DOI: 10.31648/sp.9581

Anna Lichosik
Uniwersytet Śląski w Katowicach
ORCID: 0000-0002-6727-6648
anna.lichosik@us.edu.pl

DORA jako prawny instrument ochrony cyfrowego bezpieczeństwa rynku finansowego

Rewolucja cyfrowa jako przyczynek do zmian legislacyjnych – uwagi wprowadzające i kontekstowe

Przyszło nam żyć w erze cyfrowej. Nowe technologie stanowią pomost w zasadzie do nieograniczonych źródł informacji, nawiązywania nowych kontaktów, rozwoju nieosiągalnych wcześniej zasobów. Odległość geograficzna nie stanowi już żadnej przeszkody do zawierania transakcji handlowych z partnerami po drugiej stronie globu.

Rewolucja cyfrowa nazywana jest czwartą rewolucją przemysłową, w której to świat cyfrowy przenika się ze światem fizycznym[1]. Jako przykład zdumiewającego postępu teleinformatycznego można wskazać wręcz galopująco rozwijającą się sztuczną inteligencję, która nareszcie doczekała się uwagi i obecnie wręcz żywego zaiteresowania ustawodawcy unijego[2].

Zwiększony poziom cyfryzacji nie pozostaje jednak bez wpływu na stopień bezpieczństwa obrotu prawnego i gospodarczego oraz ochronę praw konsumentów[3].

---

[1] Zob. M. Xu, J.M. David, S.Hi., *The fourth industrial revolution: opportunities and challenges*, „International Journal of Financial Research" 2018, vol. 9, nr 2, s. 90–91, https://www.researchgate.net/publication/3236389 14_The_Fourth_Indu.

[2] Warto wskazać, że obecnie trwają intensywne prace nad uregulowaniem sztucznej inteligencji (AI). Już w kwietniu 2021 r. Komisja Europejska zaproponowała pierwsze unijne ramy legislacyjne dotyczące sztucznej inteligencji. Dokonano wówczas analizy i klasyfikacji systemów AI, które mogą być używane w różnych aplikacjach, według ryzyka, jakie stwarzają dla użytkowników. Wskazuje się, że priorytetem jest dopilnowanie, aby systemy sztucznej inteligencji stosowane w Unii Europejskiej były bezpieczne, przejrzyste, identyfikowalne, niedyskryminujące i przyjazne dla środowiska. Systemy sztucznej inteligencji powinny być nadzorowane przez ludzi, aby zapobiegać szkodliwym skutkom. Na temat regulacji dotyczącej sztucznej inteligencji w kontekście oczekiwań Parlamentu Europejskiego zob. https://www.europarl.europa.eu/news/pl/headlines/society/20201015STO89417/regulacje-ws-sztucznej-inteligencji-oczekiwania-parlamentu.

[3] W celu ochrony tych dóbr unijny prawodawca przewiduje wprowadzenie prawnych mechanizmów związanych z zapobieganiem nadużyciom w komunikacji elektronicznej oraz ich

Któż bowiem z nas nie napotkał (a co gorsza nie padł ofiarą) takich zjawisk, jak phishing[4], smishing[5] czy spoofing[6]. Przedsiębiorcy telekomunikacyjni oraz inni dostawcy usług stają obecnie przed ogromem wyzwań związanych z zapewnieniem bezpieczeństwa w komunikacji elektronicznej, a także zapobieganiu i zwalaczaniu coraz bardziej wysublimowanych nadużyć.

Powszechne wykorzystanie technologi informacyjnych stanowi obecnie nieodłączny element życia społecznego i gospodarczego. Coraz większy stopień cyfryzacji w zasadzie jest immanentnie wpisany w funkcjonowanie w szczególności sektora gospodarki, jakim jest rynek finansowy. Technologie informacyjno-komunikacyjne, poza korzyściami, jakie oferują, mogą jednak powodować także szereg cyberzagrożeń.

Technologie informacyjno-komunikacyjne (ang. *Information and Communication Technologies* – ICT) odgrywają zasadniczą rolę w sektorze finansów i mają podstawowe znaczenie dla realizacji bieżących zadań instytucji finansowych. Cyfryzacja obejmuje codzienne płatności (odchodzenie od systemu gotówkowego), rozliczanie i rozrachunek papierów wartościowych, handel elektroniczny oraz algorytmiczny czy finansowanie *peer to peer* z wykorzytaniem kryptoaktywów[7].

---

zwalczaniem. Przyjęta dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz. Urz. UE L 321 z 17.12.2018, s. 36, Dz. Urz. UE L 334 z 27.12.2019, s. 164 oraz Dz. Urz. UE L 419 z 11.12.2020, s. 36), która w 2023 r. zaimplementowana została w polskim akcie prawnym, tj. w ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. 1703), dalej jako u.z.n.k.e.

[4] Zgodnie z art. 3 ust. 1 pkt. 4 u.z.n.k.e. przez nieuprawnioną zmianę informacji adresowej (tzw. *phishing*) rozumie się niezgodne z prawem modyfikowanie informacji adresowej uniemożliwiające albo istotnie utrudniające ustalenie, przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu, informacji adresowej użytkownika wysyłającego komunikat.

[5] Zgodnie z art. 3 ust. 1 pkt. 2 u.z.n.k.e. przez *smishing* rozumie się wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania.

[6] Zgodnie z art. 3 ust. 1 pkt. 3 u.z.n.k.e. przez *CLI spoofing* (ang. *Caller ID Spoofing*) rozumie się nieuprawnione posłużenie się lub korzystanie przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służące podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu, poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego zachowania, zwłaszcza do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania.

[7] Co istotne, w tym obszarze ustawodawca dostrzega pilną potrzebę uściślenia regulacji prawnej. W dniu 29 czerwca 2023 r. weszło w życie 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 nr L 150/40 z 9.6.2023), ang. *Market in Crypto Assets Regulation*, dalej jako rozporządzenie MiCA. Rozporządzenie MiCA reguluje m.in. publiczne oferowanie, wydawanie

Nie może jednak umykać z pola widzenia fakt, że rosnąca cyfryzacja wzmacnia wzajemne połączenia i zależności w ramach sektora finansowego, w tym z zewnętrznymi dostawcami usług (zewnętrzną infrastrukturą). W tego rodzaju zależnościach upartuje się słabej strony o charakterze systemowym, gdzie mogą występować niekorzystne konsekwencje dla stabilności unijnego systemu finansowego jako całości i powodować utratę płynności oraz ogólną utratę pewności i zaufania do rynków finansowych.

Ryzyka związane z technologiami informacyjno-komunikacyjnymi niejako wymuszają potrzebę określenia zharmonizowanych standardów regulacyjnych również w zakresie wzmocnienia odporności cyfrowej systemów finansowych[8].

Bezpieczeństwo dotyczące technologi informacyjno-komunikacyjnych i odporność cyfrowa, jako element ryzyka operacyjnego, stały się obecnie wiodącym przedmiotem otoczenia regulacyjnego obejmującego wszystkie państwa członkowskie Unii Europejskiej. W harmonizacji przepisów obowiązujących w obszarze zarządzania ryzykiem dotyczącym technologi informacyjno-komunikacyjnych, ale także w zakresie udostępniania informacji, jak i operacyjnym testowaniu cyfrowych procesów oraz nadzoru nad kluczwymi zewnętrznymi dostawcami usług, upatruje się szansy na wzrost konkurencyjności w ramach jednolitego rynku wewnętrznego usług finansowych[9].

Dla regulacji powyższego wybrano formę prawną rozporządzenia, aby zapewnić skuteczne, bezpośrednio i w jednolity sposób stosowane przepisy prawa we wszystkich państwach członkowskich, z zachowaniem zasady proporcjonalności. W elemencie spójności upatruje się jednocześnie wartości przeciwdziałania cyfrowemu ryzyku operacyjnemu, co wpływa na ochronę stabilności systemu finansowego i wzmocnienie zaufania do jego uczestników.

Wobec powyższego w dniu 14 grudnia 2022 r. przyjęto rozporządzenie Parlamentu Europejskiego i Rady nr 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE)

---

i dopuszczanie do obrotu na platformach obrotu kryptoaktywów innych niż tokeny powiązane z aktywami i tokeny będące e-pieniądzem, tokenów powiązanych z aktywami (ART), tokenów pieniądza elektronicznego (EMT) i usługi związane z pośrednictwem na rynku kryptoaktywów. Zob. szerzej: T. Tomczak, *Ewolucja definicji kryptoaktywów w projekcie rozporządzenia MiCA*, „Przegląd Prawa Handlowego" 2023, nr 3; R. Bujalski, *UE reguluje rynki kryptoaktywów (MiCA)*, 2023, Lex; E. Mazurkiewicz, S. Jelonek, I. Sobieski, *Emisja tokenów i odpowiedzialność cywilna emitenta oraz członków jego organów w rozporządzeniu MICA ze szczególnym uwzględnieniem tokenów będących pieniądzem elektronicznym*, „Monitor Prawa Bankowego" 2023, nr 10; W. Srokosz, *Supervisory issues over blockchain-based activities*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Innovation in financial services. Balancing public and private interests*, London–New York 2021.

[8] Szerzej: M. Mariański, *Problematyka regulacji rynku finansowego w ujęciu transgranicznym. Analiza na przykładzie prawa polskiego i prawa francuskiego*, Olsztyn 2020.

[9] Zob. M. Fedorowicz, *Osiąganie konwergencji nadzorczej mikroostrożnościowej i makroostrożnościowej w prawie rynku finansowego Unii Europejskiej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2018, nr 4.

nr 1060/2009, (UE) nr 648/2012, (UE) 600/2014 oraz (UE) nr 909/2014[10], które ma na celu dokonanie konsolidacji i aktualizacji przepisów w zakresie zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi, udostępniania informacji, testowania oraz monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT[11].

Zgodnie z art. 3 pkt. 1 rozporządzenia DORA (ang. *Digital Operational Resilience Act*) przez cyfrową odporność operacyjną rozumie się zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej integralności operacyjnej z technologicznego punktu widzenia przez zapewnianie, bezpośrednio albo pośrednio (korzystając z usług zewnętrznych dostawców usług ICT), pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość, w tym w trakcie zakłóceń.

Stąd też podmioty objęte zakresem rozporządzenia DORA będą zobowiązane do systematycznego kontrolowania stosowanych narzędzi teleinformatycznych oraz identyfikowania źródeł cyberzagrożeń. Natomiast wprowadzenie ujednoliconych norm w tym zakresie w założeniu powinno zagwarantować powstanie powszechnej cyfrowej odporności operacyjnej w całym unijnym systemie finansowym.

Przyjmując powyższy akt prawny, podnoszono konieczność zachowania zasady pomocniczności oraz proporcjonalności, upartując potrzebę harmonizacji w dysproporcjach poszczególnych systemów regulacji państw członkowskich, które częstokroć pokrywają jedynie część wymogów mających zastosowanie do podmiotów finansowych, które np. prowadzą działalność transgraniczną lub posiadają więcej niż jedno zezwolenie na prowadzenie działalności na rynku finansowym.

W odniesieniu do zachowania zasady proporcjonalności wnioskodawcy wprowadzenia jednolitej regulacji klarownie wskazują: „Proponowane przepisy nie wykraczają poza to, co jest konieczne do osiągnięcia celów wniosku. Obejmują one jedynie te aspekty, których państwa członkowskie nie mogą osiągnąć samodzielnie i w których obciążenia i koszty administracyjne są współmierne do celów szczególnych i ogólnych, które mają zostać osiągnięte”[12].

---

[10] Dz.Urz. UE nr L 333/1 z 27.12.2022, dalej jako rozporządzenie DORA.

[11] Ogłoszenie projektu rozporządzenia DORA miało miejsce jeszcze we wrześniu 2020 roku, kiedy to Komisja Europejska dnia 24 września 2020 r. przedstawiła wniosek dotyczący przyjęcia przez Parlament Europejski i Radę rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego. Prace nad rozporządzeniem trwały do 28 listopada 2022 r., gdy Rada Unii Europejskiej przyjęła projekt rozporządzenia DORA. Rozporządzenie zawiera 24-miesięczne *vacatio legis*, stąd też zacznie obowiązywać od 17 stycznia 2025 r.

[12] Uzasadnienie wniosku Komisji Europejskiej z dnia 24 września 2020 r. dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE)

Opracowaniu regulacji przyświecała intencja zapewnienia, aby nowe przepisy obejmujące wszystkich profesjonalnych uczestników rynku finansowego jednocześnie były dostosowane do ryzyka i potrzeb z uwzględnieniem ich rozmiaru oraz przedmiotu prowadzonej działalności.

Zakres podmiotowy rozporządzenia DORA

Rozporządzenie DORA swoim zakresem obejmuje takie podmioty finansowe, jak: instytucje kredytowe, instytucje płatnicze, instytucje pieniądza elektronicznego, firmy inwestycyjne, dostawców usług w zakresie kryptoaktywów[13], centralne depozyty papierów wartościowych, kontrahentów centralnych, systemy obrotu, repozytoria transakcji, zarządzających alternatywnymi funduszami inwestycyjnymi i spółki zarządzające, dostawców usług w zakresie udostępniania informacji, zakłady ubezpieczeń i zakłady reasekuracji, pośredników ubezpieczeniowych, instytucje pracowniczych programów emerytalnych, agencje ratingowe, biegłych rewidentów i firmy audytorskie, administratorów kluczowych wskaźników referencyjnych i dostawców usług finansowania społecznościowego.

W ocenie prawodawcy tak szeroki zakres pozwoli na jednolite i spójne stosowanie wszystkich elementów zarządzania ryzykiem w obszarach związanych z technologiami informacyjno-komunikacyjnymi – to wszystko przy uwzględnieniu rozmiaru podmiotów finansowych, ich różnego profilu działalności oraz faktu, że większe podmioty finansowe z reguły posiadają większe zasoby. Z tego względu podmioty niebędące mikroprzedsiębiorcami będą miały obowiązek wdrożenia złożonych zasad zarządzania, ustanowienia specjalnych stanowisk kierowniczych, przeprowadzania cyklicznych analiz ryzyka i testowania ciągłości działania oraz planów reagowania i przywrócenia gotowości do pracy przy uwzględnieniu scenariuszy pracy awaryjnej, a niektóre z nich będą obowiązane do przeprowadzania specjalistycznych testów penetracyjnych w obszarze wyszukiwania zagrożeń[14].

---

nr 600/2014 oraz (UE) nr 909/2014, s. 4, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020PC0595. Por. P. Izdebski, *Akty prawa miękkiego jako współczesny instrument nadzoru nad rynkiem finansowym – rola oraz charakter prawny. Część 1*, „Przegląd Prawa Publicznego" 2021, nr 3; A. Nadolska, *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021.

[13] Zob. szerzej: M. Mariański, *Problematyka kwalifikacji prawnej wirtualnej waluty we Francji*, „Państwo i Prawo" 2015, nr 10; W. Srokosz, *Publicznoprawne ograniczenia kryptowalut*, [w:] E. Ura, E. Feret, S. Pieprzny (red.), *Jednostka wobec działań administracji publicznej*, Rzeszów 2016; W. Srokosz, *Prawna regulacja kryptoaktywów, tokenów płatniczych oraz pieniądza elektronicznego w UE*, „Monitor Prawa Bankowego" 2021, nr 9.

[14] Zgodnie z art. 3 pkt 17 rozporządzenia DORA testy penetracyjne pod kątem wyszukiwania zagrożeń (TLPT) oznaczają ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które

Mimo szerokiego zakresu podmiotowego rozporządzenia DORA nie obejmuje ono wszystkich podmiotów czynnie uczestniczących w procesach unijnego rynku finansowego. Jak wskazano w uzasadnieniu wniosku w sprawie przyjęcia rozporządzenia, nie obejmuje ono operatorów systemów zdefiniowanych w art. 2 lit. p dyrektywy 98/26/WE Parlamentu Europejskiego i Rady z dnia 19 maja 1998 r. w sprawie zamknięcia rozliczeń w systemach płatności i rozrachunku papierów wartościowych[15] (tzw. dyrektywy o ostateczności rozrachunku), jak i uczestników systemu, poza przypadkiem gdy taki uczestnik sam jest podmiotem finansowym regulowanym na szczeblu unijnym i jako taki będzie objęty zakresem rozporządzenia DORA we własnym imieniu (tj. instytucja kredytowa, firma inwestycyjna, kontrahent centralny). Ponadto rozporzadzenie DORA nie obejmie swym zakresem unijnego rejestru uprawnień do emisji, który funkcjonuje – zgodnie z dyrektywą 2003/87/WE Parlamentu Europejskiego i Rady z dnia 13 października 2003 r. ustanawiającą system handlu przydziałami emisji gazów cieplarnianych we Wspólnocie oraz zmieniającą dyrektywę Rady 96/61/WE[16].

Jednocześnie w tym zakresie dostrzega się konieczność dalszego przeglądu zagadnień prawnych i politycznych związanych z operatorami i uczestnikami systemów, o jakich mowa w dyrektywie 98/26/WE w sprawie zamknięcia rozliczeń w systemach płatności i rozrachunku papierów wartościowych. Komisja Europejska będzie także na bieżąco oceniać konieczność i wpływ dalszego rozszerzenia zakresu rozporządzenia DORA na podmioty i infrastruktury technologi informacyjno-komunikacyjnych wykraczających obecnie poza jego zakres.

Cele i wyzwania jakie stawia przed rynkiem finansowym rozporządzenie DORA

Rozporządzenie DORA ustanawia jednolite wymogi w zakresie bezpieczeństwa sieci i systemów informatycznych przedsiębiorców działających w unijnym sektorze finansowym, jak i kluczowych zewnętrznych dostawców usług związanych z technologiami informacyjno-komunikacyjnymi. Podmioty objęte zakresem rozporządzenia DORA mają obowiązek zapewnić warunki techniczne i organizacyjne pozwalające wytrzymać różnego rodzaju zakłócenia i zagrożenia związane z technologiami informacyjno-komunikacyjnymi[17].

zapewniają kontrolowane, dostosowane do konkretnych zagrożeń, oparte na analizie zagrożeń (*red team*) testy działających na bieżąco krytycznych systemów produkcji podmiotu finansowego.

[15] Dz.U.UE.L.166 z 11.6.1998, s. 45.

[16] Dz.U.UE.L.275 z 25.10.2003, s. 32.

[17] Zob. R. Bujalski, *Operacyjna odporność cyfrowa sektora finansowego (DORA)*, 2023, Lex.

Rozporządzenie DORA jest częścią szerszego pakietu regulacyjnego w zakresie finansów cyfrowych na szczeblu europejskim, gdzie szczególną wartość upatruje się w dbaniu o innowacyjność i konkurencyjność rozwoju technologicznego, przy jednoczesnym zapewnieniu stabilności finansowej i ochrony konsumentów.

Z technologiami informacyjno-komunikacyjnymi wiążą się zarówno szanse, jak i zagrożenia. Dlatego też ustawodawca unijny, dostrzegając potencjał szans, stara się wprowadzić mechanizmy mitygujące ryzyka i minimalizujące szkodliwe zdarzenia. W tym celu projektuje się ramy prawne zwiększające odporność cyfrową przedsiębiorców finansowych.

Rozporządzenie DORA stawia przed przedsiębiorcami finansowymi wyzwania w charakterze makro i mikro skali. Będą to zarówno wymagania w zakresie efektywnego dostosowania strategii biznesowych, jak i odpowiedniego modelowania procesu zarządzania ryzykiem operacyjnym związanym z technologiami komunikacyjno-informacyjnymi. Identyfikacja, ochrona i zapobieganie, ale także wykrywanie, reagowanie i przywrócenie integralności i bezpieczeństwa sieci i systemów informatycznych, zapewnienie poufności danych, jak i rozwój oraz komunikacja stanowią obecnie wiodące zadania stawiane przed przedsiębiorcami finansowymi[18]. Stworzenie systemowej operacyjne odporności cyfrowej w skali unijnej wymaga utworzenia i utrzymywania odpornych systemów i narzędzi technologii komunikacyjno-informacyjnych. Od podmiotów finansowych wymaga to ciągłego identyfikowania źródeł ryzyk związanych z technologiami cyfrowymi oraz tworzenia środków ochrony i mechanizmów szybkiego wykrywania nietypowych zdarzeń. Dążenie do systemowej odporności operacyjnej wiąże się z dostosowaniem strategii utrzymania ciągłości działania podmiotów oraz planów przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej do nowych, nadzwyczajnych realiów.

W przypadku zagrożenia podmiotów finansowych cyberatakami szczególnego znaczenia nabiera, z jednej strony, ograniczenie potencjnych szkód, z drugiej zaś – niezwłoczne i bezpieczne przywrócenie gotowości do działania. Rozporządzenie DORA nie wskazuje na konkretne standardy w tej kwestii, ale w swym holistycznym podejściu bazuje na europejskich i międzynarodowych uznanych standardach technicznych, jak i dotychczasowych praktykach rynkowych.

Do innych wymogów przewidzianych dla podmiotów finansowych należy zaliczyć obowiązek ustanowienia i wdrożenia procesu monitorowania i rejestrowania incydentów związanych z technologiami komunikacyjno-informacyjnymi, a także konieczności klasyfikowania ich w oparciu o kryteria szczegółowo wskazane w rozporządzeniu, celem określenia progów istotności.

---

[18] Uzasadnienie wniosku Komisji Europejskiej..., s. 11.

Przedsiębiorcy finansowi mają obowiązek zgłaszania właściwym organom poważnych incydentów związanych z technologiami komunikacyjno-informacyjnymi. Co więcej, podmioty finansowe powinny informować swoich klientów o danym zdarzeniu, jeżeli ma ono lub może mieć wpływ na ich sytuację finansową.

Kolejnym istotnym, acz częstokoroć niedocenianym wymogiem dla przedsiębiorców finansowych jest proces testowania operacyjnej odporności cyfrowej. Okresowe testy w zakresie gotowości i wykrywania podatności wrażliwych na ataki oraz niezwłoczne wdrażanie działań naprawczych stanowią nieodłączny element zarządzania ryzykiem. Harmonizacja działań na szczeblu unijnym powinna pomóc zlikwidować niejednolite podejścia do testowania, które występują w różnych państwch członkowskich[19].

Rozporządzenie DORA w stosowaniu wymogów w zakresie testowania operacyjnej odporności cyfrowej zważa na zasadę proporcjonalności, z uwzględnieniem rozmiaru, profilu działalności i profilu ryzyka podmiotów finansowych. Jednocześnie zakłada się, że wszyscy przedsiębiorcy finansowi powinni przeprowadzać testy narzędzi i systemów technologi komunikacyjno-informacyjnych, a część podmiotów, które zostały uznane za istotne i dojrzałe pod względem cyfrowym, będą miały obowiązek przeprowadzania zaawansowanych testów na podstawie testów penetracyjnych wykorzystujących scenariusz zagrożenia[20].

Przepisy rozporządzenia DORA przewidują także mechanizmy monitorowania ryzyk związanych z zewnętrznymi dostawcami usług technologi komunikacyjno-informacyjnych, m.in. poprzez harmonizację wymogów relacji kontraktowych, które powinny zawierać pełny opis usług wraz ze wskazaniem lokalizacji, w których mają być przetwarzane dane. Stosowne postanowienia w sprawie dostępności, integralności, bezpieczeństwa i ochrony danych osobowych oraz gwarancje dostępu i odzyskiwania danych w przypadku awarii zewnętrznych dostawców usług, a także kwestie kontroli i audytu oraz przejrzyste prawa do odstąpienia od umowy, w tym specjalne strategie wyjścia, również nie były obce twórcom rozporządzenia DORA.

Przestrzeganie regulacji wprowadzających konieczność monitorowania przez przedsiębiorców finansowych ryzyk związanych z technologiami komunikacyjno-informacyjnymi w założeniu powinno przyczynić się do zwiększenia odporności cyfrowej uczestników rynku finansowego.

---

[19] Por. M. Lemonnier, *Rola badań porównawczych i interdyscyplinarnych w kwestiach rynku i nadzoru finansowego*, [w:] A Jurkowska-Zeidler, M. Olszak (red.), *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Warszawa 2015.

[20] Uzasadnienie wniosku Komisji Europejskiej…, s. 12.

Uwagi podsumowujące

W przyjęciu rozporządzenia DORA upatruje się narzędzia, które może znacząco wzmocnić bezpieczeństwo w cyfrowym sektorze finansowym Unii Europejskiej. Przepisy rozporządzenia w założeniu powinny uprościć legislacyjną stronę finansów cyfrowych, a jednocześnie przyczynić się do zwiększenia pewności prawa, powiązanej ze wsparciem dla spójności w zakresie nadzoru. Ustanowienie wspólnych ram operacyjnej odporności cyfrowej podmiotów finansowych na poziomie Unii Europejskiej powinno pozwolić efektywnie zarządzać ryzykiem związanym z technologiami informacyjno-komunikacyjnymi oraz intensywnie reagować na cyberzagrożenia.

Wyzwania stawiane przed podmiotami, które wykorzystują cyberprzestrzeń do świadczenia usług finansowych z pewnością obciążą je nowymi obowiązkami związanymi z koniecznością identyfikacji zagrożeń płynących z cyberprzestrzeni. Intensyfikacji muszą bowiem podlegać kwestie zapewnienia integralności, bezpieczeństwa i odporności infrastruktur fizycznych i urządzeń, które wspierają wykorzystywanie technologi komunikacyjno-informacyjnych.

Mimo wielu wyzwań stawianych uczestnikom unijnego rynku finansowego, trzeba zaznaczyć, że działania te są konieczne dla stworzenia bezpiecznej przestrzeni do rozwoju cyfrowych usług finansowych, a jednocześnie zaprojektowane z uwzględnieniem zasady proporcjonalności w zakresie wielkości tych podmiotów i zakresu prowadzonej przez nich działalności. Ustawodawca unijny dostrzega bowiem ryzyka mogące wiązać się z nadmiernym stopniem reżimu legislacyjnego, a w efekcie podemuje próbę wyważenia zakresu i skali nowych obowiązków, tak aby zarówno wzmacniać oraz rozwijać rynek finansowy, a także stwarzać odpowiednie warunki konkurencji.

Wykaz literatury

Bujalski R., *Operacyjna odporność cyfrowa sektora finansowego (DORA)*, 2023, Lex.

Bujalski R., *UE reguluje rynki kryptoaktywów (MiCA)*, 2023, Lex.

Fedorowicz M., *Osiąganie konwergencji nadzorczej mikroostrożnościowej i makroostrożnościowej w prawie rynku finansowego Unii Europejskiej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2018, nr 4.

Izdebski P., *Akty prawa miękkiego jako współczesny instrument nadzoru nad rynkiem finansowym – rola oraz charakter prawny. Część 1*, „Przegląd Prawa Publicznego" 2012, nr 3.

Lemonnier M., *Rola badań porównawczych i interdyscyplinarnych w kwestiach rynku i nadzoru finansowego*, [w:] A Jurkowska-Zeidler, M. Olszak, (red.), *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Wolters Kluwer, Warszawa 2015.

Mariański M., *Problematyka kwalifikacji prawnej wirtualnej waluty we Francji*, „Państwo i Prawo" 2015, nr 10.
Mariański M., *Problematyka regulacji rynku finansowego w ujęciu transgranicznym. Analiza na przykładzie prawa polskiego i prawa francuskiego*, Wyd. UWM, Olsztyn 2020.
Mazurkiewicz E., Jelonek S., Sobieski I., *Emisja tokenów i odpowiedzialność cywilna emitenta oraz członków jego organów w rozporządzeniu MICA ze szczególnym uwzględnieniem tokenów będących pieniądzem elektronicznym*, „Monitor Prawa Bankowego" 2023, nr 10.
Nadolska A., *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, C.H. Beck, Warszawa 2021.
Srokosz W., *Publicznoprawne ograniczenia kryptowalut*, [w:] E. Ura, E. Feret, S. Pieprzny (red.), *Jednostka wobec działań administracji publicznej*, RS Druk, Rzeszów 2016.
Srokosz W., *Prawna regulacja kryptoaktywów, tokenów płatniczych oraz pieniądza elektronicznego w UE*, „Monitor Prawa Bankowego" 2021, nr 9.
Srokosz W., *Supervisory issues over blockchain-based activities*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Innovation in financial services. Balancing public and private interests*, Routledge, London–New York 2021.
Tomczak T., *Ewolucja definicji kryptoaktywów w projekcie rozporządzenia MiCA*, „Przegląd Prawa Handlowego" 2023, nr 3.
Xu M., David J.M., Hi S., *The fourth industrial revolution: opportunities and challenges*, „International Journal of Financial Research" 2018, vol. 9, nr 2, https://www.researchgate.net/publication/3236389 14_The_Fourth_Indu.

Summary

DORA as a legal instrument for protecting the digital security of the financial market

Keywords: law, DORA, ICT, financial market, IT.

The article aims to present the extremely current issue of the development of the digital financial market, which, using information and communication technologies, offers many benefits but may also be exposed to burdensome cyber threats. The EU legislator decided to introduce the DORA (Digital Operational Resilience Act) regulation, which it sees as a tool that can significantly strengthen security in the digitized financial sector of the European Union. The provisions of the regulation should simplify the legislative side of digital finance and at the same time contribute to increasing legal certainty, combined with support for supervisory consistency. Despite the many challenges faced by the participants of the EU financial market, it is worth emphasizing that these activities are necessary to create a safe space for the development of digital financial services, and at the same time, they should be shaped taking

into account the principles of proportionality and subsidiarity. The challenges faced by entities that use cyberspace to provide financial services will certainly burden them with new obligations, but the risks related to information and communication technologies somehow enforce the need to define harmonized regulatory standards in terms of strengthening the digital resilience of financial systems.