Obowiązek zapewnienia cyberbezpieczeństwa w obrocie kryptoaktywami


*Artur Piechocki**

*Katarzyna Gorzkowska***

Niniejszy artykuł omawia nowe regulacje prawne dla branży kryptoaktywów, które zostały zaproponowane przez Komisję Europejską. Pomimo, że nad przepisami prowadzone są jeszcze prace legislacyjne, projektowane rozwiązania znacznie wpłyną na emisję i obrót wirtualnymi walutami. Szczególne znaczenie będzie miało objęcie branży obowiązkami z zakresu cyberbezpieczeństwa.

Wprowadzenie

W dniu 24.9.2020 r. Komisja Europejska zaprezentowała projekt rozporządzenia w sprawie rynków kryptoaktywów[1] (w skrócie: MICA). MICA, wraz z projektem rozporządzenia pilotażowego DLT[2], składa się na część pakietu przepisów, które z założenia mają uporządkować działalność w obszarze finansów cyfrowych. Zaproponowane regulacje dotyczą zarówno procesu emisji tzw. walut wirtualnych, jak również obrotu kryptoaktywami. Warto wskazać, że zgodnie z projektem rozporządzenia MICA przez „kryptoaktywa" należy rozumieć cyfrowe odzwierciedlenie wartości lub praw, nadających się do przenoszenia i przechowywania w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii[3].

Zaproponowane przepisy stanowią próbę kompleksowej regulacji obszaru cieszących się dużym zainteresowaniem kryptoaktywów, w tym walut wirtualnych. Pomimo znacznej popularności, branża ta do dzisiaj nie doczekała się jednolitych ram prawnych. Nowe rozwiązania z założenia zostały przygotowane z myślą o stworzeniu warunków umożliwiających bezpieczne wykorzystanie potencjału, jaki posiadają cyfrowe finanse oraz wspieranie rozwoju branży finansowej w zakresie jej innowacyjności i konkurencyjności. Projektowane przepisy mają na celu ograniczenie ryzyka związanego z korzystaniem z cyfrowych finansów.

Zgodnie z przyjętymi założeniami ochroną mają zostać objęci użytkownicy kryptoaktywów, w szczególności konsumenci, którzy zazwyczaj nie posiadają odpowiedniej wiedzy na temat ryzyka związanego z nabyciem kryptoaktywów i nie są świadomi niebezpieczeństw związanych z inwestowaniem w produkty oparte na DLT[4]. Przy czym, brak odpowiedniego poziomu świadomości dotyczy zwłaszcza niebezpieczeństw wynikających z zagrożeń w postaci ataków hackerskich, czy działania złośliwego oprogramowania. W tym miejscu należy zaznaczyć, że jedną z głównych przyczyn utraty środków inwestorów stanowią ataki wymierzone w giełdy i portfele kryptoaktywów. W związku z powyższym, projekt rozporządzenia MICA przewiduje liczne obowiązki dla podmiotów uczestniczących w obrocie kryptoaktywami. Do obowiązków należy m.in. zapewnienie cyberbezpieczeństwa w procesie świadczenia usług.

Aktualna sytuacja i zagrożenia cybernetyczne

Obecnie brakuje przepisów, które nakładałyby na podmioty uczestniczące w obrocie kryptoaktywami szczególne wymagania w zakresie zapewnienia cyberbezpieczeństwa. Aktualnie obszar kryptowalut objęty jest zazwyczaj wymaganiami dotyczącymi przeciwdziałania praniu pieniędzy. Ze względu na brak regulacji, nierzadko mają miejsce sytuacje utraty środków inwestorów, w wyniku umyślnych działań osób trzecich. Środki przechowywane na tzw. giełdach (tzn. platforma internetowa przeznaczona do transakcji kryptowalutami) stawały się celem bezpośrednich ataków hackerów, podobnie jak oprogramowanie używane do „przechowywania" kryptowalut (tzw. *wallet*/portfel). Jako przykłady głośnych spraw można wskazać atak na japońską giełdę Mt. Gox[5], w następstwie którego doszło do uchwalenia regulacji dla giełd kryptowalut działających w Japonii, czy niedawne ataki na inne japońskie giełdy, takie jak Zaif[6], Coincheck[7] czy Liquid[8]. Aktualnie działalność japońskich giełd podlega regulacjom,

* Autor jest radcą prawnym, założycielem i partnerem zarządzającym kancelarii APLAW Artur Piechocki.

** Autorka jest prawnikiem w kancelarii APLAW Artur Piechocki; ORCID: 0000-0001-5408-6530.

[1] Projekt rozporządzenia w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0593 (dostęp: 5.2.2022 r.); dalej jako: projekt rozporządzenie MICA.

[2] Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020PC0594&from=EN (dostęp: 19.2.2022 r.).

[3] Art. 3 ust. 1 pkt 2 projektu rozporządzenia MICA.

[4] Motyw 3 projektu rozporządzenia MICA.

[5] Atak na japońską giełdę Mt. Gox uznawany jest za największą kradzież kryptowaluty w historii. Źródła podają, że doszło do kradzieży ok 5% światowych zasobów wirtualnej „monety", https://businessinsider.com.pl/gielda/kryptowaluty/najwieksza-kradziez-kryptowaluty-w-historii/q1k8fmn (dostęp: 8.1.2022 r.).

[6] Źródło: https://comparic.pl/kolejna-japonska-krypto-gielda-zhackowana-skradziono-60-mln/ (dostęp: 8.1.2022 r.).

[7] Źródło: https://gieldykryptowalut.pl/japonska-gielda-kryptowalut-coincheck-zhakowana/ (dostęp: 8.1.2022 r.).

[8] Źródło: https://exeria.com/pl/japonska-gielda-liquid-zhakowana-haker-posiada-74-miliony-dolarow-w-kryptowalutach/ (dostęp: 8.1.2022 r.).

w tym w zakresie cyberbezpieczeństwa, co nie daje jednak gwarancji zapewnienia bezpieczeństwa środkom inwestorów. Incydenty nie dotyczą jednak wyłącznie japońskiego rynku, ataki wymierzone są również w podmioty prowadzące działalność w Europie i Ameryce[9]. Incydentom często towarzyszą podejrzenia kierowane wobec osób zaangażowanych w prace nad danym projektem.

Ryzyka związane z nowymi technologiami wciąż stanowią wyzwanie dla odporności operacyjnej, wydajności i stabilności unijnego systemu finansowego. Dlatego decydenci i organy nadzoru zwracają coraz większą uwagę na zagrożenia wynikające z uzależnienia od technologii informacyjnych i komunikacyjnych (ang. *Information and Communication Technologies*, w skrócie: ICT). W przypadku branży kryptoaktywów, próby objęcia uczestników obrotu obowiązkami z zakresu zapewnienia cyberbezpieczeństwa należy ocenić jako słuszne, zważywszy na wspomniane wcześniej liczne incydenty, jak również problemy z przypisaniem odpowiedzialności. W szczególności trudności dotyczą ustalenia odpowiedzialności osób zarządzających. Tymczasem projektowane regulacje w obszarze rynków finansowych skupiają się na odpowiedzialności organów zarządzających danym podmiotem za zapewnienie cyberbezpieczeństwa. Przepisy procedowanego rozporządzenia ICT skupiają się na tym, aby na organie zarządzającym spoczywał obowiązek utrzymania aktywnej roli w zarządzaniu ryzykiem związanym z ICT, jak również odpowiedniej higieny cyberbezpieczeństwa.

Obowiązki podmiotów uczestniczących w obrocie kryptoaktywami

Wejście w życie rozporządzenia MICA spowoduje objęcie podmiotów prowadzących działalność w obszarze kryptoaktywów licznymi obowiązkami. Regulacjom będzie podlegała m.in. działalność polegająca na dostarczaniu usług w zakresie kryptoaktywów. Prowadzenie tego typu aktywności będzie wymagało uprzedniego uzyskania zezwolenia.

Zgodnie z treścią projektowanego art. 3 ust. 1 pkt 8, przez **dostawcę usług w zakresie kryptoaktywów** należy rozumieć każdą osobę, której działalność zawodowa lub działalność gospodarcza polega na profesjonalnym świadczeniu na rzecz osób trzecich, co najmniej jednej usługi w zakresie kryptoaktywów. Chodzi zatem o jakąkolwiek usługę lub działalność związaną z kryptoaktywami spośród działalności zawartych w katalogu. Do rodzaju takich działalności zostały zaliczone przechowywanie kryptoaktywów i zarządzanie nimi w imieniu osób trzecich, prowadzenie platformy obrotu kryptoaktywami, wymiana kryptoaktywów na walutę fiat będącą prawnym środkiem płatniczym, wymiana kryptoaktywów na inne kryptoaktywa, wykonywanie zleceń związanych z kryptoaktywami w imieniu osób trzecich, subemisja kryptoaktywów, przyjmowanie i przekazywanie zleceń związanych z kryptoaktywami w imieniu osób trzecich, doradztwo w zakresie kryptoaktywów. Przez **przechowywanie i zarządzanie kryptoaktywami** w imieniu osób trzecich należy rozumieć przechowywanie kryptoaktywów lub środków dostępu do takich kryptoaktywów, w stosownych przypadkach, w postaci prywatnych kluczy kryptograficznych, lub sprawowanie nad nimi kontroli w imieniu osób trzecich. Osobną grupę, również objętą regulacjami, będą stanowili emitenci kryptoaktywów, których podział został dokonany ze względu na rodzaj emitowanego kryptoaktywa.

Jak zostało wspomniane, rozporządzenie MICA przewiduje szereg **obowiązków, jakim będą musiały sprostać określone podmioty uczestniczące w obrocie kryptoaktywami**. Przykładowo, do obowiązków dostawcy usług w zakresie kryptoaktywów, będzie należało zawarcie umowy z klientami w celu określenia obowiązków i zakresu odpowiedzialności. Katalog minimalnych wymagań co do treści umowy został zawarty w art. 67 projektu rozporządzenia MICA. Umowa powinna zawierać co najmniej następujące elementy[10]: określenie tożsamości stron umowy, charakteru świadczonej usługi wraz z opisem usługi, określenie środków komunikacji między dostawcą usług w zakresie kryptoaktywów a klientem, w tym system uwierzytelniania klienta; ponadto opis systemów bezpieczeństwa stosowanych przez dostawcę usług oraz opłaty pobierane przez dostawcę usług, jak również prawo właściwe dla umowy. Wymagania w zakresie uwierzytelnienia klienta i systemów niewątpliwie przełożą się na zwiększenie bezpieczeństwa transakcji.

Projekt rozporządzenia MICA wyróżnia kategorię **dostawców usług w zakresie kryptoaktywów, którzy posiadają zezwolenie na przechowywanie kryptoaktywów i zarządzanie nimi w imieniu osób trzecich**. Rozporządzenie zastrzega, że ta grupa podmiotów będzie obowiązana do ustanawiania polityki w zakresie przechowywania kryptoaktywów wraz z wewnętrznymi zasadami i procedurami w celu zapewnienia przechowywania lub kontroli takich kryptoaktywów lub środków dostępu do nich, takich jak klucze kryptograficzne. Wdrożenie procedur będzie miało na celu zabezpieczenie przed utratą przez dostawcę kryptoaktywów klientów, czy praw związanych z tymi aktywami z powodu oszustw, zagrożeń dla cyberbezpieczeństwa lub zaniedbań. Zatem widoczne jest skupienie uwagi na kwestii zapewnienia bezpieczeństwa zarówno ICT, jak również odpowiednich środków organizacyjnych i technicznych.

Podobnie sytuacja będzie wyglądała w przypadku **podmiotów prowadzących platformy obrotu**. Przy czym warto zauważyć, że tego rodzaju działalność również będzie wymagała uzyskania stosownego zezwolenia na jej prowadzenie. Do obowiązków operatorów platform będzie należało posiadanie skutecznych systemów, procedur i mechanizmów zapewniających odporność ich systemów obrotu. Ponadto taki podmiot będzie musiał wykazać, że jego systemy zostały kompleksowo przetestowane w celu zapewnienia spełnienia warunków oraz zapewniają ciągłość działania w celu zapewnienia ciągłości ich usług w przypadku jakiejkolwiek awarii systemu obrotu[11].

Podobne obowiązki, według projektu, mają zostać nałożone na **emitentów tokenów powiązanych z aktywami**[12]. Ta katego-

[9] Jako przykłady można wskazać ataki z 2019 r. na giełdy: Binance, Bithumb, https://bithub.pl/wiadomosci/najwieksze-ataki-hakerskie-na-gieldy-kryptowalut-w-2019-roku/ (dostęp: 8.1.2022 r.).

[10] Art. 67 projektu rozporządzenia MICA.

[11] Art. 68 projektu rozporządzenia MICA.

[12] Art. 16 i n. projektu rozporządzenia MICA.