

Analiza krytyczna efektywności unijnych sankcji finansowych zastosowanych wobec Federacji Rosyjskiej

Critical analysis of the effectiveness of EU financial sanctions against the Russian Federation

ANGELA PACHOLCZAK

Autorka niezależna

 <https://orcid.org/0009-0000-4670-2364>

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 97–129

 CC BY-NC-SA 4.0

<https://doi.org/10.4467/20801335PBW.24.004.19606>

ARTYKUŁ

Abstrakt

Artykuł jest poświęcony problematyce międzynarodowych sankcji finansowych w kontekście wyzwań, jakie stawia dla ich skuteczności rynek kryptowalutowy. Punktem odniesienia dla tej analizy są sankcje nałożone przez Radę Unii Europejskiej (wspierane zastosowaniem komplementarnych sankcji przez część społeczności międzynarodowej) na Federację Rosyjską w związku z jej agresją na Ukrainę. Celem artykułu jest ukazanie różnych płaszczyzn oceny skuteczności sankcji, a zwłaszcza wskazanie przyczyn, dla których w większości wypadków, pomimo osłabiania potencjału gospodarczego sankcjonowanego kraju, nie realizują one pierwotnego celu ich nałożenia, czyli powstrzymania działań militarnych. W tym przedmiocie osią zainteresowania jest aktualny oraz perspektywny wpływ rozwiązań finansowych opartych na technologii blockchain na tworzenie istotnej luki w systemie sankcyjnym, która pozwala eliminować lub marginalizować skutki międzynarodowych sankcji finansowych. To zagadnienie jest oceniane także przez pryzmat aktualnie wdrażanych unijnych regulacji rynku kryptowalut, w tym zastosowania do transakcji kryptowalutowych tzw. *travel rule*.

Słowa kluczowe

Federacja Rosyjska, finansowe sankcje międzynarodowe, kryptoaktywa, zdecentralizowane finanse, DeFi, cyfrowy pieniądz banku centralnego, CBDC, rozporządzenie MiCA

Abstract

The article focuses on the issue of international sanctions of a financial nature in the context of, in particular, the challenges to their effectiveness generated by the cryptocurrency market. An essential point of reference for this analysis is the current case of sanctions imposed by the Council of the European Union (supported by the application of complementary sanctions by part of the international community) on the Russian Federation in relation to that country's military aggression against Ukraine. The aim of this article is to show different perspectives on the assessment of the effectiveness of sanctions and, in particular, to identify the sources why, in a key number of cases, while weakening the economic potential of the sanctioned state, they nevertheless fail to achieve the original objective of their imposition, i.e. the deterrence of military action. In this subject, the axis of interest is the current and prospective impact of blockchain-based financial solutions on the creation of an important loophole in the sanctions regime to eliminate or marginalise the effects of international financial sanctions. The issue is also assessed through the prism of the crypto-asset market regulation entering into force in the European Union in the near future and the implementation of the so-called travel rule for cryptocurrency transactions.

Keywords

Russian Federation, financial international sanctions, crypto-assets, decentralised finance, DeFi, central bank digital currency, CBDC, MiCA regulation

Wojna jest tylko kontynuacją polityki innymi środkami.

Carl von Clausewitz, *O naturze wojny* (1832)

Zaangażowanie się w działania militarne przez społeczność międzynarodową w odpowiedzi na naruszenie prawa międzynarodowego przez jedno z państw trudno uznać za dobre rozwiązanie, gdy celem nadrzędnym jest uniknięcie eskalacji konfliktu zbrojnego. W związku z tym lepszym, a czasem jedynym wyborem dla społeczności międzynarodowej staje się zastosowanie sankcji, które są postrzegane jako liberalna alternatywa wobec wojny. Jednak w kontekście osiągnięcia głównego celu zastosowania sankcji, czyli powstrzymania agresji militarnej, bardziej stanowią one

sygnał¹, niż mają realny wpływ na stronę nimi objętą, zwłaszcza jej decydentów politycznych oraz środowiska powiązane z ośrodkami władzy.

Pojęcie sankcji wiąże się przede wszystkim z zastosowaniem narzędzi ekonomicznych bezpośrednio odnoszących się do sfery gospodarczej, które polega na zaprzestaniu lub groźbie zaprzestania istniejących relacji handlowych lub finansowych. Sankcje to coś więcej niż jedynie dyplomatyczna deklaracja, a ich rzeczywista skuteczność jest warunkowana wywołaniem drastycznego wpływu na gospodarkę sankcjonowanego kraju.

Należy podzielić pogląd, że skuteczna egzekucja sankcji finansowych jest zdecydowanie łatwiejsza niż egzekucja sankcji handlowych², co wynika z tego, że instytucje finansowe i państwa są istotnymi dostawcami lub gwarantami przepływów finansowych. Ponadto zdecydowanie większy nadzór istnieje nad rynkiem finansowym niż nad rynkiem handlu. Działalność finansowa zatem, przynajmniej w założeniu, powinna być łatwiejsza do monitorowania i ewentualnego identyfikowania naruszeń sankcji. Poza tym w badaniach potwierdzono większą skuteczność sankcji finansowych w porównaniu z sankcjami handlowymi³. Nie można bowiem pominąć, że w uwarunkowaniach gospodarczych działalność handlowa wymaga dostępu do zasobów finansowych. Tym samym sankcje finansowe mają komplementarny wpływ na przepływy handlowe, gdyż pozwalają na uniknięcie problemu egzekwowania sankcji w nie wymierzonych⁴. Jednak wbrew pozorom, podobnie jak innego rodzaju sankcje, również te finansowe mogą mieć niehumanitarny charakter i wyrządzać nieodwracalne szkody dla ludności cywilnej sankcjonowanego kraju, ale niekoniecznie muszą mieć bezpośredni wpływ na sytuację jego decydentów politycznych.

¹ Wynika to ze sposobu rozumienia podstaw normatywnych, zgodnie z którym przyjmuje się, że przez karanie i zawstydzanie jest możliwe kreowanie motywacji moralnych. Wiąże się to z pojmowaniem sankcji międzynarodowych jako negatywnej reakcji społeczności międzynarodowej wobec państwa, które narusza jej normy. Zob. R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Warszawa 2003, s. 24.

² G.C. Hufbauer i in., *Economic Sanctions Reconsidered: Supplemental case histories*, Washington 2007, s. 97–98.

³ W badaniach Gary'ego C. Hufbauera, Jeffrey'ego J. Schotta i Kimberly A. Elliott przeprowadzonych w 1985 r. (zaktualizowanych w 1990 r. i 2007 r.), w odniesieniu do przypadków zastosowania sankcji finansowych za sukces uznano 19 przypadków z 53 związanych ze stosowaniem wyłącznie tych sankcji (36%), w 32 przypadkach na 101 spraw obejmujących zastosowanie sankcji finansowo-handlowych (32%) oraz w 8 na 21 w sytuacji zamrożenia aktywów (38%). Dla odmiany w sytuacji zastosowania wyłącznie sankcji handlowych pozytywny rezultat odnotowano w 10 przypadkach na 40 weryfikowanych (25%). Zob. G.C. Hufbauer i in., *Economic Sanctions Reconsidered...*, s. 98.

⁴ Tamże, s. 47–48, 97.

Pojawia się przy tym istotna wątpliwość dotycząca wpływu przemian na rynkach finansowych, w skali globalnej obserwowanych od ponad dekady (w tym innowacyjnych alternatyw dla tradycyjnych systemów bankowych oddziałujących w coraz większym stopniu na państwowe systemy monetarne i walutowe), na osłabienie skuteczności sankcji międzynarodowych. Można bowiem postawić pytanie nie tylko o obowiązywanie odpowiednich przepisów prawa, lecz także o możliwość wyrażenia w nich norm w pełni regulujących nowe rozwiązania stosowane na rynkach finansowych, co pośrednio zapewniałoby skuteczność egzekucji ustanawianych sankcji. Celem artykułu jest ukazanie złożoności tej problematyki w kontekście dostępu do nowych instrumentów finansowych i ich wykorzystania przez aparaty państwowe. Nie ograniczono się wyłącznie do badań metodą dogmatyczną nad tą problematyką, lecz z uwagi na postrzeganie prawa jako wielopłaszczyznowego zjawiska kulturowego⁵, odniesiono się do wyników ekonomicznych i politologicznych badań naukowych nad skutecznością sankcji międzynarodowych, z uwzględnieniem przeglądu innowacyjnych instrumentów finansowych istotnych z punktu widzenia unijnych sankcji nałożonych na Federację Rosyjską (FR) w związku z jej agresją zbrojną na Ukrainę.

Nieskuteczność sankcji ekonomicznych

Z sankcjami wiąże się błędne przekonanie, że wymuszenie oczekiwanej normy zachowania zostanie wywołane przez samą obawę o wyniki gospodarcze ze strony objętego nimi państwa. Wbrew temu założeniu badania ekonomiczne przeprowadzone w 1990 r. przez Gary'ego C. Hufbauera, Jeffrey'ego J. Schotta i Kimberly A. Elliott wykazały, że skuteczność sankcji gospodarczych była stosunkowo niska i wynosiła ok. 34%⁶. W wyniku analizy krytycznej tych badań w ujęciu politologicznym Robert A. Pape uznał, że ze wskazanych w nich 40 przypadków tylko pięć można byłoby uznać za rzeczywisty sukces zastosowania sankcji⁷.

⁵ Zob. K. Opalek, J. Wróblewski, *Zagadnienia teorii prawa*, Warszawa 1969; ciż sami, *Prawo. Metodologia, filozofia, teoria prawa*, Warszawa 1991.

⁶ Badania z 1990 r. objęły 116 przypadków zastosowania sankcji. W 40 sprawach uznano, że ich zastosowanie przyniosło pozytywny efekt.

⁷ Pape skorygował liczbę zbadanych przypadków – było ich 115, a nie 116. Uznał, że 5 spraw stanowi powtórzenie, podobnie wśród 40 przypadków zakwalifikowanych jako sukces zidentyfikował 1 powtórzenie, w 18 przypadkach rozstrzygnięcie w rzeczywistości wynikało z bezpośredniego lub pośredniego użycia siły, w 8 przypadkach sankcje nie przyniosły żadnego efektu, gdyż państwa nimi objęte nie poczyniły żadnych ustępstw, a 6 przypadków dotyczyło sporów handlowych, a nie stricte sankcji gospodarczych dla celów politycznych. W 3 przypadkach ewaluacja pod kątem

Na nieefektywność sankcji wpływa wiele czynników, przede wszystkim są to nieadekwatność i niewystarczalność zastosowanych środków. Ułatwia to uniknięcie sankcji lub przynajmniej zminimalizowanie ich negatywnych implikacji. W tym kontekście podstawowym warunkiem skuteczności jest jednomysłność społeczności międzynarodowej w sprawie nałożenia sankcji na dane państwo. Brak tej solidarności otwiera drogę do możliwości ograniczenia i neutralizacji skutków sankcji. Dla przykładu w zakresie wymiany handlowej otwiera to nowe kierunki importowe oraz zmianę rynków zbytu dla eksportu. Jednocześnie za pośrednictwem nowych destynacji handlowych staje się możliwy „przełom” towarów objętych sankcjami do krajów formalnie je stosujących⁸. W odniesieniu natomiast do systemu finansowego jest możliwe jego zabezpieczenie przez tzw. zaszczepienie gospodarki (ang. *vaccinate the economy*) polegające na jej izolowaniu od wpływu sankcji przez zabezpieczenie remedium na te sankcje albo uzyskanie łatwego dostępu do alternatywnych rozwiązań⁹.

Z sankcjami wiąże się także zjawisko nasilenia się postaw nacjonalistycznych w państwie, wobec którego są one stosowane. Zwraca na to uwagę Pape, który jednoznacznie wskazuje na nieskuteczność sankcji w sytuacji, gdy nie tylko aparat państwowy, lecz także obywatele są skłonni znosić dotkliwe ograniczenia w imię interesów narodowych. Takie tendencje charakteryzują zwłaszcza systemy autokratyczne, w których władza może zaakceptować wysokie koszty społeczne, jeżeli to umożliwi jej osiągnięcie własnych celów¹⁰. Tym samym ten fenomen zaprzecza twierdzeniom, że uderzenie w interesy ekonomiczne obywateli danego kraju musi wiązać się z opowiedzeniem się przez nich za zmianami politycznymi.

Aktualnie nieskuteczność sankcji finansowych wiąże się także ze wzrostem znaczenia w skali globalnej kryptoaktywów. Mogą one odgrywać istotną rolę w minimalizowaniu sankcji zarówno indywidualnych, jak i obejmujących system finansowy danego państwa.

skuteczności sankcji jest niemożliwa. Zob. R.A. Pape, *Why Economic Sanctions Do Not Work*, „International Security” 1997, t. 22, nr 2, s. 93, 99.

⁸ Oczywiście wiąże się to mimo wszystko z negatywnymi konsekwencjami dla państwa objętego sankcjami w związku ze spadkiem cen eksportowanych surowców i towarów.

⁹ A. Demarais, *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022, s. 35–50.

¹⁰ R.A. Pape, *Why Economic Sanctions...*, s. 106.

Kazus rosyjski

Z uwagi na działania wojenne przeciwko Ukrainie oraz nielegalne aneksje obwodów: donieckiego, ługańskiego, zaporoskiego i chersońskiego (2022 r.), a także z uwzględnieniem środków ograniczających nałożonych na FR w związku z aneksją Krymu (2014 r.), m.in. Unia Europejska (UE)¹¹ podjęła decyzję o objęciu tego kraju kolejnymi sankcjami. Były to środki ograniczające w postaci sankcji zarówno indywidualnych, jak i gospodarczych oraz wizowych. Według stanu na 5 marca 2024 r. Rada UE przyjęła 13 pakietów sankcji.

Koncentrując się wyłącznie na zagadnieniu bezpośredniego oddziaływania na rosyjski system finansowy, należy wskazać następujące sankcje unijne:

- zakaz finansowania rządu rosyjskiego i Centralnego Banku Federacji Rosyjskiej, CBFR (ros. Центральный банк Российской Федерации lub Банк России; ang. The Central Bank of Russian Federation lub Bank of Russia) oraz wszelkich transakcji związanych z zarządzaniem jego rezerwami i aktywami (zamrożenie rezerw walutowych), a także organami, podmiotami lub osobami działającymi w imieniu lub pod jego kierownictwem [np. Fundusz Dobrobytu Narodowego (Фонд национального благосостояния)];
- zakaz eksportu banknotów oraz sprzedaży zbywalnych papierów wartościowych¹² do Rosji denominowanych w euro oraz w pozostałych walutach urzędowych UE¹³;
- zakaz inwestowania w projekty współfinansowane przez rosyjski Fundusz Inwestycji Bezpośrednich (Российский фонд прямых инвестиций), a także uczestniczenia w projektach lub dokonywania innego wkładu w te projekty¹⁴;

¹¹ Poza sankcjami UE (oraz jej krajów członkowskich, które zachowały możliwość nakładania odrębnych, dodatkowych sankcji) na Rosję środki nałożyły także: USA, Wielka Brytania, Kanada, Szwajcaria, Japonia, Singapur, Korea Południowa, Australia, Nowa Zelandia oraz Tajwan. Zakres tych sankcji nie jest w wielu przypadkach jednorodny. Singapur np. zdecydował się wyłącznie na nałożenie ograniczonych sankcji finansowych oraz kontrolę eksportu w zakresie broni i przedmiotów służących ofensywnym operacjom cybernetycznym. Zob. *Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine*, Ministry of Foreign Affairs Singapore, 5 III 2022 r., <https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions> [dostęp: 5 III 2024].

¹² Z tym zakazem łączy się zakaz prowadzenia rachunków rosyjskich klientów przez unijne centralne depozyty papierów wartościowych.

¹³ Wyjątki obejmują środki niezbędne do osobistego użytku podróżujących do Rosji lub oficjalnych celów misji dyplomatycznych, konsularnych, organizacji międzynarodowych.

¹⁴ W tym zakresie przewidziano ściśle określone odstępstwa dotyczące umów zawartych przed 2 marca 2022 r.

- zakaz przeprowadzania wszelkich transakcji z niektórymi rosyjskimi przedsiębiorstwami państwowymi z różnych sektorów, tworzących militarno-przemysłowy kompleks Kremla¹⁵, a także zakaz zajmowania stanowisk w organach zarządzających tych przedsiębiorstw;
- zakaz dopuszczenia do obrotu giełdowego akcji rosyjskich podmiotów państwowych w unijnych systemach obrotu i świadczenia związanych z nimi usług;
- zakaz bezpośredniego lub pośredniego kupna, sprzedaży lub świadczenia usług inwestycyjnych lub pomocy w emisji i innych czynności w odniesieniu do zbywalnych papierów wartościowych i instrumentów rynku pieniężnego w odniesieniu do m.in. rządu Rosji i CBFR, osób prawnych, podmiotów oraz organów działających w ich imieniu, a także podmiotów wskazanych w załącznikach V i VI *Rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie* (dalej: rozporządzenie 833/2014);
- zakaz świadczenia bezpośrednio lub pośrednio usług dla biznesu, takich jak usługi w zakresie rachunkowości, audytu, badania ustawowego, prowadzenia ksiąg rachunkowych i doradztwa podatkowego, doradztwa informatycznego, doradztwa prawnego, architektury i inżynierii, doradztwa w zakresie zarządzania, public relations, badań rynku i opinii publicznej, badań i analiz technicznych, reklamy i usług ratingowych;
- zakaz świadczenia na rzecz kluczowych rosyjskich banków specjalistycznych usług w zakresie komunikatów finansowych, wykorzystywanych do wymiany danych finansowych w ramach Society for Worldwide Interbank Financial Telecommunication (SWIFT)¹⁶;
- zakaz udzielania finansowania publicznego lub pomocy finansowej na rzecz handlu ze stroną rosyjską lub inwestycji na terenie FR¹⁷;

¹⁵ Kompletna lista wyżej wymienionych podmiotów została określona w wykazie z załącznika XIX *Rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*.

¹⁶ Sankcje w ramach trzeciego pakietu z 2 marca 2022 r. objęły siedem rosyjskich banków, tj. Банк Открытие (Bank Otkrytije), Новикомбанк (Nowikombank), Промсвязьбанк (Promswiaz'bank), Банк „Россия” (Bank „Rossiya”), Совкомбанк (Sowkombank), Vnesheconombank (VEB, VEB.RF) i Банк ВТБ (WTB Bank), a także wszystkie osoby prawne, podmioty lub organy z siedzibą w Rosji, w których ponad 50% praw własności należy bezpośrednio lub pośrednio do ww. instytucji. Następnie w ramach szóstego pakietu z 3 czerwca 2022 r. wyłączenie ze SWIFT rozszerzono na Сбербанк России (Sbierbank Rossii), Московский кредитный банк (Moskowskij kredittnyj bank) i Российский сельскохозяйственный банк (Rossielchozbank) – (Rossijskij sielskochozjaistwiennyj bank, Rossielchozbank).

¹⁷ Wyjątkami są: zastrzeżenie możliwości sfinalizowania kontraktów zawartych przed 26 lutego 2022 r. oraz szczególne przypadki dotyczące handlu produktami spożywczymi, środkami do celów

- zakaz udziału rosyjskich wykonawców w zamówieniach publicznych i koncesjach udzielanych w państwach członkowskich UE;
- zakaz prowadzenia rachunków rosyjskich klientów przez unijne centralne depozyty papierów wartościowych oraz sprzedaży im papierów wartościowych denominowanych w euro;
- zakaz przyjmowania depozytów od obywateli lub rosyjskich rezydentów, osób prawnych, podmiotów lub organów mających siedzibę na terenie Rosji lub osób prawnych, podmiotów lub organów mających siedzibę poza UE, w przypadku których ponad 50% praw własności należy bezpośrednio lub pośrednio do obywateli rosyjskich lub osób fizycznych zamieszkałych na terenie Rosji, jeżeli łączna wartość ich depozytów na instytucję kredytową przekracza kwotę 100 000 euro;
- zakaz świadczenia usług doradztwa w zakresie planowania finansowego i trustów oraz przyjmowania dużych depozytów przez banki z UE;
- zakaz świadczenia usług kryptograficznych pierwotnie o wysokiej wartości (tj. 10 000 euro), a następnie niezależnie od wartości.

Jednocześnie po wprowadzeniu trzynastego pakietu sankcji skierowanych przeciwko Rosji łącznie wobec 2177 osób i podmiotów¹⁸ przyjęto sankcje indywidualne polegające m.in. na zamrożeniu aktywów oraz wprowadzeniu zakazu udostępniania funduszy lub zasobów gospodarczych. Ustanowiono także nowe sankcje wobec Białorusi (z uwagi na działania podważające integralność terytorialną, suwerenność i niezależność Ukrainy) oraz Iranu (w związku z udzielonym wsparciem wojskowym w postaci dostaw bezzałogowych statków powietrznych). W przypadku sankcji indywidualnych nałożonych na Białoruś zostały one zastosowane wobec 271 osób i podmiotów¹⁹, na Iran – wobec 280 osób i podmiotów²⁰.

rolniczych, medycznych lub humanitarnych, a także dotyczące programów unijnych dla małych i średnich przedsiębiorstw – do określonej kwoty.

¹⁸ Zgodnie z załącznikiem I *Rozporządzenia Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających* – przy czym według stanu na 5 marca 2024 r. 36 osób i podmiotów zostało skreślonych z listy, zatem 2141 osób i podmiotów pozostaje objętych sankcjami.

¹⁹ Zgodnie z załącznikiem I *Rozporządzenia Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy*, przy czym według stanu na 5 marca 2024 r. 1 podmiot został skreślony z listy, zatem 270 osób i podmiotów pozostaje objętych sankcjami.

²⁰ Zgodnie z załącznikiem I *Rozporządzenia Rady (UE) nr 359/2011 z dnia 12 kwietnia 2011 r. dotyczącego środków ograniczających skierowanych przeciwko niektórym osobom, podmiotom i organom w związku z sytuacją w Iranie* – przy czym według stanu na 5 marca 2024 r. 8 osób zostało skreślonych z listy, zatem 272 osoby i podmioty pozostają objęte sankcjami.

Egzekucja sankcji nakładanych przez Radę UE ciąży na państwach członkowskich, które są odpowiedzialne za ich wdrożenie. W tym zakresie wsparcia udziela im Komisja Europejska (KE), odpowiadająca za jednolitość tych działań i ich koordynację międzynarodową²¹.

Sankcje unijne wymierzone w Rosję i Białoruś są uzupełniane w Polsce przez sankcje krajowe. W tym zakresie najważniejszy akt prawny to *Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*, statuująca m.in. ustanowienie dodatkowej krajowej listy sankcyjnej prowadzonej przez ministra właściwego do spraw wewnętrznych²².

Zgodnie z przepisami tej ustawy karze pieniężnej, nakładanej przez Szefa Krajowej Administracji Skarbowej w drodze decyzji administracyjnej, w wysokości do 20 mln zł²³ podlegają osoba lub podmiot, które w stosunku do osoby lub podmiotu wpisanego na listę nie dopełniają: obowiązku zamrożenia środków finansowych, funduszy lub zasobów gospodarczych lub zakazu udostępniania środków finansowych, funduszy lub zasobów gospodarczych, określonego w art. 2 ust. 1 lub 2 *Rozporządzenia Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy* (dalej: rozporządzenie 765/2006) lub art. 2 *Rozporządzenia Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających* (dalej: rozporządzenie 269/2014), albo obowiązku niezwłocznego przekazywania informacji, wymaganych na podstawie art. 4 ust. 2 lub art. 5 rozporządzenia 765/2006 lub na podstawie art. 7 ust. 1 lub art. 8 rozporządzenia 269/2014; bądź nie stosują się do zakazu świadomego i celowego udziału w działaniach, których celem lub skutkiem jest ominięcie stosowania środków określonych w art. 2 ust. 1 lub 2 rozporządzenia 765/2006 lub art. 2 rozporządzenia 269/2014.

²¹ W tym celu KE powołała grupę zadaniową Freeze and Seize, której zadaniem jest koordynowanie na szczeblu UE wdrożenia indywidualnych sankcji wobec osób fizycznych. Grupa ta odpowiada również za współpracę w ramach grupy zadaniowej REPO (Russian Elites, Proxies, and Oligarchs), zarządzającej współpracą UE z krajami G7 (Group of Seven) oraz Australią.

²² Lista jest niezależna od wykazów osób i podmiotów określonych w rozporządzeniach 765/2006 i 269/2014, gdyż zakres środków stosowanych wobec osób i podmiotów wpisanych na nią nie może powielać zakresu środków określonych względem nich w tych rozporządzeniach (art. 2 ust. 2 ustawy). Według stanu aktualizacji listy na dzień 29 lutego 2024 r. przez MSWiA obejmowała ona 427 osób fizycznych oraz 82 podmioty. Jednocześnie z listy w latach 2022–2023 wykreślono 1 osobę fizyczną i 8 podmiotów. W efekcie wskazanego dnia sankcjami pozostawało objętych 426 osób fizycznych i 74 podmioty.

²³ Artykuł 6 *Ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*.

Należy zgodzić się z Pape'em, że pomimo kompleksowości sankcji ich nałożenie na FR okazało się niepowodzeniem. Bez wątplenia są one dotkliwe dla gospodarki²⁴, jednak w rzeczywistości nie zmuszają Rosji do zaprzestania prowadzonej „operacji wojskowej”²⁵. Przykład tego kraju pokazuje pełen zakres ograniczeń co do skuteczności systemu sankcji międzynarodowych.

Głównym czynnikiem determinującym niewielką skuteczność zastosowanych sankcji był – jak wspomniano wyżej – brak jednomyślności społeczności międzynarodowej w tym przedmiocie, a zwłaszcza postawa Chin, Indii, Iranu oraz państw dawnych republik radzieckich Azji Środkowej i Kaukazu czy Turcji, które negatywnie odniosły się do wprowadzenia sankcji. Przewidzenie przez Rosję braku jednomyślności społeczności międzynarodowej pozwoliło na zaszczerpienie jej gospodarki oraz znalezienie alternatyw pozwalających na zmniejszenie dotkliwości sankcji, czego przykładem może być odnotowywany w latach poprzedzających agresję na Ukrainę wzrost wysokości utrzymywanych rezerw walutowych i w złocie²⁶. Pomimo zamrożenia w wyniku zastosowania sankcji części rosyjskich rezerw walutowych ich kluczowe zasoby zostały zachowane wskutek utrzymywania przez CBFR największego poziomu rezerw w złocie (tzw. złoto monetarne) zdeponowanym w skarbcach na terytorium FR (21,7%), a także ulokowania ok. 13,8% wszystkich rezerw w Chinach. Ważne jest również to, że rezerwy walutowe nie obejmowały wyłącznie euro i dolara, lecz były sukcesywnie lokowane przede wszystkim w renminbi (yuan), a także np. w jenach i rupiach²⁷. Polityka CBFR pozwoliła w nowych uwarunkowaniach na zachowanie środków niezbędnych dla podejmowania interwencji na rynku walutowym i dłużnym. Również utrata dostępu do SWIFT nie okazała się, jak przewidywano, „finansową bronią nuklearną”²⁸. Pomimo zastosowania tej drastycznej sankcji banki

²⁴ Potwierdzeniem tego jest m.in. odnotowany spadek rosyjskiego produktu krajowego brutto (PKB). Zgodnie z analizami Banku Światowego, Międzynarodowego Funduszu Walutowego i Organizacji Współpracy Gospodarczej i Rozwoju w 2022 r. rosyjski PKB obniżył się o 2,1%, przy wzroście na poziomie 3% prognozowanym przed inwazją przez Federalną Służbę Statystyki Państwowej, Rosstat (Федеральная служба государственной статистики, Росстат). Zob. *Wpływ sankcji na rosyjską gospodarkę*, Rada UE, <https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/> [dostęp: 5 III 2024].

²⁵ R.A. Pape, wpis na portalu LinkedIn, https://www.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [dostęp: 5 III 2024].

²⁶ *Annual value of international reserves of Russia from 2012 to 2022, by type*, Statista, <https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/> [dostęp: 5 III 2024].

²⁷ *Bank of Russia foreign exchange and gold asset management report*, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [dostęp: 5 III 2024].

²⁸ Francuski minister finansów Bruno Le Maire po spotkaniu ministrów finansów UE w dniu 25 lutego 2022 r. wyraził opinię, że wyłączenie FR z międzynarodowego systemu płatności SWIFT

rosyjskie nadal mogą funkcjonować i pozyskiwać zasoby gotówkowe umożliwiające prowadzenie działalności i interakcje z rynkami zewnętrznymi. Wynika to z dostępności różnych alternatywnych rozwiązań, które pozwalają ominąć sankcje. Wskutek obaw o wykluczenie ze SWIFT rosyjskiego sektora bankowego CBFR już podczas aneksji Krymu w 2014 r. rozpoczął testowanie systemu transmisji komunikatów finansowych – SPFS (Система передачи финансовых сообщений). Według oświadczenia CBFR już w lipcu 2023 r. system ten przetwarzał 70% krajowych transakcji finansowych²⁹. Nie jest on jednak przeznaczony wyłącznie do rozliczeń krajowych. Według informacji ze stycznia 2024 r. korzysta z niego 557 podmiotów, w tym 157 podmiotów zagranicznych z 20 państw³⁰. Opcją obejścia sankcji jest również posłużenie się transgranicznym międzybankowym systemem płatniczym – CIPS (Chinese Cross-Border Interbank Payment System), a także jego ewentualna integracja z SPFS, zwłaszcza w odniesieniu do chińsko-rosyjskich rozliczeń transgranicznych.

Pomimo negatywnego wpływu na gospodarkę i uwarunkowania społeczne sankcje również nie wywołały istotnych przemian politycznych, a wręcz przeciwnie – uwolniły duży potencjał adaptacyjny, który ułatwił ustabilizowanie się sytuacji gospodarczej. Prognozuje się, że w perspektywie czasu, wskutek zwiększania kontroli gospodarki i ugruntowania modelu kapitalizmu państwowego, może to również przyczynić się do dalszego wzmocnienia pozycji władz³¹.

powinno być traktowane jako rozwiązanie ostateczne. Stwierdził, że „SWIFT jest finansową bronią nuklearną. (...) Faktem pozostaje, że mając w rękach broń nuklearną, myśli się, zanim jej użyje. Niektóre kraje członkowskie wyraziły zastrzeżenia, bierzemy je pod uwagę”. Tłumaczenia w tekście pochodzą od autorki (dop. red.). Zob. G. Leali, *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022 r., <https://www.politico.eu/article/Frances-le-maire-not-againstcutting-russia-out-of-swift/> [dostęp: 5 III 2024]. Należy podkreślić, że tę sankcję uważano za najbardziej drastyczną, co w czasie rosyjskiej inwazji na Krym w 2014 r. skutkowało odrzuceniem apeli o wykluczenie już wówczas FR ze SWIFT, gdyż uznano ten krok za nadmierną eskalację konfliktu.

²⁹ В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT, Известия, 3 VII 2023 r., <https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossiiskogo-trafika-u-nacionalnogo-analoga-swift> [dostęp: 5 III 2024].

³⁰ Российский аналог SWIFT распространяется на Восток, News.Ru, 27 I 2024 r., <https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie> [dostęp: 5 III 2024].

³¹ I. Wiśniewska, *Rosyjska gospodarka w roku 2022. Adaptacja i rosnący deficyt budżetu*, OSW, 16 II 2023 r., <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-02-16/rosyjska-gospodarka-w-roku-2022-adaptacja-i-rosnacy-deficyt> [dostęp: 5 III 2024].

Kryptoaktywa jako przedmiot sankcji nałożonych na Federację Rosyjską

W lutym 2022 r. Bloomberg, powołując się na szacunki rosyjskiego rządu³², podał, że obywatele rosyjscy posiadają aktywa kryptograficzne o wartości 16,5 bln rubli (214 mld dolarów), co stanowiło 12% całkowitej wartości tych aktywów na świecie. Szacowano, że tego rodzaju aktywa posiadało ponad 17 mln Rosjan³³. Według ocen Cambridge Centre for Alternative Finance (CCAF) z przełomu 2021 i 2022 r. Rosja była także jednym z pięciu największych ośrodków wydobywczych bitcoina – zapewniała 4,66% jego światowej produkcji³⁴. Potwierdzeniem obaw, że kryptoaktywa mogą być istotną luką w systemie sankcji finansowych wymierzonych w Rosję i sposobem na ograniczenie ich skutków, były odnotowane wzrosty wolumenu obrotów między rublem a najważniejszymi kryptowalutami³⁵. W odpowiedzi na to zagrożenie w tzw. *Compliance package* z 9 marca 2022 r. odnoszącym się do Białorusi doprecyzowano, że w rozporządzeniu 269/2014 niewyczerpująca definicja funduszy obejmuje także kryptowaluty, a definicja zasobów gospodarczych może dotyczyć również niektórych kryptoaktywów. W związku z tym kryptoaktywa miały podlegać przepisom dotyczącym zamrożenia aktywów oraz zakazowi udostępniania funduszy lub zasobów gospodarczych osobom umieszczonym na listach sankcyjnych. Uznano także, że w rozumieniu rozporządzenia 833/2014 zbywalne papiery wartościowe obejmują kryptoaktywa z wyjątkiem instrumentów płatniczych. Ponadto podkreślono, że kryptoaktywów nie należy wykorzystywać do obchodzenia jakichkolwiek sankcji unijnych³⁶.

Najważniejsze ograniczenia w tym obszarze wprowadzono jednak dopiero w ramach piątego pakietu sankcji z 8 kwietnia 2022 r. Podjęto wówczas decyzję

³² Oszacowanie zostało przeprowadzone na podstawie m.in. analizy adresów IP największych użytkowników giełd kryptowalutowych.

³³ E. Pismennaya, *Russia Values Local Crypto at \$200 Billion as Rules Near*, Bloomberg, 1 II 2022 r., <https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg> [dostęp: 5 III 2024].

³⁴ *Bitcoin Mining Map*, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [dostęp: 5 III 2024].

³⁵ Po wprowadzeniu sankcji w lutym 2022 r. wzrost obrotów zaobserwowano zwłaszcza na transakcjach zakupu tethera i bitcoina, co było uwarunkowane przede wszystkim początkowym drastycznym spadkiem wartości rubla. Zob. T. Wilson, *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022 r., <https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/> [dostęp: 5 III 2024].

³⁶ Komunikat prasowy Komisji Europejskiej: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022 r., https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [dostęp: 5 III 2024]; *Crypto-assets. Relevant provision: Article 5b(2) of Council Regulation (EU) No 833/2014. Frequently asked questions*, UE, 21 III 2023 r., https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 5 III 2024].

o zakazie świadczenia usług, których przedmiotem jest udostępnianie portfeli służących do przechowywania kryptoaktywów, prowadzenia rachunków lub przechowywania kryptoaktywów, na rzecz obywateli rosyjskich lub osób fizycznych zamieszkałych na terenie Rosji lub osób prawnych, podmiotów lub organów z siedzibą w tym kraju, jeżeli całkowita wartość kryptoaktywów osoby fizycznej lub prawnej, podmiotu lub organu na dostawcę portfela lub rachunku lub na podmiot przechowujący kryptoaktywa przekracza 10 000 euro³⁷. Ta sankcja została zaostżona w ósmym pakiecie z 5 października 2022 r. przez przyjęcie całkowitego zakazu świadczenia tego rodzaju usług na rzecz ww. osób i podmiotów, niezależnie od wartości kwoty portfela³⁸.

Kryptoaktywa jako źródło luki w systemie międzynarodowych sankcji finansowych

Część komentatorów³⁹ nie przypisywała dużego znaczenia możliwości wytworzenia się luki w systemie sankcji finansowych. Wskazywano przede wszystkim na ograniczenie płynności rynku kryptowalut, który nie mógłby zaspokoić skali rosyjskich potrzeb. Stąd uznawano, że FR nie byłaby w stanie w takim samym wymiarze powielić strategii Iranu, który w obliczu sankcji zalegalizował płatności kryptowalutowe w imporcie. Należy jednak zauważyć, że w sytuacji zaostżania zachodnich sankcji strona rosyjska rozważała sformalizowanie możliwości użycia kryptowalut w rozliczeniach transgranicznych⁴⁰.

³⁷ Artykuł 1 pkt 18 *Rozporządzenia Rady (UE) 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*.

³⁸ Artykuł 1 pkt 10 *Rozporządzenia Rady (UE) 2022/1904 z dnia 6 października 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*.

³⁹ Zob. *Cryptocurrencies: a way to evade sanctions?*, BAFFI – Centre on Economics, Finance and Regulation, <https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-evade-sanctions> [dostęp: 5 III 2024].

⁴⁰ Głównym przeciwnikiem wdrożenia takiego rozwiązania jest CBFR, który podchodzi sceptycznie do rynku kryptowalut. Instytucja ta miała również największy wpływ na treść ustawy federalnej nr 331-FZ „W sprawie zmiany niektórych aktów ustawodawczych Federacji Rosyjskiej oraz w sprawie zawieszenia niektórych przepisów art. 5 ust. 1 ustawy federalnej «O bankach i działalności bankowej»”, nowelizującej ustawę federalną nr 259-FZ „W sprawie cyfrowych aktywów finansowych, waluty cyfrowej oraz zmian w niektórych aktach prawnych Federacji Rosyjskiej”, przez dodanie w jej art. 4 ust. 10 o treści: „Zabrania się przyjmowania cyfrowych aktywów finansowych jako środka płatniczego lub innego wynagrodzenia za przekazane dobra, wykonaną pracę, świadczone usługi, a także w jakikolwiek inny sposób umożliwiający zapłatę za towary (pracę, usługę) cyfrowym aktywem finansowym,

Podkreślano także błąd postrzegania decentralizacji jako gwarancji zachowania pełnej anonimowości użytkowników⁴¹. Technologia blockchain jest publiczną księgą aktywności, umożliwiającą monitorowanie przepływów środków pomiędzy portfelami. Ten argument był odrzucany wobec wskazania, że identyfikacja na blockchainie następuje na podstawie adresów kluczy publicznych, a nie rzeczywistej tożsamości, co potencjalnie może umożliwić uniknięcie sankcji w sytuacji posłużenia się nieprawdziwą tożsamością. Sceptycy uznawali takie zagrożenie za marginalne wobec faktu, że większość obrotów kryptowalutowych odbywa się z udziałem pośredników, takich jak kantory i giełdy kryptowalutowe czy dostawcy portfeli kryptowalutowych. Z uwagi na te czynniki w większości jurysdykcji ten obrót podlega regulacjom przeciwdziałającym praniu pieniędzy oraz finansowaniu terroryzmu. Duża część giełd kryptowalutowych wdraża także zasady Know Your Customer, KYC (pol. poznaj swojego klienta)⁴².

Dla przykładu w polskiej *Ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu*, w związku z wprowadzeniem do niej definicji legalnej pojęcia waluty wirtualnej (art. 2 ust. 2 pkt 26), rozszerzono katalog instytucji obowiązanych o podmioty, które prowadzą działalność gospodarczą polegającą na świadczeniu usług w zakresie: wymiany między walutami wirtualnymi i środkami płatniczymi, wymiany między samymi walutami wirtualnymi, pośrednictwa w ich wymianie, a także prowadzenia ich rachunków (tzw. portfeli)⁴³.

z wyjątkiem przypadków przewidzianych w ustawach federalnych”. Jednak wobec artykułowania przez rosyjskie Ministerstwo Finansów oczekiwania co do możliwości wykorzystania kryptowalut jako środka rozliczeń transgranicznych, CBFR promuje w tym zakresie wykorzystanie cyfrowego rubla. Zob. *ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года*, RBC.ru, 10 X 2023 r., <https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430> [dostęp: 5 III 2024].

⁴¹ Zob. C.S. Wright, *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019 r., <https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/> [dostęp: 5 III 2024]. Należy odróżnić koncepcję anonimowości od prywatności i poufności. Całkowita anonimowość może być elementem niepotrzebnym i w większości przypadków niepożądanym, jest natomiast możliwe zachowanie prywatności i poufności przy akceptacji wymogu udowodnienia swojej tożsamości. Tym samym prywatność ukrywa szczegóły transakcji przed szeroko rozumianą opinią publiczną, ale nie przed osobami, które brały udział w wymianie, a także nie przed tymi, których prawo upoważnia do monitorowania wymian.

⁴² KYC to obowiązkowy proces identyfikacji i weryfikacji przez instytucje finansowe tożsamości klienta przy otwieraniu przez niego rachunku, a następnie cykliczne poddawanie tego klienta ponownej ewaluacji.

⁴³ W art. 2 ust. 1 pkt 12 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu uznano ww. podmioty za instytucje obowiązane, które m.in. są zobligowane do stosowania środków bezpieczeństwa w przypadku transakcji okazjonalnej z wykorzystaniem waluty wirtualnej o równowartości 1000 euro lub większej (art. 35 ust. 1 pkt 2 lit. c ww. ustawy). Jednocześnie sama działalność w zakresie

W efekcie podmioty świadczące tego rodzaju usługi pozostają zobowiązane do realizacji zadań AML/CFT⁴⁴.

Niemniej kryptoaktywa, jak wspomniano, mogą zapewnić rozwiązania pozwalające na uniknięcie sankcji finansowych, zwłaszcza indywidualnych. Są to np.:

- *chain-hopping* (pol. przeskakiwanie łańcuchów) – polegające na szybkiej zmianie zasobów kryptograficznych w celu dokonania zmiany blockchaineda utrudniającej śledzenie przepływu środków⁴⁵,
- *mixers, tumblers, foggers* – usługi polegające na mieszaniu potencjalnie identyfikowalnych lub skażonych funduszy kryptowalutowych z innymi, w celu uniemożliwienia ustalenia ich rzeczywistego źródła pochodzenia,
- portfele niehostowane – umożliwiające przenoszenie środków bez podlegania monitoringowi giełd kryptowalutowych, w przeciwieństwie do udostępnianych przez nie portfeli hostowanych; wymagają one jednak ujawnienia w przypadku chęci wymiany kryptowaluty na walutę fiducyjną. Niemniej jest możliwe wówczas skorzystanie z giełd w jurysdykcjach o niskich wymogach AML/CFT lub KYC,
- kryptowaluty nastawione na prywatność, tzw. monety prywatności (ang. *privacy token* lub *private coin*) – ich zastosowanie jest bliskie realizacji idei anonimowych transakcji, pomimo bowiem uwidocznienia samej transakcji w księdze publicznej (blockchain) adresy portfeli stron transakcji pozostają niewidoczne. Przykładem może być kryptowaluta monero, wykorzystująca w transakcjach ukryte adresy w celu ochrony prywatności odbiorcy⁴⁶, dla ochrony nadawcy natomiast stosująca tzw. podpisy pierścieniowe, które polegają na łączeniu klucza konta użytkownika z kluczami publicznymi z blockchaineda,

walut wirtualnych jest działalnością regulowaną w rozumieniu przepisów *Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców* i może być wykonywana po uzyskaniu wpisu do rejestru działalności w zakresie walut wirtualnych dokonywanego przez ministra do spraw finansów publicznych. Jednocześnie jest konieczne spełnienie wymogów niekaralności i posiadania odpowiedniej wiedzy lub doświadczenia przy wykonywaniu tego rodzaju działalności (art. 129m–129w ustawy).

⁴⁴ AML/CFT (ang. *Anti Money Laundering/Counter Financing of Terrorism*) – zbiorcze określenie przepisów i zasad, których stosowanie jest wymagane od podmiotów świadczących usługi finansowe w celu zapobiegania praniu pieniędzy i finansowaniu terroryzmu.

⁴⁵ Tę technikę skutecznie wykorzystywała m.in. północnokoreańska grupa Lazarus w celu ukrycia ścieżki transferów środków skradzionych giełdom kryptowalutowym.

⁴⁶ W celu uniknięcia zapisu adresu portfela odbiorcy na blockchainie jest używany system *Stealth Address*, w którym każdą transakcję wysła się do unikalnego, jednorazowego adresu. Odbiorca ma dostęp do środków przesłanych na ukryty adres, bez ujawniania połączeń do prawdziwego publicznego portfela i historii transakcji.

- zdecentralizowane finanse (ang. *decentralized finance*, DeFi) – oparte na wymianie *peer-to-peer* (P2P)⁴⁷.

Pomimo istotnego znaczenia jednostek analityki finansowej (Financial Intelligence Units)⁴⁸ w odniesieniu do kryptowalut kluczowa rola egzekucji sankcji finansowych przypada komercyjnym instytucjom finansowym. Te, podlegając ścisłym regulacjom nadzorczym ze strony państw, są zmuszone śledzić źródła przepływu pieniędzy i weryfikować, czy strony transakcji nie figurują na listach sankcyjnych. W sytuacji objęcia danego podmiotu sankcjami finansowymi staje się konieczne poszukiwanie przez niego alternatywnych rozwiązań w celu zachowania możliwości przepływu kapitału. Właśnie w tym obszarze tkwi potencjał kryptoaktywów jako instrumentu obchodzenia sankcji. Istnienie zasobów cyfrowych w przestrzeni wirtualnej ma tę zasadniczą zaletę, że transakcje finansowe mogą następować z pominięciem monitorowanych rynków, globalnych sieci płatniczych czy ściśle regulowanych systemów finansowych.

W momencie wprowadzania sankcji unijnych rynek tokenów płatniczych (bitcoin, altcoin i stablecoin) oraz tokenów inwestycyjnych i użytkowych pozostawał w praktyce poza regulacjami oraz nadzorem UE i jej krajów członkowskich.

Zgodnie z polskimi regulacjami rynek kryptoaktywów nie jest identyfikowany jako segment rynku finansowego w rozumieniu przepisów *Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym*. Tym samym Komisja Nadzoru Finansowego sprawuje nadzór wyłącznie nad działalnością giełd i kantorów wymiany walut wirtualnych związany ze świadczeniem przez te podmioty usług płatniczych na podstawie przepisów *Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych*.

Wymiana kryptowalut odbywa się przez szyfrowane przelewy pomiędzy portfelami za pomocą dwukluczowego mechanizmu: przelewy wymagają klucza publicznego, czyli adresu portfela, oraz klucza prywatnego, który pełni funkcję hasła. Oba klucze to kody alfanumeryczne. Jak wcześniej wspomniano, portfele mogą mieć charakter kustodialny (powierniczy, hostowany), co wiąże się z powierzeniem przez inwestora stronie trzeciej zarządzania i ochrony swoimi kluczami do portfela. To skutkuje przejęciem przez powiernika odpowiedzialności za własność inwestora. Na przeciwnym biegunie są tzw. portfele niekustodialne (niepowiernicze, niehostowane). Między tymi rodzajami portfeli istnieją istotne różnice. Przede wszystkim właściciele portfeli depozytowych powierzają swoje klucze prywatne dostawcom usług w zakresie

⁴⁷ Na taki katalog ewentualnych rozwiązań wskazano m.in. w dokumencie K.E. Busch, P. Tierno, *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022 r., <https://crsreports.congress.gov/product/pdf/IN/IN11920> [dostęp: 5 III 2024].

⁴⁸ W Polsce głównym elementem systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest Generalny Inspektor Informacji Finansowej, który realizuje swoje zadania przez Departament Informacji Finansowej wyodrębniony w strukturze Ministerstwa Finansów.

kryptoaktywów (ang. *crypto-asset service providers*, CASPs), podczas gdy zarówno klucze prywatne, jak i publiczne portfeli niepowierniczych pozostają w wyłącznej dyspozycji ich właścicieli, którzy dokonują transferów za pośrednictwem transakcji P2P. Dostawcy usług, będący platformą pośredniczącą, w celu dokonania identyfikacji klienta będą wymagać ujawnienia informacji co najmniej w zakresie danych dotyczących rachunku bankowego lub karty kredytowej. Portfele niepowiernicze natomiast nie wymagają zaufanego pośrednika w postaci zewnętrznej instytucji, która gwarantowałaby bezpieczeństwo transakcji. Drugą istotną różnicą jest to, że transakcji pomiędzy portfelami depozytowymi nie przechowuje się na blockchainie do czasu wycofania środków od CASP, podczas gdy transakcje P2P są natychmiast rejestrowane.

CASPs w porównaniu z sektorem bankowym mają zdecydowanie mniejsze instrumenty egzekwowania prawa w zakresie identyfikacji klientów, mimo że formalnie obowiązują je takie same wymogi AML/CFT, jakie dotyczą instytucji finansowych. Wiąże się to z trudnościami w przypadku portfeli niepowierniczych, ponieważ jedynie niektóre dane na temat transakcji na blockchainie są rejestrowane przez transfery P2P. W efekcie ustalenie własności takich portfeli wymagałoby połączenia szczegółów transakcji z adresami IP jej stron⁴⁹.

Tę sytuację zmieni, przynajmniej częściowo, wejście w życie przepisów *Rozporządzenia 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* (tzw. rozporządzenie MiCA). Ustanowiono w nim ramy prawne dla dostawców usług zarówno w zakresie kryptoaktywów, jak i ochrony konsumentów. Regulacje te mają wzmocnić ochronę nabywców i posiadaczy kryptoaktywów, a w konsekwencji wpłynąć nie tylko na bezpieczeństwo obrotu, lecz przede wszystkim na jego przejrzystość. W rozporządzeniu wyróżnia się trzy rodzaje kryptoaktywów, tj. tokeny powiązane z aktywami (ART),

⁴⁹ Osobnym problemem jest to, że nielegalne transfery pieniężne ułatwia także podatność blockchaina i CASPs na cyberataki, co wiąże się z wtórnymi lukami. Przykładem jest przejęcie kontroli nad 51% mocy obliczeniowej blockchaina (ang. *hush rate*), a w efekcie uzyskanie możliwości modyfikacji lub zmiany szczegółów transakcji, które nie zostały jeszcze zatwierdzone. Podobnie istnieje możliwość wykorzystywania tzw. mostów międzyłańcuchowych (ang. *cross-chain bridges*), które są zdecentralizowanymi platformami zapewniającymi transfer tokenów pomiędzy odrębnymi sieciami i gwarantują interoperacyjność ekosystemów kryptowalutowych. Jednocześnie ataki umożliwiają zachowanie anonimowości w transakcjach P2P. W normalnych warunkach takie transfery są szyfrowane, ale nie anonimowe. Pozwala to na identyfikację płatników dzięki szczegółom i zaszyfrowanym aliasom przechowywanym na blockchainie przez łączenie transakcji z komputerami osobistymi za pośrednictwem adresów IP. W związku z maskowaniem lub zmianą tych informacji na łańcuchu bloków przed zatwierdzeniem cyberataki pozwalają na dokonanie nielegalnych transakcji bez ryzyka identyfikacji. W przypadku CASPs zastosowanie wobec nich procedurów przestępczych jest o tyle łatwiejsze, że te instytucje są powiernikami dla wielu portfeli.

tokeny będące pieniądzem elektronicznym (EMT) i tokeny użytkowe. Świadczenie usługi w zakresie kryptoaktywów będzie dopuszczalne wyłącznie przez osoby prawne mające siedzibę statutową w państwie członkowskim UE, które uzyskały zezwolenie na prowadzenie działalności w charakterze dostawcy takich usług⁵⁰. Przy czym rozporządzenie MiCA ułatwia ich świadczenie podmiotom takim, jak: instytucje kredytowe, domy maklerskie, depozyty papierów wartościowych czy instytucje pieniądza elektronicznego, ponieważ nie wymaga od nich uzyskania zezwolenia na świadczenie usług w zakresie kryptoaktywów. Ustanawia się jedynie wymóg powiadomienia o tym właściwego organu nadzoru⁵¹.

W rozporządzeniu MiCA szczególną uwagę w odniesieniu do sankcji zwraca się na kwestie dotyczące prania pieniędzy i finansowania terroryzmu. Poza tym, że CASPs będą zaliczeni do katalogu instytucji obowiązanych na gruncie AML, to jednocześnie wątki związane z AML i prywatnością (anonimowością) odnoszą się m.in. do zakazu dopuszczania do obrotu kryptoaktywów, które mają wbudowaną funkcję anonimizacji⁵². CASP prowadzący platformę obrotu kryptoaktywami będzie musiał dysponować procedurami zapobiegającymi wykorzystywaniu jego infrastruktury do celów prania pieniędzy lub finansowania terroryzmu, a samo narazenie działalności przez organ zarządzający CASP na ryzyko prania pieniędzy jest obligatoryjną przesłanką odmowy udzielenia zezwolenia. Brak skutecznych procedur wewnętrznych w zakresie AML będzie natomiast obligatoryjną przesłanką cofnięcia zezwolenia. Ponadto obecny obowiązek stosowania procedur KYC od 1000 euro w przypadku niewystępowania żadnych podejrzeń w stosunku do klienta przeprowadzającego transakcję w przyszłości zostanie obniżony do 1 euro. To spowoduje obowiązek weryfikacji każdej operacji i tym samym korzystania ze środków bezpieczeństwa

⁵⁰ Wniosek o uzyskanie zezwolenia na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów będzie musiał zawierać przede wszystkim: opis procedury i systemu wykrywania nadużyć na rynku, opis zasad funkcjonowania platformy obrotu kryptoaktywami, opis systemów informatycznych i rozwiązań stosowanych przez dostawcę w zakresie bezpieczeństwa. Rejestr dostawców usług w zakresie kryptoaktywów będzie prowadzić Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (European Securities and Markets Authority, ESMA).

⁵¹ Jednocześnie w rozporządzeniu MiCA jest wskazane wprost, że pewne usługi mogą być świadczone tylko przez określone podmioty. Dotyczy to m.in. dokonania oferty publicznej lub ubiegania się o dopuszczenie do obrotu EMT, co może zostać dokonane wyłącznie przez instytucję kredytową lub instytucję pieniądza elektronicznego, która jednocześnie jest emitentem takiego tokena (art. 48 ust. 1 rozporządzenia MiCA). Podobnie instytucje kredytowe nie będą zobowiązane do uzyskania zezwolenia na ofertę publiczną lub ubieganie się o dopuszczenie do obrotu ART. Tak jak w przypadku licencji CASP, w tym zakresie instytucja kredytowa jest zobowiązana do sporządzenia dokumentu informacyjnego, odpowiedniej dokumentacji oraz do notyfikowania organowi nadzoru [pkt (44) preambuły i art. 17 rozporządzenia MiCA].

⁵² Poza wyjątkiem, gdy CASP prowadzący platformę obrotu będzie w stanie zidentyfikować posiadaczy kryptoaktywów i historię transakcji.

finansowego. W znacznym stopniu wpłynie to na anonimowość, szczególnie pod kątem wymiany kryptowalut na waluty fiat. Podmioty spoza UE co do zasady utracą możliwość oferowania usług z zakresu kryptowalut na terenie Unii. Na ten moment w rozporządzeniu MiCA nie ma natomiast odniesień do sytuacji podmiotów z Europejskiego Stowarzyszenia Wolnego Handlu (European Free Trade Association, EFTA) i Europejskiego Obszaru Gospodarczego (European Economic Area, EEA). Terytorialny zakres rozporządzenia MiCA jest jednak ograniczony w związku z dopuszczeniem wykonywania działalności objętej jego zakresem przez firmy z państw trzecich w modelu *reverse solicitation*, czyli z wyłącznej inicjatywy klienta⁵³.

Przepisy MiCA w obszarze, w którym wprowadzają transparentne regulacje przepływu kryptoaktywów, są postrzegane jako źródło podniesienia skuteczności sankcji. Należy jednak uwzględnić, że unijne rozporządzenie formalnie zacznie obowiązywać dopiero od 30 grudnia 2024 r., przy czym nawet do 1 lipca 2026 r. może trwać okres przejściowy, w którym CASPs będą mogli kontynuować świadczenie usług w sposób nieregulowany. Istotne jest, że rozporządzenie MiCA nie objęło wielu newralgicznych zagadnień⁵⁴, w tym związanych z sankcjami międzynarodowymi, co dotyczy w szczególności zdecentralizowanych finansów⁵⁵ oraz cyfrowego pieniądza banku centralnego (ang. Central Bank Digital Currency, CBDC)⁵⁶.

⁵³ Na podstawie utrwalonych interpretacji na gruncie m.in. regulacji *Dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE* (tzw. Markets in Financial Instruments Directive, MiFID II) model świadczenia usługi z wyłącznej inicjatywy klienta nie powinien jednak znaleźć zastosowania w sytuacjach: podejmowania akcji promocyjnych ukierunkowanych na dany rynek, stworzenia stałego modelu biznesowego opierającego się na *reverse solicitation*, aktywnego pozyskiwania usługoborców z innego państwa, posiadania przez usługodawcę strony internetowej z daną domeną krajową, a także inicjowania publikacji notek prasowych w portalach lub magazynach przeznaczonych dla danego rynku.

⁵⁴ MiCA nie odnosi się np. do tzw. tokenów zabezpieczających (ang. *security token*), które można uznać za zbywalne papiery wartościowe oraz do innych kryptoaktywów stanowiących instrumenty finansowe w rozumieniu MiFID II, jak również depozytów, pozycji sekurytyzacyjnych oraz produktów ubezpieczeniowych i emerytalnych. Podobnie rozporządzenie MiCA w najważniejszym zakresie nie obejmuje problematyki tokenów unikatowych (niewymiennych) – (ang. *non-fungible token*, NFT), chyba że replikują one instrument finansowy lub w przypadku których emitent tworzy „zbiór” aktywów do zakupu.

⁵⁵ Punkt (22) preambuły rozporządzenia MiCA statuuje wyłączenie stosowania przepisów rozporządzenia do usług w zakresie kryptoaktywów świadczonych w sposób w pełni zdecentralizowany bez pośredników. Niemniej rozporządzenie MiCA zawiera klauzule przeglądowe wynikające z art. 140 ust. 2 lit. t i art. 142 ust. 2 lit. a – w zakresie odnoszącym się do zdecentralizowanych finansów, które nakazują dokonywanie sprawozdawczości z oceny rozwoju DeFi na rynkach kryptoaktywów i odpowiedniego traktowania regulacyjnego zdecentralizowanych systemów kryptoaktywów, w tym ocenę konieczności i wykonalności regulacji zdecentralizowanego finansowania.

⁵⁶ Punkt (13) preambuły rozporządzenia MiCA precyzuje, że nie ma ono zastosowania do aktywów cyfrowych emitowanych przez banki centralne działające w charakterze organu kształtującego

Wraz z wejściem w życie rozporządzenia MiCA zacznie obowiązywać komplementarne z nim *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849* (dalej: rozporządzenie TFR). Wdraża ono zalecenia Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (Financial Action Task Force, FATF) dotyczące tzw. *travel rule*. W tym zakresie nastąpi rozszerzenie obowiązków monitorowania przez unijnych dostawców usług płatniczych (w tym CASPs) transferów zarówno środków pieniężnych, jak i kryptoaktywów, co będzie polegało na obowiązku podawania szczegółowych informacji na temat płatnika (inicjatora) i odbiorcy transakcji (beneficjenta). *Travel rule*, tak jak w przypadku MiCA, nie znajdzie jednak zastosowania w sytuacji, gdy inicjujący transakcję i beneficjent są dostawcami usług płatniczych lub CASPs działającymi we własnym imieniu, a także w transferach między osobami przeprowadzanymi bez udziału CASP (art. 2 ust. 4 rozporządzenia TFR)⁵⁷.

Luka sankcyjna zdecentralizowanych finansów

Jak zasygnalizowano wcześniej, pkt (22) preambuły rozporządzenia MiCA precyzuje, że w zakres regulacji nie wchodzi określone w rozporządzeniu usługi związane z kryptowalutami, gdy są świadczone w sposób w pełni zdecentralizowany, bez pośredników. Pomimo to kwestia DeFi budzi na gruncie rozporządzenia MiCA sporo wątpliwości. Pojawia się np. problem dotyczący świadczenia usług wymiany kryptowalut lub obsługi platform handlu nimi w ramach zdecentralizowanych giełd (tzw. DEX). Trudność sprawia bowiem rozstrzygnięcie, czym jest pełna decentralizacja w rozumieniu tego rozporządzenia. Dotyczy to specyfiki budowy sieci blockchain, która powoduje, że DeFi wykorzystuje hierarchiczną architekturę warstwową o różnych celach⁵⁸. Na gruncie rozporządzenia MiCA pozostaje

politykę pieniężną, co obejmuje także CBDC. Podobnie ramom unijnym nie podlegają powiązane usługi świadczone przez te banki centralne działające w charakterze władz monetarnych.

⁵⁷ Pierwszy wyjątek wynika bezpośrednio z faktu, że rozporządzenie TFR nie ma zastosowania do transferu środków pieniężnych, dla których płatnik i odbiorca są dostawcami usług płatniczych działającymi na własny rachunek (art. 2 ust. 4 lit. c rozporządzenia TFR). Drugi wyjątek wynika natomiast z zakresu określonego w art. 2 ust. 1 rozporządzenia TFR, tj. zastosowania wyłącznie do dostawców usług płatniczych, dostawców usług w zakresie kryptoaktywów lub pośredniczących dostawców usług płatniczych mających siedzibę w UE.

⁵⁸ Rozróżnia się trzy zasadnicze warstwy, tj. rozliczenia, protokołu oraz interfejsów. Warstwa rozliczenia (warstwa pierwsza) składa się z technologii rozproszonej księgi rachunkowej (DLT) i jej natywnego zasobu, zawierającego podstawowe zasady funkcjonowania ekosystemu. Warstwa protokołu (warstwa druga) obejmuje kompilator, zapewniając możliwość tworzenia interfejsów programowania

nierozstrzygnięte o jaki aspekt decentralizacji chodzi, ponieważ można mówić o niej w odniesieniu zarówno do warstwy rozliczenia (ang. *settlement layer*)⁵⁹, sposobu przechowywania kryptowalut, jak i do zarządzania organizacją i własnością protokołu. W związku z niedoprecyzowaniem tego zagadnienia w rozporządzeniu MiCA ocenę stopnia zdecentralizowania pozostawia się wyłącznemu uznaniu dostawcy usług kryptograficznych, który przez ten pryzmat ma dookreślić swój model biznesowy.

W obecnych uwarunkowaniach rozwoju technologicznego trudno sobie wyobrazić ustanowienie nad zdecentralizowanymi finansami ram regulacyjnych, które dawałyby realną możliwość ich egzekwowania. Przemawia za tym problem określenia właściwego porządku prawnego regulującego zasady dostępu do rynku i nadzoru, wynikający z dużego rozproszenia geograficznego użytkowników oraz z braku centralnych podmiotów odpowiedzialnych za świadczenie usług. Z uwagi na to rzeczywistą lukę w systemie sankcji międzynarodowych będą w przyszłości stanowić zdecentralizowane finanse, jako nowy model organizacji transferów finansowych bez żadnych pośredników, z automatyczną realizacją transakcji zawieranych za pomocą inteligentnych kontraktów (ang. *smart contracts*), będących protokołami, które działają w sieci blockchain.

DeFi, jako swoisty ekosystem zdecentralizowanych aplikacji finansowych opartych na tej technologii, oferuje możliwość zawierania szerokiego spektrum umów. System ten w istocie powiela istniejące modele usług finansowych z pominięciem ich scentralizowanych pośredników⁶⁰. W efekcie w ramach DeFi użytkownicy zachowują pełną kontrolę nad swoimi aktywami w drodze synergii z ekosystemem przez zdecentralizowane aplikacje typu P2P. Aplikacje te nie potrzebują również podmiotów rozstrzygających ewentualne spory⁶¹, gdyż wstępnie określony

aplikacji. Interfejs programowania aplikacji (ang. *application programming interface*, API) to zbiór definicji i protokołów do budowania i integrowania oprogramowania aplikacyjnego. W warstwie interfejsów (warstwa trzecia) są tworzone aplikacje zorientowane na użytkownika, umożliwiające interakcję z aplikacją za pośrednictwem strony internetowej. Zob. G. Maia, J. Vieira dos Santos, *MiCA and DeFi („Proposal for a Regulation on Market in Cryptoassets” and „Decentralised Finance”)*, „Revista Electrónica de Direito” 2022, t. 28, nr 2, s. 63–65.

⁵⁹ W tej warstwie sieć węzłów niepolegająca na centralnym serwerze lub centralnej organizacji składa się z niewymagającego uprawnień blockchaina przez połączenia P2P pomiędzy niepowiązаныmi i niezależnymi agentami.

⁶⁰ E. Avgouleas, A. Seretakis, *How Should Crypto Lending Be Regulated Under EU Law?*, „European Business Organization Law Review” 2023, t. 24, z. 3, s. 423–424. <https://doi.org/10.1007/s40804-023-00293-3>.

⁶¹ Poprzez podejście probabilistyczne blockchain rozwiązał kwestię uzgadniania rozważaną w teorii gier, kryptografii oraz teorii systemów rozproszonych, określoną w 1980 r. przez Marshalla Pease’a, Leslie Lamporta i Roberta Shostaka jako problem generałów bizantyjskich. Zob. M. Pease, L. Lamport, R. Shostak, *The Byzantine Generals Problem*, „ACM Transactions on Programming Languages and Systems” 1982, t. 4, z. 3, s. 382–401. <https://doi.org/10.1145/357172.357176>.

kod dokona tego samodzielnie w przewidywalnych sytuacjach, jako tzw. *Lex Cryptographia*⁶², a więc zgodnie z zasadami regulowanymi przez samowykonujące się inteligentne kontrakty i zdecentralizowane (autonomiczne) organizacje⁶³. Z akceptacją idei „kod jest prawem” (ang. *code is law*) wiąże się jednak skutek w postaci wypierania przez technologię państwowych systemów prawnych⁶⁴.

Przy analizie problematyki inteligentnego kontraktu należy odnieść się do pierwotnej definicji tego pojęcia zaproponowanej przez Nicka Szabo, który określił go jako skomputeryzowany protokół transakcyjny, automatycznie realizujący warunki umowy. Celami projektowania są: spełnienie typowych warunków umownych, zminimalizowanie występowania wyjątków (zarówno złośliwych, jak i przypadkowych) oraz eliminacja jakichkolwiek zaufanych pośredników⁶⁵. Idea ta opiera się bowiem na wykluczeniu potrzeby istnienia zaufania między stronami w związku ze zwiększeniem pewności wykonania umowy, zgodnie z tym, jak została ona zaprojektowana, wskutek gwarancji niezmienności kontraktu (kodu). W efekcie z ekonomicznego punktu widzenia redukuje się mentalne i obliczeniowe koszty dodatkowe, obniżając straty związane z potencjalnymi oszustwami, kosztami arbitrażu i egzekucji oraz kosztami transakcyjnymi.

Aktualnie termin „inteligentny kontrakt” definiuje się jako kod wdrożeniowy działający w środowisku blockchain⁶⁶. W tym sensie jest to kod algorytmiczny w programie komputerowym, wpisany oraz opierający się na danych w blockchainie⁶⁷.

⁶² Blockchain w istotny sposób zmienia sposób rozumienia prawa przez oderwanie go od potrzeby istnienia jakiegokolwiek oparcia kulturowego czy legitymizacji autorytetem państwa. Według Katrin Becker blockchain oddziela pojęcie prawa od trzech kluczowych wymiarów, jakim są terytorium, język (i związana z tym interpretacja) oraz materia. Zob. K. Becker, *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, „Law and Critique” 2022, t. 33, s. 113–130. <https://doi.org/10.1007/s10978-021-09317-8>.

⁶³ A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, preprint, SSRN, 12 III 2015 r., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, s. 4 [dostęp: 5 III 2024]. <http://dx.doi.org/10.2139/ssrn.2580664>.

⁶⁴ D.A. Zetsche, D.W. Arner, R.P. Buckley, *Decentralized Finance*, „Journal of Financial Regulation” 2020, t. 6, z. 2, s. 184. <https://doi.org/10.1093/jfr/fjaa010>.

⁶⁵ N. Szabo, *Smart Contracts*, 1994 r., <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> [dostęp: 5 III 2024]; tenże, *Smart Contracts: Building Blocks for Digital Markets*, 1996 r., https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [dostęp: 5 III 2024].

⁶⁶ V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014 r., https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [dostęp: 5 III 2024].

⁶⁷ R. Wilkens, R. Falk, *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019, s. 3–4.

Wszelkie zobowiązania w inteligentnych kontraktach pozostają zgodne z klasyczną logiką Boole'a⁶⁸, stanowiącą podstawę całego przetwarzania cyfrowego, tj. „jeżeli-to” (ang. *if this then that*, IFTTT).

W kontekście sankcji międzynarodowych istotnym zagrożeniem dla ich realnej skuteczności jest możliwość dokonania agregacji wielu kontraktów przez stworzenie aplikacji o zaawansowanych funkcjonalnościach. Przykładami mogą być platformy pożyczkowe⁶⁹, pule płynności⁷⁰, platformy mediów społecznych czy rozproszone systemy zarządzania aktywami (tzw. *decentralised autonomous organisations*). Należy podkreślić, że inteligentne kontrakty wymykają się regulacjom prawnym rozporządzenia MiCA, nie są także definiowane w polskim ustawodawstwie oraz w innych reżimach prawnych. Oczywiście można przyjąć, że konstrukcja tych kontraktów przypomina specyficzny rodzaj zautomatyzowanego depozytu (ang. *escrow*) lub elektronicznego weksla. W sensie prawnym inteligentny kontrakt mógłby być traktowany jako szczególna forma umowy, ale wyłącznie przy założeniu, że jego zawarcie oparto by na świadomym oświadczeniu woli stron, że chcą one między sobą zawrzeć umowę o określonej treści⁷¹. Tą treścią mógłby być co do zasady kod zamieszczony na blockchainie. Wywołanie funkcji kodu na łańcuchu bloków stanowiłoby złożenie

⁶⁸ George Boole w 1854 r. stworzył tzw. algebrę Boole'a – strukturę matematyczną złożoną z trzech działań binarnych: \vee (lub, or, alternatywa) – działanie podobne jak dodawanie; \wedge (i, and, koniunkcja) – odpowiednik mnożenia; \sim (nie, not, zaprzeczenie logiczne) oraz wyróżnionych elementów 0 (fałsz), 1 (prawda). Zob. S. Givant, P. Halmos, *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009, s. 8–9.

⁶⁹ Środki pożyczane na platformach pożyczkowych są zapewniane przez samych użytkowników, w konsekwencji dostarczanie środków tego rodzaju usługom to *staking* w obrębie tej samej platformy. Przykładem jest projekt MakerDAO umożliwiający posiadaczom Ethereum (ETH) pożyczanie między członkami społeczności pieniędzy w postaci stablecoina DAI (starającego się utrzymać wartość 1:1 do dolara amerykańskiego). System polega na blokowaniu pewnej ilości ETH w inteligentnych kontraktach, co pozwala inwestorom wybijać nowe DAI i tym samym ustanawiać zabezpieczenie pożyczek. Po spłacie zadłużenia wraz z odsetkami następuje odblokowanie ETH. W sytuacji jednak, gdy wartość ETH spadnie poniżej kwoty pożyczonej w DAI, następuje likwidacja pożyczki poprzez sprzedaż ETH w celu spłaty pożyczonego DAI. Sama groźba likwidacji odstrasza od zaciągania nadmiernych pożyczek. W przypadku bowiem, gdy cena ETH gwałtownie spada, likwiduje się pożyczki w DAI, a wówczas posiadacze tokenów Maker (MKR) są pożyczkodawcami ostatniej szansy. MKR jest tworzony i sprzedawany w celu spłaty pożyczek, są w nich również uiszczane wszystkie opłaty w ramach MakerDAO. Kary likwidacyjne natomiast wykorzystuje się na odkup MKR, które następnie ulegają spalaniu.

⁷⁰ Pule płynności (ang. *liquidity pools*) to zbiór środków zablokowanych na inteligentnym kontrakcie, będących podstawą zdecentralizowanych giełd (DEX), takich jak Uniswap, które wykorzystują inteligentne kontrakty dla ułatwienia transakcji.

⁷¹ Artykuł 60 *Ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny*.

dyspozycji generującej realizację umowy. Uznanie jednak inteligentnego kontraktu za umowę w rozumieniu prawa cywilnego oznaczałoby przyjęcie, że rzeczywiście doszło do w pełni świadomego złożenia oświadczenia woli. Spełnienie tego warunku wymagałoby samodzielnego tworzenia kodu przez strony inteligentnego kontraktu albo przynajmniej posiadania przez nie zdolności jego odczytania, czyli znajomości języka programowania, w którym ten inteligentny kontrakt został zakodowany⁷². Powstaje wątpliwość, czy w przypadku złożenia oświadczenia w formie kodu jest w ogóle możliwe przypisanie waloru świadomego oświadczenia woli co do treści umowy. Hipotetycznie taki problem mógłby zostać pominięty w sytuacji, gdyby inteligentny kontrakt był przedmiotem wcześniejszych negocjacji, których ustalenia zostałyby spisane w języku naturalnym, a dopiero następnie zakodowane w inteligentnym kontrakcie. Wówczas kod można byłoby potraktować wyłącznie w kategoriach narzędzia realizującego zobowiązania umowne, a nie podstawy powstania tych zobowiązań. Nie istnieje jednak żaden wymóg sporządzania inteligentnego kontraktu w języku naturalnym. Ponadto zdefiniowanie wszystkich elementów w samym kodzie automatycznie stanowi gwarancję zachowania pełnej anonimowości stron inteligentnego kontraktu.

Cyfrowy rubel – scentralizowana kryptowaluta

Kolejnym czynnikiem związanym z kryptowalutami i technologią blockchain, który może wpływać na osłabienie systemu sankcji finansowych, jest rozwój cyfrowego pieniądza banku centralnego (ang. Central Bank Digital Currency, CBDC). Bank Rozrachunków Międzynarodowych definiuje CBDC jako (...) *cyfrowy instrument płatniczy denominowany w krajowej jednostce rozliczeniowej, stanowiący bezpośrednio zobowiązanie banku centralnego*⁷³.

Z dniem 1 sierpnia 2023 r. weszły w życie przepisy ustawy federalnej nr 339-FZ „Zmieniającej w art. 128 i 140 części pierwszej, części drugiej oraz art. 1128 i 1174 części trzeciej Kodeksu cywilnego Federacji Rosyjskiej” oraz ustawy federalnej nr 340-FZ „Zmieniającej niektóre akty prawne Federacji Rosyjskiej”. Regulacje te ukonstytuowały rubla cyfrowego opartego na blockchainie jako nową walutę narodową FR. Przepisy te określiły zasady wprowadzenia go do obiegu oraz warunki zastosowania w rozliczeniach. Dookreślono również uprawnienia CBFR jako operatora

⁷² Obecnie najbardziej znaczącą platformą dla wdrażania inteligentnych kontraktów jest Ethereum, który implementuje kompletny język programowania Turinga pod nazwą Solidity.

⁷³ *Central bank digital currencies: foundational principles and core features*, Bank for International Settlements, 2020 r., <https://www.bis.org/publ/othp33.pdf>, s. 3 [dostęp: 5 III 2024].

jego platformy, a także rolę instytucji kredytowych przy przeprowadzaniu transakcji przez klientów oraz podstawy organizacyjne wykorzystania rubla cyfrowego przez osoby fizyczne i prawne jako nowej metody płatności, w tym w operacjach dokonywanych na rzecz cudzoziemców.

Do 31 grudnia 2024 r. Rada Dyrektorów CBFR wraz z Federalną Służbą Monitoringu Finansowego Federacji Rosyjskiej (Федеральная служба по финансовому мониторингу, Rosfinmonitoring) muszą określić zakres użytkowników platformy cyfrowego rubla, którzy będą uprawnieni do przeprowadzania transakcji rublami cyfrowymi na platformie, a także listę dopuszczalnych rodzajów transakcji oraz wartości progowe kwot dla takich operacji. Zgodnie z pierwotnymi założeniami możliwość dostępu do platformy cyfrowego rubla stwarza konieczność otwarcia cyfrowego konta rubla, będącego nowym rodzajem rachunku bankowego. Stronami umowy rachunku cyfrowego w rublu będą użytkownik i CBFR, a instytucja finansowa, w której użytkownik posiada klasyczny rachunek bankowy, będzie pośrednikiem reprezentującym CBFR w jego relacjach z użytkownikiem w celu korzystania z platformy cyfrowego rubla. Rosja powieła więc w tym zakresie pozytywne doświadczenia chińskie związane z wdrażaniem cyfrowego yuana (e-CNY).

Różnica między kryptowalutami a cyfrowymi walutami narodowymi jest fundamentalna. CBDC może przypominać tzw. stablecoin – cyfrową walutę (tokena płatniczego), której wartość jest powiązana ze stabilnym aktywem rezerwowym pozostającym w obrocie (np. walutą fiat lub złotem). CBDC, podobnie jak stablecoin, a w odróżnieniu od altcoina, podlega (przynajmniej teoretycznie) marginalnym wahaniom wartości. Najważniejsza różnica polega na tym, że CBDC jest, w przeciwieństwie do kryptowalut, prawnym środkiem płatniczym w kraju emisji, wspieranym przez rząd⁷⁴. Scentralizowane cyfrowe waluty narodowe, zarządzane przez narodowe banki centralne, nie mogą jednak zapewnić użytkownikom pełnej anonimowości. O ile bowiem obie strony transakcji zachowują anonimowość w relacji zewnętrznej, o tyle nie będą już anonimowe z punktu widzenia banku centralnego, co da władzom możliwość pełnego monitoringu przepływów finansowych w czasie rzeczywistym⁷⁵.

⁷⁴ Z uwagi na swoją specyfikę stablecoiny, co do zasady, mogłyby spełnić wymogi definicji pieniądza elektronicznego ustanowione w ustawie o usługach płatniczych.

⁷⁵ Taki wariant dotyczy modelu opartego na rachunku, w którym zatwierdzenie transakcji przez zleceniodawcę i beneficjenta następuje na podstawie weryfikacji tożsamości użytkowników, gdyż ich transakcje są przypisywane do rachunków opartych na tożsamości. Inne rozwiązanie to CBDC bazujący na tokenach, gdzie transakcja zostaje zatwierdzona przez zleceniodawcę i beneficjenta na podstawie pary kluczy publiczno-prywatnych oraz podpisów cyfrowych. Taki system nie wymaga dostępu do tożsamości użytkownika, co zapewnia mu wysoki poziom prywatności. Zob. *Central Bank Digital Currencies. Building Block of the Future of Value Transfer*, Deloitte, <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf> [dostęp: 5 III 2024].

Z perspektywy państwa CBDC dostarcza nowych narzędzi polityki monetarnej i może być skutecznym instrumentem wpływu m.in. na dynamikę podaży pieniądza w gospodarce. Najważniejszym celem wdrażania tego instrumentu w kontekście obsługi wymiany transgranicznej jest oczekiwanie przełamania dominacji dolara w rozliczeniach handlowych. Należy zauważyć, że pełne wdrożenie cyfrowego rubla obejmuje plany uruchomienia platformy rozliczeń transgranicznych w ramach przestrzeni postradzieckiej Euroazjatyckiej Unii Gospodarczej i Wspólnoty Niepodległych Państw, a także w odniesieniu do krajów BRICS⁷⁶. W konsekwencji rozwój CBDCs z perspektywy tych państw może znacząco przyczynić się do marginalizacji znaczenia zachodnich sankcji międzynarodowych w związku z uzyskaniem przez te państwa zdolności do dokonywania płatności bez udziału zagranicznych banków komercyjnych i infrastruktury finansowej takiej jak SWIFT⁷⁷. To właśnie banki komercyjne są kluczowym ogniwem egzekwowania zachodnich sankcji, nie tylko z powodu uprawnień tych banków, lecz także ze względu na ponoszenie przez nie odpowiedzialności za blokowanie transakcji z udziałem podmiotów objętych sankcjami. Z uwagi przede wszystkim na amerykańskie sankcje nawet instytucje w krajach formalnie ich niestosujących, w przypadku wystąpienia elementu dolarowego lub innego łącznika amerykańskiego, muszą podchodzić z dużą ostrożnością do transakcji ze stroną rosyjską w związku z obawą nałożenia na te instytucje wtórnych sankcji.

W tym kontekście cyfrowy rubel w przyszłości mógłby umożliwić płatności transgraniczne bez konieczności korzystania z systemu bankowego innych krajów, dzięki obsłudze transakcji odbywającej się wyłącznie za pośrednictwem platformy cyfrowego rubla CBFR.

⁷⁶ BRICS jest formą współpracy państw o charakterze polityczno-gospodarczym. Pierwotnie grupa obejmowała Brazylię, Rosję, Indie i Chiny, a od 2011 r. także Republikę Południowej Afryki. Od stycznia 2024 r. miała ona poszerzyć swój skład o kolejne państwa, tj. Argentynę, Egipt, Etiopię, Arabię Saudyjską, Iran oraz Zjednoczone Emiraty Arabskie. Według oficjalnego przekazu ostatecznie Argentyna odstąpiła od planu przystąpienia do grupy, w przypadku Arabii Saudyjskiej natomiast nadal oficjalnie nie potwierdzono jej członkostwa. Główny cel tej grupy to stworzenie nowego systemu walutowego. Zob. BRICS Information Portal, <http://infobrics.org/> [dostęp: 5 III 2024]; K. Karwowski, *Jeden statek – różni kapitanowie. Grupa BRICS po rozszerzeniu*, Instytut Nowej Europy, 20 III 2024 r., <https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/> [dostęp: 26 III 2024].

⁷⁷ K. Izenman, *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021 r., <https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions> [dostęp: 5 III 2024].

Wnioski

Kazus rosyjski dobrze obrazuje problem oceny skuteczności sankcji gospodarczych. Przy założeniu, że ich celem jest dyscyplinowanie i ukaranie krajów⁷⁸, na które są one nakładane, należałoby uznać, że sankcje zastosowane wobec FR spełniają swoją funkcję. Bezsprzecznie wpływają negatywnie na rosyjską gospodarkę i jej system finansowy, ograniczają władzom dostępne wybory gospodarcze i polityczne, co powoduje większą centralizację gospodarki i uzależnienie od dostępnych partnerów handlowych. Z perspektywy pierwotnego i podstawowego celu, jakim było doprowadzenie do zaniechania przez FR ofensywy wojskowej w Ukrainie, zastosowane sankcje nie przyniosły jednak oczekiwanego rezultatu. Pojawia się także zasadniczy problem, że narastającym skutkiem sankcji gospodarczych, negatywnie odbijającym się na wzroście gospodarczym i zdolnościach inwestycyjnych tego kraju, towarzyszy naturalna tendencja tworzenia się odporności na nie, ponieważ kształtują się możliwości ich skutecznego obchodzenia.

Przedstawiona analiza potwierdza wskazaną na wstępie wątpliwość dotyczącą realnej skuteczności sankcji w perspektywie rozwoju innowacyjnych instrumentów finansowych. W tym kontekście niewłaściwe byłoby niedostrzeganie rosnącego potencjału zasobów cyfrowych, w szczególności w wariacie DeFi oraz ich specyficznej odmiany w postaci walut cyfrowych banków centralnych. Te instrumenty w bliskiej przyszłości mogą pozwolić na stworzenie nowych, alternatywnych kanałów przepływów finansowych, niezależnych od obecnie istniejących zachodnich systemów płatności. Ich dalszy rozwój może wykreować bezsankcyjną przestrzeń transakcji finansowych i spowodować, że skutki ewentualnie nakładanych sankcji, zarówno w wymiarze finansowym, jak i handlowym, będą nieść za sobą wyłącznie lub w przeważającym zakresie negatywne skutki dla państw je stosujących. To, co teraz stanowi niszę i w marginalnym stopniu pozwala na uchylanie się przed egzekucją sankcji międzynarodowych, w nieodległym czasie może stać się potężnym narzędziem kształtującym nowy porządek międzynarodowy. Stanie się to wyzwaniem nie tylko dla systemów nadzoru rynków finansowych, lecz także dla podmiotów odpowiedzialnych za przeciwdziałanie zjawiskom prania pieniędzy i finansowania terroryzmu.

Niestety nie można jednoznacznie odpowiedzieć na pytanie, jakie środki prawne w pełni wyeliminowałyby istnienie luk w systemie finansowych sankcji międzynarodowych, w szczególności w odniesieniu do kazusu dużych światowych gospodarek, a także w perspektywie dalszego rozwoju możliwości wykorzystania

⁷⁸ J. Field, *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023 r., <https://coingeek.com/sanctions-russia-and-crypto-crime/> [dostęp: 5 III 2024].

technologii blockchain. Utopijne jest również oczekiwanie uzyskania międzynarodowej jednorodności decyzyjnej zarówno w sprawie objęcia danego państwa środkami prewencyjnymi, jak i co do tożsamości skali i rodzaju stosowanych sankcji. Niemniej w przypadku krajów UE postulatem powinno być właściwe i sprawne wdrożenie rozporządzenia MiCA, przy dążeniu do jasnego doprecyzowania zakresu definicji legalnej pojęcia tzw. pełnej decentralizacji. Chodzi przede wszystkim o uniknięcie sytuacji, w której działalność zdecentralizowana bezpodstawnie wyłączałyby się ramom regulacyjnym bądź też zostałyby stworzona przestrzeń uznaniowości regulatorów co do jej klasyfikacji. Tym samym w odniesieniu do zdecentralizowanych finansów *condicio sine qua non* pozostaje wypracowanie podstawowego mechanizmu klasyfikacji (taksonomii) dla tego pojęcia na poziomie wszystkich krajów członkowskich oraz szerzej – w skali globalnej⁷⁹.

Bibliografia

Avgouleas E., Seretakis A., *How Should Crypto Lending Be Regulated Under EU Law?*, „European Business Organization Law Review” 2023, t. 24, z. 3, s. 421–438. <https://doi.org/10.1007/s40804-023-00293-3>.

Becker K., *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, „Law and Critique” 2022, t. 33, s. 113–130. <https://doi.org/10.1007/s10978-021-09317-8>.

Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne*, Warszawa 2003.

Demarais A., *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022.

Givant S., Halmos P., *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009.

Hufbauer G.C. i in., *Economic Sanctions Reconsidered: Supplemental case histories*, Washington 2007.

Maia G., Vieira dos Santos J., *MiCA and DeFi* („Proposal for a Regulation on Market in Cryptoassets” and „Decentralised Finance”), „Revista Electrónica de Direito” 2022, t. 28, nr 2, s. 57–82.

⁷⁹ Potrzebę wprowadzenia jednolitej systematyki dla DeFi i zasobów cyfrowych (ang. *digital assets*) zasygnalizowano m.in. w dokumencie: *Decentralised Finance – Principles for building a robust digital economy*, AFME, 6 VI 2023 r., <https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf> [dostęp: 5 III 2024].

Opalek K., Wróblewski J., *Prawo. Metodologia, filozofia, teoria prawa*, Warszawa 1991.

Opalek K., Wróblewski J., *Zagadnienia teorii prawa*, Warszawa 1969.

Pape R.A., *Why Economic Sanctions Do Not Work*, „International Security” 1997, t. 22, nr 2, s. 90–136.

Pease M., Lamport L., Shostak R., *The Byzantine Generals Problem*, „ACM Transactions on Programming Languages and Systems” 1982, t. 4, z. 3, s. 382–401. <https://doi.org/10.1145/357172.357176>.

Wilkens R., Falk R., *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019.

Zetsche D.A., Arner D.W., Buckley R.P., *Decentralized Finance*, „Journal of Financial Regulation” 2020, t. 6, z. 2, s. 172–203. <https://doi.org/10.1093/jfr/fjaa010>.

Źródła internetowe

Annual value of international reserves of Russia from 2012 to 2022, by type, Statista, <https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/> [dostęp: 5 III 2024].

Bank of Russia foreign exchange and gold asset management report, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [dostęp: 5 III 2024].

Bitcoin Mining Map, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [dostęp: 5 III 2024].

BRICS Information Portal, <http://infobrics.org/> [dostęp: 5 III 2024].

Busch K.E., Tierno P., *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022 r., <https://crsreports.congress.gov/product/pdf/IN/IN11920> [dostęp: 5 III 2024].

Buterin V., *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014 r., https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [dostęp: 5 III 2024].

Central Bank Digital Currencies. Building Block of the Future of Value Transfer, Deloitte, <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf> [dostęp: 5 III 2024].

Central bank digital currencies: foundational principles and core features, Bank for International Settlements, 2020 r., <https://www.bis.org/publ/othp33.pdf> [dostęp: 5 III 2024].

Cryptocurrencies: a way to evade sanctions?, BAFFI – Centre on Economics, Finance and Regulation, <https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-eva-de-sanctions> [dostęp: 5 III 2024].

Crypto-assets relevant pro-vision: Article 5b(2) of Council Regulation (EU) No 833/2014 – frequently asked questions, UE, 21 III 2023 r., https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 5 III 2024].

Decentralised Finance – Principles for building a robust digital economy, AFME, 6 VI 2023 r., <https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf> [dostęp: 5 III 2024].

Field J., *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023 r., <https://coingeek.com/sanctions-russia-and-crypto-crime/> [dostęp: 5 III 2024].

Izenman K., *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021 r., <https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions> [dostęp: 5 III 2024].

Karwowski K., *Jeden statek – różni kapitanowie. Grupa BRICS po rozszerzeniu*, Instytut Nowej Europy, 20 III 2024 r., <https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/> [dostęp: 26 III 2024].

Komunikat prasowy Komisji Europejskiej: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022 r., https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [dostęp: 5 III 2024].

Leali G., *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022 r., <https://www.politico.eu/article/Frances-le-maire-not-against-cutting-russia-out-of-swift/> [dostęp: 5 III 2024].

Pape R.A., wpis na portalu LinkedIn, https://uk.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [dostęp: 5 III 2024].

Pismennaya E., *Russia Values Local Crypto at \$200 Billion as Rules Near*, Bloomberg, 1 II 2022 r., <https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg> [dostęp: 5 III 2024].

Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine, Ministry of Foreign Affairs Singapore, 5 III 2022 r., <https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions/> [dostęp: 5 III 2024].

Szabo N., *Smart Contracts*, <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> [dostęp: 5 III 2024].

Szabo N., *Smart Contracts: Building Blocks for Digital Markets*, 1996 r., https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [dostęp: 5 III 2024].

Wilson T., *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022 r., <https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/> [dostęp: 5 III 2024].

Wiśniewska I., *Rosyjska gospodarka w roku 2022. Adaptacja i rosnący deficyt budżetu*, OSW, 16 II 2023 r., <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-02-16/rosyjska-gospodarka-w-roku-2022-adaptacja-i-rosnacy-deficyt> [dostęp: 5 III 2024].

Wpływ sankcji na rosyjską gospodarkę, Rada UE, <https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/> [dostęp: 5 III 2024].

Wright A., De Filippi P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, preprint, SSRN, 12 III 2015 r., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [dostęp: 5 III 2024]. <http://dx.doi.org/10.2139/ssrn.2580664>.

Wright C.S., *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019 r., <https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/> [dostęp: 5 III 2024].

Rosyjskie źródła internetowe

В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT, Известия, 3 VII 2023 r., <https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossijskogo-trafika-u-natsionalnogo-analoga-swift> [dostęp: 5 III 2024].

ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года, RBC.ru, 10 X 2023 r., <https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430> [dostęp: 5 III 2024].

Российский аналог SWIFT распространяется на Восток, News.Ru, 27 I 2024 r., <https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie> [dostęp: 5 III 2024].

Akty prawne

Rozporządzenie Rady (UE) 2024/745 z dnia 23 lutego 2024 r. zmieniające rozporządzenie (UE) nr 833/2014 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L z 23 II 2024 r.).

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 150/40 z 9 VI 2023 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (Dz. Urz. UE L 150/1 z 9 VI 2023 r.).

Rozporządzenie Rady (UE) 2022/1904 z dnia 6 października 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 259/3 z 6 X 2022 r.).

Rozporządzenie Rady (UE) 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 111/1 z 8 IV 2022 r., ze zm.).

Rozporządzenie Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 229/1 z 31 VII 2014 r., ze zm.).

Rozporządzenie Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78/6 z 17 III 2014 r., ze zm.).

Rozporządzenie Rady (UE) nr 359/2011 z dnia 12 kwietnia 2011 r. dotyczące środków ograniczających skierowanych przeciwko niektórym osobom, podmiotom i organom w związku z sytuacją w Iranie (Dz. Urz. UE L 100/1 z 14 IV 2011 r., ze zm.).

Rozporządzenie Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczące środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134/1 z 20 V 2006 r., ze zm.).

Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. DzU z 2023 r. poz. 1497, ze zm.).

Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. DzU z 2023 r. poz. 221, ze zm.).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. DzU z 2023 r. poz. 1124, ze zm.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. DzU z 2022 r. poz. 2360, ze zm.).

Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. DzU z 2023 r. poz. 753, ze zm.).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. DzU z 2023 r. poz. 1610, ze zm.).

Rosyjskie akty prawne

Федеральный закон от 31.07.2020 № 259-ФЗ „О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации”, Kremlin.ru, <http://www.kremlin.ru/acts/bank/45766/page/1> [dostęp: 5 III 2024].

Федеральный закон от 14.07.2022 № 331-ФЗ „О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений статьи 5.1 Федерального закона «О банках и банковской деятельности»”, <http://publication.pravo.gov.ru/Document/View/0001202207140083?index=1> [dostęp: 5 III 2024].

Федеральный закон от 24.07.2023 № 339-ФЗ „О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации”, <http://publication.pravo.gov.ru/document/0001202307240009> [dostęp: 5 III 2024].

Федеральный закон от 24.07.2023 № 340-ФЗ „О внесении изменений в отдельные законодательные акты Российской Федерации”, <http://publication.pravo.gov.ru/Document/View/0001202307240024> [dostęp: 5 III 2024].

Angela Pacholczak

Absolwentka studiów doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego.

Kontakt: angelapacholczak@gmail.com