EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Odpowiedzi Europejskiego Kongresu Finansowego[1] w konsultacjach Komisji Europejskiej dotyczących FinTech [2]

Metodologia opracowania odpowiedzi

Opracowanie stanowiska przebiegało w następujących etapach:

Etap 1

Do wzięcia udziału w badaniu zaproszono grupę ekspertów z polskiego sektora finansowego, do których przesłano wybrane fragmenty dokumentu konsultacyjnego Komisji Europejskiej oraz wybrane przez EKF pytania konsultacyjne. Ekspertom zagwarantowana została anonimowość.

Etap 2

Na bazie uzyskanych opinii opracowana została propozycja syntezy odpowiedzi. Odpowiedzi uzyskano od ekspertów reprezentujących:

- banki uniwersalne,
- firmy FinTech,
- instytucje infrastruktury rynku finansowego,
- firmy konsultingowe.

Propozycję tę przekazano ekspertom, którzy wzięli udział w konsultacjach. Zwrócono się do nich z prośbą o zaznaczenie w syntezie tych sformułowań, które powinny zostać zmodyfikowane i zaproponowanie modyfikacji czy dodatkowych zapisów, jak również zaznaczenie tych opinii, z którymi się nie zgadzają i które powinny być z ostatecznej syntezy usunięte.

Etap 3

Po uwzględnieniu uwag ekspertów opracowane zostały ostateczne syntetyczne odpowiedzi Europejskiego Kongresu Finansowego przedstawione poniżej.

---

[1] Celem Europejskiego Kongresu Finansowego (www.efcongress.com) jest debata nt. bezpieczeństwa i rozwoju sektora finansowego Unii Europejskiej i Polski.

[2] https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf

Odpowiedzi Europejskiego Kongresu Finansowego[3]

1.2. ***Czy istnieją dowody na to, że zautomatyzowane doradztwo finansowe dociera do większej liczby konsumentów, firm, inwestorów w różnych obszarach usług finansowych (usługi inwestycyjne, ubezpieczenia itp.) oraz w jakim tempie się to odbywa? Czy te usługi są lepiej dostosowane do potrzeb użytkowników?***

Jest kilka powodów, dla których usługi robodoradztwa docierają do coraz większej liczby klientów:

- Niewielu ludzi stać na wyspecjalizowanego doradcę inwestycyjnego, a zaletą robo-doradców są znacznie niższe opłaty za zarządzanie aktywami klientów,
- Pokolenie Millenialsów korzysta z usług finansowych za pomocą smartfonów i ma znacznie większe zaufanie do technologii niż pokolenie ich rodziców,
- Doskonale wypracowane algorytmy w przyszłości będą prawdopodobnie znacznie szybciej i skuteczniej reagować na zmiany rynkowe niż człowiek.

Zautomatyzowane doradztwo finansowe, poza obszarem technologicznym, jest jednym z najczęściej i najchętniej rozwijanych obszarów przez rynek FinTech. Wpisuje się to wprost w potrzeby współczesnych odbiorców usług doradczych, w tym w szczególności finansowych/ubezpieczeniowych. Dobrym przykładem tego typu usług są zautomatyzowane usługi doradztwa w ekosystemach wspierających działalność gospodarczą dostarczanych przez banki, firmy doradcze i dostawców systemów do zarządzania działalnością gospodarczą. Analiza zachowań przedsiębiorcy, przepływu środków czy tzw. księgowość w czasie rzeczywistym, pozwalają na natychmiastowe reagowanie na jego potrzeby i rozwiązywanie pojawiających się problemów. Znane są już na rynku polskim tego typu rozwiązania i należy się spodziewać dalszego dynamicznego i szybkiego ich rozwoju. Rozwój tego typu usług w obszarze konsumentów rozwija się mniej dynamicznie z uwagi na ograniczenia regulacyjne dotyczące ochrony danych osobowych. Pojawiające się szanse związane z wdrożeniem nowych regulacji (np. PSD2) mogą jednak bardzo zdynamizować tempo rozwoju usług doradczych w tym obszarze. Obserwacje rynku pokazują, że mechanizmy zautomatyzowanej obsługi trafiają do coraz szerszego kręgu podmiotów, w tym firm z sektora finansowego – automatyzacja postępuje, niemniej brak jest publicznie dostępnych twardych danych statystycznych o efektach opisywanych zmian. Warto podkreślić, że podobnie jak swego czasu internetowe kanały samoobsługowe zrewolucjonizowały rynek usług bankowych oraz umożliwiły tańsze, a nawet darmowe oferowanie usług podstawowych klientom, tak przyszłe mechanizmy automatyzacji typu robo advisory mogą pozwolić zaoferować nowe usługi mniej zamożnym klientom, dla których obsługa przez wyspecjalizowanych pracowników banków lub innych instytucji finansowych będzie bądź zbyt droga, bądź przez wysoki narzut kosztów produkty te były zbyt drogie dla wielu segmentów.

[3] Pytania zostały wybrane z szerszej listy pytań w materiale konsultacyjnym Komisji Europejskiej. Zachowano oryginalną numerację pytań.

1.4. ***Jakie minimalne cechy i ilość informacji o użytkowniku usługi oraz portfelu produktów (jeśli występuje) należy uwzględnić w algorytmach używanych przez usługodawców (np. w odniesieniu do profilu ryzyka)?***

Algorytmy powinny uwzględniać przede wszystkim szczegółowe informacje na temat samego inwestora, t.j.:

- Skłonność do ryzyka
- Oczekiwana stopa zwrotu z inwestycji
- Wiek
- Wykształcenie
- Branża, w której pracuje
- Określenie czy inwestor akceptuje aktywa np. nowych technologii, np. bitcoin oraz np. spółki „nieetyczne" tzn. np. z branży tytoniowej czy zbrojeniowej

oraz samej inwestycji i wybranego rynku:

- Horyzont czasowy inwestycji
- Minimalna liczba aktywów w portfelu
- Płynność rynku, na którym zawierane są transakcje
- Wartość nominalna tworzonego portfela
- Rezerwa płynnościowa jakiej potrzebuje inwestor (dla określenia jaki procent inwestycji mogą stanowić aktywa niepłynne)

Na tej podstawie algorytm powinien stworzyć profil ryzyka danego użytkownika. Klienci indywidualni powinni być szczególnie chronieni przed wystawieniem na ryzyko rynkowe i poinformowani o wszystkich możliwych scenariuszach danej inwestycji.

Dostawca usług powinien posiadać możliwości identyfikowania osoby, a informacja o produkcie powinna być dostosowana do odbiorcy. Minimalne informacje powinny dotyczyć kwot, których dotyczą produkty, okresu, rodzaju produktu, uczciwej oceny możliwych efektów i oceny ryzyka, a także wskazanie scenariusza pesymistycznego, z którym może się wiązać produkt (np. utrata całych inwestowanych środków). Polityka zarządzania ryzykiem powinna znajdować się po stronie dostawcy usług i być rozwijana wraz z rozwojem usług i ich skali.

1.7. ***W jaki sposób Komisja może wspierać dalszy rozwój rozwiązań typu FinTech w zakresie finansowania pozabankowego, tj. pożyczek typu peer-to-peer/marketplace, crowdfundingu, finansowania faktur i finansowania łańcucha dostaw?***

Komisja Europejska może odegrać znaczącą rolę w obszarze rozwoju FinTech poprzez działania takie jak:

- Inicjatywy legislacyjne regulujące ten obszar rynku (np. pod kątem ryzyka rynkowego i kontrahenta, fraudów czy przepływu danych osobowych), jednocześnie stwarzające przyjazne ramy do działania firm w tym obszarze
- Wspieranie w krajach europejskich projektów sandbox (piaskownic regulacyjnych), które umożliwiają rozwój startującym firmom technologicznym
- Rozpowszechnianie polityki informacyjnej w odniesieniu do mechanizmów działania finansowania alternatywnego

- Rozpowszechnianie programów promujących rozwój tej branży (np. akceleratory, hackatony, projekty badawcze)
- Współpraca z regionalnymi stowarzyszeniami zrzeszającymi ecosystem FinTechowy
- Wsparcie w projektach mających na celu ulepszanie modeli scoringowych, na podstawie których udzielane są pożyczki peer-to-peer (póki co dane społecznościowe ciągle są niewystarczającym źródłem, które łatwo jest zmanipulować)

Mając na względzie cele, którym służą kampanie crowdfundingowe, należy zauważyć iż możliwe jest osiąganie tych celów opierając się o wzbogacone instrumenty inwestycyjne obecne w obrocie tradycyjnym. Aby to było możliwe należy wspierać przepisy pozwalające na:

- elektroniczną rejestrację działalności gospodarczej z użyciem usług zaufania zgodnych z normami wprowadzonymi dyrektywą eIDAS – dobrym przykładem jest stosowana w Polsce procedura S24 pozwalająca na rejestracje działalności w formie spółki z o. o., spółki komandytowej oraz spółki komandytowo-akcyjnej (trwają prace nad rozszerzeniem możliwości stosowania tej procedury również w odniesieniu do spółek akcyjnych)
- pełna dematerializacja instrumentów finansowych (w tym w szczególności emitowanych przez firmy niepubliczne) pozwalająca na całkowicie zautomatyzowany obrót tymi instrumentami (zarówno pierwotny jak i wtórny) jak również zapewnienie wykonania praw z takich instrumentów (zarówno majątkowych jak i korporacyjnych), w sposób dostępny obecnie głównie dla papierów publicznych.
- jednolite i konsekwentne stosowanie przepisów o ofercie publicznej w tym w odniesieniu do instrumentów dystrybuowanych z użyciem platform crowdfundingowych.
- Komisja powinna wspierać generalną zasadę „jedna działalność – jedne regulacje – jeden nadzór" niezależnie od rozwiązań technologicznych użytych do takiej działalności.

1.8. ***Jaki minimalny poziom przejrzystości powinien obowiązywać podmioty zbierające fundusze i platformy? Czy inicjatywy samoregulacji (promowane przez niektóre stowarzyszenia branżowe i poszczególne platformy) są wystarczające?***

Z uwagi na charakter działalności tego typu instytucji należy przede wszystkim dążyć do zachowania niezbędnego bezpieczeństwa stron zawieranych transakcji. Poziom uregulowania nie powinien dyskryminować żadnego uczestnika rynku finansowania. Zasady i normy oraz przepisy prawne powinny być na zbliżonym poziomie. Dobrym rozwiązaniem mogłyby być regulacje umożliwiające/nakazujące wymianę informacji dot. stron transakcji oraz jej przedmiotu, podobnie jak dzieje się to na rynku tradycyjnego finansowania bankowego. Z pewnością regulatorzy powinni konsultować swoje działania regulacyjne ze środowiskiem, którego one dotyczą, ponieważ to te podmioty najlepiej wiedzą, na co narażony jest użytkownik korzystający z platform crowdfundingowych. Chcąc się rozwijać i zyskiwać większe zaufanie społeczeństwa, firmy te muszą stwarzać bezpieczne i transparentne zasady zbierania funduszy. W tym celu ważne jest, aby stworzyć taki poziom przejrzystości, w którym użytkownicy mają zaufanie, że środki zostały przeznaczone na opisany cel i nie będą miały miejsca przypadki, gdy nieznany portal podszyje się pod platformę crowdfundingową zbierającą środki na szczytny cel. Tego rodzaju platformy powinny podlegać podstawowym regulacjom, które zapewnią bezpieczeństwo i transparentność klientom korzystającym z takich rozwiązań. Na przykład dane osobowe powinny być chronione, klienci powinni być świadomi ryzyka zawieranych transakcji, a transparentność danych powinna uniemożliwiać nadużycia.

2.3. ***Jakiego wpływu na zatrudnienie można oczekiwać w wyniku wdrożenia rozwiązań FinTech? Jakie umiejętności winny towarzyszyć takiej zmianie?***

Nastąpi zmiana wymaganych kompetencji. Nowe rozwiązania wyeliminują tzw. prace proste. Zmiany nastąpią w back-office, mniej będzie prac dokumentacyjnych. Bardziej będą wymagane kompetencje związane z odpowiednim rozumieniem funkcjonowania nowych rozwiązań. W przypadku np. analityków, główne zadanie zmieni się. Nie będzie istotne zebranie i uporządkowanie danych. Istotna będzie właściwa interpretacja otrzymanych wyników i analiz. Oznacza to zapotrzebowanie na o wiele bardziej kompetentny personel. Co do kwestii ilościowych – spodziewać się należy zmniejszenia zatrudnienia, ale ze względu na specyficzne wymagania kompetencyjne nie należy spodziewać się spadku kosztów osobowych.

Rozwój technologii na rynku finansowym z pewnością będzie miał wpływ na zmianę struktury tego sektora zatrudnienia. Tradycyjny model bankowości oparty na sieci placówek bankowych ustępuje coraz bardziej rozwijanej bankowości elektronicznej i mobilnej. W momencie, gdy nowe rozwiązania, takie jak wideoweryfikacja czy skanowanie dokumentów, biometria, pozwalają założyć rachunek czy wziąć kredyt całkowicie online, a wirtualni asystenci coraz lepiej obsługują klientów, spada potrzeba zatrudnienia w obszarach takich jak bezpośrednia sprzedaż czy obsługa klienta. Dodatkowo, jeśli technologia Distributed Ledger Technology (DLT) stanie się standardem, spadnie zapotrzebowanie na pracowników działów płatności transgranicznych. Zwiększy się natomiast zapotrzebowanie na pracowników w działach IT, nowych technologii, a także w compliance, co wynika z konieczności wdrożenia nowych regulacji międzynarodowych.

Współpraca ze start-upami jest szansą na rozwój nowych kompetencji – zwinnych rozwiązań, kreatywności, przedsiębiorczości, skrócenia czasu opracowania nowych produktów. Z drugiej strony wymaga od nas nowych kompetencji, a także połączenia różnych kompetencji, co w szczególności oznacza:

- większe zapotrzebowanie na pracowników, którzy potrafią budować rozwiązania biznesowe z wykorzystaniem technologii,
- większe zapotrzebowanie na specjalistów IT, którzy potrafią pracować nad rozwiązaniami od strony potrzeby klientów,
- zapotrzebowanie na specjalistów IT, którzy znają nowe technologie np. blockchain,
- zapotrzebowanie na specjalistów z zakresu data science,
- wykorzystywanie potencjału pracowników i ich umiejętności bardziej w obszarze asystowania klientom niż sprzedaży.

2.5. ***Jakie przeszkody natury regulacyjnej lub nadzorczej uniemożliwiają usługodawcom finansowym korzystanie z usług przetwarzania danych w chmurze? Czy kwestia ta wymaga podjęcia działań na poziomie UE?***

Prawnie i regulacyjnie można korzystać z usług w chmurze, chociaż wymaga to pewnych zmian i dodatkowych działań. Największe obawy organów nadzoru w kwestii przetwarzania danych w chmurze (“cloud computing”) przez instytucje finansowe dotyczą bezpieczeństwa przetwarzania danych poufnych oraz środowiska teleinformatycznego banku, jak również nadmiernego stopnia koncentracji dostawców rozwiązań chmurowych . Polski organ nadzoru wydał rekomendację, w której zaznacza, że przy przetwarzaniu danych poufnych poza infrastrukturą banku bank powinien:

- wprowadzić odpowiednie mechanizmy kontrolne zapewniające poufność tych danych (np. poprzez ich szyfrowanie),
- zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę,
- posiadać informacje o tym, w jakich lokalizacjach geograficznych dane te są przetwarzane oraz jakie przepisy prawa obowiązują tam w przedmiotowym zakresie, oraz zapewnić zgodność świadczonych usług z przepisami prawa obowiązującymi w Polsce,
- zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia – wraz ze wszystkimi kopiami – przez dostawcę usług),
- przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia obowiązku przedstawiania przez dostawcę certyfikatów w zakresie zgodności z uznanymi międzynarodowymi normami dotyczącymi bezpieczeństwa informacji (szczególne w przypadku przetwarzania danych poza granicami Europejskiego Obszaru Gospodarczego),
- monitorować jakość usługi i możliwość sprawowania kontroli (audytu) nad działalnością zewnętrznego usługodawcy w zakresie dostarczanych bankowi usług i określić jasne zasady wymiany i ochrony informacji poufnych.
- Powyższe wymagania są do spełnienia ale w praktyce wymagają szczegółowych uzgodnień i wielu interakcji z regulatorem, co wydłuża cały proces. Każde rozwiązanie chmurowe jest rozpatrywane oddzielnie na wniosek banku.

2.6.1. *Czy komercyjnie dostępne rozwiązania chmurowe spełniają minimalne wymogi, których muszą przestrzegać dostawcy usług finansowych?*

Komercyjnie dostępne rozwiązania chmurowe są zgodne z minimalnymi wymogami, które muszą spełniać instytucje finansowe. Należy zacząć od usług niebędących usługami kluczowymi z punktu widzenia stabilności i ciągłości działalności banku i w kolejnych krokach, po zebraniu doświadczeń, rozszerzać zakres możliwych rozwiązań. Światowi liderzy udostępniający rozwiązania chmurowe zapewniają wysoki poziom bezpieczeństwa przetwarzanych danych (mocne zespoły bezpieczeństwa, wysokie standardy zabezpieczeń, replikacja danych między Data Centers, certyfikacje ISO 27001, szyfrowanie danych, solidne bezpieczeństwo fizyczne Data Centers). W przypadku usług przetwarzania danych w chmurze, objęcie zadań realizowanych dla banku wysokimi standardami bezpieczeństwa spełnianymi przez dostawców tych usług, podlegających audytom i spełniających wymogi m.in. normy ISO 27001, będzie prowadziło do podwyższenia poziomu bezpieczeństwa danych i zastosowania jeszcze bardziej zaawansowanych narzędzi ich ochrony w porównaniu ze specjalistycznymi usługami IT świadczonymi lokalnie. Poziom ryzyka związany z wykorzystaniem usług chmurowych do pracy operacyjnej banku jest akceptowalny. Należy także podkreślić, że po odpowiednim dostosowaniu infrastruktury banku, jest możliwa integracja z istniejącymi systemami bezpieczeństwa banku wymaganymi przez KNF, takimi jak ograniczenie dostępu do danych bankowych wyłącznie do komputerów służbowych, kontrola przesyłanych e-maili przez system DLP (monitoring wycieku danych). Od strony technologicznej nie ma większych trudności w przygotowaniu integracji ze standardami technologicznymi używanymi przez banki. Problemy i przeszkody w ewentualnym wykorzystaniu rozwiązań chmurowych pojawiają się w momencie próby zastosowania tych rozwiązań w obszarach (danych, produktach, usługach) regulowanych przez ustawy bądź rekomendacje (krajowe lub UE). Przy obecnie obowiązujących przepisach,

każdy przypadek użycia musi być rozpatrywany indywidualnie, biorąc pod ocenę wszelkie ryzyka i aspekty procesów, w których „chmura" miałaby znaleźć zastosowanie (a zwłaszcza w kontekście danych, które w tej chmurze miałyby być przechowywane). Często nawet zastosowanie szyfrowania przesyłanych i przetwarzanych w chmurze danych nie wystarcza do spełnienia wymogów regulacyjnych, lub niweluje korzyści/możliwości, jakie mogłyby wyniknąć z zastosowania tego typu rozwiązań w miejsce infrastruktury informatycznej istniejącej wewnątrz organizacji.

2.6.2. *Czy komercyjnie dostępne rozwiązania chmurowe uwzględniają w tym celu konkretne zobowiązania umowne?*

Umowa na usługi chmurowe musi zawierać określone zapisy gwarantujące zgodność z przepisami dotyczącymi zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. Firmy z sektora finansowego powinny zapewnić umownie takie warunki, jakie są na nie nakładane przez odpowiednich regulatorów oraz spełnić takie SLA, jakie są wymagane w ramach świadczonego przez nie biznesu. Warunki powinny być ustalane między podmiotami, a ich szczegółowe zapisy mogłyby łatwo prowadzić do przeregulowania, narzucającego nieuzasadnione koszty na podmioty z sektora finansowego.

Kwestią oczywistą są zapisy z zakresu zachowania poufności danych przechowywanych w takich rozwiązaniach chmurowych. Jako dodatkowe zapisy/zapewnienia, które w takich komercyjnych chmurach również mogłyby być oferowane, wskazalibyśmy opcję wyboru lokalizacji serwerów, na których dane banku (instytucji z obszaru finansowego) mogłyby być przechowywane (możliwość wyboru konkretnych serwerów, krajów w których serwery mogą się znajdować, lub regionów/kontynentów, które chce się wykluczyć z listy akceptowalnych lokalizacji potencjalnych serwerowni). Zapewnienie takich zobowiązań mogłoby spowodować powstawanie również kolejnych uzgodnień gwarantujących pełną kontrolę lub monitoring nad powierzanymi przez instytucje danymi.

2.8. *Jakie są główne wyzwania dotyczące wdrożenia rozwiązań DLT (np. problemy technologiczne, standaryzacja danych oraz interoperacyjność systemów DLT)?*

W dalszym ciągu istnieje wiele wyzwań technologicznych. Wśród nich najważniejszym jest chyba opracowanie komercyjnie akceptowalnego algorytmu uzyskiwania konsensusu. Nie wydaje się, aby klasyczny proof-of-work mógł mieć głębsze komercyjne zastosowanie, a prace nad proof-of-stake idą znacznie wolniej, niż tego się spodziewano. Warto zwrócić też uwagę na kwestie skalowalności i wydajności tej klasy rozwiązań. W tym zakresie nadal doświadczenie jest niezmiernie małe. Największym wyzwaniem na obecnym etapie rozwoju DLT wydaje się być stworzenie standardu jej wykorzystania i ustalenie wspólnych regulacji na poziomie międzynarodowym. W obszarze samej technologii natomiast wyzwaniem z pewnością będzie stworzenie infrastruktury, a następnie kwestie wydajności i pojemności tego systemu. Potrzebna jest też znacznie większa współpraca pomiędzy bankami, firmami technologicznymi i regulatorami. Obecnie banki podchodzą do technologii DLT z rezerwą, angażując się jedynie w konsorcja powoływane do testowania tych rozwiązań (np. Ripple, R3, Linux). Technologia rozproszonych rejestrów (DLT) stanowi tylko i aż technologię. Kluczowym wyzwaniem jest znalezienie takiego modelu biznesowego, w którym technologia ta okazałaby się albo istotnie tańsza, albo niosąca wystarczająco dużo korzyści, w tym bezpieczeństwo i efektywność (nowych zastosowań przynoszących dodatkową wartość), które uzasadnią inwestycje w nią.

2.9. ***Jakie są główne przeszkody natury regulacyjnej lub nadzorczej (wynikające z przepisów UE lub krajowych) dotyczące wdrożenia rozwiązań DLT (i mechanizmów potwierdzania transakcji) w sektorze finansowym?***

Niewątpliwie największe bariery rozwoju technologii DLT wynikają z faktu, że rozwijają się one w niepewnym środowisku prawnym. Potrzebne są wspólne (ponadnarodowe) regulacje, które pozwolą na ustanowienie standardów umożliwiających łączenie różnych rozproszonych systemów (np. ponadgraniczne współdziałanie systemów krajowych wykorzystujących DLT). Jedną z najistotniejszych kwestii w tym obszarze jest standaryzacja tożsamości cyfrowej i mechanizmów potwierdzania transakcji (smart contracts). Istnieją co prawda już pierwsze próby standaryzacji (Chain Open Standard 1), jednak potrzebna jest znacznie szersza współpraca banków, FinTech i regulatorów. Barierą dla rozwoju tego typu technologii mogą być również regulacje typu RODO. Nowe technologie (w tym DLT) działają w obszarze tych samych regulacji, w których działają rozwiązania tradycyjne. Trudności interpretacji przepisów mogą więc wynikać z braku bezpośrednich odniesień do sfery technologicznej oraz możliwości przetwarzania poszczególnych rodzajów informacji i wykonywania określonych czynności (np. w zakresie outsourcingu czynności bankowych, przetwarzania danych osobowych). Główną przeszkodą prawną w implementacji technologii DLT jest brak odpowiednich regulacji, które pozwoliłyby na swobodne działanie podmiotów w tym obszarze. Komisja Europejska jest dopiero na etapie "demistyfikacji" tego tematu, czyli inicjowania projektów zwiększających wiedzę wśród członków instytucji unijnych.

W związku z tym, iż w ramach technologii DLT mogą przepływać informacje obejmujące swoją treścią dane osobowe, będą musiały być spełnione wymagania ustawy w zakresie przetwarzania danych osobowych. Kwestią, na którą warto zwrócić uwagę jest zapewnienie osobie fizycznej prawa do zmiany, modyfikacji danych czy też zaprzestania przetwarzania danych. Może być to trudne do spełniania, gdyż DLT z zasady nie przewiduje możliwości wykreślenia i modyfikacji danych. Problematyczne jest także wskazanie administratora danych, co również nie będzie w zgodnie z obecnym brzmieniem w/w ustawy. A zatem sprawne funkcjonowanie DLT wiąże się ze zmianami legislacyjnymi między innymi w sferze ochrony danych osobowych.

2.11. ***Czy dotychczasowe wymogi dotyczące outsourcingu w prawodawstwie dotyczącym usług finansowych są wystarczające? Kto jest odpowiedzialny za działalność dostawców zewnętrznych i w jaki sposób dostawcy są nadzorowani? W jakich obszarach potrzebne są dalsze działania i na czym powinny takie działania polegać*****?***

Regulacje zawarte w polskim prawie bankowym dotyczące outsourcingu bankowego oraz w ustawie o obrocie instrumentami finansowymi dotyczące outsourcingu inwestycyjnego są regulacjami poddającymi outsourcing bankowy i inwestycyjny dość dużemu nadzorowi polskiego regulatora – Komisji Nadzoru Finansowego. W porównaniu z regulacjami europejskimi dot. outsourcingu bankowego i inwestycyjnego, polskie regulacje są bardziej restrykcyjne, co wynika z oczywistego podejścia, zgodnie z którym nadzorowi, poddawane są czynności składające się na działalność instytucji finansowej, bez względu na to kto i gdzie czynności te wykonuje. Wymogi prawne w zakresie korzystania z outsourcingu wpływają w sposób istotny na podejmowanie przez instytucje finansowe decyzji o korzystaniu z usług zewnętrznych dostawców, często powodując unikanie tej formy współpracy ze względu na wymogi bezpieczeństwa. Polskie prawo zasadniczo nie reguluje zjawiska outsourcingu, poza pewnymi wyjątkami sektorowymi. Takim wyjątkiem jest outsourcing bankowy, którego stosowanie i warunki są limitowane na mocy przepisów rangi ustawowej. Zakres czynności, które mogą być przedmiotem outsourcingu został w sposób stosunkowo kazuistyczny

uregulowany w przywołanej ustawie. Szczegółowo zostały również określone wymogi i sposób wykonania umowy. Najistotniejszą kwestią jest solidarna odpowiedzialność banku i dostawcy IT za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy outsourcingu – odpowiedzialności tej nie można wyłączyć ani ograniczyć. W Polsce wymagania dotyczące outsourcingu są restrykcyjne. Nie wydaje się wskazane wprowadzenie dodatkowych regulacji w obszarze outsourcingu, chyba że miałyby one na celu harmonizację wymagań dla całej Unii Europejskiej.

3.4. ***Czy UE powinna wprowadzić nowe kategorie licencjonowania dla działalności FinTech ze zharmonizowanymi i proporcjonalnymi wymogami regulacyjnymi i nadzorczymi, w tym paszportowania takiej działalności na jednolitym rynku UE? Jeśli tak, to w jakich obszarach powinno to nastąpić i jaką rolę powinna odgrywać ESA? Na przykład, czy ESA powinny mieć swój udział w unijnej rejestracji i nadzorze nad firmami FinTech?***

FinTechy mogą funkcjonować na prawach rynkowych, zupełnie na tej samej zasadzie, co inne działalności gospodarcze lub spółki. Tworzenie dodatkowych form licencjonowania i kategoryzowania branżowego rodzi biurokrację i formalizm, co często przeszkadza w tworzeniu innowacji. Wszyscy uczestnicy rynku powinni być traktowani równo. Znoszenie barier wejścia na rynek i ułatwianie funkcjonowania startupów finansowych powinno być wprowadzane bardzo rozważnie z uwagi na duże ryzyko dla całego sektora. Jak słusznie stwierdza się w dokumencie konsultacyjnym, taki sam rodzaj działalności powinien podlegać takim samym zasadom. Fakt, iż w przypadku pewnych rodzajów działalności znajdują zastosowanie nowoczesne rozwiązania technologiczne, nie może uzasadniać stosowania wobec nich taryfy ulgowej. Co więcej, owa nowoczesna technologia wymaga bardziej ostrożnego podejścia, zwłaszcza w początkowym okresie jej stosowania.

3.7. ***Czy trzy zasady neutralności technologicznej, proporcjonalności i integralności mogą stanowić podstawy podejścia regulacyjnego w przypadku działalności FinTech?***

Neutralność, proporcjonalność i integralność są uniwersalnymi zasadami, nie tylko dla działania FinTechowego. Oczywiście, są one właściwe, ale nie jedyne. Dyskusja dotyczy stosowania rozwiązań technologicznych w instytucjach finansowych. Nowe technologie mogą funkcjonować na rynku samodzielnie, jako niezależne przedsiębiorstwa, które wykonują pewne czynności na rzecz instytucji finansowych. Mogą też wchodzić do wnętrza organizacji, jako jej część. Jeśli mamy do czynienia z samodzielnym podmiotem, niezbędne jest odwołanie się jeszcze do czwartej zasady: nowe rozwiązania nie mogą w żaden sposób pogarszać bezpieczeństwa danej instytucji i zgromadzonych w niej środków finansowych. Zasadzie tej niechętni są outsourcerzy. Jednak jej nieprzestrzeganie może zagrozić bezpieczeństwu systemu finansowego, nawet w bardzo dużej skali z powodu ryzyka operacyjnego i efektu zarażania.

3.8. ***W jaki optymalny sposób Komisja lub ESA mogą koordynować, uzupełniać lub łączyć poszczególne praktyki i inicjatywy podejmowane przez władze krajowe w celu wspierania FinTech (np. centrów innowacji, akceleratorów lub projektów sandbox) i uczynić całą UE centrum innowacji FinTech? Jakie byłyby korzyści z gromadzenia wiedzy specjalistycznej w ESA?***

Komisja Europejska oraz ESA powinny wspierać tworzenie Innovation hubów, akceleratorów i piaskownic regulacyjnych (regulatory sandbox). Spodziewamy się, że rolą takich rozwiązań będzie wspieranie innowacyjnych przedsięwzięć oraz pomoc w zapewnieniu zgodności

z wymaganiami regulacyjnymi. W pierwszej kolejności takie rozwiązania powinny zostać uruchomione na poziomie poszczególnych państw członkowskich, gdyż tam znajduje się nadzór nad rynkiem finansowym.

Lokalne praktyki tego rodzaju mogą potencjalnie napotykać na ograniczenia tam, gdzie prowadzone projekty mierzą się z problemami związanymi ze stosowanymi wprost regulacjami wspólnotowymi (rozporządzenia Komisji Europejskiej). Ponadto, coraz częściej prowadzone projekty mają zasięg transgraniczny i wsparcie ze strony wyłącznie lokalnego regulatora może okazać się niewystarczające. Wreszcie, niektóre przedsięwzięcia opierają się na integracji technologicznej z infrastrukturą ponadnarodową, jak wspólna waluta (Euro - również w oczekiwanej formie wirtualnej), systemy rozliczeniowe Target2, T2S czy też SEPA. W takich sytuacjach dla sprawnego funkcjonowania lokalnych rozwiązań niezbędne jest utworzenie odpowiedniego partnerskiego ośrodka na poziomie UE zapewniającego wsparcie w zakresie regulacji wspólnotowych, a ponadto koordynację i harmonizację podejmowanych inicjatyw takich jak:

- wspieranie w krajach europejskich projektów sandbox (piaskownic regulacyjnych), które umożliwiają rozwój startującym firmom technologicznym,
- rozpowszechnianie programów promujących rozwój tej branży (np. akceleratory, hackatony, projekty badawcze),
- współpraca z regionalnymi stowarzyszeniami zrzeszającymi ekosystem FinTechowy,
- tworzenie miejsc coworkingowych w przestrzeni publicznej,
- programy funduszy unijnych przeznaczonych na rozwój nowych technologii.

3.12.1. *Czy opracowanie norm technicznych i interoperacyjności dla FinTech w UE jest w wystarczającym stopniu uwzględnione w ramach Europejskiego Systemu Nadzoru Finansowego?*

Specyfiką i siłą FinTech jest brak lub ograniczone regulacje, pozwalające tworzyć innowacje, często dostosowane do poszczególnych rynków. Nie widać potrzeby regulacji wymuszających interoperacyjność. Co więcej, na obecnym etapie rozwoju Internetu oraz podejścia API, można zakładać, że interoperacyjność, o ile będzie miała uzasadnienie biznesowe, pojawi się bez inicjatyw regulacyjnych.

3.12.2. *Czy obecny poziom standaryzacji i interoperacyjności danych stanowi przeszkodę w pełnym wykorzystaniu możliwości outsourcingu?*

Standaryzacja i interoperacyjność nie stanowi bariery uniemożliwiającej outsourcing. Różnorodność rozwiązań jest genezą innowacji i pełna standaryzacja wszystkich procesów nie byłaby korzystna dla rynku. Wystarczająca jest standaryzacja w wybranych kluczowych obszarach (dobrym przykładem są np. przelewy SEPA – SCT czy eIDAS).

3.13. *W jakich obszarach normy na poziomie unijnym i globalnym mogą ułatwić efektywność i interoperacyjność rozwiązań FinTech? Jakie byłoby najbardziej skuteczne i konkurencyjne podejście do opracowania tych norm?*

Normy unijne powinny przede wszystkim ujednolicić prawo w obszarze nowych technologii finansowych i sprawić, by było ono przejrzyste i zrozumiałe dla młodych firm wchodzących na ten rynek. Z pewnością takie projekty jak sandbox zwiększają efektywność i ułatwiają wdrożenie

rozwiązań FinTechowych. Rozwój standardowych komunikatów API w ramach np. ISO 20022 etc. może być pomocny dla rozwoju. Należy jednak pamiętać, że cykle rozwoju standardów, np. ISO, nie są wystarczająco szybkie i nie należy limitować rynku do korzystania tylko ze standardów już istniejących, ponieważ utrudniałoby to innowacje, które z założenia potrzebują możliwości wychodzenia poza istniejące standardy.

4.2. ***W jakim stopniu rozwiązania DLT mogą stanowić niezawodne narzędzie do przechowywania i udostępniania informacji finansowych? Czy istnieją alternatywne rozwiązania technologiczne?***

Choć skala wykorzystania technologii nie może być porównywana z tradycyjnymi technologiami, to doświadczenia na rynku wirtualnych walut (Bitcoin) pokazują, że rozwiązania DLT są bezpieczne i niezawodne i mogą być powszechnie stosowane i stanowić alternatywę dla obecnych rozwiązań. W naszej opinii jest tylko kwestią czasu wykorzystanie technologii w szerszym kontekście, co pozwoli na duże oszczędności związane z przechowywaniem i zabezpieczeniem danych (brak pośredników, redukcja kosztów zabezpieczenia i utrzymania). DLT umożliwia tworzenie zdecentralizowanych sieci przechowujących i zarządzających danymi, w których nie jest już potrzebny ośrodek centralny. Ponadto, informacje przechowywane w DLT są z definicji odporne na próby nieuprawnionej ingerencji, czyli w rzeczywistości dane, które zostaną prawidłowo wprowadzone do DLT, pozostają niezmienne. Jest to wyróżniająca cecha DLT, która czyni je odpowiednim narzędziem do przechowywania dowodów własności lub istnienia. Istnieje wiele procesów finansowych i usług, które mogą korzystać z tego niezmiennego składowania. Informacje o klientach, informacje o umowach, prawa własności, klucze kryptograficzne zastępujące własnoręczne podpisy to tylko niektóre z rodzajów informacji, które mogłyby zostać zapisane w DLT.

4.8. ***Jakie bariery regulacyjne lub inne ewentualne przeszkody o różnym charakterze utrudniają lub uniemożliwiają dzielenie się informacjami o cyberprzestępczości między dostawcami usług finansowych oraz z władzami publicznymi? Jak można je usunąć?***

Największymi barierami są:

- ograniczenia w ochronie danych osobowych przy dostępie, informowaniu, przeciwdziałaniu lub dochodzeniach związanych z wykrywaniem przestępstw lub przeciwdziałaniem oszustwom,
- różne regulacje poszczególnych krajów – różna klasyfikacja prawna poszczególnych przestępstw lub wykroczeń,
- brak możliwości bardzo szybkiego reagowania na cyberprzestępstwa dokonywane między kilkoma krajami (brak współpracy policji w trybie rzeczywistym real-time; brak czegoś w rodzaju policji internetowej).

Różnorodność rozwiązań stosowanych przez podmioty z sektora finansowego jest elementem bezpieczeństwa tych usług. Pełna standaryzacja oznaczałaby zwiększenie ryzyka systemowego w przypadku złamania zabezpieczeń. Korzystna dla bezpieczeństwa sektora finansowego różnorodność oraz podejście risk-based approach powoduje jednak brak pełnej interoperacyjności systemów, co stanowi naturalną, choć drugorzędną barierę dla wymiany informacji. Kluczowe bariery to naturalna ochrona własnych danych przed konkurencją oraz ograniczenia regulacyjne w zakresie danych osobowych czy tajemnicy bankowej, co powoduje, że nie wszystkie potencjalnie cenne dla zwalczania cyberprzestępstw dane mogę być współdzielone. W celu dzielenia się wiedzą o cyberzagrożeniach konieczna jest współpraca

sektorowa (np. między bankami, między dostawcami infrastruktury telekomunikacyjnej, w ramach sektora publicznego) oraz międzysektorowa, tak aby ułatwiać identyfikowanie zagrożeń. W Polsce bariery tego typu praktycznie nie istnieją. Instytucje finansowe od wielu lat współpracują ze sobą oraz z instytucjami państwowymi, policją i innymi dedykowanymi instytucjami i wymieniają informacje poprzez dedykowaną platformę. W 2016 roku zostało utworzone Centrum Cyberbezpieczeństwa (Cyber Security Centre), gdzie banki, telekomy i reprezentanci instytucji rządowych wypracowują efektywne formy współpracy, komunikacji i wymiany informacji.