

DOMINIKA GAŁUS

Studentka V roku prawa, członkini Koła Naukowego Prawa Bankowego
oraz Centrum Badań nad Prawnymi Aspektami Technologii Blockchain
Wydział Prawa i Administracji, Uniwersytet Warszawski

Wykorzystanie technologii *blockchain* w zakresie przechowywania dokumentów na gruncie prawa bankowego

Wprowadzenie

W ostatnich latach coraz większym zainteresowaniem ze strony banków oraz instytucji finansowych cieszą się rozwiązania oparte na wykorzystaniu nowych technologii. Skutkuje to z jednej strony pojawianiem się coraz większej liczby start-upów, które oferują innowacyjne rozwiązania w zakresie usług dotyczących sektora finansowego, z drugiej zaś coraz większym zainteresowaniem (czy wręcz koniecznością) wdrażania nowych technologii w obszary tradycyjnej działalności banków – zarówno w formie wyodrębniania wewnątrz banków departamentów odpowiedzialnych za opracowanie i wprowadzenie innowacyjnych rozwiązań w działalność banku, jak i poprzez podejmowanie współpracy ze start-upami oferującymi wdrożenie opracowanych przez nie innowacji. Elementem innowacyjności w świecie instytucji finansowych,

który staje się coraz bardziej znany i implementowany do operacji mających miejsce na rynku finansowym, jest technologia *blockchain*.

Zainteresowanie nowymi technologiami (w tym rozwiązaniami wykorzystującymi technologię *blockchain*) nie ogranicza się jedynie do przedsiębiorców, ale w równym stopniu odnosi się także do instytucji finansowych, takich jak Krajowy Depozyt Papierów Wartościowych SA¹. Wpływ nowoczesnych technologii na rynek finansowy przejawia się również w działaniach podejmowanych przez Komisję Nadzoru Finansowego (KNF), która zintensyfikowała działania mające na celu tworzenie środowiska regulacyjnego i nadzorczego sprzyjającego funkcjonowaniu FinTechów² oraz podmiotów chcących wprowadzić innowacyjne produkty na polski rynek finansowy³. Komisja Nadzoru Finansowego planuje także rozpoczęcie nowych inicjatyw w zakresie wsparcia rozwoju technologii *blockchain* oraz DLT (*Distributed Ledger Technology* – technologia rozproszonych rejestrów) w formie nawiązywania strategicznych partnerstw skupiających się na testowaniu nowych produktów i usług, wykorzystaniu omawianych technologii w ramach SupTech oraz RegTech (kolejno – stosowania innowacji w zakresie nadzoru oraz regulacji rynku finansowego). Całkowicie nowym pomysłem jest utworzenie piaskownicy z zakresu technologii rozproszonych rejestrów, a w jej ramach tzw. *eVoting* oraz trwałego nośnika⁴.

Przejawy innowacyjnego entuzjazmu dostrzegalne są również w nowelizowanych oraz nowo wprowadzanych aktach prawnych,

¹ W tym kontekście warto wspomnieć o inicjatywie Krajowego Depozytu Papierów Wartościowych SA w zakresie wprowadzenia usługi zdalnego udziału i głosowania na walnych zgromadzeniach spółek (które przewidywały możliwość wykorzystania takiej opcji) za pośrednictwem aplikacji *eVoting*, uruchomionej w ramach Platformy Blockchain dla Rynku Kapitałowego; por. szerzej: KDPW, *Platforma Blockchain dla Rynku Kapitałowego* <<https://blockchain.kdpw.pl/>> [dostęp: 30.03.2020].

² Rozumianych jako innowacyjne technologie finansowe.

³ Komisja Nadzoru Finansowego, *Cyfrowa Agenda Nadzoru – plan działań Urzędu KNF w zakresie m.in. nowoczesnych technologii, innowacji oraz cyberbezpieczeństwa* <https://www.knf.gov.pl/knf/pl/komponenty/img/Cyfrowa_agenda_nadzoru_68264.pdf> [dostęp: 30.03.2020].

⁴ R. Tomaszewski, *FinTech 2020. Plany KNF i podsumowanie działalności Innovation Hub* <<https://fintek.pl/fintech-2020-plan-y-knf-i-podsumowanie-dzialalnosci-innovation-hub/>> [dostęp: 30.03.2020].

na podstawie których podmioty funkcjonujące w gospodarce uprawnione są do stosowania innowacyjnych rozwiązań. Tak jest np. na gruncie przepisów dotyczących prostej spółki akcyjnej czy aktu wydanego na podstawie upoważnienia wynikającego z art. 7 ust. 4 Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe⁵. Rozporządzenie Rady Ministrów z dnia 9 marca 2020 r. w sprawie dokumentów związanych z czynnościami bankowymi, sporządzanych na informatycznych nośnikach danych⁶ dotyczy bowiem tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania, w tym przy zastosowaniu podpisu elektronicznego dokumentów, o których mowa w art. 7 ust. 2 Prawa bankowego. Rozporządzenie to ma na celu zagwarantowanie bezpieczeństwa obrotu oraz ochrony interesów banków i ich klientów i ma wejść w życie w dniu 19 września 2020 r. Wprowadzenie nowych regulacji wynika z konieczności dostosowania rozwiązań stosowanych na gruncie polskich przepisów do treści Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania⁷, a ponadto zostało wykorzystane przez prawodawcę w zakresie zaakcentowania jego proinnowacyjnej orientacji poprzez wyraźne wskazanie w treści art. 5 ust. 2 Rozporządzenia, że dokumenty związane z czynnościami bankowymi mogą być przechowywane w formie rozproszonej i zdecentralizowanej bazy danych.

1. Pojęcie trwałego nośnika

W ramach Ustawy z dnia 1 marca 2018 r. o zmianie ustawy o obrocie instrumentami finansowymi oraz niektórych innych ustaw⁸

⁵ T.j. Dz.U. z 2020 r., poz. 321 ze zm., dalej: Prawo bankowe.

⁶ Rozporządzenie Rady Ministrów z dnia 9 marca 2020 r. w sprawie dokumentów związanych z czynnościami bankowymi, sporządzanych na informatycznych nośnikach danych (Dz.U. z 2020 r., poz. 476), dalej: Rozporządzenie.

⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającą dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z dnia 28 sierpnia 2014 r., s. 73–114).

⁸ T.j. Dz.U. z 2018 r., poz. 685.

do Prawa bankowego wprowadzono art. 4 ust. 1 pkt 46 wskazujący definicję trwałego nośnika, w której określono go jako „nośnik umożliwiający użytkownikowi przechowywanie adresowanych do niego informacji w sposób umożliwiający dostęp do nich przez okres odpowiedni do celów, którym te informacje służą, i pozwalający na odtworzenie przechowywanych informacji w niezmienionej postaci”. Przed wprowadzeniem tejże definicji podmioty funkcjonujące w ramach sektora bankowego posługiwały się w szczególności definicją trwałego nośnika zawartą w Ustawie z dnia 12 maja 2011 r. o kredycie konsumenckim⁹, Ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych¹⁰ oraz licznych dyrektywach, z których najważniejszą z perspektywy banków jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego¹¹ oraz poprzedzająca ją Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego¹², ponieważ na jej podstawie Trybunał Sprawiedliwości Unii Europejskiej (TSUE) dokonał wykładni i określenia elementów pozwalających na przyjęcie, że dany nośnik jest trwałym nośnikiem.

Z perspektywy możliwości przechowywania dokumentów sporządzanych na informatycznych nośnikach danych w formie rozproszonej i zdecentralizowanej bazy danych zorganizowanej przez dany bank za najistotniejsze należy uznać określenie cech trwałego środka. Ustalenie tych cech pozwala bowiem na stwierdzenie, czy prowadzona przez bank baza danych na *blockchain* spełnia te wymogi. Jednocześnie

⁹ T.j. Dz.U. z 2019 r., poz. 1083.

¹⁰ T.j. Dz.U. z 2019 r., poz. 659 ze zm.

¹¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L 337 z dnia 23 grudnia 2015 r., s. 35-127).

¹² Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Dz.Urz. UE L 319/1 z dnia 5 grudnia 2007 r.).

realizacja tych wymogów skutkować będzie mitygacją ryzyka nałożenia na bank potencjalnych sankcji administracyjnych w tym obszarze.

Wymogi dotyczące niezbędnych cech trwałego nośnika zostały sprecyzowane na gruncie orzeczenia TSUE w sprawie C-375/15 *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG przeciwko Verein für Konsumenteninformation*¹³, w treści którego Trybunał zwrócił uwagę na następujące kwestie dotyczące elementów warunkujących uznanie danego instrumentu za trwały nośnik: (i) dawanie gwarancji przechowywania informacji zapisanych na trwałym nośniku w taki sposób, aby zapewnić dostępność dla użytkowników przez odpowiedni czas; (ii) możliwość odtworzenia zapisanej informacji w niezmienionej formie; (iii) uniemożliwienie jednostronnej zmiany lub usunięcia informacji zawartych na trwałym nośniku; (iv) konieczność aktywnego zachowania dostawcy polegającego na przekazaniu użytkownikom informacji o istnieniu oraz udostępnieniu danych informacji; (v) otwartość katalogu instrumentów, które mogą zostać uznane za trwały nośnik (postulat neutralności technologicznej).

W pierwszej kolejności, odnosząc się do orzeczenia TSUE, należy zaznaczyć, że trwałym nośnikiem jest jakikolwiek instrument, który – także zgodnie z poglądem wyrażonym przez D. Szafrąńskiego¹⁴ – kumulatywnie i przy założeniu minimalnych wymogów (które dany instrument musi spełniać) powinien charakteryzować się następującymi cechami: zdolnością do przechowywania informacji, umożliwianiem odtworzenia zapisanej informacji w niezmienionej formie oraz trwałością, która gwarantuje dostęp do zapisanych na nośniku informacji przynajmniej w ciągu odpowiedniego czasu. Prócz elementu konstytutywnego, czyli możliwości zapisu informacji na nośniku, głównym aspektem umożliwiającym uznanie konkretnego nośnika za trwały nośnik, jest wykluczenie możliwości jednostronnej zmiany bądź usunięcia informacji, przy czym istotne jest to, aby gwarancja odtworzenia

¹³ Wyrok TSUE z dnia 25 stycznia 2017 r., *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG v. Verein für Konsumenteninformation*, C-375/15, ECLI:EU:C:2017:38, curia.europa.eu.

¹⁴ D. Szafrąński, *Blockchain a prawo*, Warszawa 2018, Rozdział IV, § 1. Pojęcie trwałego nośnika, Legalis/el.

informacji w niezmienionej postaci miała charakter techniczny, a nie tylko proceduralny. Ponadto warto wskazać, że w odniesieniu do charakteru „odpowiedniości czasu” możliwości odtworzenia informacji przekazywanych przez bank w formie trwałego nośnika należy stwierdzić, iż pojęcie to powinno być rozumiane jako umożliwienie klientowi dostępu do danego dokumentu na tak długi okres, na jaki jest to dla niego istotne w celu ochrony jego interesów wynikających ze stosunków umownych łączących go z bankiem¹⁵. Konkludując, informacje zapisane na trwałym nośniku powinny być możliwe do odtworzenia także po dacie rozwiązania czy wypowiedzenia umowy między klientem a bankiem.

2. Technologia *blockchain* a trwałe nośniki

Blockchain (dosł. łańcuch bloków) stanowi technologię będącą niejako połączeniem istniejących wcześniej technologii, tj. sieci wymiany plików (*peer-to-peer*), kryptografii asymetrycznej oraz modelu akceptacji danych na zasadzie dowodu wykonanej pracy (*proof of work*)¹⁶. Te trzy filary stanowią o innowacyjności oraz ogromnym potencjale tej technologii, a także *de facto* stanowią podwaliny pod możliwość wykorzystania tego rozwiązania w formie trwałego nośnika w działalności banku, zgodnie z treścią przepisu z art. 5 ust. 2 Rozporządzenia.

Blockchain to technologia umożliwiająca przechowywanie informacji w rozproszonych bazach danych, w ramach której uczestnicy, posiadający co do zasady tożsame uprawnienia, mogą wprowadzać, zapisywać, udostępniać oraz przechowywać dowolne dane¹⁷ (w tym

¹⁵ Tak: W. Iwański, M. Sowiński, *Istota trwałego nośnika polega na szczegółach* <<https://skslegal.pl/pl/publikacje/istota-trwalego-nosnika-polega-na-szczegolach/>> [dostęp: 30.03.2020].

¹⁶ Tak: P. Polański, *Inwigilacja, dostępność, blockchain i sztuczna inteligencja: pytania o kierunki rozwoju prawa nowych technologii w erze rewolucji internetowej*, „Monitor Prawniczy” 2019, nr 2, Legalis/el.

¹⁷ Tak: K. Bielecki, *ABC Blockchaina*, Warszawa 2018, s. 19.

zakresie widoczny jest niejako jeden z filarów *blockchainu* w postaci wykorzystania sieci wymiany plików). Informacja raz zapisana w *blockchainie* nie może ulec zmianie, jest dostępna dla pozostałych uczestników danej sieci, a ponadto zostaje uszeregowana w stosunku do informacji ją poprzedzających i następujących po niej¹⁸. Co istotne, dane zawarte w *blockchainie* nie są zapisywane tylko na poziomie mikro (tj. w ramach łańcucha pojedynczych danych), ale także na poziomie makro, a więc po chronologicznym uporządkowaniu informacji na poziomie mikro zostają uszeregowane w ramach większego bloku informacji mieszczącego określoną liczbę pojedynczych danych. Każdy z tych bloków na poziomie makro zawiera odnośnik kryptograficzny do bloku poprzedzającego, co pozwala na zachowanie chronologii dodawanych w *blockchainie* bloków, a także zapewnia bezpieczeństwo danych ze względu na wykorzystanie kryptografii i autentyfikacji (uwierzytelniania), a to stanowi przejaw realizacji zasady wykorzystania kryptografii asymetrycznej. Chronologiczne i niezmiennie uszeregowanie poszczególnych danych oraz równy dostęp zapisanych danych dla wszystkich użytkowników systemu (w rozumieniu tzw. węzłów), w tym dostęp nie tylko do danych aktualnych, ale i do wszystkich archiwalnych zapisów dokonanych w ramach danej sieci *blockchain*, pozwala na wykluczenie możliwości ingerencji przez podmioty nadzorujące określone bazy danych w treść dokumentów zamieszczonych na *blockchainie*, a także w strukturę tychże dokumentów. Niemożliwe jest zatem usunięcie konkretnego dokumentu z bazy danych bez powstania informacji – dostępnej dla wszystkich uczestników – że określony dokument został usunięty, co zapewnia przejrzystość systemu oraz jego audytowalność¹⁹.

Kolejnym elementem konstytutywnym *blockchainu* – jednocześnie zapewniającym integralność, niezmienność i transparentność zapisanych na nim danych – jest decentralizacja, przejawiająca się w dwóch

¹⁸ Por. szerzej: M. Demeyer, *Blockchain technology and smart contracts from a financial law perspective*, Ghent 2018, s. 15 i n.; H. Dikariev, M. Miłosz, *Technologia blockchain i jej zastosowania*, „Journal Computer Sciences Institute” 2018, t. 6, s. 59–61.

¹⁹ Tak: Polska Izba Informatyki i Telekomunikacji, *Blockchain w Polsce. Możliwości i zastosowania* <www.raportblockchain.pl> [dostęp: 30.03.2020].

aspektach. Po pierwsze, decentralizacja widoczna jest w uniezależnieniu sieci od centralnego podmiotu, który zarządza, nadzoruje, wprowadza oraz ewentualnie zmienia albo usuwa dane wprowadzane do systemu (takim podmiotem centralnym może być bank). Drugi aspekt decentralizacji przejawia się we wprowadzeniu systemu, w ramach którego mamy do czynienia z wieloma podmiotami, posiadającymi równe uprawnienia oraz działającymi zgodnie z ustalonymi wewnątrznie zasadami²⁰. Podmioty te określane są jako węzły, które powinny zostać ulokowane u wielu podmiotów regulowanych. Działanie takie zapewni odpowiedni poziom profesjonalizmu w toku funkcjonowania konkretnej sieci, w ramach której zamieszczone zostaną dokumenty związane z czynnościami bankowymi. Uniezależnienie systemu przechowywania dokumentów od jednego podmiotu centralnego mającego całkowity wpływ na sieć dzięki uwzględnieniu zasady decentralizacji pozwala na wykluczenie możliwości jednostronnej kontroli nad strukturą danych (co stanowi jeden z elementów koniecznych do spełnienia przez instrument w celu uznania go za trwały nośnik) oraz wyklucza możliwość wystąpienia jednostkowego punktu awarii. Cecha decentralizacji uniemożliwia ingerencję banku lub innego podmiotu pełniącego rolę węzła w strukturę opublikowanych i przechowywanych w formie rozproszonej między poszczególnymi węzłami w systemie *blockchain* dokumentów, co oznacza spełnienie wymogu niezmienności.

Dopuszczenie przez prawodawcę (w świetle art. 5 ust. 2 Rozporządzenia) wykorzystania technologii *blockchain* do przechowywania dokumentów związanych z czynnościami bankowymi wskazuje na dwie okoliczności. Przede wszystkim stanowi potwierdzenie przez prawodawcę, że technologia ta może spełniać wymogi stawiane trwałemu nośnikowi przy odpowiednim zaprojektowaniu konkretnych rozwiązań technicznych (zwłaszcza ze względu na cechę decentralizacji bazy danych, co podkreśla prawodawca²¹). Równocześnie przyjęte rozwiązanie przesądza o tym, że technologia *blockchain* stanowi

²⁰ Tak: K. Bielecki, op. cit., s. 22 i n.

²¹ Uzasadnienie projektu Rozporządzenia <<https://legislacja.rcl.gov.pl/projekt/12313400/katalog/12519689#12519689>> [dostęp: 30.03.2020].

rodzaj (formę) postaci elektronicznej. Takie stwierdzenie prawodawcy można z jednej strony odbierać jako wyraz zmniejszenia możliwości wystąpienia ryzyka politycznego związanego z zastosowaniem technologii *blockchain* – można bowiem wyobrazić sobie sytuację, w której wobec banku mogłyby zostać zastosowane środki nadzorcze wskazane w treści art. 138 Prawa bankowego na skutek wyrażenia przez organ nadzoru stanowiska, że wykorzystanie technologii *blockchain* w zakresie przechowywania dokumentów związanych z czynnościami bankowymi nie spełnia w zupełności wymogów zawartych w przepisach Rozporządzenia. Ponadto wskazanie przez prawodawcę, że dopuszczalną formą przechowywania dokumentów jest rozproszona i zdecentralizowana baza danych, pozwala także na zwrócenie uwagi podmiotów funkcjonujących w obrębie sektora bankowego nie tyle na poprawność samego wykorzystania technologii *blockchain* w tym zakresie, ile przede wszystkim na dodatkowe zalety wdrożenia tej technologii w działalność banku. Niewątpliwie, taką zaletą jest znaczące obniżenie kosztów związanych z obsługą klientów, którzy decydują się na zawieranie umów w postaci elektronicznej. Sam fakt zawarcia i przechowywania związanej z tym dokumentacji bez konieczności jej wydrukowania, składowania w formie materialnej i archiwizacji znacząco obniża koszty ponoszone przez bank, co zauważył również Naczelny Sąd Administracyjny (NSA) w wyroku z dnia 7 listopada 2019 r., wskazując, że „przekształcanie informacji przez przeniesienie na nośnik papierowy lub elektroniczny generuje dodatkowe koszty”²².

3. Prowadzenie bazy danych w formie wykorzystującej *blockchain* – obowiązki banku

W art. 5 ust. 2 zd. 2 Rozporządzenia prawodawca nałożył na bank wykorzystujący technologię *blockchain* w zakresie przechowywania dokumentów związanych z dokonywanymi czynnościami bankowymi obowiązek prowadzenia bazy danych w sposób zapewniający bezpieczeństwo i integralność zawartych w niej dokumentów. Obowiązek ten

²² Wyrok NSA z dnia 7 listopada 2019 r., I OSK 547/18, Legalis nr 2291324.

składa się z dwóch równorzędnych elementów, a mianowicie prowadzenie bazy danych powinno się odznaczać zachowaniem adekwatnego poziomu bezpieczeństwa zgromadzonej w niej dokumentacji, a także powinno się charakteryzować zachowaniem integralności dokumentów zawartych w tej bazie. Odnosząc się do pierwszego z tych wymogów, należy stwierdzić, że zapewnienie bezpieczeństwa dokumentacji zgromadzonej w bazie danych ogniskuje się w zapewnieniu przez bank, iż dostępność do dokumentu jest ograniczona wyłącznie do osób uprawnionych, dokument jest chroniony przed przypadkowym lub nieuprawnionym zniszczeniem oraz zastosowane są metody i środki ochrony dokumentu, których skuteczność w okresie ich zastosowania jest powszechnie uznawana. Jednocześnie treść art. 6 Rozporządzenia należy odczytywać łącznie z treścią art. 5 ust. 2 zd. 2 Rozporządzenia, jako zobowiązanie banku do (i) systematycznego dokonywania analizy zagrożeń dla bezpieczeństwa dokumentów; (ii) opracowywania i stosowania procedur ochrony informacji i systemów ich przetwarzania, włączając procedury dostępu; (iii) stosowania środków bezpieczeństwa adekwatnych do zagrożeń oraz (iv) bieżącego kontrolowania funkcjonowania wszystkich organizacyjnych i techniczno-informatycznych sposobów ochrony informacji, a także okresowego dokonywania oceny skuteczności tych sposobów. W zakresie realizacji zadania zapewnienia integralności dokumentów zgromadzonych w prowadzonej przez bank bazie danych należy wskazać, że bank musi przez cały okres prowadzenia bazy danych przy zastosowaniu technologii *blockchain* utrzymywać koherentność treści dokumentów umieszczonych w bazie, a także zapewniać spójność struktury tych dokumentów, tj. dokumenty wprowadzane do bazy danych muszą być w niej chronologicznie uszeregowane, ich kolejność oraz treść nie powinna być zmieniana, a ponadto dokumenty nie powinny być usuwane, z wyłączeniem określonych i uzasadnionych sytuacji uregulowanych stosownymi przepisami prawa.

Bank jest jedynym podmiotem odpowiedzialnym za prawidłowość działań związanych z prowadzeniem bazy danych²³. Naruszenie przez bank przepisu art. 5 ust. 2 zd. 2 Rozporządzenia może się

²³ Uzasadnienie projektu rozporządzenia <<https://legislacja.rcl.gov.pl/projekt/12313400/katalog/12519689#12519689>> [dostęp: 30.03.2020].

zmaterializować w dwóch postaciach: (i) naruszenie może wynikać z działania banku, np. w formie ingerencji w treść dokumentu czy próby usunięcia konkretnego dokumentu z bazy danych zapisanych na *blockchain*; (ii) działanie niezgodne z treścią art. 5 ust. 2 Rozporządzenia może także polegać na zaniechaniu banku w formie braku opracowania przez bank procedury ochrony informacji i systemu, w którym są one przetwarzane. W przypadku wystąpienia deliktu dotyczącego sposobu prowadzenia bazy danych z wykorzystaniem technologii *blockchain* Komisja Nadzoru Finansowego jest w pierwszej kolejności uprawniona do wystosowania do banku pisemnego upomnienia. W przypadku braku podjęcia przez bank działań naprawczych na skutek przekazanego przez KNF pisemnego upomnienia organ nadzoru może zastosować różne środki w stosunku do banku dopuszczającego się deliktu administracyjnego, tj. (i) wystąpić do właściwego organu banku z wnioskiem o odwołanie prezesa, wiceprezesa lub innego członka zarządu banku bezpośrednio odpowiedzialnego za stwierdzone nieprawidłowości; (ii) zawiesić (co oznacza *de facto* wyłączenie z podejmowania decyzji za bank w zakresie jego praw i obowiązków majątkowych) w czynnościach członków zarządu, wskazanych w punkcie pierwszym, do czasu podjęcia uchwały w sprawie wniosku o ich odwołanie przez radę nadzorczą na najbliższym posiedzeniu; (iii) ograniczyć zakres działalności banku lub jego jednostek organizacyjnych; (iv) nałożyć na bank karę pieniężną w wysokości do 10% przychodu wykazanego w ostatnim zbadanym sprawozdaniu finansowym, a w przypadku braku takiego sprawozdania – karę pieniężną w wysokości do 10% prognozowanego przychodu określonego na podstawie sytuacji ekonomiczno-finansowej banku; lub też zastosować najbardziej dolegliwy środek w postaci (v) uchylenia zezwolenia na utworzenie banku i podjęcie decyzji o likwidacji banku.

W toku wydawania decyzji administracyjnej w przedmiocie nałożenia sankcji na bank Komisja Nadzoru Finansowego jest zobowiązana do respektowania wymogów wynikających z konstytucyjnoprawnej zasady proporcjonalności (art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej²⁴). Oznacza to w szczególności, że nie można się zgodzić

²⁴ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., Nr 78, poz. 483 ze zm.).

z obecnymi w doktrynie poglądami, iż „kolejność, w której są wymienione [środki nadzoru wskazane w art. 138 ust. 3 Prawa bankowego], również w odniesieniu do nich nie jest przypadkowa. Komisja powinna stosować je kolejno, jednak – jak się uważa – w sposób adekwatny do konkretnej sytuacji”²⁵. W konsekwencji KNF zobowiązana jest do stosowania sankcji administracyjnych dostosowanych (pod względem ich dolegliwości) w jak najwyższym stopniu do okoliczności konkretnej sprawy administracyjnej. Wobec tego należy jednoznacznie stwierdzić, że organ nadzoru w przypadku naruszenia przez bank art. 5 ust. 2 Rozporządzenia jest uprawniony do zastosowania, bez wcześniejszego wykorzystania innych instrumentów odpowiedzialności administracyjnej wskazanych w art. 138 ust. 3 pkt 1–3a Prawa bankowego, instrumentu odpowiedzialności administracyjnej w postaci uchylenia zezwolenia na utworzenie banku i podjęcia decyzji o likwidacji banku, o ile okoliczności konkretnego przypadku naruszenia art. 5 ust. 2 Rozporządzenia uzasadniałyby zastosowanie tak dolegliwej sankcji.

Podsumowanie

Postępujące procesy digitalizacji odnoszące się do stosowanych rozwiązań w ramach prowadzonej przez banki działalności gospodarczej trzeba uznać za naturalny wynik pogłębiających się zjawisk globalizacji gospodarki, otwartości rynków oraz przyspieszającego rozwoju technologicznego²⁶. Należy jednoznacznie podkreślić, że efektywne wykorzystywanie innowacyjnych rozwiązań na gruncie świadczenia usług bankowych klientom stanowi jedno z głównych wyzwań stawianych obecnie przed tradycyjnymi bankami, a w perspektywie najbliższych kilkunastu, może kilkudziesięciu lat – kwestia dostępności oraz mobilności świadczonych usług może stanowić o istnieniu (lub nie) określonych podmiotów na rynku. Z tej perspektywy słuszne jest

²⁵ Tak, błędnie: G. Sikorski, *Komentarz do art. 138*, [w:] idem, *Prawo bankowe. Komentarz*, Warszawa 2015, Legalis/el.; zob. także wyrok NSA z dnia 9 sierpnia 2018 r., II GSK 168/18, CBOSA; postanowienie Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 października 2011 r., VI SA/Wa 1663/11, LEX nr 1093530.

²⁶ Tak: D. Szafranski, op. cit., Rozdział III, § 1. Wprowadzenie.

twierdzenie, że wykorzystywanie nowoczesnych technologii w działalności banków pozwala na utrzymanie przewagi w stosunku do FinTechów, które oferując klientom nowoczesne rozwiązania w połączeniu z mobilnością, wygodą i szybkością realizacji określonych usług, stanowią poważną konkurencję dla przedstawicieli tradycyjnej bankowości.

W tym kontekście należy pozytywnie ocenić działania prawodawcy, który wprowadza w treści art. 5 ust. 2 Rozporządzenia przepis ugruntowujący możliwość wykorzystania technologii *blockchain* przez instytucje działające w polskim sektorze bankowym. Co prawda, ze względu na immanentny charakter prawa jako instrumentu następczego wobec zmieniających się warunków technologicznych, ekonomicznych czy społecznych, należy stwierdzić, że banki po spełnieniu kryteriów stawianych trwałemu nośnikowi i tak mogłyby wykorzystywać technologię *blockchain*. Co istotne, to dokonane przez prawodawcę potwierdzenie możliwości stosowania technologii *blockchain* w obszarze bankowości oraz obserwowane działania organu nadzoru nad sektorem bankowym, w tym zwłaszcza pozytywne stanowisko Komisji Nadzoru Finansowego dotyczące możliwości stosowania technologii *blockchain* w zakresie przechowywania dokumentacji dotyczącej czynności bankowych, wyrażone w procesie konsultacji projektu Rozporządzenia²⁷, świadczą o tendencji oraz pewnej aksjologii, którą kieruje się prawodawca, tj. wspieraniu innowacyjności, co znajduje też odzwierciedlenie na gruncie prawa handlowego w formie wprowadzenia do Kodeksu spółek handlowych nowego typu spółki – prostej spółki akcyjnej, w przypadku której technologia *blockchain* również może znaleźć zastosowanie.

Zaakceptowanie przez prawodawcę rozwiązania technologicznego wykorzystującego technologię *blockchain* w celu przechowywania danych i dokumentów związanych z czynnościami bankowymi powinno być odczytywane jako pozytywne dla podmiotów funkcjonujących

²⁷ Tak np. stanowisko Komisji Nadzoru Finansowego z dnia 13 lipca 2018 r., znak: DP-P-W0P1.0211.18.2018.IW <<https://legislacja.rcl.gov.pl/docs//3/12313400/12519664/12519667/dokument380563.pdf>> [dostęp: 30.03.2020]; stanowisko Komisji Nadzoru Finansowego z dnia 17 lipca 2018 r., znak: DPP-W0P1.0211.18.2018.IW(2) <<https://legislacja.rcl.gov.pl/docs//3/12313400/12519664/12519667/dokument380564.pdf>> [dostęp: 30.03.2020].

w ramach sektora bankowego. Działanie prawodawcy w pewnym sensie ogranicza ryzyko polityczne związane z wykorzystywaniem innowacyjnych rozwiązań w ramach tradycyjnych czynności bankowych oraz stanowi formę akceptacji pewnych proponowanych oddolnie przez banki rozwiązań. Ponadto decyzja ta może być odczytywana jako pewien wyznacznik zarówno orientacji prawodawcy, jak i tendencji, na które sektor bankowy powinien zwrócić większą uwagę i które będą w przyszłości miały ogromny wpływ na funkcjonowanie podmiotów w obszarze tego sektora.

Usage of blockchain technology for storing documents under Banking Law

Summary

The article presents the analysis of theoretical and practical issues related to the legislator's admittance under article 5(2) of the Regulation of the Council of Ministers of 9 March 2020 on documents related to banking activities, drawn upon computerized data mediums (Journal of Laws of 2020, item 476), of the possibility for banks to use blockchain technology in the scope of storing documents related to their banking activities. The main motive for the analysis was, in fact, low awareness of the blockchain technology, its features enabling its usage in the activities of institutions operating in the banking sector as a durable medium, as well as the analysis of the possibility of the bank incurring administrative liability in the event of committing an administrative delict, as provided for in article 5(2) of that Regulation. Due to the innovative and forward-looking nature of the usage of new technologies in the scope of business activity conducted by banks, the author decided that a thorough analysis of the content of article 5(2) of the Regulation is necessary to present the possibilities and practical aspects related to the use of blockchain technology.