E-administracja

Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej

REDAKCJA
Sławomir Dudzik · Inga Kawka · Renata Śliwa

Krakow Jean Monnet Research Papers

E-administracja

Krakow Jean Monnet Research Papers

1

E-administracja

Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej

REDAKCJA

Sławomir Dudzik · Inga Kawka · Renata Śliwa

WYDAWNICTWO KSIĘGARNIA AKADEMICKA

Kraków 2022

Sławomir Dudzik
Uniwersytet Jagielloński, Kraków
s.dudzik@uj.edu.pl

Inga Kawka
Uniwersytet Jagielloński, Kraków
inga.kawka@uj.edu.pl

Renata Śliwa
Uniwersytet Pedagogiczny im. KEN, Kraków
renata.sliwa@up.krakow.pl

Recenzja: dr hab. Agata Jurkowska-Gomułka, prof. WSIiZ

Opracowanie redakcyjne: Patrycjusz Pilawski, Piotr Art

Projekt okładki: Marta Jaszczuk

ISBN 978-83-8138-673-9
https://doi.org/10.12797/9788381386739

Publikacja dofinansowana przez Wydział Prawa i Administracji Uniwersytetu Jagiellońskiego oraz Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie

With the support of Jean Monnet Activities within ERASMUS+ Programme of the European Union

Wsparcie Komisji Europejskiej dla produkcji tej publikacji nie stanowi poparcia dla treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie może zostać pociągnięta do odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl

Księgarnia internetowa: https://akademicka.com.pl

Spis treści

https://doi.org/10.12797/9788381386739.02

Magdalena Fedorowicz[1]

E-administracja nadzorcza na rynku finansowym UE a stabilność finansowa z perspektywy projektów rozporządzeń DORA i MiCA

Abstrakt: W opracowaniu dokonano analizy dwóch projektów rozporządzeń UE dotyczących odporności cyfrowej (DORA) i regulacji rynków kryptoaktywów (MiCA) z perspektywy nowej materii prawnorynkowej wiązanej z zapewnieniem bezpieczeństwa produktów i usług świadczonych i realizowanych w otoczeniu cyfrowym przez szeroko pojęte podmioty finansowe i obejmowanej unijno-krajowym nadzorem, a także z odniesieniami do zagadnienia cyfrowych innowacyjnych narzędzi i instrumentów nadzorczych (SupTech). W artykule sformułowano wniosek o potrzebie funkcjonalnego nadzorczego, wielopłaszczyznowego podejścia do nowej, ujednolicanej na poziomie UE „cyfrowej" materii prawnorynkowej.

Słowa kluczowe: cyfrowa stabilność finansowa, ryzyko ICT, nadzór UE nad cyfrowym rynkiem finansowym, cyfrowy pakiet finansowy, operacyjna odporność cyfrowa

E-supervision on the EU Financial Market and the Financial Stability from the DORA and MiCA Draft Regulations Perspective

Abstract: This paper contains the analysis of EU draft regulations DORA and MiCA related to digital operational resilience and crypto-asset provisions from the

[1] Prof. dr hab. Magdalena Fedorowicz, Zakład Prawa Finansowego Wydziału Prawa i Administracji UAM w Poznaniu, https://orcid.org/0000-0002-5578-5170.

new financial market issues connected with the safety and stability of digital financial products and services, which are planned to be supervised by domestic and EU supervision authorities, also with references to digital supervisory tool issues (SupTech). Conclusions of this paper are focusing on the functional supervisory, multilevel approach to the new, uniform regulated digital financial market issues (e-supervision).

Keywords: digital financial stability, ICT risk, EU supervision on the digital financial market, Digital Finance Package, digital operational resilience

1. Uwagi wstępne

We wrześniu 2020 r. Komisja Europejska przyjęła tzw. pakiet finansów cyfrowych, którego celem jest zwiększenie konkurencyjności i innowacyjności Unii Europejskiej (UE) w sektorze finansowym w obszarze strategii w zakresie finansów cyfrowych, w zakresie płatności detalicznych oraz w sprawie unijnych ram regulacyjnych dotyczących kryptoaktywów[2] (ang. *Markets in Crypto-Assets Act*, dalej: MiCA[3]) i operacyjnej odporności cyfrowej (ang. *Digital Operational Resiliance Act*, dalej: DORA[4]). To właśnie projekty rozporządzeń DORA i MiCA[5], uzupełnione o raport Rady Stabilności Finansowej z 2020 r. *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions. Market Developments and Financial Stability Implications* o wyzwaniach stojących przed nadzorcami rynku finansowego, będący analizą dotyczącą potrzeby rozwoju technologii i narzędzi wspierających organy nadzoru finansowego, zmienią jak się wydaje w sposób znaczący kształt rynku finansowego UE w perspektywie nadzorczej[6].

Wdrożenie tych regulacji wywoła skutki prawnorynkowe dla cyfrowych finansów i będzie wyzwaniem dla nadzorców na rynku finansowym UE w obszarach m.in.: ograniczenia ryzyka cyfrowego, ICT (*information communications technology risk*, ryzyko związane z technologiami informacyjno-komunikacyjnymi) i właściwego

---

[2] Dnia 24.11.2021 r. Rada przyjęła stanowisko w sprawie dwóch projektów składających się na pakiet dotyczący finansów cyfrowych: rozporządzenia o rynkach kryptoaktywów (MiCA) i rozporządzenia o operacyjnej odporności cyfrowej (DORA). Przyjęte teksty są mandatem negocjacyjnym Rady w ramach negocjacji trójstronnych z Parlamentem Europejskim, zob. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0265(OLP) (28.01.2022).

[3] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0593 (3.05.2021).

[4] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020PC0595&from=EN (3.05.2021).

[5] W wersji projektów opublikowanych w tzw. pakiecie finansów cyfrowych z września 2020 r., które są podstawą analiz dokonywanych w niniejszym opracowaniu.

[6] https://www.fsb.org/wp-content/uploads/P091020.pdf (4.05.2021).

nim zarządzania; ochrony konsumentów i rynku finansowego; ochrony przed cyberprzestępczością; przed ryzykiem koncentracji technologii cyfrowych z państw trzecich, które nie mogą zostać poddane skutecznemu nadzorowi; przed ryzykiem walutowym w przypadku tokenów będących e-pieniądzem elektronicznym i nadzoru rynku finansowego, działającego w technologii DLT i blockchain w dziedzinie kryptoaktywów[7].

Wskazane projekty rozporządzeń przeciwdziałać mają lukom nadzorczym w tym zakresie w mikro- i co słuszne makroostrożnościowym, wielopłaszczyznowym wymiarze. Dotychczas brak było jednolitej unijnej regulacji we wskazanych materiach. Na tym tle powstają pytania: jakie są nowe e-materie nadzorcze na rynku finansowym i jak mają lub powinny być nadzorowane, aby realizować cel stabilności finansowej? Jakie mają być nowe obowiązki i uprawnienia nadzorcze na cyfrowym rynku finansowym UE? Za pomocą jakich narzędzi ma chronić nadzór i jak ma być realizowana ochrona klienta na cyfrowym rynku finansowym?

W analizach podjęta zostanie próba definicyjnego ujęcia e-nadzoru i e-administracji nadzorczej na rynku finansowym oraz ocena uwzględnienia w komentowanych projektach zasady proporcjonalności i granic dla e-nadzoru.

Niewątpliwie w projektach DORA i MiCA następuje poszerzenie funkcji nadzorczych tak podmiotowo (w zakresie dostawców zewnętrznych usług ICT, jak i dostawców usług w zakresie kryptoaktywów), jak i przedmiotowo o nowe prawnorynkowe materie cyfrowe (regulacji ryzyka ICT, regulacji rynku kryptoaktywów), co rodzi pytania o sprawowanie jak najbardziej skutecznego nadzoru nad nimi i optymalizacji dotychczasowych czy stosowania nowych cyfrowych innowacyjnych narzędzi nadzorczych (SupTech) w ramach dokonującej się przecież również cyfryzacji nadzoru nad rynkiem finansowym UE. Dla materii regulacyjnej DORA i MiCA oraz analizy rozlicznych obowiązków raportacyjnych nałożonych na podmioty finansowe „tradycyjne" instrumenty i narzędzia mogą okazać się niewystarczające i nazbyt kosztowne. Uzasadnione są pojawiające się głosy o inflacji oraz dublowaniu obowiązków informacyjnych w różnych systemach i za pomocą różnych kanałów raportacyjnych w sytuacji generowania coraz większych, również nadzorczych *Big Data*.

Zbiorczo można argumentować o potrzebie rozwijania w świetle DORA i MiCA funkcjonalnego e-podejścia nadzorczego dla realizacji celu stabilności cyfrowej, która jako pojęcie staje się dalszą konkretyzacją, uszczegółowieniem pojęcia „stabilności

[7] Szeroko na temat DLT i blockchain w prawie zob. D. Szostek, *Blockchain a prawo*, Warszawa 2018, *passim*.

finansowej"[8]. To funkcjonalne podejście nadzorcze obejmuje nie tylko nowe e-materie nadzorcze na rynku finansowym, ale również pokazuje wyzwania stojące przed unijnymi i krajowymi nadzorcami w procesach nadzorczych na rynku finansowym i konieczność posługiwania się e-nadzorczymi instrumentami.

Metodą badawczą stosowaną w niniejszym opracowaniu jest metoda dogmatycznoprawna.

2. E-nadzór w ujęciu funkcjonalnym

Cyfrowa stabilność finansowa ma być osiągana za pomocą norm prawa publicznego (nadzorczych, zgodnie ze zmianą paradygmatu regulacyjnego na rynku finansowym na nadzorczy) i za pomocą norm prawa prywatnego (w które ma ingerować tak nadzór unijny, jak i krajowy), ponieważ projektuje się określać pewną pożądaną treść umów zawieranych przez podmioty finansowe z dostawcami usług ICT czy udzielanie dostawcom zezwoleń na prowadzenie usług w zakresie kryptoaktywów, poddanych wzmocnionemu nadzorowi krajowemu i unijnemu, temu ostatniemu w przypadku dostawców kluczowych czy kryptoaktywów znaczących [np. art. 18 ust. 1, lit. a), pkt 2 DORA, art. 25, 27, 28-39 DORA i art. 55 MiCA]. Wzmocniony nadzór ma polegać w tym przypadku na możliwości zobligowania przez nadzorców podmioty finansowe do zawieszenia czy wypowiadania rodzących różnego rodzaju ryzyka umów z dostawcami, np. w sytuacji pojawiającego się ryzyka koncentracji czy ryzyka geolokalizacji dostawcy usług ICT poza UE, ryzyka związanego z niemożnością prowadzenia procesów kontrolno-nadzorczych w takich podmiotach (m.in. art. 26 ust. 2 DORA, art. 37, 44 DORA), a w przypadku MICA m.in. na udzielaniu zezwoleń dostawcom usług w zakresie kryptoaktywów wyłącznie osobom prawnym posiadającym siedzibę statutową w UE (art. 53 i 55 MiCA) i określeniu zasad outsourcingu usług w zakresie kryptoaktywów, w tym również dla osób trzecich zaangażowanych w outsourcing (art. 66 MiCA).

Przy funkcjonalnym podejściu do e-nadzoru chodzi zwłaszcza o analizę skutecznego pełnienia funkcji przez nadzorców krajowych i unijnych w materiach dotychczas skąpo lub wcale dotąd nieregulowanych, dla których wspólnym normatywnym mianownikiem staje się przeniesienie usług czy tworzenie produktów na rynku finansowym do rzeczywistości cyfrowej przy wykorzystaniu narzędzi i nowoczesnych technologii

[8] O pojęciu stabilności finansowej zob. M. Fedorowicz, *O normatywnym pojęciu stabilności finansowej na rynku finansowym Unii Europejskiej w nowej architekturze nadzorczej*, „Studia Europejskie" 2017, nr 4, s. 73-94.

inżynierii finansowej. Funkcjonalne podejście do e-nadzoru obejmowałoby, po pierwsze, e-nadzór w wąskim rozumieniu i, po drugie, e-nadzór w szerokim rozumieniu, gdyż dopiero takie zestawienie pomaga w dopasowaniu najbardziej efektywnych narzędzi nadzorczych do nowo regulowanych materii w projektach DORA i MiCA[9].

E-nadzór w wąskim rozumieniu analizowany jest z punktu widzenia sposobu realizacji obowiązków nadzorczych wykonywanych przez instytucje finansowe w nowych technologiach (przesyłanie zbiorów danych w e-formule lub wykorzystaniu nowoczesnych technologii cyfrowych: blockchain i DLT, przechowywanie danych nadzorczych w chmurze), ale i z punktu widzenia stosowania przez organy nadzoru narzędzi wykorzystujących technologie cyfrowe, SupTech dla celów analityczno-nadzorczych. Z uwagi na fakt przyszłego pełnienia unijno-krajowego nadzoru w sprawach objętych DORA i MiCA e-narzędzia nadzorcze powinny być w zakresie analizowanych projektów stosowane przez nadzorców na poziomie krajowym i UE [algorytmizacja, automatyzacja, API, ML, technologie blockchain[10] i DLT, AI, technologie chmury, piaskownice regulacyjne, HUB, wykorzystywanych w celach nadzorczych (SupTech)]. Jest to związane z potrzebą tworzenia aplikacji do zarządzania dokumentami[11], kreatorów raportów, automatycznej dekretacji, rozpoznawania dokumentów przychodzących i ich porządkowania, segregowania do odpowiednich zbiorów informacji w zależności od realizowanych celów nadzoru, w tym zwłaszcza w odniesieniu do rozbudowanego w DORA i MiCA raportowania danych niezbędnych do procesów kontrolno-nadzorczych w układzie pionowym (do nadzorców unijnych czy EBC) oraz w układzie poziomym także pomiędzy nadzorcami krajowymi i w niezbędnym zakresie w całej sieci stabilności finansowej dla zapewnienia tej stabilności w jej cyfrowym wymiarze. Jest to niewątpliwie bardziej techniczne podejście do nadzoru. Potrzeba stosowania w szerszym zakresie nowoczesnych e-narzędzi nadzorczych jest pilna zwłaszcza w odniesieniu do obowiązków raportacyjnych instytucji finansowych, realizowanych na rzecz nadzorców, jednak sposób wykonywania e-nadzoru i jego e-narzędzia muszą

---

[9] Z pojęciem e-nadzoru wiąże się także pojęcie e-administrowania nadzorczego na rynku finansowym. Charakterystyczna dla tego ostatniego jest wielopłaszczyznowość, czyli zarządzanie i nadzór nad ryzykiem cyfrowym na poziomie krajowym i unijnym w wymiarze mikro- i makroostrożnościowym.

[10] Została zastosowana dla wdrożenia skutków orzeczenia o trwałych nośnikach w zakresie bankowości elektronicznej TS z 25.01.2017 r., C-375/15, EU:C:2017:38.

[11] Zarządzanie strukturyzowanymi danymi i niestrukturyzowanymi danymi (m.in. e-maile), zebranie tych informacji w różnych kanałach informacji i za pomocą różnych narzędzi może utrudniać analizę. Analiza danych strukturyzowanych wydaje się łatwiejsza, ale niestrukturyzowane dane mogą się wymykać standaryzacji i automatyzacji, podlegać zespoleniu z danymi niestrukturyzowanymi, pojawia się tutaj zatem obszar do wykorzystania odpowiednich jakościowo i ilościowo e-narzędzi nadzorczych.

być efektywne i dostosowane do ilości i jakości nadzorczych *Big Data* oraz ich ważności dla nadzorców z punktu widzenia realizowanych przez nich celów analitycznych. Nadzór realizowany za pomocą nowych technik nadzorczych powinien poprawić zdolności nadzorcze. Wykonywanie działań nadzorczych za pomocą e-narzędzi jest już oczywiście realizowane w praktyce[12], ale brak jeszcze ujednoliconych, spójnych kompleksowych rozwiązań e-nadzorczych, a skala zadań i administrowania nadzorczego, zwłaszcza w projektach DORA i MiCA, będzie tego zdecydowanie wymagać[13]. Pilna staje się potrzeba cyfrowego wsparcia nadzoru nad rynkiem finansowym i rozwoju nadzorczych strategii, wspierających obowiązki nadzorcze[14], tym bardziej że, jak np. podano w raporcie Rady Stabilności Finansowej, ok. 1/3 ankietowanych nadzorców zbiera dane od podmiotów nadzorowanych za pomocą zastanych systemów, a 2/3 za pomocą dedykowanych portali (web), mniej natomiast niż połowa nadzorców rozwinęła API, dzięki któremu nadzorowani przesyłają dane do nadzorców[15]. Zauważalna jest potrzeba zharmonizowania wspólnego na rynku finansowym w UE procesu zbierania danych (standaryzacja) w UE od nadzorowanych w zakresie ujednolicanej na poziomie UE materii prawnorynkowej, a DORA i MiCA wpisują się w dokonujący się proces potrzebnej nadzorczej standaryzacji.

Z kolei e-nadzór w szerokim znaczeniu to także nadzór rozpatrywany z punktu widzenia e-materii prawnorynkowej, rozumiany jako objęcie nadzorem (za pomocą narzędzi tradycyjnych i cyfrowych) materii, która dotychczas nie była regulowana lub była regulowana fragmentarycznie, a dotyczy ryzyka cyfrowego (ICT) czy świadczenia cyfrowych usług i oferowania produktów finansowych, w tym cyfrowych (stanowiąc w ten sposób finansową e-materię prawnorynkową), dla której dotychczasowe narzędzia nadzorcze muszą być, jak się wydaje, uzupełnione i poszerzone również cyfrowymi. Wyodrębnianie e-materii prawnorynkowej ma posłużyć do dyskusji na temat wyzwań stojących przed unijnymi i krajowymi nadzorcami, aby nadzór był efektywny i urze-

[12] Np. WebService KNF w zakresie raportowania informacji zawartych m.in. w art. 4 rozporządzenia MAR, obowiązki raportacyjne z art. 22, 26, 27 rozporządzenia MIFIR czy też raportowanie w jednolitych formatach przygotowywanych przez ESA, np. European Single Electronic Format, w ramach którego emitenci, których papiery wartościowe zostały dopuszczone do obrotu na rynku regulowanym na terytorium UE, mają obowiązek sporządzania raportów rocznych w jednolitym europejskim formacie raportowania.

[13] EBC tworzy standardy cyfrowej kultury nadzorczej dla nadzorców od 2018 r. i wydaje się to zapowiedzią istotnych zmian w zakresie cyfryzacji nadzoru. EBC postuluje rozwój kultury cyfrowej jako ważny element długofalowej strategii cyfrowej i dzielenia się wiedzą cyfrową wśród nadzorców, którzy koncentrować się mają na zarządzaniu i nadzorze nad *Big Data* nadzorczymi i innowacyjnymi nadzorczymi e-narzędziami.

[14] Raport FSB, s. 11.

[15] Raport FSB, s. 20.

czywistniał także cyfrową stabilność finansową, tym bardziej że w projektach DORA i MiCA, jak wspomniano, następuje znaczące poszerzenie zakresu przedmiotowego i podmiotowego nadzoru na rynku finansowym o materie odporności cyfrowej i regulacji kryptoaktywów. Z kolei w aspekcie funkcjonalnym e-nadzoru uwaga skoncentrowana być musi na odpowiednim instrumentarium prawnym i narzędziach technicznych, pozwalających na realizację funkcji nadzorczej w cyfrowym wymiarze. W jednym i drugim przypadku punktem wyjściowym i w tym opracowaniu głównym rozważań jest zatem nowa materia nadzorcza w projektowanych rozporządzeniach DORA i MiCA.

Takie funkcjonalne podejście do e-nadzoru wydaje się użyteczne, gdyż najistotniejsze jest pytanie, za pomocą jakich narzędzi i w odniesieniu do jakiej materii prawnorynkowej nadzór może najefektywniej realizować swoje funkcje nadzorcze przy postępującej cyfryzacji (funkcjonalne podejście do e-nadzoru, uwzględniające obszary, w których potrzebny byłby rozwój SupTech z uwagi na materię regulacyjną i efektywną realizację celów nadzorczych), i to w taki sposób, aby nie „zadławić" rozwoju innowacyjnych technologii finansowych nieproporcjonalnymi rozwiązaniami nadzorczymi, a zarazem zapewniać stabilność finansową. Jest to w istocie również pytanie o granice nadzoru w cyfrowym środowisku z punktu widzenia e-nadzoru zarówno w wąskim, jak i szerokim ujęciu.

3. Zapewnianie odporności cyfrowej na rynku finansowym UE w świetle projektu DORA

W DORA nastąpi wspomaganie nadzorców poprzez m.in. poszerzenie *compliance* o zagadnienia cyfrowe związane z zarządzaniem ryzykiem ICT w jednolitych, wiążących ramach prawnych tego rozporządzenia. Ryzyko ICT wyodrębniło się z ryzyka operacyjnego i wybiło na regulacyjną „niezależność", a dowodem na to jest właśnie regulacja DORA (regulacja, gdyż rozporządzenie to będzie uzupełniane RTS-ami, wytycznymi EBA, rekomendacjami krajowych nadzorców). Oczywiście już wcześniej EBA wydawała wytyczne dotyczące tego ryzyka[16], teraz jednak jego regulacja została zaprojektowana w bezpośrednio skutecznym i stosowalnym rozporządzeniu DORA, ujednolicającym podejście do tego ryzyka w skali całej UE.

Zgodnie z art. 1 DORA ustanowione mają być jednolite wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych wspierających procesy bizne-

[16] Np. wytyczne z 28.11.2019 r. EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT, EBA/GL/2019/04.

sowe podmiotów finansowych, niezbędne do osiągnięcia wysokiego wspólnego poziomu operacyjnej odporności cyfrowej, umożliwiając jednocześnie proporcjonalne stosowanie wymogów w odniesieniu do podmiotów finansowych będących mikroprzedsiębiorstwami. Z kolei w art. 3 DORA wyjaśniono, że „operacyjna odporność cyfrowa" oznacza zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej integralności operacyjnej z technologicznego punktu widzenia przez zapewnianie, bezpośrednio albo pośrednio (korzystając z usług zewnętrznych dostawców usług ICT), pełnego zakresu możliwości w obszarze ICT, niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość). Odporność cyfrowa ma być osiągana dzięki prawidłowemu zarządzaniu i nadzorowi nad ryzykiem związanym z ICT, czyli każdą dającą się racjonalnie określić okolicznością związaną z użytkowaniem sieci i systemów informatycznych, czy też po prostu z ryzykiem cyfrowym.

Filozofia regulacyjna odporności cyfrowej w DORA może być rekonstruowana w następujący, wielopłaszczyznowy sposób: po pierwsze, odporność ma być zapewniana przez podmioty finansowe i zewnętrznych dostawców; po drugie, nad nimi ma być sprawowany nadzór krajowy i unijny, a po trzecie, rozwijana ma być nadzorcza współpraca z rynkami państw trzecich na poziomie globalnym. Dbałość o prawidłowe zarządzanie tym ryzykiem spoczywa w pierwszej kolejności na podmiotach finansowych, zgodnie bowiem z art. 4 DORA podmioty te mają obowiązek posiadania wewnętrznych ram zarządzania i kontroli, zapewniających zarządzanie ryzykiem ICT.

Odporność cyfrowa i jej skuteczność jest zatem uzależniona od ram prawnych na poziomie podmiotów finansowych oraz ich polityk, strategii i przyjmowanych wewnętrznych rozwiązań jednak nie jak dotychczas różnorodnych, ale opartych na ujednolicanym unijnym wzorcu prawnym. Proces nabywania odporności cyfrowej następuje w sieci konwergencji nadzorczej[17], przy zapewnieniu wymiany informacji między podmiotami finansowymi, nadzorcami krajowymi i unijnymi oraz krajowymi organami restrukturyzacji i uporządkowanej likwidacji. Zarządzanie ryzykiem cyfrowym ma obejmować: tworzenie w podmiotach finansowych strategii odporności cyfrowej i zarządzania ryzykiem ICT, zgłaszanie incydentów związanych z ryzykiem cyfrowym do jednego systemu[18], a przez to wyeliminowanie obowiązku zgłoszeń do

[17] M. Fedorowicz, *Osiąganie konwergencji nadzorczej mikroostrożnościowej i makroostrożnościowej w prawie rynku finansowego Unii Europejskiej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2018, nr 4, s. 155-169.

[18] Proces zarządzania incydentami związanymi z ICT (ich klasyfikacja i gradacja) ma być doprecyzowany za pomocą RTS-ów. O incydentach informowane będą ESA, EBC, organy publiczne

różnych systemów, przeprowadzanie ujednoliconych testów odporności cyfrowej[19], a także kontrolę zewnętrznych dostawców usług ICT.

Podmioty finansowe, do których DORA oprócz instytucji finansowych w poszczególnych segmentach rynku finansowego UE zalicza także dostawców usług w zakresie kryptoaktywów, centralne depozyty papierów wartościowych, kontrahentów centralnych, systemy obrotu, repozytoria transakcji, agencje ratingowe i dostawców usług w zakresie udostępniania informacji i finansowania społecznościowego, będą zobligowane do przygotowywania strategii i procedur zarządzania ryzykiem ICT w ramach prawnych wyznaczonych DORA. W tym kontekście należy się zapewne spodziewać również zmian w rozporządzeniu MF do art. 9f ustawy Prawo bankowe z 1997 r., jeśli chodzi o sektor bankowy rynku finansowego. Można też przewidywać zmiany w rekomendacjach D i M KNF. Oczywiście, rozporządzenie jest bezpośrednio skuteczne i stosowalne, ale krajowe akty będą podlegały zapewne uszczegółowieniu i modyfikacjom w kierunku zapewnienia wykonania prawa UE. W tym sensie można zatem również mówić o e-administrowaniu na poziomie podmiotów finansowych w ramach 3 płaszczyzn ochronnych przed ryzykiem cyfrowym, a polegających na rozdzieleniu zarządzania od kontroli i audytu, dalej o e-administrowaniu nadzorczym na poziomie krajowym oraz e-administrowaniu nadzorczym na poziomie UE, a także e-współpracy nadzorczej w tych sprawach pomiędzy wskazanymi poziomami i organami nadzoru z państw trzecich, czyli również na poziomie współpracy międzynarodowej, w tym np. z Bazylejskim Komitetem ds. Nadzoru Bankowego.

---

czy ESBC. Na podstawie tego powiadomienia właściwe organy podejmą niezbędne środki w celu ochrony bieżącej stabilności systemu finansowego, i tu ma następować harmonizacja treści i wzorów zgłoszeń (art. 18 DORA) za pomocą RTS. ESA mają sporządzać wspólne sprawozdanie. Dla zgłaszania poważnych incydentów przez podmioty finansowe ma zostać ustanowiony jeden unijny węzeł informacyjny. Wydaje się, że jest to idealny obszar dla zastosowania nowoczesnych e-narzędzi nadzorczych. Z punktu widzenia ochrony klientów podmiotów finansowych jest przewidziane, aby w przypadku gdy poważny incydent będzie miał wpływ na interesy finansowe użytkowników usług i klientów, podmioty finansowe będą informowały swoich użytkowników usług i klientów o incydencie oraz o wszystkich środkach podjętych w celu ograniczenia jego niekorzystnych skutków (art. 17 ust. 2 DORA). Organy nadzorcze będą jak najszybciej przekazywać podmiotowi finansowemu niezbędne informacje zwrotne, wytyczne, ostrzeżenia, w szczególności w celu omówienia środków zaradczych na poziomie danego podmiotu lub sposobów ograniczenia do minimum negatywnych skutków we wszystkich sektorach. Z uwagi na konieczność szybkiego działania potrzebne jest przyjęcie e-narzędzi kontaktu w czasie rzeczywistym, jest to również obszar szerokiego uwzględnienia e-narzędzi nadzorczych, a ich stosowanie przyczyni się także do potanienia kosztów nadzoru oraz wyeliminowania dublujących się obowiązków informacyjno-raportacyjnych z tego zakresu.

[19] Chodzi o wzajemne uznawanie wyników zaawansowanych testów operacyjnej odporności cyfrowej dotyczących podmiotów prowadzących działalność transgraniczną. Podmioty finansowe co najmniej raz w roku będą testować wszystkie kluczowe systemy i aplikacje ICT.

Osiąganie odporności cyfrowej nastąpi też poprzez rozbudowanie obowiązków raportacyjnych podmiotów finansowych, ale na podstawie jednolitych wzorców UE, a nad tymi materiami nadzór pełnić będzie KNF i ESA na poziomie UE. Taka filozofia regulacyjna oznacza kilka poziomów zarządzania ryzykiem cyfrowym, co nawiązuje do *Wspólnej porady Europejskich Urzędów Nadzoru skierowanej do Komisji Europejskiej dotyczącej konieczności wprowadzenia usprawnień legislacyjnych związanych z wymogami w zakresie zarządzania ryzykiem związanym z ICT w unijnym sektorze finansowym*[20] i oznaczać też może potanienie kosztów nadzoru, zwłaszcza jeśli do tych nowych materii regulacyjnych dobierze się adekwatne e-narzędzia nadzorcze, rozumiane jako posługiwanie się narzędziami i technikami nadzorczymi bazującymi na FinTech: technologie chmurowe, AI, algorytmizacja, API zwłaszcza w zakresie raportowania o istnieniu strategii w bankach i kanałów informacji o incydentach[21].

Istotnym elementem materii regulacyjnej DORA staje się w szczególności nadzorcze monitorowanie ryzyka związanego z zewnętrznymi dostawcami usług ICT. Tu bowiem głównie upatruje się ryzyka i zaburzeń w odporności cyfrowej przy usługach i produktach świadczonych na cyfrowym rynku finansowym. Chodzi tu również o przeciwdziałanie ryzyku koncentracji, także pomiędzy sektorami rynku finansowego, i ochronę przed wystąpieniem efektu domina w odniesieniu do unijnego sektora finansowego. W tych obszarach potrzeba szerokiego zastosowania e-narzędzi nadzorczych jest pilna. Dokładny kształt ram prawnych UE w tym zakresie będzie doprecyzowany przez ESA w RTS-ach, niemniej już teraz można zaobserwować położenie nacisku na pełniony przez krajowych nadzorców nadzór nad zewnętrznymi dostawcami usług ICT, a także ich odróżnienie od dostawców kluczowych, co będzie domeną bezpośredniego nadzoru ESA. Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT będzie należało do podmiotów finansowych, które będą prowadzić i aktualizować na poziomie podmiotu oraz na poziomie subskonsolidowanym i skonsolidowanym rejestr informacji w odniesieniu do wszystkich ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT udostępniany na wniosek organu nadzoru. Ścisły nadzór krajowy nad dostawcami usług ICT wiązany jest także w DORA z umowami dotyczącymi dalszego zlecania podwykonawstwa lub ważnych funkcji przez zewnętrznego dostawcę usług ICT innym dostawcom usług ICT. Podmioty finansowe mają tu rozważać korzyści i ryzyko, z uwagi na skuteczność nadzoru, które mogą wystąpić w związku z takim ewentualnym podwykonawstwem,

[20] JC 2019 26 (2019).

[21] Szeroko na temat AI w prawie zob. m.in. zbiorcze opracowanie *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020, *passim*; A. Chłopecki, *Sztuczna inteligencja. Szkice prawne i futurologiczne*, wyd. 2, Warszawa 2021, *passim*.

w szczególności w przypadku podwykonawcy ICT mającego siedzibę w państwie trzecim. Bardzo precyzyjnie uszczegółowiono w DORA, jakie treści powinny stać się przedmiotem ustaleń umownych, a także przedumowną ocenę ryzyka i ustaleń przez podmioty finansowe, np. w zakresie prawa kontroli, audytu realizowanych przez podmiot finansowy, częstotliwość zdalnych audytów (art. 27 ust. 2 DORA). Również tutaj ESA opracują ujednolicające projekty RTS, które podmiot finansowy będzie musiał uwzględnić, zlecając podwykonawstwo kluczowych lub ważnych funkcji. Nadzór jest tu zatem pomyślany zarówno jako prawo organu nadzoru do pozyskania informacji z rejestru ustaleń umownych, jak i poprzez uregulowanie w DORA minimalnej treści umów z dostawcami zewnętrznymi, w tym zwłaszcza treści umów z dalszymi podwykonawcami przewidzianej do uwzględnienia przez podmioty finansowe w nadzorczych RTS-ach.

Nadzór *sensu stricto* nad zewnętrznymi dostawcami usług ICT, którzy w ocenie ESA (jako wiodących organów nadzoru) mają charakter kluczowy, będzie pełniony bezpośrednio na poziomie UE przez właściwe ESA i tu także nieodzowne wydaje się posłużenie e-narzędziami nadzoru z uwagi na skalę i zróżnicowanie obowiązków nadzorczych, podanych poniżej dla zilustrowania potrzeby stosowania SupTech. To ESA będą oceniać, czy zewnętrzni, kluczowi dostawcy usług ICT wprowadzili kompleksowe, skuteczne zasady, procedury i mechanizmy służące do zarządzania ryzykiem ICT. Zaszeregowanie dostawców usług ICT przez ESA nastąpi na podstawie łącznie spełnianych kryteriów o systemowym znaczeniu, co nawiązuje do potrzeby uwzględnienia celów regulacji makroostrożnościowych również w zakresie ICT i w poszanowaniu zasady proporcjonalności (art. 28 ust. 2 DORA). Bezpieczeństwo na cyfrowym rynku finansowym ma być także zapewnione w drodze realizacji zasady przejrzystości, ESA bowiem będą sporządzać, publikować i każdego roku aktualizować wykaz kluczowych zewnętrznych dostawców usług ICT na poziomie UE. Właściwe sektorowo ESA przyjmą szczegółowe indywidualne plany nadzoru dla każdego kluczowego zewnętrznego dostawcy usług ICT. ESA jako wiodące organy nadzorcze będą miały silne uprawnienia *stricte* nadzorcze, w tym kompetencje do prowadzenia postępowań nadzorczych, nastawionych na nadzór podwykonawstwa i zapewnienie bezpiecznego działania dla podmiotów finansowych korzystających z zewnętrznych dostawców usług ICT (art. 31 DORA), a także wydawania decyzji sankcyjnych względem zewnętrznych dostawców usług ICT[22]. Normatywnym wyrazem silnych kompetencji nadzorczych ESA będzie m.in. prawo do występowania z wnioskiem o przekazanie

[22] Od decyzji tych przysługiwać będą środki odwoławcze z rozporządzeń o ESA oraz prawo do zaskarżenia decyzji ESA do TSUE.

wszystkich stosownych informacji i dokumentów od zewnętrznych dostawców usług ICT, prowadzenie ogólnych dochodzeń i kontroli na miejscu, nakładanie okresowych kar pieniężnych na zewnętrznych dostawców usług ICT, występowanie z wnioskiem o złożenie sprawozdań po zakończeniu działań nadzorczych, w których omówiono działania podjęte lub środki zaradcze wdrożone przez kluczowych zewnętrznych dostawców usług ICT w związku z zaleceniami, np. związanymi z umowami podwykonawstwa, w tym podoutsourcingu, które kluczowi zewnętrzni dostawcy usług ICT zamierzają zawrzeć z innymi zewnętrznymi dostawcami usług ICT lub z podwykonawcami usług ICT z siedzibą w państwie trzecim wszelkiego planowanego podwykonawstwa, w tym podoutsourcingu, w przypadku którego wiodący organ nadzorczy uważa, że dalsze podwykonawstwo może wywołać ryzyko dla świadczenia usług przez podmiot finansowy lub ryzyko dla stabilności finansowej i zwłaszcza wydawanie zaleceń w sprawie odstąpienia od zawarcia umowy dalszego podwykonawstwa, jeżeli przewidzianym podwykonawcą jest zewnętrzny dostawca usług ICT lub podwykonawca usług ICT z siedzibą w państwie trzecim i podwykonawstwo dotyczy kluczowej lub ważnej funkcji podmiotu finansowego. Z kolei bieżący nadzór nad kluczowymi zewnętrznymi dostawcami ICT ma być pełniony wspólnie przez ESA i krajowe organy nadzoru w ramach Wspólnego Zespołu ds. Kontroli. Co ważne, wszyscy jego członkowie muszą posiadać wiedzę fachową z zakresu ICT i ryzyka operacyjnego. Zalecenia ESA adresowane będą także do kluczowych zewnętrznych dostawców usług ICT, a oceną wdrożenia zaleceń zajmą się nadzorcy krajowi.

Siła nadzorcza nad zewnętrznymi kluczowymi dostawcami usług ICT przejawi się zwłaszcza w postanowieniach art. 37 w zw. z art. 44 DORA, jako że krajowi nadzorcy mogą zobowiązać podmioty finansowe do tymczasowego zawieszenia, w części albo w całości, korzystania z usługi świadczonej przez kluczowego zewnętrznego dostawcę usług ICT lub jej wdrażania do czasu wyeliminowania ryzyka zidentyfikowanego w zaleceniach skierowanych do kluczowych zewnętrznych dostawców usług ICT albo nakazać podmiotom finansowym wypowiedzenie, w części lub w całości, stosownych ustaleń umownych zawartych z kluczowymi zewnętrznymi dostawcami usług ICT.

Istotne, że przewiduje się także wzmożoną współpracę międzynarodową między ESA a organami nadzoru i regulacyjnymi z państw trzecich na podstawie zawieranych porozumień administracyjnych, aby niwelować obszar ryzyka ze strony zewnętrznych dostawców usług ICT w różnych sektorach finansowych. Obszar tej współpracy powinien być także zagospodarowany odpowiednimi narzędziami nadzoru cyfrowego.

Zastosowanie nowoczesnych e-narzędzi nadzorczych wydaje się szczególnie potrzebne przy wymianie informacji i współpracy na poziomie pomiędzy podmiotami finansowymi, zgodnie z art. 40 DORA, co powinno mieć miejsce w czasie rzeczywistym,

aby realne było przeciwdziałanie ryzyku cyfrowemu i ryzyku koncentracji technologicznej, a zarazem technologii wymiany informacji gwarantujących zachowanie poufnego charakteru wymienianych informacji i poszanowanie tajemnicy przedsiębiorstwa, ochrony danych osobowych i wytycznych dotyczących polityki konkurencji. Tym bardziej że właśnie w odniesieniu do tych platform wymiany informacji o istotnym znaczeniu nadzorczym przewiduje się możliwość uczestnictwa organów publicznych i włączenia ich do ustaleń dotyczących wymiany informacji, a także szczegóły elementów operacyjnych, w tym korzystania ze specjalnych platform informatycznych (art. 40 ust. 2 DORA). Jest to obszar wymiany informacji, który powinien być dostępny tak dla organów sieci stabilności finansowej, jak i organów przeciwdziałających praniu pieniędzy w systemach krajowych.

Obszarem stosowania e-narzędzi nadzorczych powinny stać się zwłaszcza podejmowane na podstawie art. 43 DORA ćwiczenia wykonywane między sektorami finansowymi oraz komunikacja, wymiana informacji i współpraca między tymi sektorami. ESA wspólnie z krajowymi nadzorcami będą mogły bowiem ustanowić mechanizmy umożliwiające wymianę praktyk między sektorami finansowymi, aby identyfikować wspólne dla sektorów luki i rodzaje ryzyka w cyberprzestrzeni. Będą to ćwiczenia z zakresu zarządzania kryzysowego i sytuacji awaryjnych obejmujące scenariusze cyberataków w celu wypracowania kanałów komunikacyjnych i stopniowego umożliwiania skutecznej skoordynowanej reakcji na poziomie UE w przypadku poważnego transgranicznego incydentu związanego z ICT.

Skuteczność nadzorców unijnych i krajowych na cyfrowym rynku finansowym UE uzależniona będzie przede wszystkim od stosowania w przyszłości w większym niż dotychczas zakresie innowacyjnych e-narzędzi nadzorczych. Wymaga tego realizacja założeń ambitnego nadzorczo[23] projektu DORA. Trzeba też przy okazji pochwalić twórców DORA za zasadniczo prawidłowe uwzględnienie w proponowanych regulacjach zasady proporcjonalności, która tu działać będzie także jako naturalna granica przed hamowaniem rozwoju FinTechów[24].

---

[23] Już wcześniej na mocy regulacji PSD, rekomendacji D i M KNF, wytycznych EBA, a od lipca 2021 r. wytycznych EIOPA wzmacniane było i jest monitorowanie oraz zarządzanie ryzykiem cyfrowym.

[24] Przejawiać się to będzie w rozlicznych zwolnieniach z wymogów raportacyjno-zarządczych dla mikroprzedsiębiorców zatrudniających mniej niż 10 pracowników lub z obrotem poniżej 2 mln euro. Będzie to zarazem podstawowe wyzwanie dla nadzorców, aby nie wprowadzać nieproporcjonalnych uciążliwości regulacyjno-nadzorczych dla mikroprzedsiębiorców.

4. Nowa materia nadzorcza w świetle projektu MiCA

Jeśli w przypadku projektu DORA chodzi o jednolite w UE uregulowanie monitorowania i przeciwdziałania ryzyku ICT, tak w przypadku projektu MiCA akcent normatywny położony został na jednolite uregulowanie całego rynku kryptoaktywów w UE (i wyeliminowanie różnorodności regulacyjnej na poziomie państw członkowskich, utrudniającej transgraniczne świadczenie usług), co odbywa się poprzez wskazanie ram regulacyjnych nadzoru rynku kryptoaktywów, tak w elementach mikroostrożnościowych, jak i makroostrożnościowych. Rynek kryptoaktywów, co słusznie podkreślono w preambule do MiCA, może generować zagrożenia dla stabilności finansowej w jej makroostrożnościowym wymiarze (tu zwłaszcza tzw. stabilne kryptowaluty). Celem tej regulacji ma stać się stworzenie jednolitych ram prawnych dla tego rynku, wspieranie innowacyjnych technologii na rynku finansowym, przy jednoczesnym zapewnieniu dobrego poziomu ochrony dla konsumentów i inwestorów oraz stabilności finansowej na rynku kryptoaktywów.

Krajowe i unijne organy nadzoru nad rynkiem kryptoaktywów pełnić będą szeroko pojęty nadzór nad tym rynkiem, w tym nad dostawcami usług z zakresu kryptoaktywów w zakresie udzielania zezwolenia na świadczenie przez nich usług: przechowywania kryptoaktywów i zarządzania nimi w imieniu osób trzecich; prowadzenia platformy obrotu kryptoaktywami; wymiany kryptoaktywów na walutę fiat lub inne kryptoaktywa; wykonywania zleceń związanych z kryptoaktywami w imieniu osób trzecich; subemisji kryptoaktywów; przyjmowania i przekazywania zleceń w imieniu osób trzecich czy doradztwa w zakresie kryptoaktywów, a także uprawnienia nadzorców krajowych lub unijnych do zawieszenia lub zakazania emisji kryptoaktywów lub świadczenia usług w zakresie kryptoaktywów, a także do prowadzenia dochodzeń w sprawie naruszeń przepisów dotyczących nadużyć na rynku.

Niewątpliwie MiCA będzie rozporządzeniem, którego założeniem jest posługiwanie się najnowocześniejszymi technologiami na rynku finansowym DLT. Skoro przyjęty na rynku finansowym regulacyjny paradygmat jest nadzorczy, to powstaje pytanie o możliwość i wręcz konieczność stosowania e-narzędzi nadzorczych przez krajowych i unijnych nadzorców dla zapewnienia bezpieczeństwa finansowego na rynku kryptoaktywów. EBA mocno przygotowuje się do e-nadzoru w projekcie MiCA; wskazuje się na potrzebę zatrudnienia specjalistów z zakresu ryzyka ICT i rynku kryptoaktywów.

MiCA reguluje tzw. zjawisko tokenizacji rynku finansowego, w projekcie bowiem wskazano na wymogi nadzorcze dotyczące emisji 3 grup tokenów (rodzajów kryptoaktywów): tokenów powiązanych z aktywami, tokenów będących pieniądzem elektronicznym (czy e-pieniądzem) oraz tokenów użytkowych.

Nadzorem w MiCA proponuje się objąć nie tylko emitentów kryptoaktywów, ale również dostawców usług z zakresu kryptoaktywów oraz ich outsourcerów (art. 66 MiCA), przy czym dobrze ustalono podział zadań między nadzorców krajowych i unijnych, tym ostatnim przyporządkowując bezpośredni nadzór z prawem do stosowania środków nadzorczych *sensu stricto*, włącznie z prawem do wydawania decyzji sankcyjnych nad tzw. znaczącymi tokenami. Klasyfikacja znaczących tokenów przez EBA (w zakresie kryptoaktywów powiązanych z aktywami i kryptoaktywów będących pieniądzem elektronicznym)[25] następować będzie na podstawie interesującego art. 39 MiCA, który powinien uwzględniać szeroko e-narzędzia nadzorcze, tak dla krajowych, jak i unijnych nadzorców. Skoro na postawie art. 39 MiCA EBA zaklasyfikuje tokeny jako znaczące na podstawie m.in.: wielkości bazy klientów, wartości wyemitowanych tokenów, liczby i wartości transakcji na tych tokenach czy znaczenia działalności transgranicznej emitenta tokenów, to informacja o tych kryteriach zbierana przez nadzorców krajowych od emitentów kryptoaktywów (na których zostaną nałożone obowiązki raportacyjne) i w tym zakresie przekazywana do EBA (co najmniej raz w roku) powinna być kompletowana i przechowywana za pomocą najnowocześniejszych i najskuteczniejszych e-narzędzi nadzorczych. Zaklasyfikowanie tokenu jako znaczącego spowoduje objęcie bezpośrednim nadzorem tych kryptoaktywów przez EBA na podstawie art. 98 MiCA.

Krajowe organy nadzorcze, choćby już tylko z uwagi na własne uprawnienia nadzorcze *stricte* nadzorcze i dochodzeniowe oraz konieczność zapewnienia współpracy transgranicznej (np. w zakresie paszportu europejskiego dla dostawców kryptoaktywów czy wymiany informacji nadzorczej) oraz z EBA i ESMA, będą musiały mocno rozwinąć e-narzędzia nadzorcze w celu wykonania różnorodnych obowiązków nadzorczych. Jak zawsze w unijnych rynkowych regulacjach nadzorczych zakres informacji, wzory formularzy, a być może także sposób i narzędzia realizacji procesów kontrolno-nadzorczych określone zostaną w RTS-ach i BTS-ach. W ramach nadzoru bezpośredniego nad tokenami znaczącymi EBA będzie miał m.in. prawo przeprowadzania dochodzeń, prawo do żądania przesyłu danych, zobowiązania do udzielenia niezbędnych informacji od emitentów, instytucji finansowych, ale i określonych podmiotów trzecich, z którymi znaczący emitenci zawarli ustalenia umowne; prawo do kontroli na miejscu; kontroli i oceny funkcjonowania systemów DLT emitenta.

Nadzór unijny i krajowy musi mieć możliwość analizy rozlicznych obowiązków raportacyjnych i monitorowania podmiotów nadzorowanych, co powinno się odbywać

[25] Projekt MiCA dopuszcza też dobrowolną klasyfikację tokenów jako znaczących przez ich emitentów w procesie ubiegania się o zezwolenie na emisję, co także oznacza konieczność stworzenia sprawnych kanałów przepływu informacji między nadzorcami poziomu krajowego a EBA.

w systemie internetowym za pomocą e-narzędzi, dających gwarancje szybkości analizy i wyselekcjonowania dzięki nowoczesnym funkcjom technicznym sytuacji zagrożeń w czasie rzeczywistym (zasadne wydaje się tu zwłaszcza wykorzystanie na większą skalę API, chmury, algorytmizacji nadzorczej i DLT).

Objęcie nadzorem dostawców zewnętrznych w rozporządzeniu MiCA to nie tylko ochrona dla klientów rynku finansowego, ale także dla stabilności finansowej poszczególnych segmentów tego rynku. Wyzwaniem nadzorczym dla organów nadzoru krajowych i unijnych stanie się również dbałość o poszanowanie przez podmioty finansowe zasady neutralności technologicznej (by nie forsować jednej tylko technologii), a tym samym i w tym aspekcie przeciwdziałać ryzyku koncentracji.

Wśród szczególnie istotnych postanowień MiCA trzeba zwrócić uwagę na obowiązek publikowania przez emitentów kryptoaktywów dokumentu informacyjnego[26] dotyczącego kryptoaktywów oraz spełnianie wymogów dotyczących ujawniania informacji. Dopiero po opublikowaniu dokumentu informacyjnego emitent kryptoaktywów będzie mógł oferować swoje kryptoaktywa w UE lub ubiegać się o dopuszczenie takich kryptoaktywów do obrotu na platformie obrotu (art. 10 MiCA). Natomiast organy nadzoru po zgłoszeniu dokumentu będą dysponowały kompetencją do zawieszenia lub zakazania danej emisji, żądania uwzględnienia w dokumencie informacyjnym dotyczącym kryptoaktywów dodatkowych informacji lub opublikowania informacji o niespełnianiu przez emitenta wymogów rozporządzenia. ESMA będzie prowadziła rejestr wszystkich dostawców usług w zakresie kryptoaktywów w UE wraz z informacjami na temat dokumentu informacyjnego dotyczącego kryptoaktywów przekazanego przez właściwe organy. W MiCA przewiduje się również rozpatrywanie skarg kierowanych przez klientów i inwestorów do nadzorców na naruszenia rozporządzenia MiCA także w formie elektronicznej (art. 95 MiCA).

Skalę przyszłych obowiązków raportacyjnych, stanowiących dobre pole dla rozwoju i stosowania SupTech, pokazuje dobrze także art. 112 MiCA, zgodnie z którym Komisja we współpracy z EBA i ESMA będzie przygotowywała sprawozdania dotyczące m.in.:

- liczby emisji kryptoaktywów w UE,
- liczby dokumentów informacyjnych dotyczących kryptoaktywów zarejestrowanych przez właściwe organy,
- rodzaju kryptoaktywów, ich kapitalizacji rynkowej,

[26] Małe i średnie przedsiębiorstwa, dla urzeczywistnienia zasady proporcjonalności, będą zwolnione z obowiązku publikowania takiego dokumentu informacyjnego w przypadku, gdy całkowita wartość emisji kryptoaktywów w okresie 12 miesięcy jest niższa niż 1 000 000 euro. Emitenci stabilnych kryptowalut nie będą podlegali obowiązkowi uzyskania zezwolenia właściwego organu krajowego, jeżeli wartość pozostających w obrocie stabilnych kryptowalut wynosi mniej niż 5 000 000 euro.

- liczby kryptoaktywów dopuszczonych do obrotu na platformie obrotu kryptoaktywami,
- oszacowania liczby mieszkańców UE, którzy posługują się kryptoaktywami wyemitowanymi w UE lub w nie inwestują,
- liczby i wartości przypadków nadużyć, ataków hakerskich i kradzieży związanych z kryptoaktywami zgłoszonych w UE,
- rodzajów nieuczciwych zachowań,
- liczby skarg otrzymanych przez dostawców usług w zakresie kryptoaktywów i emitentów tokenów powiązanych z aktywami,
- liczby skarg otrzymanych przez właściwe organy oraz informacji na temat przedmiotu otrzymanych skarg.

Oznacza to, że wcześniej informacje te będą gromadzone i przechowywane przez nadzór krajowy oraz przekazywane do EBA i ESMA. Jest to zatem obszar rodzący potrzebę stosowania w szerokim zakresie e-narzędzi nadzorczych, aby nadzór ten był skuteczny zarówno jeśli chodzi o działania nadzorcze *ex ante*, jak i *ex post*.

5. Uwagi końcowe

Kompetencje nadzorcze organów w analizowanych projektach rozporządzeń są silne, ale skuteczność nadzorcza będzie zależała do szerszego stosowania e-narzędzi służących realizacji tych kompetencji nad poszerzonymi podmiotowo i przedmiotowo cyfrowymi materiami prawnorynkowymi w DORA i MiCA. Skuteczność nadzoru będzie też powiązana z prawidłowym e-zarządzaniem ryzykiem ICT na poziomie podmiotów finansowych i również e-współpracą nadzorczo-zarządzającą między podmiotami finansowymi a nadzorcami krajowymi i unijnymi. Zarówno w DORA, jak i w MiCA kładzie się nacisk na *ex ante* pozyskiwanie informacji o zagrożeniach, które mogą mieć wpływ na stabilność rynku finansowego. Słusznie zakłada się w komentowanych regulacjach, że możliwe są zakłócenia systemu finansowego zagrożeniami w tzw. cyberprzestrzeni i że te zakłócenia mogą potencjalnie stanowić źródło ryzyka systemowego.

Skuteczność e-nadzoru uzależniona będzie w znacznym stopniu również od e-współpracy finansowej administracji nadzorczej skoncentrowanej na materii prawnorynkowej związanej z ryzykiem ICT, gdzie w sferze zainteresowania pozostają podmioty czynne i bierne tego zarządzania, a nacisk położony jest na jego cyfrową

formę[27]. *Sine qua non* tego procesu administrowania jest dostęp do infrastruktury internetowej oraz bezpieczne z niej korzystanie, co jest najistotniejsze w relacji instytucja finansowa i klient, a w sferze bezpieczeństwa systemu finansowego w ujęciu treściowym zabezpieczenie nowych form, usług i produktów finansowych przed ich negatywnym wpływem na stabilność finansową tak w wymiarze mikroostrożnościowym, jak i makroostrożnościowym (np. przeciwdziałanie praniu pieniędzy, nadzór nad kryptoaktywami), przy czym przy e-administrowaniu nadzorczym ważne jest również zapewnienie bezpieczeństwa w pozostałych obszarach prawa, np. ochrony danych osobowych klientów. Istotna staje się również ochrona przed cyfrowym wykluczeniem.

E-zarządzanie nadzorcze na rynku finansowego UE na przykładzie projektów DORA i MiCA obejmuje siatkę połączeń między podmiotami, którym przyporządkowano określone obowiązki, których funkcją jest nadzór nad cyfryzacją rynku finansowego UE. Chodzi tu zarówno o podmioty czynne, czyli ściśle współpracujące ze sobą organy nadzoru krajowego i unijnego, jak i podmioty bierne, a więc podmioty nadzorowane, które „pod okiem" nadzorców mają zarządzać ryzykiem ICT czy ryzykiem związanym z dostawcami usług kryptoaktywów na podstawie ujednoliconych w DORA i MiCA ram prawnych. Objęci nadzorem zostaną także dostawcy usług ICT i usług kryptoaktywów oraz ich outsourcerzy. Forma e-administracji nadzorczej wykorzystywana przy kontaktowaniu się podmiotów czynnych i biernych powinna wykorzystywać infrastrukturę internetową i cyfrową, bazującą na nowoczesnych innowacyjnych technologiach finansowych z obszaru SupTech.

E-administracja nadzorcza korzysta przede wszystkich z norm prawa publicznego, głównie powszechnie wiążących, ale może także posługiwać się normami *compliance* i *soft law*, konkretyzując wzorzec normatywny wyznaczany w rozporządzaniach i RTS-ach. Znamienne również, że nadzór krajowo-unijny uzyskał w analizowanych projektach mocne uprawnienia monitorowania ustaleń umownych między podmiotami finansowymi a zewnętrznymi dostawcami usług ICT czy między dostawcami usług kryptoaktywów a outsourcerami.

Filozofia przeciwdziałania ryzyku cyfrowemu związana jest ze współpracą między podmiotami finansowymi a organami nadzoru i jest to współpraca sieciowa i wielopłaszczyznowa, uwzględniająca zasadniczo prawidłowo zasadę proporcjonalności.

Niewątpliwie wzmocniona algorytmizacja nadzoru, która wypiera losowość, automatyczne integrowanie danych w sieci w celach analitycznych, bardziej efektywne

[27] Na marginesie warto wspomnieć, że e-proceduralne elementy dotyczące także kwestii nadzorczych pojawiają się w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, istotnej również dla kontaktów na rynku finansowym.

zarządzanie ryzykiem, monitoring w czasie rzeczywistym, postawienie na e-nadzór *ex ante* za pomocą e-narzędzi nadzoru spowoduje redukcję kosztów nadzoru. Stosowanie na szeroką skalę, co wydaje się niezbędne po wejściu w życie DORA i MiCA, e-narzędzi nadzoru powinno spowodować szerszą automatyzację, algorytmizację niektórych funkcji nadzorczych w obszarze raportowania i ryzyka zarządzania i *compliance*, które służyć mają kontroli materii realizowanej w środowisku cyfrowym.

E-nadzór jest potrzebny w obszarach, gdzie istnieje potrzeba wzmocnienia monitoringu napływających danych (które w DORA i MiCA znacząco się poszerzą) w czasie rzeczywistym i jak najszybszego reagowania na zagrożenia rynkowe, co może pomóc również w *ex ante* przeciwdziałaniu ryzykom makroostrożnościowym.

SupTech powinien w założeniu poprawić zdolności nadzorcze poprzez szybsze reagowanie, poprzez poznawanie w czasie rzeczywistym wskaźników ryzyka i reagowania w czasie rzeczywistym (API), co dać ma automatyzacja i przeniesienie się z form tradycyjnych na formy elektroniczne. W świetle projektów DORA i MiCA SupTech staje się strategią priorytetową dla nadzorców i niemożliwe będzie skuteczne prowadzenie nadzoru bez szeroko i systemowo stosowanych cyfrowych narzędzi o przeznaczeniu nadzorczym[28]. Potrzebny wydaje się wręcz swoisty nadzorczy *single rulebook* z e-narzędziami nadzorczymi. Na rozrost aktów prawnych i związanych z nimi obowiązków sprawozdawczo-raportacyjnych pomóc może ścisła, systemowa i pogłębiona automatyzacja oraz algorytmizacja niektórych obszarów nadzorczych[29].

Cyfryzacja nadzorcza nie może jednak powodować swoistej technologicznej zależności od dostawców technologii, aby nie kreować nowego ryzyka koncentracji i nie pozostawiać obszarów regulacyjnych poza polem nadzoru. Cyfryzacja nadzoru oznacza też konieczność poprawienia kompetencji cyfrowej wśród pracowników nadzoru, a nade wszystko, co słusznie podkreślono w raporcie FSB, istnieje konieczność zachowania nadzoru tradycyjnego z czynnikiem ludzkim i tradycyjnej interwencji, zwłaszcza w zakresie rozstrzygnięć nadzorczych[30].

Odpowiedź na pytanie, czy wszystkie kompetencje nadzorcze można realizować za pomocą nowoczesnych technologii, brzmi (na razie!?) „nie". E-narzędzia nadzorcze powinny dotyczyć kwestii technicznych, rutynowych, formalnych rozumianych jako przeniesienie sposobu załatwiania spraw na poziom informatyczny i za pomocą nowoczesnych e-narzędzi, jednak nie w tych kwestiach merytorycznych, w których potrzebna jest bardziej analiza dokumentacji przez człowieka (np. przed wydaniem

---

[28] Raport FSB z 2020 r. https://www.fsb.org/wp-content/uploads/P091020.pdf (3.05.2021), s. 1 i n.

[29] Poza ramami niniejszego opracowania pozostaje (bardzo ważne) zagadnienie dostępności, jawności i transparentności konstrukcji algorytmów.

[30] Raport FSB, s. 10.

decyzji administracyjnych, sankcyjnych). Algorytmizacja nadzoru nie może zakłócić procesu merytorycznej kontroli danych, kończącej się wydaniem decyzji nadzorczej. Wydaje się, że element personalny nadzoru jest i będzie zawsze potrzebny, aby na podstawie zinterpretowanych danych wydać decyzje nadzorcze.

Pożądane są natomiast wszelkie technologie chmurowe, algorytmy do optymalnego wykorzystania w procesach kontrolno-nadzorczych w zakresie integrowania i analizowania danych pozyskiwanych od podmiotów nadzorowanych oraz interfejsy programistyczne tworzone z myślą o podmiotach sieciowego i wielopłaszczyznowego e-zarządzania nadzorczego, pozwalające na pozyskiwanie informacji w czasie rzeczywistym. Narzędzia cyfrowe są już i mogą być w poszerzonej formule stosowane przez nadzór przy przeciwdziałaniu praniu pieniędzy, oszustwach finansowych, raportowaniu, zarządzaniu ryzykiem.

Cyfryzacja i elektronizacja są nieuniknione i potrzebne na rynku finansowym, ale potrzebny jest w związku z tym silny nadzór z silnymi instrumentami, w tym skutecznego technicznego oddziaływania nadzorczego w środowisku cyfrowym. Potrzebne jest także rozsądne wyznaczenie granic dla procesu cyfryzacji nadzorczej, aby z jednej strony nie została rozmyta odpowiedzialność na rynku finansowym, a zarazem z drugiej strony, aby nie „zadławić" innowacyjności i konkurencyjności FinTech i RegTech nieproporcjonalnymi rozwiązaniami nadzorczymi oraz rozsądnie ilościowo i jakościowo kształtować obowiązki raportacyjno-sprawozdawcze dla instytucji finansowych.

Skuteczność nadzoru na cyfrowym rynku finansowym zależy od tego, czy nadzorcy rozwiną swoje systemy nadzorcze i będą w większym stopniu niż dotychczas posługiwać się e-narzędziami nadzorczymi, i to zarówno jeśli chodzi o dane ilościowe, jak i jakościowe. Osiągnięcie celów nadzorczych DORA i MiCA zależy od możliwości objęcia nowej materii regulacyjnej skutecznymi i proporcjonalnymi dla nadzorowanych e-narzędziami nadzorczymi.

Bibliografia

Chłopecki A., *Sztuczna inteligencja. Szkice prawne i futurologiczne*, wyd. 2, Warszawa 2021.

Fedorowicz M., *O normatywnym pojęciu stabilności finansowej na rynku finansowym Unii Europejskiej w nowej architekturze nadzorczej*, „Studia Europejskie" 2017, nr 4, s. 73-94.

Fedorowicz M., *Osiąganie konwergencji nadzorczej mikroostrożnościowej i makroostrożnościowej w prawie rynku finansowego Unii Europejskiej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2018, nr 4, s. 155-169, https://doi.org/10.14746/rpeis.2018.80.4.12.

Prawo sztucznej inteligencji, L. Lai, M. Świerczyński (red.), Warszawa 2020.

Szostek D., *Blockchain a prawo*, Warszawa 2018.

Książka powstała w ramach realizowanego przez Katedrę Prawa Europejskiego Uniwersytetu Jagiellońskiego i koordynowanego przez prof. Sławomira Dudzika i dr hab. Ingę Kawkę projektu Jean Monnet Module pt. „E-administracja – europejskie wyzwania dla administracji publicznej w państwach członkowskich UE i krajach partnerskich/eGovEU+".

Zebrane w monografii artykuły naukowe dotyczą szerokiego spektrum zagadnień związanych z cyfrową transformacją administracji publicznej w Europie. Pierwsza część książki została poświęcona analizie e-administracji z perspektywy prawa europejskiego. Następnie cyfryzację administracji przedstawiono jako katalizator transformacji administracji otwartej, odpowiedzialnej i świadczącej e-usługi dla obywateli. Książka ukazuje również wspływ digitalizacji na funkcjonowanie polskiej administracji publicznej. Ostatnia część opracowania dotyczy e-administracji jako czynnika zwiększającego potencjał administracji w państwach członkowskich UE i państwach stowarzyszonych oraz na szczeblu międzynarodowym.

Monografia adresowana jest do badaczy zajmujących się administracją, prawem administracyjnym i europejskim, praktyków: sędziów, prokuratorów, urzędników państwowych, adwokatów i radców prawnych oraz studentów i doktorantów prawa, administracji i ekonomii. Mamy nadzieję, że publikacja poszerzy wiedzę na temat cyfryzacji administracji w Polsce i Europie oraz zachęci do dalszych studiów w tej dziedzinie.

WYDAWNICTWO
KSIĘGARNIA AKADEMICKA

https://akademicka.pl

ISBN 978-83-8138-673-9