Studia i Materiały, 1/2021 (34): 102–118
ISSN 1733-9758, © Wydział Zarządzania UW
https://doi.org/10.7172/1733-9758.2021.34.8

Platformizacja gospodarki cyfrowej – nowe wyzwania dla regulacji

Włodzimierz Szpringer[*]

Celem artykułu jest zbadanie zmieniającej się roli regulacji w gospodarce cyfrowej opartej na danych. Inspiracją dla niniejszego opracowania są najnowsze koncepcje regulacji platform cyfrowych (bigtechów), literatura z prawa i ekonomii, systemowa analiza prawa, praktyki i compliance, innowacje regulacyjne. Prawo powinno być technologicznie neutralne. Problem polega na akcentowaniu regulacji usług z uwzględnieniem prawnego kontekstu innowacji: ochrony konkurencji, zapobiegania nadużywaniu władzy rynkowej, np. w przypadku platform cyfrowych działających na dwu-(wielo)-stronnych rynkach. Prawa, często uchwalane w epoce analogowej, również muszą jednak dotrzymywać kroku technologii. Nowością jest uwypuklenie problemu wspierania prawa kodem lub przekształcania prawa w kod, nadzoru nad implementacją algorytmów opartych na sztucznej inteligencji, a także redefinicja roli prawa jako instrumentu zarządzania technologią.

Słowa kluczowe: platformy cyfrowe, rynki cyfrowe, usługi cyfrowe, finanse cyfrowe, zarządzanie technologiami, datafikacja, regulacja.

Nadesłany: 10.03.2021 | Zaakceptowany do druku: 18.06.2021

Platformization in the digital economy – new challenges for regulation

The aim of the article is to examine the changing role of regulation in a digital economy based on data. Inspiration of the study is based on the latest concepts of regulating digital platforms (BigTech), literature in the field of law and economics, systemic analysis of law, practice and compliance, regulatory innovations. The law should be technologically neutral. The problem consists in emphasizing the regulation of services, taking into account the legal context of innovation: competition protection, prevention of misuse of market power, e.g. in the case of digital platforms operating on two- (multi-)sided markets. However, the rights, often adopted in an analogue era, must also keep up with technology. It is a novelty to emphasize the problem of supporting the law by code or transforming the law into code, supervision over the implementation of algorithms based on artificial intelligence, as well as redefine the role of law as a technology management instrument.

Keywords: digital platform, digital platform, digital services, digital finance, technology management, datafication, regulation.

JEL: K24, L51

[*] **Włodzimierz Szpringer** – prof. dr hab., Katedra Prawnych Problemów Administracji i Zarządzania, Wydział Zarządzania, Uniwersytet Warszawski, Polska, https://orcid.org/0000-0003-3874-8906.
Adres do korespondencji: Wydział Zarządzania Uniwersytetu Warszawskiego, ul. Szturmowa 1/3, 02-678 Warszawa, Polska; e-mail: wszpringer@wz.uw.edu.pl.

1. Nowe technologie – problemy regulacji

Wzrost popularności produktów cyfrowych oraz rozwój systemów płatności wzmacniają trend platformizacji. Nowe technologie cyfrowe, szczególnie usługi chmury, AI i ML, analityka danych (Big Data) oraz coraz lepszy i tańszy dostęp do internetu, do urządzeń mobilnych, przyspieszają rozwój modeli pośrednictwa między stronami rynku. Istnieje kilka cech sprzyjających rozwojowi platform cyfrowych: usieciowienie, datafikacja, personalizacja. Platformizacja obejmuje sektory, w których kluczowe znaczenie mają dane, ale poszerza się także na inne sektory, które do tej pory w niewielkim stopniu korzystały z efektu sieci. Platformizacja dynamizuje innowacje i tworzy nowe szanse dla innych firm, które współpracują z platformami cyfrowymi (a zwłaszcza – z bigtechami) w ramach łańcucha (pętli) wartości czy wokół osi innowacji (Szpringer, 2020b, s. 49; Pakulska i Poniatowska-Jaksch, 2021, s. 35).

Regulacja może mieć znaczący wpływ na rozwój nowych technologii. To, czy jest to konstruktywne, zależy od tego, jak przepisy są ustanawiane i wprowadzane w życie. Czasami przepisy mogą pomóc w rozkwicie nowej technologii: dysponowanie przestrzenią do eksperymentowania było kluczowe dla rozwoju internetu. Obecnie neutralność sieci jest przedmiotem debaty, która może chronić start-upy (fintechy) przed zasiedziałymi operatorami próbującymi ograniczyć ich innowacyjność. Innym razem regulacja może być przeszkodą w rozwoju. Na przykład prawa autorskie zostały wprowadzone w internecie w taki sposób, że nadal utrudniają dostęp do wiedzy i realizację współpracy w wielu dziedzinach (Sunstein, 2014, s. 1385; Szpringer, 2020a, s. 50).

Komisja Europejska przedstawiła projekt nowych regulacji dotyczących wykorzystania technologii sztucznej inteligencji (AI). Zastosowanie technologii sztucznej inteligencji zostało podzielone na cztery kategorie ryzyka. Można je przedstawić w formie piramidy, na której szczycie znajdują się technologie niebezpieczne, stanowiące najwęższą grupę, np. systemy sztucznej inteligencji stanowiące niedopuszczalne ryzyko dla ludzi, w szkodliwy sposób manipulujące zachowaniem człowieka, a u jej podstawy technologie stanowiące minimalne ryzyko, np. filtry wyłapujące spam w poczcie elektronicznej. Systemy te nie stanowią zagrożenia dla praw ani bezpieczeństwa obywateli lub ryzyko to jest minimalne, więc nie potrzebują dodatkowych obostrzeń (DW 2021).

W sektorze finansowym regulacje tworzą przejrzystość, która zwiększa zaufanie do udziału w rynku. W ten sposób chroni się inwestorów i integralność rynku – dwa ważne cele, które w obecnych trendach ofert tokenów i giełd kryptowalut nie są w pełni osiągane. Jeśli te cele nie zostaną osiągnięte, inwestorzy mogą zostać oszukani i stracić zaufanie do rynku kapitałowego. Było wiele oszustw związanych z publicznymi ofertami monet (Initial Coin Offerings – ICO). Nawet jeśli ICO nie jest oszustwem, to jasne jest, że nie ujawnia się tak dużo ofert, jak mogłoby być, zakładając, że ICO podlegają regulacjom rynku kapitałowego. Obecnie wiele ICO omija przepisy dotyczące papierów wartościowych (Belcher i Narula, 2018).

Jeśli chodzi o kryptowaluty, wyzwania stojące przed organami regulacyjnymi, aby znaleźć odpowiednią równowagę, są szczególnie poważne. Jednym z powodów rozkwitu internetu w Stanach Zjednoczonych, a nie w Europie, były niewielkie regulacje. W niektórych przypadkach przestrzeganie litery prawa w systemie zdecentralizowanym może być uciążliwe, niepotrzebne lub po prostu niemożliwe. Kryptowaluty i blockchain tworzą nowy paradygmat regulacyjny i chociaż regulacja jest ważna, byłoby niefortunne, gdyby nadmierna regulacja spowodowała przeniesienie ciekawych projektów poza daną jurysdykcję. Jeśli przestrzeń jest zbyt ograniczona, inteligentni ludzie odchodzą, by pracować na innych obszarach, inwestycje są ograniczone, a tempo rozwoju spada (Szpringer, 2019, s. 30).

Co ciekawe, wiele elementów z tej technologii nie będzie podlegać regulacji w ramach obecnego paradygmatu regulacyjnego lub może wymagać zupełnie innych *rodzajów* regulacji; czasami regulacja jest wbudowana w technologię. Jednym z wyzwań jest ustalenie, które przepisy powinny mieć zastosowanie, a które nie pomagają osiągać celów zakładanych w regulacji. Na przykład wiele regulacji opiera się na istnieniu pośredników, takich jak giełdy, maklerzy czy centralne depozyty. W prawdziwie zdecentralizowanych sie-

ciach, podobnie jak w przypadku blockchaina bitcoin, sieć może w przejrzysty sposób utrzymywać zapisy i transfery ICO, a każdy może je audytować i weryfikować.

Compliance jest niezbędnym czynnikiem we współczesnym świecie, dbającym o bezpieczeństwo i zapobieganie szkodom dla konsumentów. Pomimo wielu starań o przejrzystość i odpowiedzialność w kwestii zgodności z przepisami jest to nie tylko techniczny problem, ale i kwestia zaufania. Teoretyczny model zgodności regulacyjnej ma na celu poprawę rozliczalności za systemy i dane i wprowadza wyższy stopień przejrzystości w zarządzaniu i kontroli. Podkreśla się w nim znaczenie dwóch technologii – Internetu rzeczy (IoT) i blockchaina, oraz pokazuje, jak lepiej wykorzystać i dostosować te technologie do kwestii prawnych i wzmocnić zaufanie do zgodności z przepisami. Technologie IoT i blockchain mogą pomóc w ustanowieniu większej odpowiedzialności i przejrzystości w dziedzinie regulacji i *compliance* (Chowdhury 2019).

Technologia regulacyjna („regtech") to stosunkowo nowy termin, używany do opisania nowych technologii zaprojektowanych w celu zmniejszenia rosnącego obciążenia związanego ze skutecznym zarządzaniem ryzykiem oraz przestrzeganiem przepisów nałożonych na organizacje w ostatnich latach, często w odpowiedzi na kryzysy, nadużycia i oszustwa. Regtech ma swoje korzenie w kryzysie finansowym z 2008 roku wynikające z „tsunami" regulacji wprowadzonych na całym świecie. Istnieją możliwości zastosowania technologii blockchain do celów regulacyjnych i compliance oraz zmniejszania kosztów przestrzegania przepisów i łagodzenia obciążeń regulacyjnych (Gozman, Lebenau i Aste 2020). Na przykładzie projektu sprawozdawczości regulacyjnej w dziedzinie kredytów hipotecznych zidentyfikowano ryzyko utraty kontroli i nadzoru oraz wyzwania i kompromisy nieodłącznie związane ze zdecentralizowanym podejściem do regulacji.

Platforma cyfrowa jako logika organizacyjna w znaczący sposób przekształciła działalność innowacyjną w wielu sektorach. Platformy cyfrowe są badane z dwóch perspektyw: ekonomicznej (tj. jako jedno- wielostronny rynek) i technologicznej (czyli jako infrastruktura innowacji) (Runyu, 2021). Technologia blockchain może generować różne korzyści. Mogą one zmienić nie tylko płatności, ale także branżę papierów wartościowych, bankowość inwestycyjną, rachunkowość i audyt itd. Jest to wciąż innowacja i musi pokonać różne przeszkody, zanim osiągnie swój pełny potencjał. Regulacje mogą mieć wpływ na to, jak daleko i jak szybko technologia może się rozwijać. W związku z tym podejścia regulacyjne musiałyby zrównoważyć korzyści innowacyjności, a także problem zapobiegania aktualizacji ryzyka systemowego dla systemu finansowego (Yeoh, 2017). Przykładowo – amerykańska Komisja Giełd i Papierów Wartościowych (Securities and Exchange Commission – SEC) jest skłonna zwolnić niektóre aktywa cyfrowe oparte na łańcuchu bloków z traktowania ich jako papierów wartościowych (HLRev. 2019).

DLT Blockchain i inne technologie rozproszonych rejestrów mają ogromny potencjał tworzenia wartości biznesowej, ale nie jest to jeszcze szeroko przyjęte. Korporacyjne systemy blockchain są uznawane za rozwiązania istniejących problemów operacyjnych, ale ich potencjał dostarczania wartości poprzez możliwości strategiczne nie zawsze jest dobrze rozumiany. Czerpiąc z literatury na temat sojuszy strategicznych z perspektywy firmy opartej na zasobach, można zidentyfikować ścieżki, dzięki którym systemy blockchain mogą przyczyniać się do strategicznych zdolności firmy, a co za tym idzie, do jej trwałej przewagi konkurencyjnej. Uczestnictwo w blockchain może ułatwić korzystanie z istniejących zdolności strategicznych, a także wzmacniać możliwości współpracy i dalszego rozwoju firmy (Yuthas, Sarason i Aziz, 2021).

Ekosystemy zdecentralizowanych finansów (DeFi) często działają poza granicami regulacji. W niektórych obszarach ustalenie, czy działalność wykracza poza ten obszar, może być stosunkowo proste. W innych obszarach analiza regulacyjna może być niezwykle złożona i zniuansowana. Zrozumienie otoczenia regulacyjnego we wszystkich odpowiednich jurysdykcjach i odpowiednich ustaleniach strukturalnych jest niezbędnym krokiem dla każdego, kto jest zaangażowany w działalność DeFi – niezależnie od tego, czy zamierza działać na zasadach regulowanych, czy nieregulowanych, gdyż może to mieć konsekwencje nie tylko finansowe, lecz także karne. Założyciele, deweloperzy, emitenci, operatorzy, dostawcy i użytkownicy ponoszą to ryzyko,

które może powstać niezależnie od tego, czy działanie lub zarządzanie jest scentralizowane, czy zdecentralizowane (Linklaters, 2020).

Zasób cyfrowy może być całkowicie nieuregulowany w swojej prostej formie, takiej jak bitcoin. Jeżeli jednak dana firma umożliwia zawarcie kontraktów pochodnych w odniesieniu do nieregulowanego składnika aktywów bazowych, pakietowanie lub tworzenie dwustronnych aktywów i zobowiązań związanych ze zmianami w nieregulowanym instrumencie bazowym może samo w sobie stanowić działalność regulowaną. Oznacza to, że działalność na rynku wtórnym może być regulowana niezależnie od tego, że obrót podstawowym aktywem bazowym nie jest regulowany. Niestety, na rynku kryptoaktywów nadal istnieje niepewność regulacyjna, która zamazuje kluczową z punktu widzenia prawa kwestię odpowiedzialności: „Unregulated currencies and finance are cool in theory – but who is responsible when it goes wrong?" (Emerging payments 2020).

Postępująca cyfryzacja i wielka ilość danych, z którymi muszą się zmierzyć nadzorcy, to główne powody, dla których rozwój technologii w obszarze nadzoru jest potrzebny (suptech), a także w sferze *compliance* (regtech). Automatyzacja wielu procesów może pomóc także w uniknięciu błędów ludzkich, które mogą się pojawić przy powtarzalnych zajęciach, takich jak przenoszenie danych do tabelki. W pewnej perspektywie czasowej możemy liczyć także na sprawowanie nadzoru w czasie rzeczywistym. Rozwój narzędzi RegTech i SupTech może istotnie przyczynić się do poprawy efektywności w zakresie nadzoru oraz zarządzania, gdyż kluczowe jest takie raportowanie danych (czy pozyskiwanie ich przez regulatora), które rzeczywiście są potrzebne na dany moment. Regulatorzy wskazują na możliwość korzystania z niestandardowych danych o podmiotach regulowanych (w tym w zakresie ich działalności w mediach społecznościowych).

2. Pakiet regulacji usług i rynków cyfrowych

Działania UE na rzecz pogłębienia jednolitego rynku usług cyfrowych, które zwiększą suwerenność i konkurencyjność cyfrową Europy, pozostają sprawą priorytetową i jednym z najważniejszych wyzwań. Internet nie jest taki sam jak w 2000 r., kiedy to przyjęta została dyrektywa o handlu elektronicznym (Dziennik Urzędowy L 178, 17/07/2000). Skala korzystania z usług cyfrowych, modele biznesowe i różnorodność oferowanych usług znacząco się zmieniły. Do tego państwa członkowskie przyjęły zróżnicowane podejścia do implementacji tej dyrektywy, co negatywnie oddziałuje na świadczenie usług cyfrowych w całej UE. To tylko jeden z argumentów uzasadniających prace nad nowym, unijnym aktem prawnym o usługach cyfrowych i stworzeniem jasnych, przejrzystych i systemowych regulacji wzmacniających jednolity rynek cyfrowy UE (Szpringer, 2017, s. 37; RM 2020a).

Rada UE przyjęła rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz. Urz. UE L 186/57, 11/07/2019). Celem Rozporządzenia jest stworzenie sprawiedliwych, przejrzystych i przewidywalnych warunków funkcjonowania platform internetowych i wyszukiwarek, na których małe, średnie i mikroprzedsiębiorstwa (dalej: „MŚP") oferują konsumentom swoje usługi lub towary (tzw. P2B – *Platform to Business*). U podstaw decyzji o uregulowaniu tej kwestii leżały przesłanki nadmiernego narzucania przez platformy internetowe swoich warunków, które nie zawsze były jasne i sprawiedliwe, a także ograniczały możliwości prowadzenia działalności gospodarczej przez MŚP na platformach bigtechów.

Obecnie pierwszy projekt w UE [Digital Services Act, COM(2020) 825 final 2020/0361 (COD)] wprowadza m.in. nowe przepisy dotyczące usług cyfrowych, w tym mediów społecznościowych, platform handlu elektronicznego i innych platform internetowych działających w Unii Europejskiej. Dotyka kluczowych zagadnień dla rozwoju sieci, m.in. usuwania nielegalnych treści z internetu, ochrony wolności słowa, zasad moderowania treści przez platformy internetowe, reklamy online. Drugi akt [(Digital Market Act, COM(2020) 842 final 2020/0374(COD)] jest nakierowany na zapewnienie otwartości rynku cyfrowego na konkurencję. Obie regulacje służą jednemu celowi: zagwarantowaniu, aby użytkownicy mieli dostęp do szerokiego wyboru bezpiecznych produktów i usług w internecie, a także, by przedsiębiorstwa działające

w Europie mogły swobodnie i sprawiedliwie konkurować w internecie, podobnie jak robią to poza nim (RM 2020b).

Regulacja o usługach cyfrowych (DSA) deroguje dyrektywę o handlu elektronicznym, część przepisów przeniesie do rozporządzenia, wprowadzając tam również nowe regulacje. Od czasu jej uchwalenia sytuacja platform internetowych znacznie się zmieniła. Nowy akt wprowadzi wiążące przepisy z wieloma nowymi obowiązkami w zakresie usług cyfrowych. Obejmie on wszystkie usługi cyfrowe łączące konsumentów z towarami, usługami lub treściami. Inicjatywa przewiduje m.in. zasady dotyczące usuwania nielegalnych towarów, usług i treści, obowiązki przejrzystości w działaniu algorytmów i reklamy internetowej, ułatwianie analitykom dostępu do kluczowych danych platformy, czy współpracę organów publicznych państw UE w celu egzekwowania przepisów na całym jednolitym rynku. Platformy, których obiorcami jest ponad 10% ludności UE, zostałyby objęte szczególnym nadzorem.

Regulacja o rynkach cyfrowych (DMA) dotyczy negatywnych konsekwencji niektórych działań największych platform internetowych, tzw. strażników dostępu. Platformy te – przez swoją silną pozycję – stanowią dla użytkowników biznesowych ważną drogę dostępu do swoich klientów. Mogą angażować się w nieuczciwe praktyki polegające na ograniczaniu tego dostępu. W rzeczywistości funkcjonują więc jak strażnicy ekosystemu cyfrowego. Inicjatywa Komisji Europejskiej zdefiniuje pojęcie „strażników dostępu" oraz mechanizm egzekwowania nowych obowiązków i zakazów. Sankcje będą mogły obejmować grzywny w wysokości do 10% światowego obrotu przedsiębiorstwa (UKE 2020).

W ramach tego *sui generis* kodeksu usług cyfrowych zaproponowano instrumenty prawne, mające na celu rozwiązanie problemu dominacji kilku dużych platform internetowych na cyfrowym, wspólnym rynku. Komisja Europejska zaleca powołanie specjalnego, ponadnarodowego organu na poziomie UE, którego zadaniem byłoby gromadzenie informacji pochodzących od dużych platform internetowych, pełniących funkcję „strażników dostępu" do cyfrowego rynku online. Przepisy o kontroli *ex ante* (prewencyjnej) dotyczą dużych platform internetowych, których celem jest w szczególności:

– sprecyzowanie kryteriów, na podstawie których platformy internetowe zostaną zakwalifikowane do kategorii „strażników dostępu" (przykładowo: efekty sieciowe, wielkość bazy użytkowników lub zdolność do wykorzystywania danych na różnych rynkach);
– stworzenie jasno zdefiniowanych i z góry określonych obowiązków i zakazanych praktyk obowiązujących na rynku cyfrowym (ang. *blacklisted practices*), przykładowo: zakaz pewnych form autopreferencji lub wymuszania akceptacji dodatkowych warunków handlowych, które ze względu na swój charakter nie mają związku z podstawowym stosunkiem umownym;
– wprowadzenie możliwości, w przypadkach uznanych za konieczne, nałożenia na duże platformy, działające jak „strażnicy dostępu", odpowiednich środków prewencyjnych (np. nałożenie obowiązku umożliwienia dostępu do danych nieosobowych specyficznych dla danej platformy lub nałożenie szczególnych wymogów dotyczących przenoszenia danych osobowych) (Socha 2020).

DSA reguluje zagadnienia związane z moderacją treści, pozycjonowaniem, profilowaniem reklam i wykorzystywaniem algorytmów do rekomendowania treści. DMA z kolei nakłada na największe platformy szereg dodatkowych obowiązków i wprost zakazuje wielu nieuczciwych praktyk, które platformy obecnie stosują wobec swoich użytkowników oraz klientów biznesowych. Obie regulacje wprowadzają też nowy instytucjonalny system nadzoru nad platformami, wysokie kary (do 6% rocznego obrotu w DSA i do 10% rocznego obrotu w DMA) oraz nowe narzędzia do dyspozycji organów, w tym tych krajowych.

DSA to regulacja „o usługach cyfrowych", która również dotyczy bardzo dużych platform internetowych (bigtechów), mających ponad 45 mln użytkowników. Projekt regulacji rynków cyfrowych DMA dotyczy firm o rocznym obrocie przekraczającym w Europie 6,5 mld euro w ciągu ostatnich trzech lat, o wartości rynkowej 65 mld euro i oferujących usługi w co najmniej trzech krajach UE. Proponowane przepisy określają listę nakazów (takich jak udostępnianie pewnych rodzajów danych konkurentom i organom regulacyjnym) i zakazów, wśród których jest wymóg zaprzestania faworyzowania własnych usług

na platformach należących do bigtechów. Zakładają też nałożenie kar w wysokości do 10% rocznych globalnych obrotów w przypadku firm, które nie stosują się do przepisów, a nawet umożliwiają podjęcie decyzji o podziale firmy. Przedstawiciele Google, Microsoft, Facebook oraz Apple przesłali do Komisji Europejskiej swoje opinie dotyczące możliwości powołania organu, którego celem byłoby gromadzenie informacji od dużych platform internetowych oraz nowych przepisów o kontroli *ex ante*. Zdaniem Google jakkolwiek nowe przepisy mogą być korzystne dla rynku usług cyfrowych, to zbyt restrykcyjne środki skierowane przeciwko dużym platformom internetowym mogą zahamować rozwój i innowacje. Google podkreśla, że duże platformy sieciowe napędzają rozwój gospodarki. Mapy Google umożliwiają Europejczykom zaoszczędzenie ok. 1180 milionów godzin rocznie oraz zapewniają przedsiębiorcom bezpłatny dostęp do „listowania" w wyszukiwarce Google, dzięki czemu są oni widoczni dla konsumentów, poszukujących lokalnych towarów i usług. YouTube umożliwia natomiast artystom zdobycie nowej publiczności i pomaga małym firmom zwiększyć skalę działalności.

Apple dodaje, że interwencje regulacyjne muszą uwzględniać różnorodność modeli biznesowych platform internetowych, które świadczą bardzo różne usługi cyfrowe, często na zróżnicowanych rynkach, a także inaczej spieniężają swoje usługi. W związku z tym producent sprzętu hardware apeluje o ostrożne definiowanie „strażników dostępu" i przysłowiowe niewrzucanie wszystkich dużych platform internetowych do jednego worka. Facebook z kolei podkreśla, że bariery wejścia na rynek online są niskie, natomiast zdolność do oferowania produktów i usług, które przyciągają użytkowników, jest kluczowym czynnikiem stymulującym konkurencję.

Stworzenie listy zakazanych praktyk na rynku cyfrowym może być problematyczne, ponieważ w dynamicznie rozwijających się branżach cyfrowych praktyki dzisiaj traktowane jako szkodliwe, w stosunkowo krótkim czasie, mogą okazać się nieistotne z handlowego punktu widzenia. Aby innowacja mogła się rozwijać w UE, koszt adaptacji do nowych przepisów nie może nadmiernie obciążać sektora małych i średnich przedsiębiorstw oraz start-upów (fintechów). Komisja Europejska ma obowiązek ustalić sprawiedliwe zasady gry, które nie będą sprzyjać wyłącznie wybranym, największym graczom cyfrowego rynku (bigtechom). Platformy internetowe przynoszą znaczne korzyści dla konsumentów i innowacji. Ponadto ułatwiają one handel oraz otwierają zupełnie nowe możliwości biznesowe dla przedsiębiorców, ułatwiając im ekspansję i dostęp do nowych rynków.

Niejasne jest pojęcie „dużych platform internetowych, zachowujących się jak strażnicy dostępu". Ponadto podkreśla się brak potrzeby kreowania nowych instrumentów prawnych, ponieważ istniejący reżim europejskiego prawa konkurencji jest w stanie samodzielnie rozwiązać problem dominacji kilku platform internetowych na rynku cyfrowym. Istnieje projekt stworzenia listy zakazanych praktyk na rynku cyfrowym. Powstaje pytanie, czy da się takie praktyki wyliczyć enumeratywnie. Można wskazać na pomysł powołania specjalnego organu do gromadzenia informacji od dużych platform, jak również postulat uregulowania auto-preferencji (ang. *self-preference*) stosowanej przez duże platformy internetowe (Iwańska i Głowacka, 2020).

Nie będzie możliwe arbitralne usuwanie legalnych treści; obecnie przepisy zobowiązują platformy do reakcji na bezprawne treści: jeśli wiedzą o nich, ale ich nie zablokują, mogą ponosić za nie odpowiedzialność. Sprzyja to jednak temu, że z platform, obok hejtu i innych naruszeń, znikają także legalne (i pożyteczne) materiały, a „ocenzurowani" użytkownicy nie mają szans na skuteczną obronę. Zgodnie z DSA decyzje platform o usunięciu treści będą zapadały w sposób dużo bardziej przejrzysty. Użytkownicy będą szczegółowo informowani przez platformy m.in. o przyczynach blokady oraz o tym, w oparciu o jaki mechanizm została ona nałożona. Uzyskają szansę na przedstawienie swoich argumentów oraz gwarancję, że finalnych decyzji nie będą podejmowały algorytmy. Komisja proponuje też system niezależnego nadzoru nad ostatecznymi decyzjami platform w postaci specjalnych organów pozasądowych powołanych do rozpoznawania sporów o treści (nie wyłączając jednak możliwości odwołania się do sądu).

Powyższe procedury mają dotyczyć zarówno treści zgłoszonych do moderacji jako naruszających prawo, jak i materiałów, które automatyczne filtry platformy „wyłapią" jako niezgodne z jej regulami-

nem. Niektóre z rozwiązań proponowanych w DSA funkcjonują już na poszczególnych platformach. Regulacja wprowadza jednak wyższy standard i gwarantuje użytkownikom, że firmy internetowe nie będą go dowolnie zmieniać. Gwarancje te nie odnoszą się natomiast do bardziej „miękkich" środków moderacji niż blokowanie, takich jak np. zmniejszenie zasięgów postów (tzw. *shadow bans*). Wyjaśnieniu takich praktyk może służyć przewidziany w projekcie obowiązek cyklicznego publikowania zbiorczych danych obejmujących nie tylko informacje o nałożonych blokadach, ale także właśnie m.in. o działaniach powodujących ograniczenie widoczności publikowanych materiałów. Propozycje te należy ocenić pozytywnie.

Na niektórych platformach użytkownicy mogą obecnie korzystać z bibliotek reklam i uzyskać przynajmniej podstawowe wyjaśnienie, dlaczego dana platforma zdecydowała się wyświetlić mu konkretną reklamę. Zarówno jednak treści wyjaśnień, jak i zawartość biblioteki zależą od dobrej woli platform, które w każdej chwili bez żadnych konsekwencji mogą te narzędzia zmienić lub zlikwidować. DSA przewiduje, że wszystkie platformy internetowe, które stosują reklamy, będą musiały wyjaśnić każdej osobie, jakie kryteria zadecydowały o pokazaniu jej konkretnego komunikatu, zaś bardzo duże platformy (czyli takie, które mają więcej niż 45 mln aktywnych użytkowników miesięcznie, np. Facebook czy YouTube) będą miały obowiązek prowadzić publiczną bibliotekę wszystkich reklam, zawierającą m.in. informacje o tym, do ilu osób dotarła reklama i jakie kryteria targetowania wybrali reklamodawcy (Iwańska i Głowacka, 2020).

Wymogi dla przejrzystości targetowania w propozycji Komisji są jednak zbyt ogólne. Platformy będą miały obowiązek informować tylko o „głównych" kryteriach profilowania, a nie o wszystkich, co pozostawia szerokie pole do interpretacji. Przepisy nie wspominają wyraźnie o tym, że platformy powinny wyjaśnić nie tylko kryteria wybrane przez reklamodawcę, ale również te, które dobrały ich własne algorytmy odpowiedzialne za to, kto ostatecznie zobaczy czy usłyszy daną reklamę. W praktyce może to oznaczać, że nadal trudno będzie wykryć nadużycia, takie jak pozycjonowanie i profilowanie reklam na podstawie bardzo wrażliwych cech (np. dotyczących orientacji seksualnej czy zdrowia). DSA ustanawia minimalny standard przejrzystości dla algorytmów, które platformy wykorzystują do personalizowania i rekomendowania treści, czyli np. szeregowania postów na Facebookowej osi czasu czy prezentowania rekomendacji na YouTube. Platformy będą musiały poinformować swoich użytkowników o głównych parametrach, które wykorzystują ich systemy.

Nowe zasady pozwolą też użytkownikom zupełnie zrezygnować z personalizacji (i zamiast tego np. wyświetlać treści chronologicznie). Komisja otwiera też użytkownikom możliwość zmiany parametrów tych systemów. Założenie jest dobre: takie rozwiązanie zwiększy kontrolę nad tym, jakie treści do nas docierają. Jednak wyłącznie od woli platform będzie zależało, czy takie „suwaki" w ogóle udostępnią swoim użytkownikom i co pozwolą im zmodyfikować. Takie rozwiązanie raczej nie umożliwi ingerencji w logikę algorytmu, który premiuje zaangażowanie i ma sprzyjać temu, by użytkownicy zostawiali jeszcze więcej danych i oglądali jeszcze więcej reklam.

Będzie mniej profilowania i większy wybór dla użytkowników (ale platformy nadal pozostaną „zamkniętymi ogrodami"). Po najdalej idące rozwiązania Komisja sięgnęła w Digital Markets Act. Ta regulacja będzie miała zastosowanie wyłącznie do tzw. strażników dostępu (*gatekeepers*), czyli platform, które mają największy wpływ na to, jak wygląda cyfrowa rzeczywistość. Kryteria „gatekeepera" spełniają już teraz Google, Apple, Facebook i Amazon (GAFA). Szereg zakazów, które przewiduje Digital Markets Act, daje nadzieję na ograniczenie nadużyć wobec użytkowników, zwłaszcza jeśli chodzi o profilowanie i zmuszanie ich do korzystania z określonych rozwiązań dostarczanych przez dominujące platformy.

Proponuje się szereg zakazów, z czym łączą się także zastrzeżenia i wątpliwości. Przewiduje się zakaz łączenia danych osobowych z różnych serwisów i źródeł: np. Google nie będzie mógł połączyć danych użytkowników pochodzących z YouTube'a i z wyszukiwarki Google Search, Facebook nie będzie mógł tworzyć jednego profilu dla osoby korzystającej z Facebooka i Instagrama, nie wzbogaci też tego profilu o dane zebrane z innych stron internetowych. Daje to realną szansę na ograniczenie głębokości profilowania i – w efekcie – może ukró-

cić takie praktyki jak „mikrotargetowanie" (mikroprofilowanie). Zakazuje się zmuszania użytkowników do korzystania z różnych usług tej samej platformy: w praktyce może to oznaczać, że telefon z Androidem nie będzie wymagał od użytkownika założenia konta Google (Iwańska i Głowacka, 2020).

Przewiduje się możliwość odinstalowania preinstalowanych aplikacji, a także zakaz preferowania własnych usług: np. Apple nie będzie mógł narzucić użytkownikom swoich urządzeń korzystania z przeglądarki Safari. Nadal istnieją możliwości na podstawie RODO – (Rozporządzenie o Ochronie Danych Osobowych – RODO, ang. General Data Protection Regulation – GDPR, Dz. Urz. UE L 119/1 4/05/2016) wykonywania prawa do przenoszenia danych.

Nie ma jednak wymogu otwarcia zamkniętych ekosystemów platform i zapewnienia interoperacyjności z innymi podmiotami. Taki obowiązek został wprowadzony przez Komisję jedynie w ograniczonym zakresie, który w praktyce nie doprowadzi do zmniejszenia dominacji największych platform – nie tak łatwo będzie po prostu usunąć Facebooka, jeśli nie będziemy mogli za pośrednictwem innej platformy społecznościowej porozmawiać ze znajomymi, którzy na Facebooku zostaną. Nie będziemy też mogli za pomocą niezależnych od platform narzędzi uzyskać dostępu do swojego profilu i go zmodyfikować, czy ustawić własnych filtrów treści, które chcemy lub których nie chcemy oglądać (Iwańska i Głowacka, 2020).

Można wskazać kilka mechanizmów ekonomicznych, które kształtują konkurencję między platformami. Pozytywne efekty sieciowe prowadzą zwykle do sytuacji dominacji na rynku: jedna platforma „wygrywa" rynek, nie pozostawiając prawie nic swoim konkurentom. Istnieją wszelako siły przeciwdziałające monopolizacji, które mogą pozwolić kilku konkurującym platformom utrzymać się na rynku. Interoperacyjność i multihoming zmieniają zasady gry, o ile istotnie determinują formę konkurencji istniejącej między platformami (Belleflamme, 2020a). Chociaż pozytywne efekty sieciowe skłaniają użytkowników do skupiania się na jednej platformie, istnieją inne siły, które mogą skłonić użytkowników do preferowania różnych platform. Mogą również zaistnieć sytuacje, które pozwalają konkurującym platformom współistnieć na tym samym rynku.

3. Pakiet regulacji finansów cyfrowych

Koncepcja rozporządzenia w sprawie rynków kryptoaktywów i zmieniający dyrektywę (UE) 2019/1937 Markets-In-Crypto-Assets Regulation MiCA (COM(2020) 593 final 2020/0265(COD)) stanowią próbę kompleksowego uregulowania funkcjonowania kryptoaktywów w obrocie. MiCA to akt prawny definiujący warunki prowadzenia działalności w zakresie kryptoaktywów, a równocześnie część pakietu dotyczącego finansów cyfrowych (Digital Finance Package). Pakiet ten ma na celu umożliwienie i wspieranie wykorzystania potencjału finansów cyfrowych w zakresie innowacyjności i konkurencji, przy jednoczesnym ograniczeniu ryzyka.

Oprócz regulacji rynku kryptoaktywów pakiet zawiera także projekt regulacji infrastruktur rynkowych na podstawie technologii rozproszonego rejestru DLT Blockchain (COM(2020) 594 final 2020/0267(COD)), w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience of the Financial Sector – DORA, COM(2020) 595 final 2020/0266(COD)) oraz wniosek w sprawie wyjaśnienia lub zmiany niektórych powiązanych przepisów w zakresie unijnych usług finansowych. Jako cele regulacji Komisja wskazuje zapewnienie pewności prawa, wspieranie innowacyjności, zapewnienie odpowiedniego poziomu ochrony konsumentów i inwestorów oraz integralności rynku, a także zapewnienie stabilności finansowej (PWC 2020).

Rozporządzenie MiCA reguluje status kryptoaktywów, dzieląc je na 3 następujące kategorie:

- Tokeny powiązane z aktywami (*asset-referenced tokens*) rozumiane jako kryptoaktywa, które mają utrzymywać stabilną wartość dzięki powiązaniu z wartością szeregu walut będących prawnymi środkami płatniczymi, co najmniej jednego towaru, co najmniej jednego kryptoaktywa lub połączenia takich aktywów.
- Tokeny będące pieniądzem elektronicznym/e-pieniądzem (*e-money tokens*), rozumiane jako kryptoaktywa wykorzystywane głównie jako środek wymiany, które mają utrzymywać stabilną wartość dzięki powiązaniu z walutą fiat będącą prawnym środkiem płatniczym.

- Kryptoaktywa inne niż tokeny powiązane z aktywami lub tokeny będące pieniądzem elektronicznym (*crypto-assets other than asset-referenced tokens* lub *e-money tokens*), w tym tokeny użytkowe.

Jako tokeny użytkowe Komisja wskazuje kryptoaktywa, które mają zapewnić dostęp cyfrowy do danego towaru lub usługi, dostępny w technologii rozproszonego rejestru, akceptowany wyłącznie przez emitenta tego tokena. Ustawodawca unijny wyłącza z zakresu projektu m.in. kryptoaktywa kwalifikowane jako instrumenty finansowe w rozumieniu MIFID II oraz pieniądz elektroniczny, z wyjątkiem kryptoaktywów, które kwalifikują się jako tokeny będące pieniądzem elektronicznym na podstawie stosownego rozporządzenia.

Projekt przewiduje regulacje odnoszące się zarówno do samych emitentów kryptoaktywów, jak też do podmiotów, które świadczą usługi z nimi związane. Będą to podmioty świadczące usługi m.in. w zakresie prowadzenia platformy obrotu kryptoaktywami, ich subemisji oraz przyjmowania lub przekazywania zleceń związanych z kryptoaktywami. Z zakresu rozporządzenia wyłączone zostały m.in. krajowe banki centralne państw członkowskich, gdy działają w charakterze władz monetarnych oraz osoby, które świadczą usługi w zakresie kryptoaktywów wyłącznie na rzecz swoich jednostek dominujących, swoich jednostek zależnych lub innych jednostek zależnych swoich jednostek dominujących. Regulacja przewiduje szereg obowiązków dotyczących podmiotów uczestniczących w emisji kryptoaktywów. Ustawodawca unijny różnicuje wymogi w zależności od rodzaju kryptoaktywa, podchodząc bardziej rygorystycznie do tokenów powiązanych z aktywami oraz tokenów będących pieniądzem elektronicznym.

Wymóg uzyskania zezwolenia na publiczne oferowanie tokenów i ubieganie się o dopuszczenie aktywów do obrotu na platformie obrotu dotyczy emitentów tokenów powiązanych z aktywami oraz tokenów będących pieniądzem elektronicznym. Zezwolenie mogą uzyskać wyłącznie podmioty posiadające siedzibę na terenie państwa członkowskiego, a jego uzyskanie wiąże się z możliwością świadczenia usług na terenie całej UE. Projekt przewiduje wyjątki od obowiązku uzyskania zezwolenia. Obowiązek publikacji dokumentu informacyjnego dotyczącego kryptoaktywów (*white paper*) w odpowiednim standardzie spoczywa na emitentach, którzy chcą dokonać oferty publicznej lub ubiegają się o dopuszczenie kryptoaktywów do obrotu na platformie obrotu. Dokument musi zostać przekazany właściwemu organowi nadzorczemu i opublikowany. Powinien przekazywać najważniejsze informacje dotyczące kryptoaktywa, jak informacje na temat emitenta, praw i obowiązków z nim związanych oraz powiązanego ryzyka. Dokument dotyczy wszystkich rodzajów kryptoaktywów objętych rozporządzeniem, przy czym zakres informacji ujawnianych w dokumencie różni się w zależności od rodzaju kryptoaktywa.

Projekt wyróżnia kategorie znaczących tokenów powiązanych z aktywami oraz znaczących tokenów będących pieniądzem elektronicznym. Kryptoaktywa kwalifikowane pod tym pojęciem mogą być wykorzystywane przez dużą liczbę posiadaczy oraz posiadać szczególne znaczenie pod kątem stabilności finansowej, transmisji polityki pieniężnej lub suwerenności monetarnej. Z uwagi na to kryptoaktywa kwalifikowane zostały objęte bardziej rygorystycznymi wymogami, co obejmuje m.in. wyższe wymogi kapitałowe w stosunku do emitentów, wymóg posiadania polityki zarządzania płynnością oraz objęcie nadzorem EBA (European Banking Association).

Komisja przedstawia także regulacje odnoszące się do dostawców usług w zakresie kryptoaktywów. Podmioty te zobowiązane będą m.in. do uzyskania zezwolenia na prowadzenie działalności, a jednym z wymogów jej przyznania będzie posiadanie siedziby statutowej w państwie członkowskim. Ponadto ESMA zostanie zobowiązana do utworzenia i prowadzenia rejestru dostawców w zakresie kryptoaktywów, który poza samymi informacjami na temat dostawcy obejmować będzie również zaakceptowane i opublikowane *white papers*. Rozporządzenie ustanawia ponadto przepisy regulujące zapobieganie nadużyciom na rynku kryptoaktywów oraz regulacje nadzoru nad ich rynkiem.

Ustawodawca unijny nadaje konsumentom prawo do wycofania się z nabycia kryptoaktywów w terminie 14 dni od zawarcia umowy, przy czym ogranicza to uprawnienie wyłącznie do nabycia kryptoaktywów bezpośrednio od emitenta lub od dostawcy usług dokonującego ich subemisji. Dotyczy to wyłącznie kryptoaktywów

innych niż tokeny powiązane z aktywami lub tokeny będące pieniądzem elektronicznym. Wymóg ustanowienia procedury rozpatrywania skarg dotyczy tokenów powiązanych z aktywami. Posiadacze tej kategorii tokenów uprawnieni będą do bezpłatnego złożenia skargi na wzorze udostępnionym przez emitenta. Projekt przewiduje upoważnienie dla EBA do opracowania projektów regulacyjnych standardów technicznych w celu określenia wymogów dotyczących rozpatrywania tych skarg.

Rozporządzenie w sprawie infrastruktur rynkowych opartych na DLT blockchain ma wprowadzić (pilotażowo) infrastrukturę rynkową na nowy poziom, bo z wykorzystaniem technologii rozproszonego rejestru. Zamierzeniem Komisji jest stworzenie warunków bezpiecznych do obrotu kryptoaktywami wykorzystujących DLT blockchain. Projekt określa wymagania (w tym proces uzyskiwania zezwolenia) dla tzw. wielostronnych platform obrotu (MTF) oraz systemów rozrachunku papierów wartościowych, ale wykorzystujących technologię rozproszonego rejestru. Co do zasady stosuje się reżim prawny określony w MiFID2, chyba że krajowy organ nadzoru zadecyduje o udzieleniu odstępstwa (Nowakowski, 2020a).

MTF-y korzystające z infrastruktury DLT blockchain zyskały nowe znaczenie. DLT MTF to w świetle projektu wielostronne platformy obrotu prowadzone przez firmę inwestycyjną lub operatora rynku, na których dopuszczalny jest obrót wyłącznie wymienialnymi papierami wartościowymi opartymi na technologii DLT, gdzie obowiązują przejrzyste, niearbitralne i ujednolicone zasady i procedury dotyczące: możliwości początkowego (*initial*) zapisywania papierów; rozliczania transakcji; także usług przechowywania.

W odniesieniu do papierów (instrumentów) opartych na DLT i dopuszczonych do obrotu lub rozliczanych w ramach centralnego depozytu (CSD) obowiązywać będą pewne limity, tj. 200 mln euro kapitalizacji dla danej akcji (emitenta) lub 500 mln euro dla emisji obligacji (wartość dla instrumentów wyemitowanych). Obligacje rządowe zostały wyłączone, co może dziwić w obliczu dążenia do cyfryzacji. Całkowita wartość rynku w systemie rozliczeń nie powinna przekroczyć 2,5 mld euro (podobnie, jeżeli zapisów dokonuje MTF). Obowiązek „trzymania" dziennych limitów leży oczywiście po stronie firmy inwestycyjnej lub operatora rynku, a miesięczne raporty powinny być przekazywane do organu nadzoru.

Jeżeli wartość rynku osiągnie barierę 2,25 mld euro, to dany podmiot powinien uruchomić *transition strategy* i poinformować o tym właściwy organ w najbliższym raporcie miesięcznym (wraz ze wskazaniem na jaki czas). Organ nadzoru może warunkowo dać zgodę na maksymalną wartość rynkową w wysokości 2,75 mld euro. *Transition strategy* (Strategia transformacji) to kolejny z wymogów nakładanych na CSD i MTF operujące na DLT. Każdy z tych podmiotów musi opublikować jasną strategię zamknięcia czy zawieszenia infrastruktury w przypadku, gdy mogłoby dojść do naruszenia warunków zezwolenia, ale także w sytuacji, gdy operator lub firma zdecydują się na zakończenie biznesu. Strategia musi zawierać kilka elementów, w tym m.in. sposób „zaspokojenia" uczestników, emitentów czy członków izby rozliczeniowej.

Można przewidywać „platformizację" na rynku usług sektora finansowego. Platformy mogą być różnego rodzaju (Nowakowski 2020c):

- platformy finansowe – porównywarki opłat, np. systemów płatności, kredytów hipotecznych czy innych usług finansowych;
- platformy typu Bank+, czyli takie, które umożliwiają np. bankom sprzedaż swoich produktów, ale także dają możliwość zawierania umów przez klientów z podmiotami trzecimi;
- platformy tworzące ekosystem konkretnych produktów lub usług (idea współpracy całego sektora);
- platformy, których główną osią nie są produkty finansowe, a są one jedynie „produktem" ubocznym (np. Allegro). Wiele platform e-Commerce oferuje teraz dodatkowe usługi finansowe czy ubezpieczeniowe w „pakiecie" z konkretnymi produktami czy usługami.

Istnieją wszelako bariery tak rozumianej platformizacji. Jest możliwość filtrowania produktów i usług finansowych (pewne ograniczenia mamy w kontekście produktów finansowych – MiFID2) w przekroju całego rynku; minimalnym rozwiązaniem powinna być tutaj możliwość nabycia danego produktu czy usługi oraz np. sprawdzenia swojej zdolności (np. kredytowej) czy profilu inwestycyjnego. Jest

tutaj duże pole do działania dla dostawców usługi dostępu do informacji o rachunku w trybie PSD 2 (z wyłączeniem rachunku inwestycyjnego). Z punktu widzenia klienta firmowego interesujące byłoby dobieranie (parowanie) z dostawcami usług, które będą dopasowane do sytuacji tego klienta, np. dobrze byłoby mieć możliwość wskazania, na jakie zabezpieczenia finansowania można sobie pozwolić.

Pojawia się problem cyfrowego on-boardingu (brak Digital ID to utrudnia), dostępu do API podmiotów (już nie tylko banków), kwestie cyberbezpieczeństwa, silne uwierzytelnianie klienta czy weryfikacja tzw. stron trzecich w rozumieniu PSD 2. Powstaje pytanie, czy i w jakiej mierze regulacja może dopuszczać wkraczanie w rolę agenta (różne obszary rynku finansowego mogą mieć odmienne wymagania), a to wiąże się z dodatkowymi obowiązkami po stronie platformy, jak i tego podmiotu, który się „marketuje". Pojawia się pytanie o nadzór nad takimi platformami, tj. czy sprawować go powinna KNF (inny regulator), czy też dopuszczalny jest jakiś model wyłącznie prywatny (współpracy między zainteresowanymi podmiotami). Pojawia się też kwestia ochrony konsumenta (jeżeli go dotyczy) czy obowiązki AML, RODO oraz związane z komunikacją elektroniczną, zawieraniem umów na odległość czy innymi obowiązkami informacyjnymi (Nowakowski, 2020c).

Zakres podmiotowy projektu dotyczącego operacyjnej odporności cyfrowej sektora finansowego (DORA) jest bardzo szeroki, są tam nie tylko „klasyczne" podmioty sektora finansowego, ale również dostawcy usług opartych na kryptoaktywach, platformach crowdfundingowych czy tzw. *data reporting service providers*. Zakres przedmiotowy jest również szeroki, obejmuje takie kwestie jak: zarządzanie ryzykami ICT, raportowanie istotnych incydentów z obszaru ICT; operacyjna odporność cyfrowa (*digital operational resilience*), wymiana informacji w zakresie cyberbezpieczeństwa oraz zasady zarządzania ryzykami stron trzecich (również w kontekście chmury obliczeniowej).

Projekt zakłada określenie najważniejszych wymogów dla stron trzecich w rozumieniu PSD 2 wchodzących w relacje umowne z instytucjami finansowymi, w tym w szczególności w kontekście realizacji odpowiednich kluczowych postanowień umownych (*key contractual provisions*). Istnieje także pomysł wprowadzenia instytucji nadzoru (*oversight framework*) dla krytycznych dla sektora finansowego dostawców usług ICT, w kontekście technologii cyfrowych dla nadzoru (suptech) (Nowakowski, 2020b, Nowakowski, 2020d).

Regulacja DORA wprowadza odpowiedni system zarządzania ryzykami ICT, który zapewni wysoki poziom operacyjnej odporności cyfrowej. Należy zwrócić uwagę na pojęcie znaczącego incydentu jako incydentu dotyczącego obszaru ICT, który w znacznym stopniu może wpłynąć negatywnie na systemy ICT kluczowe dla utrzymania funkcji krytycznych podmiotu). W tym kontekście należy mieć na uwadze dyrektywę NIS 2 (Directive on measures for a high common level of cybersecurity across the Union – NIS 2, COM(2020) 823 final 2020/0359(COD)), projekt dyrektywy w sprawie odporności podmiotów krytycznych (Directive on the Resilience of Critital Entities -CER Directive, COM(2020) 829 final 2020/0365(COD)), polską ustawę o systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560), czy rekomendacje D, M i Z (https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/rekomendacje_dla_bankow?articleId=8522&p_id=18) itp. Wprowadza się obowiązek posiadania strategii odporności (*Digital Resilience Strategy*), a także wiele technicznych kwestii składających się na całokształt działań związanych z zarządzania ryzykami ICT, w tym w zakresie ich identyfikacji czy planów zapasowych, ale także zobowiązanie do stworzenia ram do pozyskiwania informacji o zagrożeniach (analityki), które pozwolą na ich unikanie w przyszłości (*learning and evolving*).

Kluczowe jest: wyjaśnienie, jak system zarządzania ryzykami ICT wspiera strategię biznesową instytucji, określenie tolerancji na ryzyko ICT (to coś innego niż skłonność do ryzyka w rozumieniu Rekomendacji Z), określenie celów polityki bezpieczeństwa, architektury IT oraz zasad wprowadzania zmian (*change management*), zasad zarządzania incydentami oraz dostawcami będącymi stronami trzecimi, ustalenie wymagań w zakresie testowania odporności (*digital operational resilience testing*) oraz zasad komunikacji.

Rozporządzenie narzuca obowiązek posiadania odpowiedniego systemu zarządzania incydentami, który to umoż-

liwi, w tym będzie przekazywał stosowne alerty. Pojawiają się też konkretne wymogi w zakresie klasyfikacji „wag" incydentów i zasady raportowania tzw. *major incidents* (mandaty dla EBA – European Banking Association, ESMA – European Securities and Markets Authority, i EIOPA – Europan Insurance and Occupational Pensions Authority) do wydania standardów technicznych określających m.in. wzory formularzy zgłoszeniowych). Ma też powstać EU Hub dla zarządzania tymi incydentami. Pojawiają się także wymogi w zakresie testowania *digital operational resilience* oraz narzędzi i metod działania w tej kwestii. Ważnym wymogiem jest przeprowadzanie co najmniej raz na 3 lata tzw. Threat Led Penetration Testing. Są też wymogi dla samych testerów.

Pakiet regulacji finansów cyfrowych zawiera także strategię płatności detalicznych. Obywatele i przedsiębiorstwa w Europie korzystają z szerokiej gamy zróżnicowanych i wysokiej jakości rozwiązań płatniczych, wspieranych przy pomocy konkurencyjnego i innowacyjnego rynku płatności i opartych na infrastrukturach, które są bezpieczne, wydajne i łatwo dostępne. Dostępne powinny być konkurencyjne rozwiązania płatnicze opracowane w Europie i stosowane na skalę ogólnoeuropejską, które wspierają europejską suwerenność gospodarczo-finansową oraz wnoszą znaczny wkład w usprawnianie płatności transgranicznych realizowanych z jurysdykcjami spoza UE, tym samym wspierając międzynarodową rolę euro oraz „otwartą strategiczną autonomię" UE.

Strategia płatności detalicznych (RPS) przyjęta przez Komisję Europejską to długoterminowe ramy, które stworzono w celu wspierania rozwoju płatności detalicznych oraz wykorzystania szans cyfryzacji. Dzięki tej strategii Komisja wskazuje drogę do osiągnięcia nowoczesnego, konkurencyjnego i innowacyjnego ekosystemu płatności zorientowanego na klienta. Wraz z postępem cyfryzacji ekosystem płatności staje się coraz bardziej złożony, a wiele podmiotów – regulowanych lub nieregulowanych – ingeruje w łańcuch płatności. Ważne jest, aby regulacje były dobrze skalibrowane i odpowiednio obejmowały wszystkie podmioty i usługi, które mogą nieść ryzyko dla systemu finansowego (European Payments Council 2020).

Rada Europejska przyjęła także rozporządzenie umożliwiające platformom finansowania społecznościowego oferowanie usług transgranicznych w całej UE (Dz. Urz. UE L 347/1 20/10/2020). Dotyczyć one mają kampanii crowdfundingowych, nieprzekraczających kwoty 5 mln euro w ciągu 12 miesięcy. Nowe regulacje ujednolicają zasady prowadzenia działalności w UE. Mają także zwiększyć pewność prawną dzięki ochronie inwestorów. Stanowią część projektu unii rynków kapitałowych, która ma ułatwić dostęp do nowych źródeł finansowania. Operacje na większą skalę regulować będzie dyrektywa o rynkach instrumentów finansowych (MiFID Dz. Urz. UE L 173/349 12/06/2014) i rozporządzenie o prospekcie emisyjnym (Dz. Urz. UE L 168/12 30/06/2017). Konstrukcja usługi finansowania społecznościowego opiera się na działalności trzech podmiotów: właściciela projektu, inwestora oraz organizacji pośredniczącej (platformy usług crowdfundingowych). Wyróżnia się dwa modele usług finansowania społecznościowego: pożyczkowy oraz inwestycyjny.

4. Regulacja gospodarki opartej na danych

Unia Europejska od lat kładzie duży nacisk na wymianę danych między państwami i instytucjami, w celu poprawy warunków życia obywateli, wzmocnienia europejskich firm i realizacji misji zjednoczonej Europy, oraz aby rozwijać gospodarkę opartą na danych. Celem nowego projektu Data Governance Act (Data Governance Act – DGA COM(2020) 767 final 2020/0340(COD)) jest przede wszystkim podniesienie zaufania rynku do procesu udostępniania oraz zapewnienie bezpieczeństwa przetwarzanych danych. Dla firm i instytucji rządowych oznacza to korzyści w zakresie współdzielenia się informacjami i propagowania swojej działalności, ale również konieczność opracowania polityki zarządzania danymi.

Swobodny przepływ danych jest priorytetem w rozwoju polityki cyfrowej UE. W swojej strategii dotyczącej danych Komisja opisała wizję wspólnej europejskiej przestrzeni danych, jednolitego „rynku" danych, na którym mogłyby one być wykorzystywane bez względu na kraj ich pochodzenia. Chodzi o to, aby zreali-

zować potencjał użytkowania dobrowolnie udostępnionych danych do celów interesu ogólnego. Cele takie obejmują opiekę zdrowotną, przeciwdziałanie zmianie klimatu, poprawę mobilności, ułatwianie tworzenia oficjalnych statystyk lub poprawę świadczenia usług publicznych, np. dzięki interoperacyjności i kompatybilności.

Wizja ta realizuje się na przykład poprzez wprowadzenie platform typu Open Data. Pozwoli to zrealizować ideę Smart City – elektronicznego miasta, w którym mieszkańcy i firmy mają łatwy dostęp do wszystkich potrzebnych im informacji i portali. Dane są fundamentem transformacji cyfrowej i innowacyjności, a ich dostępność, otwarta i bezpieczna wymiana ponad granicami pozwoli na rozwiązywanie problemów, które dzisiaj dotykają państwa, społeczności i kluczowe branże gospodarki, takie jak medycyna, służba zdrowia, bezpieczeństwo czy ochrona środowiska na poziomie globalnym (Mondaq, 2020; Hoffmann i Otero, 2020; PWC, 2021).

Przepisy ogólne DGA regulują:

– warunki wykorzystywania w Unii Europejskiej niektórych kategorii danych będących w posiadaniu organów sektora publicznego;
– zasady powiadamiania i nadzoru w zakresie świadczenia usług udostępniania danych;
– zasady dobrowolnej rejestracji podmiotów, które gromadzą i przetwarzają dane udostępniane w celach altruistycznych.

Po wejściu w życie rozporządzenia DGA:

– dostawcy danych, czy to altruistyczni, czy komercyjni, uzyskają większą pewność, że ich dane nie zostaną wykorzystane niezgodnie z prawem. Warto zauważyć, że ministerstwa i agendy rządowe mogą posłużyć się udostępnianiem danych dla realizacji ich misji – np. wspierania eksporterów;
– pośrednicy danych mogą rozwinąć nowe rodzaje działalności, wiedząc, co jest dla nich dozwolone, a co nie. Czyli uzyskają możliwości rozwoju, ponosząc mniejsze ryzyko regulacyjne;
– odbiorcy uzyskają lepszy dostęp do danych, co zapewni im lepszą podstawę do podejmowania decyzji biznesowych lub dostarczania informacji swoim klientom.

Niewątpliwie dużym wyzwaniem jest uzyskanie rozsądnej proporcji między regulacjami DGA a RODO. Prawodawca UE podejmuje bowiem próbę regulacji celów w pewnej mierze przeciwstawnych. Są tu zarówno szanse lepszej współpracy w gospodarce i innowacyjności, jak i zagrożenia, np. gdy ochrona prywatności hamuje wykorzystanie danych w interesie publicznym.

Trzeba umieć „panować nad danymi", w szczególności wiedzieć, jakie dane się posiada oraz jak są one przetwarzane i wykorzystywane. W praktyce zastosowanie rozporządzenia będzie wiązało się ze zinwentaryzowaniem posiadanych danych, zaklasyfikowaniem ich zgodnie z regulacjami, pod które podlegają, a także zapewnieniem ich bezpieczeństwa. Tym samym podstawowym warunkiem do uzyskania wyżej wymienionych korzyści jest wprowadzenie systemu zarządzania danymi (Data Governance System – DGS). Wymiana danych w całej Unii Europejskiej i między strategicznymi branżami gospodarki jest niezbędna w budowaniu spójnej i konkurencyjnej gospodarki cyfrowej w Europie i na świecie. DGA jest ważnym krokiem w kierunku tworzenia ustrukturyzowanych jednolitych przestrzeni danych z poszanowaniem danych osobowych i praw autorskich (PWC, 2021)

W centrum debaty jest także problem relacji między DGA a DGPR (RODO). Europejska Rada Ochrony Danych (EDPB) wskazuje, że rozporządzenie DGA niedostatecznie chroni dane osobowe. Z jednej strony mamy do czynienia z poglądem, że trend do tworzenia ram dla *data-driven economy* (opisanej w Europejskiej Strategii dla Danych), bez odpowiednich gwarancji w zakresie ochrony danych osobowych, naruszać może nawet prawa podstawowe. Z drugiej strony mamy wskazanie, że unijne ramy prawne w zakresie ochrony danych powinny umożliwiać, a nie blokować, rozwój *data-driven economy*. RODO jest uznawane wszelako za barierę dla rozwoju gospodarki opartej na danych, szczególnie w takich dziedzinach, jak sztuczna inteligencja czy wykorzystanie big data (Nowakowski, 2021).

Tendencja do wzmocnionej ochrony danych osobowych („Privacy Shield") wypływa wszelako z orzecznictwa TSUE. W 2020 r. TSUE wydał wyrok w sprawie Data Protection Commissioner przeciwko Facebook Ireland Ltd oraz Maximillian Schrems (sprawa Schrems II https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/

orzeczenia-sadow/c-311-18-przekazywanie-danych-obywateli-panstw-523123145). Powyższy wyrok TSUE został wydany na podstawie wniosku złożonego w ramach sporu, jaki zaistniał pomiędzy irlandzkim komisarzem ds. ochrony danych a Facebook Ireland Ltd i Maximillianem Schremsem w przedmiocie wniesionej przez Maximilliana Schremsa skargi dotyczącej przekazywania danych osobowych przez Facebook Ireland Ltd do spółki Facebook Inc. w USA (Deloitte 2020).

Firmy cyfrowe, takie jak Facebook, Google i Twitter, zbierają ogromne ilości danych o swoich użytkownikach. Czasami jednak zagrażają one interesom użytkowników, od zezwalania na agresywną reklamę i umożliwiania dyskryminacji po wywoływanie uzależnienia i udostępnianie poufnych informacji stronom trzecim. Platformy internetowe mogą również krzywdzić swoich użytkowników i opinię publiczną na wiele innych sposobów, w tym przez ułatwianie rozpowszechniania dezinformacji i nękanie niektórych kategorii mówców. Unia Europejska odpowiedziała na niektóre z tych problemów, przedstawiając kompleksowe przepisy dotyczące danych osobowych, czyli ogólne rozporządzenie o ochronie danych (RODO), ale także przeciwwagę, która powinna umożliwiać korzystanie z danych w interesie publicznym (Data Governance Act).

Pojęcie „powierników informacji" znalazło się w polu dyskusji na temat regulacji platform internetowych. Koncepcja ta ma na celu przywrócenie równowagi między zwykłymi osobami a firmami cyfrowymi, które gromadzą, analizują i sprzedają ich dane osobowe w celu osiągnięcia zysku. Tak jak prawo nakłada na lekarzy, prawników i księgowych szczególne obowiązki w zakresie opieki, poufności i lojalności wobec pacjentów i klientów, tak samo powinno nakładać specjalne obowiązki na korporacje, takie jak Facebook, Google i Twitter i ich użytkowników końcowych. W ciągu ostatnich kilku lat argument ten spotkał się z niezwykle szerokim poparciem, ale nie z krytycznym sprzeciwem.

Powstaje pytanie, czy koncepcja powierników informacji jest adekwatną lub trafną odpowiedzią na problemy asymetrii informacji i nadużyć bigtechów w kontekście problemów związanych z dominacją na rynku i modelami biznesowymi, które wymagają ściślejszego nadzoru. Firmy, które można traktować jako powierników informacji, różnią się wszelako pod względem świadczonych przez nie usług, stosowanych przez nie modeli biznesowych oraz dominacji rynkowej, z której korzystają.

Tam, gdzie brakuje prawa publicznego lub ono zawodzi, poszukiwanie nowych ram rozliczalności doprowadziło do proliferacji koncepcji powiernictwa poza tradycyjne granice prawa prywatnego. Można jednak również wyrazić sceptyczny pogląd na przydatność instytucji powierników informacji. Ich krytyka jest odpowiedzią na tezę, że prawo powinno traktować dostawców usług internetowych jako „powierników informacji", opierając się na analogii do obowiązków powierniczych profesjonalistów, takich jak prawnicy i lekarze oraz definiując powiernika informacji jako osobę lub firmę, która z powodu relacji z inną osobą przyjęła specjalne obowiązki w odniesieniu do informacji uzyskanych w trakcie takiej relacji (Haupt, 2020).

Na poziomie europejskim promowanie swobodnego przepływu danych i dostępu do danych znalazło się na czele celów dotyczących gospodarki cyfrowej. Szczególnym aspektem tej gospodarki jest pojawienie się połączonych, współzależnych urządzeń, które są coraz częściej używane w kontekście Internetu rzeczy (IoT). Jeśli chodzi o te urządzenia, Komisja zidentyfikowała szczególny problem polegający na tym, że producenci mogą próbować zachować kontrolę nad danymi i odmówić dostępu do danych stronom trzecim, utrudniając tym samym rozwój innowacyjnych modeli biznesowych na wtórnych rynkach związanych z danymi.

Aby rozwiązać ten problem, należy zbadać przepisy dotyczące praw dostępu do danych użytkowników podłączonych urządzeń. Odmowę producentów urządzeń w zakresie udzielenia dostępu do danych użytkownikom można traktować jako formę nieuczciwej praktyki handlowej, w związku z czym zaleca się osadzenie praw użytkowników w zakresie dostępu do danych w kontekście europejskiego prawa o nieuczciwej konkurencji. Takie prawa dostępu byłyby uzupełnieniem innych systemów dostępu, w tym sektorowych praw dostępu do danych konkurentów na rynkach wtórnych, a także praw dostępu na mocy postanowień umów i prawa konkurencji (Drexl, 2020).

5. Konkluzja

Sukces bigtechów można w dużej mierze wytłumaczyć budowaniem ekosystemów, dwu-(wielo)-stronnymi rynkami cyfrowymi i wynikającą z tego ekonomią platform. Efekty sieciowe prowadzą do przejrzystości i obniżenia kosztów transakcji. Jednocześnie jednak efekty blokowania prowadzą do rosnącej zależności uczestników rynku. Proces cyfryzacji coraz częściej łączy się z rosnącą rolą oraz przetwarzaniem danych (*datafication*) i nowymi technologiami, takimi jak przetwarzanie w chmurze, internet rzeczy, blockchain, big data i sztuczna inteligencja w kontekście fintech i bigtech. Rozwój platform cyfrowych niesie ze sobą problemy dotyczące ochrony konkurencji i konsumenta, monopolizacji rynków, ochrony prywatności, cyberbezpieczeństwa, uczciwości algorytmicznej, prawa pracy i polityki społecznej, dostępu do infrastruktury i do kluczowych usług publicznych. Prawo konkurencji powinno krytycznie angażować się w podwójnej roli regulacji ekonomicznej i społecznej, której głównym celem jest kontrola potęgi gospodarczej napędzanej nie tylko względami ekonomicznymi, ale również etyki, przejrzystości i sprawiedliwości. Szerszy wachlarz interakcji, poza wymianą rynkową, między różnymi zainteresowanymi stronami, zachęca do poszerzenia rozumienia prawa konkurencji, wykraczającego poza monocentryczny model koncentrujący się na cenie i wydajności. Rozumiejąc rolę prawa konkurencji w tym nowym środowisku, sugeruje się szerszy zasięg polityki konkurencji, który obejmowałby pełne koszty społeczne wynikające z ograniczeń konkurencji w różnych wymiarach dobrobytu. Prawo konkurencji powinno gwarantować skuteczną ochronę wartości społecznych, na które mogą mieć wpływ podmioty o dużej władzy rynkowej. „Konkurencja cyfrowa" to koncepcja, która wysunęła się na czoło prawa konkurencji, gdyż może być postrzegana zarówno jako obiecująca, jak i ostrzegawcza: z jednej strony przynosi obietnice zwiększenia prędkości, wydajności i obiektywizmu, a z drugiej zaś pociąga za sobą potencjalne pułapki, takie jak trudne do zidentyfikowania ścieżki prowadzące do nieuczciwych cen, dominujące pozycje i ich potencjalne i trudne do wykrycia nadużycia np. danych osobowych. Prawo antymonopolowe jest wystarczająco elastyczne, aby mieć znaczenie w erze cyfrowej, ale sądy muszą przestać koncentrować się prawie wyłącznie na kwestiach cenowych i rozważyć szerszy zakres pytań dotyczących konkurencji i innowacji np. dostępu do danych, praw własności intelektualnej czy kwestii interoperacyjności. Regulacja technologii i optymalne projektowanie instytucji prawnych w środowisku niepewności są dwoma najważniejszymi wyzwaniami politycznymi XXI wieku. Innowacje mają kluczowe znaczenie dla wzrostu gospodarczego. Regulacyjne decyzje, a zwłaszcza polityka konkurencji i systemy własności intelektualnej mogą mieć głębokie konsekwencje dla wzrostu gospodarczego. Każdy reżim prawny musi próbować ocenić kompromisy regulacyjne, które chronią konsumenta czy pracownika, ale też wpływają na zachęty do innowacji, konkurencję i współpracę, wolność firm w zakresie komercjalizacji owoców ich innowacji, dostęp do infrastruktury czy łagodzenie ryzyka systemowego.

Bibliografia

Belcher, J. i Narula, N. (2018). *Another perspective on cryptocurrencies and regulation.* Pozyskano z: https://www.media.mit.edu/posts/another-perspective-on-cryptocurrencies-and-regulation/

Belleflamme, P. (2020a). *An introduction to the economics of platform competition – Part 1.* Pozyskano z: http://www.ipdigit.eu/2020/04/an-introduction-to-the-economics-of-platform-competition-part-1/

Chowdhury, N. (2019). *An IoT and Blockchain-based Approach for Ensuring Transparency and Accountability in Regulatory Compliance.* Pozyskano z: https://dl.acm.org/doi/abs/10.1145/3341162.3349320

Deloitte (2020). *RODO: orzeczenia Schrems II przeciwko Facebook*. Pozyskano z: https://techno-senior.com/2020/08/03/rodo-orzeczenia-schrems-ii-przeciwko-facebook/

Dillenberger, D., Chakraborty, S., Thomas, J.J., Walli, M.M., Vaculin, R. i Sarpatwar, K. (2019). Blockchain analytics and artificial intelligence. *IBM Journal of Research and Development*, *63*(2/3). https://ieeexplore.ieee.org/document/8645631.

Drexl, J. (2020). *Connected Devices – an Unfair Competition Law Approach to Data Access Rights of Users*. Pozyskano z: https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3746163&dgcid=ejournal_htmlemail_max:planck:institute:for:innovation:competition:research:paper:series_abstractlink

DW (2020). *UE ukróca swobodę dużych platform i grozi karami.* Pozyskano z: https://www.dw.com/pl/ue-kary-dla-du%C5%BCych-platform/a-55951761

DW (2021). *UE chce uregulować sztuczną inteligencję*. Pozyskano z: https://www.dw.com/pl/ue-chce-uregulowa%C4%87-sztuczn%C4%85-inteligencj%C4%99/a-57281515

EC (2020a). *The Digital Markets Act: ensuring fair and open digital markets*. Pozyskano z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

EC (2020b). *What are the key goals of the Digital Services Act?* Pozyskano z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Emerging payments (2020). *Regulation of Decentralized Finance (DeFi) in Europe.* Pozyskano z: https://www.emergingpayments.org/article/regulation-of-decentralised-finance-defi-in-europe/

European Payments Council (2020). *The new Retail Payments Strategy for the EU*. Pozyskano z: https://www.europeanpaymentscouncil.eu/news-insights/insight/new-retail-payments-strategy-eu

Gozman, D., Liebenau, J. i Aste, T. (2020). A Case Study of Using Blockchain Technology in Regulatory Technology. *MIS Quarterly Executive*, *19*(1). Pozyskano z: https://www.semanticscholar.org/paper/A-case-study-of-using-blockchain-technology-in-Gozman-Liebenau/de24305cc2601a0bf0978693ea5010cca1d035ca

Haupt C.A. (2020). *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*. Pozyskano z: https://harvardlawreview.org/2020/10/platforms-as-trustees/

HLRev. (2019). *SEC, Framework for "Investment Contract" Analysis of Digital Assets (2019).* Pozyskano z: https://harvardlawreview.org/2019/06/sec-framework-for-investment-contract-analysis-of-digital-assets-2019/

Hoffmann, J. i Otero, B.G. (2020). *Demystifying the role of data interoperability in the access and sharing debate*. Max Planck Institute for Innovation and Competition Research Paper Series 20-16. Pozyskano z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3705217

Iwańska, K. i Głowacka, D. (2020). *Koniec z wszechwładzą platform internetowych? Komisja Europejska zaproponowała nowe regulacje.* Pozyskano z: https://panoptykon.org/DSA-regulacja-platform

Linklaters (2020). *Decentralized Finance: navigating the rugged regulatory landscape*. Pozyskano z: https://www.linklaters.com/en/insights/blogs/fintechlinks/2020/september/decentralised-finance-navigating-the-rugged-regulatory-landscape

Mondaq (2020). *The Data Governance Act – regulating access to data held by public authorities.* Pozyskano z: https://www.elvingerhoss.lu/publications/data-governance-act-regulating-access-data-held-public-authorities?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration

MyungSan, J. (2018). Blockchain government – a next form of infrastructure for the twenty-first century. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(4). Pozyskano z: https://jopeninnovation.springeropen.com/articles/10.1186/s40852-018-0086-3

Nowakowski, M. (2020a). *Będzie rynek regulowany dla kryptoaktywów? Pierwsza analiza projektu rozporządzenia w sprawie DLT Market Infrastructure.* Pozyskano z: https://finregtech.pl/2020/10/22/bedzie-rynek-regulowany-dla-kryptoaktywow-pierwsza-analiza-projektu-rozporzadzenia-w-sprawie-dlt-market-infrastructure/

Nowakowski, M. (2020b). *SupTech, czyli technologia nadzorcza jako dobro wspólne (razem z RegTech)? Raport Financial Stability Board rzuca nowe światło*. Pozyskano z: https://finregtech.pl/2020/10/18/suptech-czyli-technologia-nadzorcza-jako-dobro-wspolne-razem-z-regtech-raport-financial-stability-board-rzuca-nowe-swiatlo/

Nowakowski, M. (2020c). *Finansowy Amazon? Czy cyfrowe platformy usług finansowych to przyszłość? Trochę przemyśleń odnośnie kierunku rozwoju sektora finansowego*. Pozyskano z: https://finregtech.pl/2020/10/15/finansowy-amazon-czy-cyfrowe-platformy-uslug-finansowych-to-przyszlosc-troche-przemyslen-odnosnie-kierunku-rozwoju-sektora-finansowego/

Nowakowski, M. (2020d). *Zarządzanie ryzykiem operacyjnym (ICT) w projekcie rozporządzenia w sprawie Digital Operational Resilience*. Pozyskano z: https://finregtech.pl/2020/10/13/zarzadzanie-ryzykiem-operacyjnym-ict-w-projekcie-rozporzadzenia-w-sprawie-digital-operational-resilience/

Nowakowski, M. (2021). *Czy Data Governance Act ma realizować dokładnie te same cele, co RODO?* Pozyskano z: https://alebank.pl/czy-data-governance-act-ma-realizowac-dokladnie-te-same-cele-co-rodo/?id=364277&catid=625.

Osiński, Ł. (2020). *KE: Nowe regulacje rynku cyfrowego dla gigantów internetowych.* Pozyskano z: https://www.obserwatorfinansowy.pl/forma/dispatches/ke-nowe-regulacje-rynku-cyfrowego-dla-gigantow-internetowych/

Pakulska, T. i Poniatowska-Jaksch, M. (2021). *Platformizacja korporacji transnarodowych.* Warszawa: Oficyna Wydawnicza SGH.

PWC (2020). *Projekt rozporządzenia w sprawie rynków kryptoaktywów (MiCA)*. Pozyskano z: https://www.pwc.pl/pl/artykuly/projekt-rozporzadzenia-w-sprawie-rynkow-kryptoaktywow-mica.html

PWC (2021). *Komisja Europejska opublikowała projekt Rozporządzenia ws. Zarządzania Danymi (Data Governance Act)*. Pozyskano z: https://www.pwc.pl/

pl/artykuly/projekt-rozporzadzenia-zarzadzania-danymi-data-governance-act.html

RM (2020a). *Regulacje usług cyfrowych w UE – oto nasze stanowisko* https://www.gov.pl/web/cyfryzacja/regulacje-uslug-cyfrowych-w-ue--oto-nasze-stanowisko

RM (2020b). *Usługi cyfrowe w UE – nowe regulacje* https://www.gov.pl/web/cyfryzacja/uslugi-cyfrowe-w-ue--nowe-regulacje

Runyu, S. (2021). *Blockchain Network as a Platform: Conceptualising its Adapted Layered Architecture Design*. Pozyskano z: https://jbba.scholasticahq.com/article/23681-blockchain-network-as-a-platform-conceptualising-its-adapted-layered-architecture-design

Socha, M. (2020). *Kodeks Usług Cyfrowych: Platformy zbyt duże, by poddać je regulacji?* Pozyskano z: https://www.rp.pl/Firma/311239972-Kodeks-Uslug-Cyfrowych-Platformy-zbyt-duze-by-poddacje-regulacji.html

Sunstein, C.R (2014). The Limits of Quantification *California Law Review*, 6.

Szpringer, W. (2017). *Nowe technologie a sektor finansowy. Fintech jako szansa i zagrożenie*. Warszawa: Poltext.

Szpringer, W. (2019). *Blockchain jako innowacja systemowa. Od internetu informacji do internetu wartości. Wyzwania dla sektora finansowego*. Warszawa: Poltext.

Szpringer, W. (2020a). *Zarządzanie przez algorytmy. Technologia – ekonomia – prawo*. Warszawa: Poltext.

Szpringer, W. (2020b). *Platformy cyfrowe i gospodarka współdzielenia*. Warszawa: Poltext.

UKE (2020). *Nowe inicjatywy regulacji platform cyfrowych.* Pozyskano z: https://www.uke.gov.pl/akt/nowe-inicjatywy-regulacji-platform-cyfrowych,365.html

Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, *25*(2). Pozyskano z: https://www.emerald.com/insight/content/doi/10.1108/JFRC-08-2016-0068/full/html#loginreload

Yuthas, K., Sarason, Y., Aziz, A. (2021). Strategic Value Creation through Enterprise Blockchain. *Journal of British Blockchain Association*, *4*(1). Pozyskano z: https://jbba.scholasticahq.com/article/21638-strategic-value-creation-through-enterprise-blockchain