowych dla infrastruktury instytucji finansowych[24]. DORA reguluje następujące grupy zagadnień:

a) wymogi podmiotów finansowych w obszarze:
- zarządzania ryzykiem ICT,
- zgłaszania poważnych incydentów operacyjnych i bezpieczeństwa,
- testowania operacyjnej odporności cyfrowej,
- wzajemnego informowania i przekazywania analiz dotyczących zagrożeń i obszarów wrażliwych na cyberataki,
- narzędzi zarządzania ryzykiem związanego z korzystaniem z usług zewnętrznych dostawców technologii;

b) elementy umów zawartych między instytucjami a zewnętrznymi dostawcami usług ICT,

c) zasady nadzoru, w tym nad usługodawcami z obszaru ICT świadczącymi usługi kluczowe dla sektora finansowego,

d) ramy współpracy między organami i egzekwowanie Rozporządzenia (art. 1 DORA).

Przy stosowaniu przepisów omawianej regulacji, koncentrujących się na kwestiach związanych z ryzykiem ICT, tj. rozdziału II–V sekcji I, podmioty finansowe powinny dostosowywać użyte narzędzia, wdrażane procedury i polityki przy po-

[23] Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów w sprawie strategii dla UE w zakresie finansów cyfrowych z dnia 24 września 2020 r., COM(2020) 591 final, s. 4–5.

[24] The European Union Agency for Cybersecurity (ENISA), *EU Cybersecurity Initiatives in the Finance Sector*, March 2021, s. 4.

mocy klasycznej zasady proporcjonalności. W tym kontekście analizie podlega wielkość i ogólny profil ryzyka, charakter oraz skala i złożoność świadczonych usług i operacji (art. 4 ust. 1 i ust. 2 DORA). Art. 6 DORA wprowadza minimum wymagane w zakresie ram zarządzania przedmiotowym ryzykiem. Podmiot finansowy jest zobligowany do zaimplementowania strategii, polityk, procedur, protokołów i narzędzi z zakresu technologii informacyjno-komunikacyjnych, a także zapewnienia odpowiedniej fizycznej infrastruktury gwarantującej bezpieczeństwo zasobów informacyjnych. Kluczową kwestię stanowią zasady wykrywania i postępowania z incydentami oraz notyfikacji organów nadzoru.

W obszarze obowiązków instytucji szczególny nacisk położono na zapewnienie ciągłości działania na okoliczność materializacji ryzyka ICT. Wszystkie zdarzenia skutkujące naruszeniem sieci lub systemów informatycznych powinny zostać zarejestrowane, zidentyfikowane i sklasyfikowane pod kątem ich priorytetu, dotkliwości i kluczowości zakłóconych usług, a następnie wyeliminowane i zgłoszone do nadzorcy (art. 17 ust. 3 lit. b DORA). Zarządzanie incydentami powinno zostać wsparte wdrożeniem systemu wczesnego ostrzegania, analogicznie jak jest to wymagane w ramach zarządzania innymi rodzajami ryzyka w działalności podmiotu finansowego.

Celem dostosowania do DORA pewne elementy ram zarządzania ryzykiem ICT będą wymagały aktualizacji, szczególnie w zakresie reagowania na incydenty, zwalczania przestojów operacyjnych i odzyskiwania sprawności. Do obszarów, w których rozporządzenie wprowadza konieczność opracowania od nowa procedur i zasad kontroli wewnętrznej, należy polityka wobec zewnętrznych dostawców usług technologicznych i zarządzanie ryzykiem ICT osób trzecich. Najwyższym priorytetem w procesie zapewnienia zgodności z DORA oznaczono opracowanie strategii operacyjnej odporności cyfrowej obejmującej, *inter alia*, metody przeciwdziałania ryzyku, limity tolerancji ryzyka, kluczowe wskaźniki i mechanizmy testowania tej odporności (art. 6 ust. 8 DORA).

Rozporządzenie 2022/2554 należy traktować jako prymarną regulację dla kwestii związanych z bezpieczeństwem informacyjnym dla rynku finansowego. W samym rozporządzeniu wskazano charakter jej relacji do horyzontalnych ram dla cyberbezpieczeństwa wynikających z NIS2, uznając bezpośrednio stosowalny akt prawny jako *lex specialis* do dyrektywy (UE) 2022/2555 (motyw 16 DORA). Tym samym NIS2 należy traktować jako główny punkt odniesienia w przedmiocie obowiązków podmiotów finansowych związanych z cyberbezpieczeństwem i ryzykiem ICT[25]. W obszarach uregulowanych przez dyrektywę CER, w których miałoby nastąpić nałożenie się przepisów prawnych, pierwszeństwo w stosowaniu nadaje się zasadom Rozporządzenia DORA. W przedmiocie relacji z NIS2 w zakresie obowiązków podmiotów z sektora infrastruktury cyfrowej przepisy CER nie powinny wykra-

[25] N. Vandezande, op. cit., s. 3.

czać poza to, co zostało już wystarczająco unormowane w dyrektywie 2022/2557, jednakże w kwestiach związanych z jej ochroną fizyczną prymat obejmuje nowsza dyrektywa[26]. Trzy wyżej wymienione regulacje stanowią najistotniejsze źródła unijnych przepisów w obszarze cyberbezpieczeństwa dla podmiotów finansowych. Należy jednak podkreślić, że obie dyrektywy NIS2 i CER oczekują implementacji do krajowych porządków prawnych, a zasady Rozporządzenia DORA podlegają stosowaniu dopiero od 17 stycznia 2025 r.

4. Źródła *soft law* w obszarze zarządzania ryzykiem ICT

W obszarach, w których generalne podejście do cyberbezpieczeństwa jest niewystarczające bądź ramy prawne zawierają luki, rolę regulatora przejmują organy nadzorcze przy wykorzystaniu dotychczasowych lub udzielonych na poczet tej kwestii uprawnień. W takich przypadkach przedsiębrane środki wtórne, w większości w postaci wytycznych czy rekomendacji, dotyczą jedynie podmiotów nadzorowanych[27]. Nie tworzą nowych obowiązków normatywnych, a ich celem jest skonkretyzowanie i doprecyzowanie wymogów i zasad wynikających z obowiązujących już przepisów. Należy wskazać, że *soft law* w prawodawstwie unijnym w sferze finansów nadano szczególną rolę związaną z priorytetowym traktowaniem zunifikowanego stosowania prawa, zapewnienia stabilności systemu finansowego i ochrony uczestników jednolitego rynku[28]. Współtworzenie przez wytyczne, rekomendacje i normy *ius cogens* otoczenia prawnego instytucji finansowych stanowi zmianę po kryzysie finansowym *subprime* paradygmatu w polityce regulacyjnej Unii[29]. Na znaczenie sfery wykonawczej wskazuje choćby zobligowanie właściwych organów i podmiotów finansowych rozporządzeniem (UE) nr 1093/2010 w sprawie ustanowienia Europejskiego Urzędu Nadzoru do dołożenia należytej staranności w dostosowaniu się do wydanych przez odpowiednich unijnych nadzorców wytycznych i zaleceń[30].

Europejski Urząd Nadzoru Bankowego (dalej: EUNB) obejmuje swoim zakresem kompetencji instytucje kredytowe, instytucje płatnicze, firmy inwestycyjne i instytucje pieniądza elektronicznego. W obszarze bezpieczeństwa informacyjnego sektora finansowego Urząd opublikował wytyczne, *inter alia*, w sprawie zarządzania

[26] W. Szpringer, op. cit., s. 163–164.

[27] M.C. Malaguti, D. Delort, C. Lee, *Legal Framework for Cybersecurity in the Financial Sector: A Comparative Study on Existing Domestic or Regional Legislation on Cybersecurity*, Washington, DC 2022, s. 5.

[28] A. Nadolska, *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021, s. 8.

[29] Ibidem, s. 9.

[30] Europejski Urząd Nadzoru Bankowego, *Sprawozdanie końcowe na temat wytycznych w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT*, EBA/GL/2019/04, 28 listopada 2019 r., s. 3.

ryzykiem związanym z technologiami i bezpieczeństwem ICT, w sprawie outsourcingu i zgłaszania poważnych incydentów zgodnie z dyrektywą PSD2 oraz Regulacyjne Standardy Techniczne dotyczące silnego uwierzytelniania klienta i bezpiecznej komunikacji w zgodzie z tą dyrektywą. Dla instytucji kredytowych, instytucji płatniczych i firm inwestycyjnych najbardziej aktualny zbiór wytycznych w obszarze cyberbezpieczeństwa stanowią wytyczne EUNB dotyczące wymogów zarządzania ryzykiem i bezpieczeństwem ICT z dnia 28 listopada 2019 r. Dokument przewiduje wymogi w zakresie zarządzania i kontroli ryzyka ICT, a odpowiedzialność za realizację zadań w tym obszarze powierza niezależnej komórce ds. kontroli. Polityka zarządzania ryzykiem powinna uwzględniać apetyt na ryzyko, identyfikację, ocenę i narzędzia ograniczające ryzyko oraz procedury w zakresie monitorowania skuteczności środków kontroli[31].

Wobec podmiotów z rynku ubezpieczeń kompetencjami nadzorczymi dysponuje Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (dalej: EIOPA). EIOPA opublikował w lutym 2020 r. dokument „Strategy on Cyber Underwriting", w którym zidentyfikowano źródła ryzyka cybernetycznego oraz zaprojektowano odpowiednie metody i rozwiązania mające na celu minimalizację zagrożeń z cyberprzestrzeni dla unijnego rynku ubezpieczeń. Organ nadzorczy wydał w styczniu 2023 r. skierowane do krajowych nadzorców wytyczne w sprawie bezpieczeństwa technologii informacyjno-komunikacyjnych i ich administracji.

W obszarze zarządzania ryzykiem ICT i odporności cyfrowej szczególne kompetencje w zakresie raportowania, doradztwa i wsparcia instytucji unijnych w kreowaniu polityki wspólnotowej powierzono wspomnianej w dyskursie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (dalej: ENISA). Usługodawcy, w tym instytucje zaliczone normatywnie do kategorii podmiotów krytycznych, mają obowiązek zgłoszenia poważnych incydentów kompetentnym organom ze swojego państwa. ENISA agreguje przekazane z państw członkowskich dane oraz opracowuje, kategoryzuje i udostępnia ich zestawienia.

Do konsultacji skierowano w czerwcu 2023 r. pakiet projektów Regulacyjnych Standardów Technicznych zgodnych z DORA w zakresie dalszej harmonizacji ram zarządzania ryzykiem ICT, klasyfikacji incydentów i poważnych cyberzagrożeń oraz administrowania ryzyka związanego z korzystaniem z usług zewnętrznych dostawców technologii. Zbiór standardów realizują art. 15 i art. 16 ust. 3 DORA, dotyczące dalszego doprecyzowania przez nadzorców unijnego sektora finansowego w konsultacji z ENISA ram prawnych dla ryzyka związanego z operacyjną odpornością cyfrową podmiotu finansowego.

[31] Ibidem, s. 10.

Podsumowanie

Do 17 stycznia 2025 r. podmioty finansowe objęte zakresem stosowania DORA powinny przeprowadzić czynności dostosowawcze w zakresie polityki zarządzania ryzykiem ICT do nowych ram cyfrowej odporności operacyjnej. Do tego czasu instytucje finansowe powinny zachować zgodność z szeregiem przepisów, na czele z NIS2 i aktami wykonawczymi do tej dyrektywy, w zależności od przedmiotu działalności czy wykorzystywanych rozwiązań informatycznych. Uproszczeniu tego żmudnego i skomplikowanego procesu służą wydane w ostatnich latach wytyczne unijnych organów nadzoru doprecyzowujące obowiązki instytucji do charakteru aktywności na rynku finansowym i związanym z tym profilem ryzyka.

Zasady określone w rozporządzeniu 2022/2554 odzwierciedlają zaadaptowane już w innych dziedzinach prawa wspólnotowego podejście oparte na ryzyku, motywując podmioty finansowe i regulatorów krajowych do porzucenia dotychczasowego punktu koncentracji, jakim była zgodność z przepisami prawa[32]. Współzależności i powiązania krajowych rynków finansowych implikują konieczność scentralizowanych i odgórnych działań polegających na mitygacji zagrożeń pochodzących z cyberprzestrzeni. Ramy operacyjnej odporności cyfrowej instytucji z sektora finansowego zostały oparte na uznaniu systemowej natury cyberryzyka, o czym świadczą wielokrotne odwołania w motywach uchwalenia regulacji do ochrony stabilności finansowej sektora i jego zależności od ekosystemu cyfrowego. Potwierdza to również poświęcenie istotnej części rozporządzenia budowie spójnego i zharmonizowanego systemu nadzoru.

Zebranie zasad z ujednoliconą terminologią i szerokimi ramami zarządzania cyberryzykiem w jednym bezpośrednio stosowalnym akcie ustawodawczym z pewnością należy uznać za dobry krok w kierunku zwiększenia cyberbezpieczeństwa zdigitalizowanego jednolitego rynku finansowego. Silne zaangażowanie instytucji unijnych w tym obszarze, wykraczające poza dotychczasowy subsydiarny charakter, wpisuje się w realizację celów strategicznych UE w obszarze transformacji cyfrowej i dążenia Unii do harmonizacji praktyk stosowania prawa, co jest szczególnie istotne w transgranicznym świadczeniu usług finansowych.

BIBLIOGRAFIA

Banasiński, C. (red.). (2023). *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa.

Calliess, C., Baumgarten, A. (2020). *Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective*. „German Law Journal" 21(6): 1149–1179.

Cebula, J.J., Popeck, M.E., Young, L.R. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

[32] P.S. Krüger, J.P. Brauchle, op. cit., s. 5.

Krüger, P.S., Brauchle, J.-P. (2021). *The European Union, Cybersecurity, and the Financial Sector: A Primer*. Washington, DC.

Lichosik, A. (2023). *DORA jako prawny instrument ochrony cyfrowego bezpieczeństwa rynku finansowego*. „Studia Prawnoustrojowe" 62: 367–377.

Malaguti, M.C., Delort, D., Lee, C. (2022). *Legal Framework for Cybersecurity in the Financial Sector: A Comparative Study on Existing Domestic or Regional Legislation on Cybersecurity*. Washington, DC.

Markopoulou, D., Papakonstantinou, V., De Hert, P. (2019). *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*. „Computer Law & Security Review" 35(6): 1–19.

Nadolska, A. (2021). *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*. Warszawa.

Pavlidis, G. (2021). *Europe in the Digital Age: Regulating Digital Finance without Suffocating Innovation*. „Law, Innovation and Technology" 13(2): 464–477.

Szpringer, W. (2022). *Platformizacja gospodarki cyfrowej – nowe wyzwania dla regulacji*. Warszawa.

Vandezande, N. (2024). *Cybersecurity in the EU: How the NIS2-directive Stacks up against Its Predecessor*. „Computer Law & Security Review" 52: article 105890.