UNIVERZITA KARLOVA

Právnická fakulta

FinTech a AML z právní perspektivy

Diplomová práce

Mikuláš Zacpal

Vedoucí diplomové práce: **JUDr. Petr Kotáb, Ph.D.**

Katedra: **Katedra finančního práva a finanční vědy**

Datum vypracování práce (uzavření rukopisu): **30. 6. 2020**

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 203 468 znaků včetně mezer.

V Praze dne 30. 6. 2020

Mikuláš Zacpal

Poděkování

Chtěl bych zde poděkovat všem, kteří mi v průběhu psaní práce poskytli cenné rady, zejména pak JUDr. Petru Kotábovi, Ph.D. za jeho odborné vedení mojí práce.

Obsah

Úvod **1**
1. FinTech a přístupy k jeho regulaci **4**
1.1. Jaké služby lze dnes považovat za FinTech? 5
1.2. Vliv na ekonomiku 11
1.3. Regulační přístupy 12
2. Vybrané povinnosti z hlediska AML **19**
2.1. Kontrola klienta 20
2.2. Politicky exponované osoby 25
2.3. Evidence skutečných majitelů 28
2.4. Podezřelý obchod a systém vnitřních zásad 33
2.5. Další povinnosti 36
3. Vzdálená identifikace **37**
3.1. Stávající typy vzdálené identifikace a jejich novelizace 37
3.2. Nové možnosti vzdálené identifikace 44
3.3. Vzdálená identifikace v zahraničí 51
3.4. Působnost AML zákona na přeshraniční služby 54
4. Působnost AML zákona na vybrané FinTech služby **59**
4.1. Neobanking 59
4.2. Crowdfunding 63
4.3. Kryptoaktiva 67
Závěr **73**
Seznam zkratek **77**
Seznam použitých zdrojů **79**
Abstrakt a klíčová slova **91**
Abstract and keywords **92**

Úvod

Tato práce se zabývá vztahem mezi novými finančními technologiemi a pravidly proti praní špinavých peněz, financování terorismu a opatřeními k provádění mezinárodních sankcí. Jedná o aktuální téma, a to z několika důvodů. V posledních letech dochází k přesunu finančních služeb do online světa, vznikají virtuální poskytovatelé platebních služeb, výrazně rostou objemy finančních prostředků, které procházejí skrze crowdfundingové platformy, a dochází k širšímu využívání kryptoaktiv, ať už jako nástrojů investiční spekulace nebo při běžných platbách.

Přiměřená aplikace AML[1] a CFT[2] pravidel na nové finanční technologie (FinTech) je tématem nejen českým či evropským, ale celosvětovým. Tvůrci právních norem musí poměřovat pozitivní vliv finančních technologií pro spotřebitele a na ekonomiku celkově se zájmem spočívajícím v dostatečné míře ochrany před praním špinavých peněz a financováním terorismu. AML a CFT pravidla jsou podrobná a jejich dodržování je nákladné. To vytváří překážky jak pro vznik nových FinTech služeb, které často vznikají jako startupy, tak i pro jejich snadné používání. Neustálý vznik a vývoj nových služeb je přitom žádoucí, neboť vytváří konkurenci tradičním institucím. Konkurence plodí inovace, snižuje ceny a zvyšuje komfort pro konečného spotřebitele.

Aktuálnost tématu lze demonstrovat i pomocí názorů, které zazněly na diskusním setkání k FinTech, které pořádalo ministerstvo financí (MF): „*Kde trh vnímá problémy pro vznik a fungování FinTech, jsou zvláště AML pravidla. Při poskytování finančních služeb online je velký problém s jejich dodržováním. (…) Něco může být vyřešeno přijetím eIDAS, ovšem pravidla AML jsou vnímána jako největší překážka vývoje fintech.*“[3]

Cílem této práce proto bude zejména objasnit, jak jsou FinTech společnosti zasaženy AML a CFT pravidly a vyhodnotit, jaké aspekty těchto pravidel vytvářejí překážky pro *compliance.*

---

[1] AML, neboli *anti-money laundering*, je boj proti praní špinavých peněz.
[2] CFT, neboli *combating the financing of terrorism*, případně též *countering the financing of terrorism*, je boj proti financování terorismu.
[3] MINISTERSTVO FINANCÍ. *Online identifikace a AML/CFT: Podkladová studie* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/podkladova-studie-financni-technologie-a-31641. Str. 3.

Dále dojde k analýze vzdálené identifikace klienta a osobní působnosti AML zákona. V průběhu práce poskytnu kritický pohled a vlastní podněty k dílčím problematikám.

Cílem práce naopak nebude snaha o kompletní výčty povinností dopadajících na FinTech společnosti, objasňování základních finančněprávních pojmů nebo zkoumání činnosti relevantních domácích i mezinárodních institucí. Taktéž nebude zkoumána historická geneze AML a CFT pravidel. Téma praní špinavých peněz částečně spadá i do oblasti trestního práva. Domnívám se však, že této dimenzi se věnuje dostatečná pozornost a zaměřím se proto na finančněprávní rovinu.

Práce je rozčleněna do čtyř kapitol. První kapitola, která poslouží jako nezbytný úvod tématu, se bude zabývat samotným pojmem FinTech, srovnáním společností a obchodních modelů, které jsou takto označovány, s tradičními finančními institucemi a dále otázkou, jaké typy služeb či technologií pod tento pojem můžeme v současnosti zařadit. Dále jaký vliv mají finanční inovace na ekonomiku a jakým způsobem k FinTech přistupují regulátoři vybraných států. V této kapitole bude využita převážně deskriptivní metoda, v menší míře pak analýza a komparace. V druhé kapitole dojde k vysvětlení a zhodnocení povinností stanovených AML pravidly a jejich dopadu na FinTech společnosti jakožto povinné osoby z hlediska náročnosti dosažení *compliance*. Rovněž budou prezentovány podněty do budoucna. Pro objasnění základních institutů bude využita metoda deskripce, avšak převažovat bude kritická analýza dopadajících povinností. Ve třetí kapitole dojde k hodnocení stávajících i budoucích možností vzdálené identifikace v české právní úpravě. Mimo to budou porovnány zahraniční právní úpravy vzdálené identifikace a na případové studii bude demonstrována problematika působnosti českého AML zákona na zahraniční subjekty. Za tímto účelem bude využita především kritická analýza, v menší míře pak deskripce, komparace i syntéza. Čtvrtá kapitola bude zkoumat působnost AML zákona ve vztahu k neobankingu, crowdfundingu a kryptoaktivům. Tyto oblasti jsem zvolil, neboť se jedná o nejvýznamnější oblasti FinTech, se kterými jsou určitá rizika v oblasti AML a CFT spojována. Bude zde využita deskripce, analýza a v menším rozsahu i komparace.

Pro účely naplnění cílů této diplomové práce byly shromážděny dostupné domácí i zahraniční zdroje. Využity zde nebudou jen právní monografie, právní normy a komentáře k nim, ale i množství článků, doporučení, stanovisek, dokumentů a studií. Pramenů k AML a CFT je v obecné rovině dostatek, avšak problematice finančních inovací se ve většině případů

podrobněji nevěnují. Menší míra probádanosti problematiky je však jedním z důvodů, proč jsem o toto téma diplomové práce požádal.

Tam, kde jsou v práci zmíněna AML pravidla, mám na mysli jak pravidla proti praní špinavých peněz, tak i pravidla proti financování terorismu a pravidla pro uplatňování mezinárodních sankcí, není-li stanoveno jinak. Česká republika v době psaní této práce stále neimplementovala pátou AML směrnici. Návrhy novely českého AML zákona a zákona o evidenci skutečných majitelů však prošly mezirezortním připomínkovým řízením a dne 1. 6. 2020 byly projednány a schváleny vládou. V práci tak budu využívat i tyto návrhy. V případě předkládání informací o konkrétních FinTech službách pak upozorňuji, že moje porozumění ohledně jejich fungování může být ovlivněno tím, že budu vycházet částečně nebo i výhradně z informací, které o sobě samy tyto služby veřejně poskytují.

1. FinTech a přístupy k jeho regulaci

FinTech je v posledních letech intenzivně diskutovaným tématem finančního sektoru. Nejedná se pouze o okrajově využívané technologie, ale o trend, který prostupuje všemi oblastmi finančních služeb. Samotné slovo FinTech je zkratka pro finanční technologie. Na jednotné definici pojmu neexistuje shoda. Užší vymezení pojmu poskytuje například slovník Oxford, který FinTech definuje jako „*počítačové programy a další technologie využité na podporu nebo umožnění bankovních a finančních služeb*“[4] (překlad autor). Investopedia definuje FinTech specifičtěji jako „*nové technologie, které usilují o zlepšení a automatizaci poskytování a používání finančních služeb. V jádru je FinTech využíván k tomu, aby pomohl společnostem, vlastníkům podniků a spotřebitelům lépe spravovat jejich finanční operace, procesy a životy pomocí specializovaného software a algoritmů, které jsou používány počítači a stále více smartphony*“[5] (překlad autor). Obecněji ale tento pojem neoznačuje pouze technologie, které jsou používány pro finanční služby, ale i typ podnikání, případně obchodní model, který je založen na využití technologie a je z určitého hlediska inovativní oproti tradičním finančním službám.[6,7] Může se jednat o úplně nové služby, nebo pouze o zefektivnění stávajících služeb s využitím stávající infrastruktury. Nutno podotknout, že technologie, které jsou FinTech službami využívány, často nejsou samy o sobě nějak revoluční (s výjimkou DLT), avšak nové je jejich využití ve finančním sektoru, případně jejich rozšíření v jeho rámci.[8] To, co bychom před dvaceti lety nazvali jako FinTech, kupříkladu internetové bankovnictví, by již dnes tento pojem nenaplňovalo a stejně tak služby, které dnes označujeme jako FinTech, o toto označení možná přijdou, protože v budoucnosti bude vysoká míra digitalizace standardem. Byť se

[4] Definition of fintech in English. *Oxford Dictionaries* [online]. Oxford University Press [cit. 2020-06-06]. Dostupné z: https://en.oxforddictionaries.com/definition/fintech.

[5] What is Fintech?. *Investopedia* [online]. 2019 [cit. 2020-06-06]. Dostupné z: https://www.investopedia.com/terms/f/fintech.asp.

[6] Např. TANDA, Alessandra a Cristiana-Maria SCHENA. *FinTech, BigTech and Banks*. Springer International Publishing, 2019, 111 s. ISBN 978-3-030-22425-7. Str. 2.

[7] Např. FINANCIAL STABILITY BOARD. *FinTech and market structure in financial services: Market developments and potential financial stability implications* [online], 2019 [cit. 2020-06-06]. Dostupné z: http://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/. Str. 1.

[8] Evropská komise dokonce označuje DLT jako příklad disruptivní inovace. Ostatní finanční inovace, které se objevují většinou na vyspělých trzích a jsou založené na vylepšování existujících služeb pomocí postupných kroků, označuje jako nedisruptivní inovace. EVROPSKÁ KOMISE. *Creating FinTech opportunities for SMEs*. Luxembourg, 2019. ISBN 978-92-76-02901-4. Str. 7.

jedná o poměrně neurčitý pojem, v této práci ho budu používat, neboť se jedná o nejpoužívanější označení.[9] Z výše uvedeného je zřejmé, že FinTech není právní pojem.

Vznik FinTech společností umožňuje zejména široce dostupný internet a vysoká míra rozšíření mobilních zařízení ve společnosti. Některé FinTech služby lze využívat pouze prostřednictvím mobilního zařízení. Služba se tímto způsobem může zbavit odpovědnosti za vývoj a zabezpečení více typů přístupových rozhraní a šetří tak náklady. Mladší generace ztratily důvěru v tradiční finanční instituce a připisují jim zavinění globální finanční krize v roce 2008. Mění se i jejich vnímání finančních služeb. Nechtějí již být pouze pasivními zákazníky, ale stávají se aktivními uživateli, kteří očekávají, že služby budou přizpůsobeny jejich potřebám.[10]

Tradiční instituce disponují širokou obchodní i technickou infrastrukturou, kterou musely v průběhu času získat a kterou musí udržovat a vylepšovat.[11] Také mají široká portfolia činností a závazky z minulosti. Obecně lze také říct, že velké společnosti inovují své služby pomaleji než společnosti nově vzniklé. Zatímco nově vzniklé FinTech společnosti vytvářejí jeden ucelený systém, jehož součástí jsou i AML procesy, tradiční instituce je často vyvíjejí samostatně a musí tyto procesy integrovat do vlastních již existujících a komplexních systémů.[12] Bylo by ovšem chybou považovat za FinTech společnosti pouze startupy, byť je jejich výskyt značný.

1.1. Jaké služby lze dnes považovat za FinTech?

1.1.1. Neobanking

V posledních několika letech začaly vznikat a získávat popularitu banky či poskytovatelé platebních služeb nového typu. Jedná se o společnosti, které poskytují své služby pouze online prostřednictvím webového nebo mobilního rozhraní a pro své služby mohou využívat i již existující bankovní infrastrukturu. Nemají pobočky ani vlastní bankomaty, ale vydávají vlastní fyzické či virtuální platební karty. Aby šetřily náklady, využívají v co nejširší míře

[9] Např. EVROPSKÁ KOMISE. *Akční plán pro finanční technologie: Za konkurenceschopnější a inovativnější evropský finanční sektor* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0109&from=CS.
[10] NICOLETTI, Bernardo. *The Future of FinTech: Integrating Finance and Technology in Financial Services*. Palgrave Macmillan, 2017, 328 s. ISBN 978-3-319-51414-7. Str. 5-6.
[11] NICOLETTI, Bernardo. *Mobile Banking: Evolution or Revolution?*. Palgrave Macmillan UK, 2014, 209 s. ISBN 978-1-349-48166-8. Str. 162.
[12] On the Frontline: Fintech vs Money Laundering. *The Economist Intelligence Unit* [online]. 2019 [cit. 2020-06-06]. Dostupné z: https://eiuperspectives.economist.com/sites/default/files/money-laundering-exposed-fintech-wp-uk_1.pdf. Str. 3.

automatizované procesy. Jejich typickým rysem je minimum poplatků za poskytování standardních služeb a zaměření se na zpoplatnění služeb prémiových. Obvykle cílí na menší klienty a poskytují rychlejší platby, výhodnější měnové konverze nebo přeshraniční převody.[13] Tento obchodní model se v posledních letech označuje jako *neobanking*. Lze se setkat i s pojmem *challenger banks*.[14] Tento pojem je ale primárně spjatý se situací ve Velké Británii, kde došlo po zmírnění přísné bankovní regulace ke vzniku nových konkurentů. Ti se stali „*vyzyvateli*" několika do té doby dominujících finančních skupin.[15] Příkladem neobank mohou být Revolut, Starling Bank nebo Monzo z Velké Británie, N26 z Německa nebo Twisto z ČR.

Do kategorie *neobanking* lze zařadit i služby, jejichž vznik umožnilo přijetí druhé směrnice o platebních službách (PSD2), která poskytovatelům platebních služeb mimo jiné ukládá, aby prostřednictvím otevřeného API[16] na vyžádání svého klienta poskytovali třetím osobám zabezpečeným způsobem informace o platebních účtech. V této souvislosti se obecně používá pojem *open banking* (otevřené bankovnictví). Snahou je přimět poskytovatele platebních účtů, aby informace o těchto účtech poskytovali konkurenci či inovátorům, a tím zvýšili komfort spotřebitelů a umožnili vznik inovací. Ty spočívají ve službách, které prostřednictvím jednoho rozhraní umožňují uživateli ovládat více platebních účtů a pomáhají mu tak snáze kombinovat výhody různých poskytovatelů a lépe spravovat vlastní finance. Tyto služby jsou tedy založeny především na využívání stávající platební infrastruktury a jejich přidanou hodnotou je analýza finančních toků, případně zjednodušení již poskytovaných služeb svému uživateli.[17] Jejich zákonný podklad tvoří §§ 161-162 zákona o platebním styku (ZPS) pod označením „*nepřímé dání platebního příkazu*" a §§ 191-192 ZPS coby „*služba informování o platebním účtu*".

Podle mého názoru lze do této kategorie řadit rovněž P2P FX služby (peer-to-peer foreign exchange). Jde o odvětví, kde dosud dominují tradiční banky. Tyto služby jsou nástrojem pro levnější konverzi měn a jejich převod do zahraničí. Jejich podstatou je, že obcházejí standardní mezinárodní bankovní systém a mezistátní převody provádějí jen v nezbytně nutné míře. V tomto ohledu lze přirovnat P2P FX k tradičnímu finančnímu převodnímu systému

---

[13] BLAKSTAD, Sofie a Robert ALLEN. *FinTech Revolution*. Springer International Publishing, 2018, 406 s. ISBN 978-3-319-76013-1. Str. 150.
[14] Např. NICOLETTI, Bernardo. *The Future of FinTech: Integrating Finance and Technology in Financial Services*. Palgrave Macmillan, 2017, 328 s. ISBN 978-3-319-51414-7. Str. 288.
[15] BOOBIER, Tony. *AI and the Future of Banking*. John Wiley & Sons, 2020, 283 s. ISBN 978-1-119-59613-4. Str. 5-6.
[16] API, neboli *application programming interface*, je soubor definic pro vzájemnou komunikaci aplikací.
[17] DELOITTE. *Jak prosperovat v nejisté budoucnosti: Otevřené bankovnictví a PSD2* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/legal/articles/psd2.html. Str. 9-13.

hawala.[18] P2P FX služby spravují mnoho bankovních účtů u bank v mnoha zemích a párují platby, které jdou proti sobě. Pokud tedy budeme chtít české koruny konvertovat na EUR a zasílat je na lotyšský bankovní účet, pošleme domácí platbu podle pokynů na český korunový účet poskytovatele služby a služba tuto operaci spáruje s protijdoucím požadavkem na směnu z EUR na koruny z Lotyšska na český bankovní účet. Ve skutečnosti se neprovede přeshraniční platba, ale pouze se přepíší údaje o odesílateli a příjemci a provedou se dva domácí bankovní převody v ČR a dva domácí bankovní převody v Lotyšsku.[19] S ohledem na požadavek oboustranné poptávky může provedení transakce trvat delší dobu. Představiteli tohoto typu služby jsou například britský TransferWise nebo český Roklen FX.

1.1.2. Crowdfunding

Crowdfunding, neboli skupinové financování, je označení situace, kdy se více osob podílí na financování určitého projektu. Možnost účastnit se financování je zpravidla otevřena komukoliv a probíhá online skrze zprostředkující platformy. Podle povahy financovaného projektu můžeme rozlišovat několik podob crowdfundingu.[20]

Odměnový crowdfunding spočívá ve skupinovém financování určitého projektu, za což při naplnění cílové částky získají účastníci odměnu, ať už se jedná o hmotnou věc, službu nebo jinou výhodu, například předběžný přístup k projektu. Přispěvatelé s vyšší částkou obvykle získávají lepší odměnu. Pokud není naplněna cílová částka projektu, portály zprostředkovávající skupinové financování nebo vlastníci projektů vrací vložené částky přispěvatelům a ti tak nenesou riziko za nenaplnění cílové částky nebo případný neúspěch projektu. Tento typ crowdfundingu může dále sloužit jako určitý test popularity, který může vzbudit pozornost profesionálních investorů.[21]

Dárcovský crowdfunding je skupinové financování určitého, často charitativního nebo jinak společensky prospěšného projektu. Dárci jsou motivování přesvědčením nebo následným dobrým pocitem a neočekávají jakoukoliv jinou návratnost. Z důvodu možné kolize s právními

[18] DE SANCTIS, Fausto Martin. *Technology-Enhanced Methods of Money Laundering*. Springer International Publishing, 2019, 174 s. ISBN 978-3-030-18329-5. Str. 56.
[19] ARSLANIAN, Henri a Fabrice FISCHER. *The Future of Finance*. Springer International Publishing, 2019, 312 s. ISBN 978-3-030-14532-3. Str. 35.
[20] CUMMING, Douglas a Lars HORNUF, ed. *The Economics of Crowdfunding: Startups, Portals and Investor Behavior*. Springer International Publishing, 2018, 283 s. ISBN 978-3-319-66118-6. Str. vii.
[21] Takovým příkladem se v minulosti stal projekt české počítačové hry Kingdom Come: Deliverance.

úpravami věřejných sbírek[22] se někdy crowdfundingové platformy vydávají za odměnový crowdfunding, přestože částka poskytovaná „*kupujícím*“ (fakticky dárcem) zjevně převyšuje poskytované protiplnění.

Investiční crowdfunding, v některých pramenech označován jako *investment-based crowdfunding*, případně specifičtěji jako *securities crowdfunding* nebo *equity crowdfunding*, je alternativní způsob financování podnikatelských záměrů. Možnost financování je určena široké veřejnosti a zpravidla je možné podílet se na financování i nižšími částkami. Investoři[23] získávají dluhový cenný papír, případně podíl ve společnosti. Výhodou pro podnikatele je, že takto získané financování může být levnější než takové, které by mu poskytla banka, pokud by ho vůbec poskytla. Investory láká potenciální vysoké zhodnocení a vyšší míru rizika jsou ochotni snést, případně ji nevnímají jako reálnou a diverzifikují své investice do většího počtu projektů. Vyšší míra diverzifikace je právě díky nižším minimálním částkám pro participaci umožněna i malým investorům. Investice taktéž zdánlivě nevyžaduje hlubší investiční znalosti a její provedení skrze platformu je uživatelsky přívětivé.

Dluhový crowdfunding, někdy též *lending-based crowdfunding* nebo *marketplace lending*, je označení situace, při které jednotlivci nebo podnikatelé za účelem finančního zhodnocení s využitím online platformy skupinově financují úvěr poskytovaný jednotlivci nebo podnikateli. V závislosti, kdo je na které straně, je možné dále rozlišovat P2B (peer-to-business, člověk – podnikatel), P2P (peer-to-peer, člověk – člověk) a teoreticky i B2P a B2B. Tyto čtyři formy se ale nejčastěji označují obecně (a někdy zavádějícím způsobem) jako *P2P lending* či P2P půjčky a jsou často uváděny jako samostatná FinTech kategorie. Domnívám se však, že crowdfunding je pro *P2P lending* služby nadřazeným pojmem. Ze všech typů crowdfundingu prochází tímto typem nejvíce finančních prostředků.[24]

Zvláštní kategorií, kterou lze částečně řadit pod *crowdfunding*, je InsurTech. Jedná se obecně o technologie, pomocí kterých dochází k transformaci pojišťovacího sektoru, ke snižování nákladů nebo zavádění nových metod pro posuzování rizika.[25] Jednou z jeho podob je i P2P

[22] V případě ČR se jedná o zákon č. 117/2001 Sb., o veřejných sbírkách a o změně některých zákonů (zákon o veřejných sbírkách), ve znění pozdějších předpisů.
[23] V rámci investičního i dluhového crowdfundingu se ti, kdo poskytují financování úvěrů nebo projektů, označují nejčastěji jako investoři.
[24] LYNN, Theo, John G. MOONEY, Pierangelo ROSATI a Mark CUMMINS, ed. *Disrupting Finance*. Springer International Publishing, 2019, 175 s. ISBN 978-3-030-02329-4. Str. 3-5.
[25] MARANO, Pierpaolo a Kyriaki NOUSSIA, ed. *InsurTech: A Legal and Regulatory View*. Springer International Publishing, 2020, 401 s. ISBN 978-3-030-27385-9. Str. 84.

InsurTech. Jedná se o skupinové vytváření pojistných fondů, ze kterých se při vzniku pojistné události vyplácí členům pojištění. Platforma poskytuje pouze propojení účastníků, kteří se pojišťují za podmínek a pro případ událostí, které si sami definují. Principiálně se taková služba neliší od klasického pojištění. Rozdílem je jednak snaha o eliminaci prostředníka a dále vrácení částek pojistného, které se nevyplatilo v rámci pojistných událostí.[26]

1.1.3. Kryptoaktiva

Kryptoaktiva[27] jsou podle ESMA „*typem majetku, který závisí hlavně na kryptografii a DLT nebo podobné technologii jako součásti jejich vnímané nebo inherentní hodnoty*“[28] (překlad autor). Je možné dělit je na investiční kryptoaktiva (ICO), platební kryptoaktiva (kryptoměny), užitné tokeny[29], případně hybridní kryptoaktiva (kombinace uvedeného).

DLT (distributed ledger technology) lze přeložit jako technologie distribuovaných záznamů nebo distribuovaných účetních knih. Tato technologie je založena na decentralizaci a sdílení informací mezi všemi jejími uživateli a je základem pro většinu kryptoaktiv. Nové informace, které vkládá některý z uživatelů, jsou do sítě uloženy až po odsouhlasení většinou jejích uživatelů. Nejznámější DLT je blockchain, který je ale pouze podmnožinou tohoto pojmu.

ICO (initial coin offering) je alternativní způsob získávání kapitálu, při kterém společnosti poskytují investorům za jejich peníze nebo kryptoměnu vlastní kryptoaktiva, nejčastěji tokeny. ICO by bylo možné zařadit i do investičního crowdfundingu, rozdíl je však v tom, že vydaná kryptoaktiva nepředstavují podíl v projektu, byť jsou na jeho úspěšnosti závislá.

---

[26] MARANO, Pierpaolo a Kyriaki NOUSSIA, ed. *InsurTech: A Legal and Regulatory View*. Springer International Publishing, 2020, 401 s. ISBN 978-3-030-27385-9. Str. 28-36.

[27] Lze se setkat s pojmy *crypto-assets*, neboli kryptoaktiva, a také *virtual assets*, neboli virtuální aktiva. Přestože pojem virtuální aktiva by byl nejspíše přesnější, neboť ne všechna virtuální aktiva jsou založena na kryptografii, EBA, ESMA i studie Evropského parlamentu pracují s pojmem kryptoaktiva. Například ve studii Evropského parlamentu je výslovně zmíněno, že pojem krypoaktiva, který studie využívá, v zásadě odpovídá pojmu virtuální aktiva, který používá FATF. Pro tuto práci jsem zvolil jsem pojem kryptoaktiva, neboť jsem usoudil, že je používanější. EVROPSKÝ PARLAMENT. *Crypto-assets: Key developments, regulatory concerns and responses* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf. Str. 46.

[28] ESMA. *Advice: Initial Coin Offerings and Crypto-Assets* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection. Str. 42.

[29] Samotný pojem „*token*“ v tomto kontextu označuje obecně reprezentaci nějakých nároků nebo kvalit, které jsou s tímto kryptoaktivem spojeny. Tokeny zpravidla využívají cizí DLT.

Kryptoměny jsou decentralizovaná virtuální aktiva založená na šifrování a DLT technologii.[30] Regulátoři většiny států je nepovažují za měnu. Většinou se vyznačují vyšší mírou volatility a jsou používána buď jako nástroj investiční spekulace, uchovatel hodnoty nebo jako platební prostředek. Nejznámější a nejpoužívanější kryptoměnou je Bitcoin. Vyznačují se též určitou mírou anonymity. Přestože jsou jednotlivé transakce u některých druhů kryptoměn veřejné, přistupovat k peněženkám a odesílat z nich peníze může pouze osoba, která disponuje příslušnými přístupovými klíči. Kryptoměny jsou využívány i v rámci trestné činnosti, a to jak při jejím financování (crime-as-a-service), tak i ve vztahu k poškozeným (například požadavek ransomware na zaplacení výkupného). Zvláštní formou kryptoměn jsou *stablecoins*. Jejich hlavním znakem je snaha o minimalizaci volatility. Za tímto účelem jsou různými způsoby navázány na standardní zákonné měny nebo na hodnotu určitých aktiv, která jejich vydavatel nebo třetí osoba drží.[31]

Užitné tokeny jsou kryptoaktiva, která v budoucnosti přinesou svému vlastníkovi nějakou formu užitku, například službu či produkt, který vytvoří společnost, která tokeny vydala jako ICO.

1.1.4. Robo-Advisory

Robo-Advisory, neboli robotické poradenství, je označení služeb, které v rámci vytváření investičních portfolií nebo investičního rozhodování využívají umělou inteligenci. Na základě klientem zvolených kritérií dojde automaticky k navržení vhodných investičních produktů a později k jejich udržování. Díky nižším nákladům na provoz jsou tyto služby obvykle dostupnější i pro menší investory.[32]

1.1.5. RegTech

RegTech, neboli regulatorní technologie, jsou nástroje a služby, které umožňují FinTech společnostem nebo i klasickým poskytovatelům lépe a efektivněji vyhovět regulatorním požadavkům.[33] AML je jednou z oblastí, kde lze očekávat výrazný rozvoj RegTech, neboť

---

[30] GIRASA, Rosario. *Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives*. Palgrave Macmillan, 2018, 274 s. ISBN 978-3-319-78508-0. Str. 11.
[31] TĚTEK, Josef. Stable coins (VŠE, CO CHCETE VĚDĚT) – Svatý grál kryptoměn?. *Alza*, 2018 [online]. [cit. 2020-06-06]. Dostupné z: https://www.alza.cz/stable-coins.
[32] ARJUNWADKAR, Parag. *FinTech: The Technology Driving Disruption in the Financial Services Industry*. CRC Press, 2018, 261 s. ISBN 978-1-138-29479-0. Str. 83.
[33] EVROPSKÝ PARLAMENT – THINK TANK. *Financial technology (FinTech): Prospects and challenges for the EU* [online], 2017 [cit. 2020-06-06]. Dostupné z: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)599348. Str. 3.

FinTech společnosti se za účelem dosažení souladu s legislativou pravděpodobně budou více snažit využívat externí specializované společnosti. Zřejmě bude též zvyšován tlak na aktivnější zapojení států coby poskytovatelů efektivní digitální infrastruktury. V úvahu může přicházet snaha o částečné zpřístupnění některých státních registrů nebo vytváření speciálních aplikací pro vykazování nebo dohled.

1.2. Vliv na ekonomiku

FinTech je pro ekonomiku přínosem z několika důvodů. Nové služby jsou vyzyvatelem tradičních institucí a vytvářejí jim konkurenci. Zároveň nejsou zatíženy infrastrukturou minulosti a často působí pouze v online prostředí. To jim umožňuje vstoupit do odvětví s nižšími náklady. Jak uvádí například důvodová zpráva návrhu nařízení o evropských poskytovatelích služeb skupinového financování pro podniky, crowdfundingové platformy mohou sloužit jako vhodný zdroj alternativního financování malých a středních podniků.[34] Z pohledu uživatelů také může jít o další investiční příležitosti, které jsou mnohdy výnosnější (a také rizikovější) než u tradičních institucí a jsou přístupné i s minimálním kapitálem. V rámci ekonomiky tak mohou přispět k živější cirkulaci finančních prostředků v rámci kapitálového trhu. Svou jednoduchostí a snadnou dostupností cílí i na uživatele, kteří by se těmito příležitostmi jinak nezabývali. Uživatelům pak dále mohou zjednodušit správu financí a vytvářet přehledy o výdajích nebo poskytovat automatizované poradenství. V případě dárcovského crowdfundingu jde pak o možnost, jak bez zprostředkujících organizací podpořit konkrétní projekty. Vidina bezprostřední pomoci může být pro dárce totiž větší motivací. V případě odměnového crowdfundingu může být veřejná kampaň testem popularity, který dá autorům projektů zpětnou vazbu ohledně ekonomických rizik jejich snažení již na počátku příprav.

Mezi spotřebitelská rizika FinTech lze řadit slabé institucionální zajištění služeb, tendence k přenosu rizika na spotřebitele bez dostatečných informací, riziko střetu zájmů poskytovatelů služeb nebo chybující algoritmy. V případě kryptoaktiv pak jde o vysokou volatilitu a omezenou likviditu. K obecným rizikům je nutno zařadit hrozbu kyberútoků, existenci

[34] EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady (EU) 2018/0048 ze dne 8. 3. 2018 o evropských poskytovatelích služeb skupinového financování pro podniky* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0113&from=CS. Bod 1.

podvodných služeb (například na principu Ponziho schématu) nebo možný úpadek začínajících společností. Z těchto důvodů je vhodné při vytváření speciálních pravidel dbát na to, aby byli spotřebitelé dostatečně seznámeni se všemi souvisejícími riziky. V některých případech, především v rámci investičního a úvěrového crowdfundingu a kryptoaktiv, totiž mohou přijít o svůj vložený majetek nebo jeho část.[35]

Rozvoj FinTech platforem v České republice by mohl mít vliv na investiční chování českých domácností. Podle MF jsou v tomto ohledu v porovnání s ostatními evropskými státy velmi opatrné a konzervativní, což lze vyčíst ze skutečnosti, že přibližně polovinu všech svých aktiv domácnosti drží v hotovosti, na bankovních účtech a vkladech.[36] Jak již bylo naznačeno, efektivní distribuce kapitálu a s tím související zvýšená likvidita a velikost trhu vytváří příznivé investiční prostředí, které má větší potenciál pro nalákání zahraničních investorů.

1.3. Regulační přístupy

Jednotlivé země přistupují k finančním inovacím různě. Ty, které se snaží FinTech aktivně podporovat, vytvářejí tzv. regulatory sandboxy[37], prostředí umožňující testovat nové služby v reálném prostředí a na skutečných klientech za soustavného dozoru regulátora, nebo alespoň tzv. innovation huby, kontaktní místa, kde inovátoři komunikují s regulátorem, který jim poskytuje svoje názory či doporučení. Nerovný přístup regulátora též může narušovat hospodářskou soutěž[38] a jeho dozor může v očích veřejnosti vytvářet falešný pocit bezpečí. Otázkou je rovněž, zda mají regulatory sandboxy reálné výsledky, které by se projevily vznikem úspěšných inovativních projektů. V následujícím textu porovnám přístupy ČR, Velké Británie jakožto vedoucí evropské země a Singapuru coby významného asijského finančního centra.[39]

---

[35] K dalším rizikům např. MINISTERSTVO FINANCÍ. *Inovace na finančním trhu a ochrana spotřebitele: Veřejná konzultace* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/o-ministerstvu/verejne-diskuze/2020/verejna-konzultace-inovace-na-financnim-37490. Str. 15-18.

[36] MINISTERSTVO FINANCÍ. *Koncepce rozvoje kapitálového trhu v České republice 2019-2023* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/aktualne/tiskove-zpravy/2019/ministerstvo-financi-predstavilo-koncepc-34656. Str. 12.

[37] Někdy se též používá doslovný překlad „*regulatorní pískoviště*".

[38] NONNEMANN, František, Regulatory sandbox: možnosti a meze nástroje pro chytrou regulaci [online]. *EPRAVO.CZ*, 2019 [cit. 2020-06-06]. Dostupné z: https://www.epravo.cz/top/clanky/regulatory-sandbox-moznosti-a-meze-nastroje-pro-chytrou-regulaci-109048.html.

[39] Podle Deloitte měla v letech 2016 a 2018 samotná Asie nadpoloviční podíl na celkových investicích do FinTech společností. DELOITTE. *FinTech v ČR i ve světě: Vliv nových technologií na finanční sektor* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/financial-services/articles/fintech-v-cr-i-ve-svete.html. Str. 24.

1.3.1. Česká republika

Česká republika patří v tomto ohledu mezi konzervativnější země. ČNB se hlásí k principu technologické neutrality, tedy že nezáleží na tom, kdo používá jaké technologie, ale co je předmětem jeho činnosti. Dále se drží zásady rovného zacházení, která by byla uvolněním pravidel pro některé vyvolené subjekty narušena.[40] Současně je třeba vzít v úvahu, že FinTech společnosti a tradiční instituce jsou často vzájemnými konkurenty. Dědek uvádí, že otázka regulace FinTech je spíše ekonomický problém a záleží na tom, kdy relevantní trh vyroste tak, že bude zvláštní pravidla vyžadovat. Případnou regulaci vidí jako žádoucí spíše na úrovni EU, neboť FinTech je z podstaty věci přeshraniční záležitost.[41] Mora uvádí, že úkolem regulace není vytváření inovací, ale centrální banka musí být zároveň inovacím otevřená.[42] ČNB na konci roku 2019 vytvořila kontaktní místo pro finanční inovace,[43] jedná se ovšem pouze o jakési vyjádření ochoty zodpovídat kvalifikované dotazy účastníků finančního trhu související s finančními technologiemi. Odpovídání na kvalifikované dotazy není u ČNB žádné novum a nabízí se tedy otázka, zda se nejedná o alibismus. Podle MF by měly být bariéry pro vstup nových hráčů do odvětví co nejnižší, nicméně pravidla by měla být pro všechny stejná. V případě příliš zatěžující regulace pro FinTech by bylo vhodné uvolnit pravidla pro všechny.[44]

Podle studie Deloitte a britského ministerstva mezinárodního obchodu z roku 2016 měl český FinTech hodnotu 190 mil. EUR a překonal tak Slovinsko nebo Rumunsko, zatímco Polsko v regionu střední a východní Evropy vedlo s 856 mil. EUR a bylo následováno Rakouskem

[40] Stejný názor zastává například i německý BaFin. RINGE, Wolf-Georg a Christopher RUOF. Regulating Fintech in the EU: the Case for a Guided Sandbox. *European Journal of Risk Regulation* [online]. 1-26 [cit. 2020-06-06]. DOI: 10.1017/err.2020.8. ISSN 1867-299X. Dostupné z: https://www.cambridge.org/core/product/identifier/S1867299X20000082/type/journal_article. Str. 15.

[41] DĚDEK, Oldřich. Balancing Fintech Opportunities and Risks: Implementing the Bali Fintech Agenda. *Česká národní banka* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/en/public/media_service/conferences/speeches/dedek_20190129_fintech.html.

[42] MORA, Marek. FinTech pohledem centrální banky [online]. Česká národní banka, 2018 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/verejnost/.galleries/pro_media/konference_projevy/vystoupeni_projevy/download/mora_20181011_bankovni_forum.pdf.

[43] Finanční inovace. *Česká národní banka* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/financni-inovace/.

[44] MINISTERSTVO FINANCÍ. *Inovace na finančním trhu a ochrana spotřebitele: Veřejná konzultace* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/o-ministerstvu/verejne-diskuze/2020/verejna-konzultace-inovace-na-financnim-37490. Str. 28.

s 588 mil. EUR.[45] Česká fintech asociace (ČEFTAS) má 39 členů[46] a jak upozorňuje Dědek, někteří z nich možná ani užívané definice FinTech nenaplňují.[47] Lze tedy konstatovat, že FinTech scéna v ČR není výjimečná, má podobnou velikost jako v ostatních srovnatelných státech a v porovnání s tradičními sektory má stále zlomkovou velikost.

V oblasti crowdfundingu nemá ČR zvláštní pravidla. Existuje stanovisko[48] z roku 2015, ve kterém ČNB odkazuje na stanoviska ESMA (investiční crowdfunding) a EBA (úvěrový crowdfunding) a stanovisko[49] ČNB z roku 2010, kde se vyjadřuje obecně ke zprostředkování úvěrů. Zmínit lze snad ještě standardy pro provozování P2P úvěrových a investičních platforem vydaných ČEFTAS.[50] Jedná se ale o velmi obecné principy, z nichž některé odpovídají tomu, co vyžadují speciální zákony o crowdfundingu přijaté v některých zemích, například minimum poskytovaných informací investorům, oddělení vlastních prostředků a prostředků svých klientů nebo zákaz diskriminace investorů. Kryptoměny ČNB označuje jako převodní tokeny a nepovažuje je za peníze v ekonomickém ani právním smyslu.[51]

1.3.2. Velká Británie

Velká Británie je v rámci Evropy z pohledu finančních inovací nejvýznamnější zemí. To se týká jak množství celkových investic, tak i počtu vznikajících FinTech společností. Bank of England (BoE) v roce 2016 spustila FinTech Accelerator. Jednalo se o projekt, jehož smyslem bylo, aby se centrální banka seznámila se současnými finančními technologiemi a aby zároveň dala společnostem, které je reprezentují, možnost nahlédnout do problematiky

---

[45] DELOITTE & DEPARTMENT FOR INTERNATIONAL TRADE. *Fintech in CEE: Charting the course for innovation in financial services technology* [online], 2016 [cit. 2020-06-06]. Dostupné z: https://www2.deloitte.com/ce/en/pages/about-deloitte/articles/fintech-cee-region.html. Str. 6.

[46] Částečně se jedná i o zahraniční společnosti nebo tradiční instituce. Členové. *Česká fintech asociace* [online], 2020 [cit. 2020-06-06]. Dostupné z: http://czechfintech.cz/clenove/#clenove.

[47] DĚDEK, Oldřich. Balancing Fintech Opportunities and Risks: Implementing the Bali Fintech Agenda. *Česká národní banka* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/en/public/media_service/conferences/speeches/dedek_20190129_fintech.html.

[48] ČESKÁ NÁRODNÍ BANKA. *Stanovisko a odpovědi ČNB na vybrané otázky z konzultačního materiálu Evropské komise „Green Paper – Building a Capital Markets Union"* [online], 2015 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/legislativni_zakladna/stanoviska_cnb/download/capital_market_union_stanovisko_cnb.pdf.

[49] ČESKÁ NÁRODNÍ BANKA. *Stanovisko k zprostředkování půjček, resp. úvěrů* [online], 2010 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/zprostredkovani_pujcek.pdf.

[50] ČESKÁ FINTECH ASOCIACE. Standard pro provozování peer-to-peer úvěrových a investičních platforem [online], 2018 [cit. 2020-06-06]. Dostupné z: http://czechfintech.cz/wp-content/uploads/2018/05/Standardy_P2P_platforem.pdf.

[51] ČESKÁ NÁRODNÍ BANKA. *Stanovisko k obchodování s tzv. převodními tokeny* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/k_obchodovani_s_prevodnimi_tokeny.pdf.

související s regulatorními úkoly centrální banky. Jedna ze společností, které se účastnily projektu, se stala stálým partnerem BoE. Centrální banka rovněž spolupracovala se společností Ripple[52] na možném vylepšení platebních systémů. V roce 2018 vznikl v rámci banky na základě dobrých zkušeností s FinTech Accelerator stálý FinTech Hub. Podle BoE fungují soukromé inovace nejlépe, když jsou podpořeny veřejnou infrastrukturou.[53,54]

BoE ve spolupráci s Financial Conduct Authority (FCA) v roce 2016 ustanovila New Bank Start-up Unit, tým určený k ulehčení autorizačního procesu a zároveň pro podrobný dohled během prvního roku působení nových bank.[55] V roce 2018 byl ustanoven obdobný tým pro pojišťovny. BoE se společně s FCA taktéž zabývá možnostmi automatizovaného regulatorního vykazování. Pokud by se zavedly standardy pro data, která regulované subjekty vykazují, a zároveň by byla tato data strojově čitelná, mohlo by to společnostem ušetřit náklady oblasti kontrolních procesů a dosahování *compliance*. Regulátoři by současně mohli automatizovat dohledovou činnost.[56]

FCA jako první na světě v roce 2016 vytvořila regulatory sandbox. Do něj se mohou přihlásit autorizované i neautorizované společnosti, které chtějí přinést nové inovace na finanční trh. V rámci regulatory sandboxu se od společností očekává, že budou pod blízkým dohledem FCA po určitou stanovenou dobu a v malém rozsahu poskytovat svou službu reálným klientům. Zároveň se očekává reálný přínos projektu, například snížení cen pro spotřebitele. Za tímto účelem může dojít ze strany FCA ke zmírnění obvyklých pravidel. Podle FCA účast v regulatory sandboxu výrazně urychluje proces získávání autorizace. Zároveň se významně

[52] Ripple je decentralizovaná platební síť a zároveň i název pro kryptoměnu, kterou tato společnost vytvořila.
[53] BANK OF ENGLAND. *Quarterly Bulletin: Embracing the promise of fintech* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2019/embracing-the-promise-of-fintech.pdf?la=en&hash=2445D5B3AF10096FDAA91564BB48F8E5F28486B9.
[54] Initiative of the year: Bank of England's FinTech Accelerator. *CENTRAL BANKING* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.centralbanking.com/awards/3333176/initiative-of-the-year-bank-of-englands-fintech-accelerator.
[55] New Bank Start-up Unit launched by the financial regulators. *Financial Conduct Authority* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/news/press-releases/new-bank-start-unit-launched-financial-regulators.
[56] FCA and Bank of England announce proposals for data reforms across the UK financial sector. *Financial Conduct Authority* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/news/press-releases/fca-and-boe-announce-proposals-data-reforms-across-uk-financial-sector.

snižuje čas mezi realizací inovace a jejím uvedením na trh.[57] Objevuje se ale i kritika, že projekty, které režim regulatory sandboxu opustí, často nejsou schopny fungovat mimo něj.[58]

Velká Británie je místem zrodu první P2P úvěrové platformy Zopa, která zahájila činnost v roce 2005 jako první na světě. Provozování těchto platforem bylo zákonem definováno jako „*provozování elektronického systému ve vztahu k půjčování*“[59] (překlad autor). Nad P2P platformami dohlíží FCA, která na toto téma vydala rozsáhlé konzultační studie, na jejichž základě došlo k vytvoření speciální právní úpravy. Mezi základní požadavky pro P2P platformy patří zajištění správy existujících úvěrů i při úpadku platformy, reportování FCA o finanční situaci, množství držených klientských prostředků nebo uskutečněných úvěrech a stížnostech. P2P platformy zároveň nespadají pod kompenzační schémata finančních služeb a investorské vklady tak nejsou chráněny. FCA zároveň upozorňuje, že dobrovolně zřizované investorské pojišťovací fondy mohou vytvářet falešný pocit bezpečí. Mezi další požadavky patří získání kompetentních zaměstnanců, oddělení účtů s penězi klientů, ochrana spotřebitele podle směrnice o spotřebitelských úvěrech, možnost zrušení investice do určité doby bez sankce v případě neexistence sekundárního tržiště nebo pravidla pro marketing a limity pro maximální investované částky u neprofesionálních investorů.[60] Velká Británie nemá speciální právní režim pro kryptoaktiva, FCA je považuje za „*směnné tokeny*“.[61]

1.3.3. Singapur

V roce 2016 došlo v Singapuru k založení samostatné instituce, FinTech Office, která má za cíl koordinovat prostředí pro finanční technologie, pomáhat se vznikem nových společností a propagovat Singapur po světě jako FinTech hub. Nejvýznamnější roli má v této oblasti dohledový orgán Monetary Authority of Singapore (MAS). Ten usiluje o to, aby se ze Singapuru stalo „*chytré finanční centrum*“, což podle něj zajistí existence regulatorního prostředí, které umožňuje inovativní využití technologií. Finanční instituce a další společnosti se mohou přihlásit do regulatory sandboxu, kde lze po omezenou dobu a v jasně definovaném

---

[57] Regulatory sandbox. Financial Conduct Authority [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/firms/innovation/regulatory-sandbox.
[58] PERRY, Michelle. Taking the next step in sandbox evolution [online]. *Raconteur*, 2020 [cit. 2020-06-06]. Dostupné z: https://www.raconteur.net/finance/fca-sandbox-fintech.
[59] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544). Article 36H.
[60] FINANCIAL CONDUCT AUTHORITY. *Loan-based ('peer-to-peer') and investment-based crowdfunding platforms: Feedback to CP18/20 and final rules* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/publication/policy/ps19-14.pdf.
[61] Cryptoassets. *Financial Conduct Authority* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/consumers/cryptoassets.

rámci experimentovat s finančními inovacemi na reálných klientech. MAS přitom dohlíží na to, aby existovaly pojistky pro případné selhání a určuje, které regulatorní nároky budou v daném případě zmírněny, nebo se vůbec nebudou aplikovat. U uchazečů o vstup do regulatory sandboxu se rovněž očekává znalost existujících pravidel, náležitá opatrnost při hodnocení možných rizik a zejména pochopení, že představovaná služba musí přinášet něco, co v daném oboru ještě nebylo aplikováno, nebo přináší nové způsoby, jak lépe provést to, co už v nějaké podobě funguje. Cílem není v první řadě prospěch navrhovaného projektu, ale prospěch celému odvětví a potenciálním klientům. Tento režim má tři fáze. Fázi přihlašovací, po které MAS informuje uchazeče o tom, zda má jejich projekt potenciál, dále fázi evaluační, při které může uchazeč v kooperaci s MAS doplňovat nebo upravovat svou přihlášku a při kladném posouzení ze strany MAS pak konečně fázi experimentální, kdy je služba spuštěna. Subjekt, který proces v rámci regulatory sandboxu podstupuje, musí o této skutečnosti informovat svoje klienty. Při úspěšném ukončení režimu sandboxu již nastává povinnost dodržet všechny regulatorní požadavky. MAS taktéž může sandbox kdykoliv ukončit, pokud účastník nedodržuje nastavená pravidla, a dále pokud se MAS domnívá, že sandbox dosáhl svého účelu nebo pokud rizika pro klienty převáží očekávaný přínos služby.[62]

Úvěrový crowdfunding ve vztahu k podnikatelům podle MAS spadá pod zákon o cenných papírech a pokud nedojde k některé zákonné výjimce, je třeba zveřejnit prospekt. Singapur dále nepovažuje kryptoměny za měny ani nástroje kapitálového trhu.[63]

1.3.4. Může být regulatory sandbox přínosný?

Pro nové a menší společnosti je obvykle těžší dostát regulatorním požadavkům finančního sektoru. Někdy také není zcela zřejmé, do jakých stávajících právních kategorií nové finanční

[62] MONETARY AUTHORITY OF SINGAPORE. *Fintech Regulatory Sandbox Guidelines* [online], 2016 [cit. 2020-06-06]. Dostupné z: http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines%2019Feb2018.pdf. Str. 3-9.

[63] ANG, Adrian, Samuel KWEK a Anil SHERGILL. FinTech in Singapore. *Business Law International* [online]. 2019, **20**(1), 51-62 [cit. 2020-06-06]. ISSN 1467632X. Dostupné z: https://www.ibanet.org/Document/Default.aspx?DocumentUid=5026E3B4-ED5B-4FEE-89A5-693304C7E079. Str. 52-53.

služby spadají. V případě, že by se pohybovaly na pomezí stávajících pravidel, by mohlo kromě právní nejistoty na straně inovátorů a regulátorů dojít i k ohrožení spotřebitelů.[64]

Při zvažování, zda je vhodné regulatory sandbox v nějaké podobě zavést, je nutné porovnat potenciální přínosy a náklady. Náklady by představovala zejména nutnost intenzivní kooperace ze strany orgánu dohledu, která by ho zatěžovala. Přínosem by pak nebyly pouze potenciální finanční inovace, ale i zlepšení porozumění novým technologiím ze strany orgánu dohledu a pravděpodobné urychlení povolovacího řízení. Čas trvání i rozsah účasti spotřebitelů nebo dalších osob by měly být omezeny. Společnost, která se sandboxu účastní, by takovou informaci měla veřejně prezentovat. Stejně tak i informaci, které normy se na ni dočasně nevztahují. Domnívám se, že v případě velmi omezeného měřítka projektů by se nemělo jednat o narušení hospodářské soutěže. Existence regulatory sandboxu by mohla inovátory dostat ze šedé zóny a zároveň jim dát najevo, že jsou jejich nápady vítány. Při splnění výše uvedených podmínek by podle mého názoru mohlo zavedení regulatory sandboxu představovat přínos.

Střízlivý přístup ČR k finančním inovacím ale není možné jednoduše kritizovat. Česká FinTech scéna je malá a neuvážené legislativní změny mohou škodit jak trhu, tak právnímu řádu. ČR jako člen EU v legislativě přirozeně postupuje v souladu s ostatními evropskými státy. Problém může nastat v případě uplatňování pravidel, která jsou bez rozumných důvodů přísnější, než by musela být. To může zhoršovat pozici domácích FinTech společností, které mají často nadnárodní ambice, a může to vzniku finančních inovací naopak bránit. Je pozitivní, že MF oblast finančních inovací alespoň vnímá a pořádá k tématu veřejné konzultace.

[64] RINGE, Wolf-Georg a Christopher RUOF. Regulating Fintech in the EU: the Case for a Guided Sandbox. *European Journal of Risk Regulation* [online]. 1-26 [cit. 2020-06-06]. DOI: 10.1017/err.2020.8. ISSN 1867-299X. Dostupné z: https://www.cambridge.org/core/product/identifier/S1867299X20000082/type/journal_article. Str. 10.

2. Vybrané povinnosti z hlediska AML

Na úvod je nezbytné vymezit smysl a jednotlivé dimenze AML pravidel. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (AML zákon) podle svého § 1 upravuje některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu a v této souvislosti stanoví práva a povinnosti. Tyto povinnosti, kterými zákonodárce přenáší část odpovědnosti v této problematice na soukromé subjekty, mají zajistit dostatečnou míru prevence před zneužitím finančních systémů k legalizaci výnosů z trestné činnosti, zabránit financování terorismu a dále zabezpečit akceschopnost příslušných orgánů veřejné moci při výkonu jejich pravomocí. V § 3 pak AML zákon definuje legalizaci výnosů z trestné činnosti jako „*jednání sledující zakrytí nezákonného původu jakékoliv ekonomické výhody vyplývající z trestné činnosti s cílem vzbudit zdání, že jde o majetkový prospěch nabytý v souladu se zákonem*.“ Zákonodárce si je vědom, že takové jednání může mít mnoho podob, proto dále pouze demonstrativně uvádí některé z nich. Financování terorismu naopak AML zákon definuje taxativně a odkazuje na příslušné teroristické trestné činy nebo jim nápomocné trestné činy, které musí být financovány s vědomím, že tyto prostředky budou alespoň zčásti použity při jejich spáchání, nebo jako odměna pro pachatele teroristických trestných činů či jejich osoby blízké.

Legalizace výnosů z trestné činnosti a financování terorismu mají společné znaky, jimiž jsou mezinárodní přesah a organizovanost vysokého množství subjektů. Jedná se tedy o ukázkový příklad oblasti, která vyžaduje harmonizaci národních legislativ a dále účinnou a rychlou mezinárodní spolupráci příslušných orgánů. Lze se domnívat, že bez aktivní součinnosti osob, kterým tato AML pravidla stanoví povinnosti, čímž je v podstatě staví proti zájmům jejich klientů a tedy i proti vlastním ekonomickým zájmům, by byla snaha příslušných orgánů naprosto neefektivní. Boj proti legalizaci výnosů z trestné činnosti a financování terorismu jsou prvními dvěma dimenzemi AML pravidel, které obvykle mívají společnou právní úpravu, neboť při jejich potírání dochází k uplatňování podobných instrumentů (např. oznamovací povinnost).[65]

[65] VYBÍRAL, Roman. Právo proti praní špinavých peněz. In: KARFÍKOVÁ, Marie a kol. *Teorie finančního práva a finanční vědy*. Praha: Wolters Kluwer ČR, 2018, 356 s. ISBN 978-80-7552-935-0. Str. 291-297.

Poslední dimenzí AML pravidel jsou mezinárodní finanční sankce upravené zákonem o provádění mezinárodních sankcí.[66] Mezinárodní sankce jsou opatřeními přijatými na politické úrovni v rámci mezinárodních organizací. Tyto sankce omezují konkrétní státy, osoby, zboží a služby nebo sektory, na něž by měly vytvářet politický nátlak za účelem zachování míru, ochrany lidských práv nebo boje proti terorismu. Českou republiku konkrétně zavazují sankce OSN a EU.[67]

2.1. Kontrola klienta

Kontrola klienta a jeho identifikace jsou pro povinné osoby jedny z nejvíce zatěžujících požadavků AML zákona. Jedná se o soustavný proces, kterým povinné osoby získávají informace o osobě klienta, jeho vlastnické struktuře, povaze obchodních vztahů nebo původu jeho finančních prostředků. Smyslem procesu poznávání svého klienta (KYC) je včasná identifikace potenciálního rizika zneužití infrastruktury povinné osoby k praní peněz či financování terorismu. Zákonná ustanovení ponechávají povinným osobám určitou volnost v tom, jaká kritéria na posouzení rizikovosti klienta aplikovat. Klientům zákon zároveň ukládá povinnost spolupráce.[68]

Navrhovaná podoba AML zákona rozlišuje tři kategorie kontroly a identifikace klienta a též výjimky z této povinnosti. Ke stávajícím kategoriím „*kontrola klienta*“ a „*zjednodušená identifikace a kontrola klienta*“ návrh zákona na základě směrnic proti praní špinavých peněz v § 9a nově zavádí kategorii „*zesílená identifikace a kontrola klienta*“.[69]

2.1.1. Kontrola klienta

Povinné osoby podle § 9 navrhované podoby AML zákona obligatorně provádějí kontrolu klienta například nejpozději před uskutečněním obchodu o objemu alespoň 15 000 EUR, pokud

---

[66] Na jeho základě došlo k vydání nařízení vlády č. 210/2008 Sb., k provedení zvláštních opatření k boji proti terorismu, které zpracovává společný postoj Rady EU a obsahuje seznam 31 fyzických osob a 18 organizovaných skupin.

[67] HURYCHOVÁ, Klára a Michal SÝKORA. *Compliance programy (nejen) v České republice*. Praha: Wolters Kluwer, 2018. 304 s. ISBN 978-80-7552-667-0. Str. 228-229.

[68] TVRDÝ, Jiří. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. 2. vydání. Praha: C.H. Beck, 2018, 584 s. ISBN 978-80-7400-688-3. Str. 66.

[69] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

je zřejmé, že takové hodnoty dosáhne, před obchodem s PEP, s osobou z vysoce rizikové třetí země nebo při převodu peněžních prostředků v hodnotě alespoň 1000 EUR. Při kontrole klient a povinná osoba zkoumá povahu obchodu a podnikání klienta, totožnost skutečného majitele z příslušné evidence a jednoho dalšího zdroje, skutečnost zda se nejedná o PEP nebo osobu ze sankčního seznamu. Povinná osoba musí průběžně sledovat, zda obchodní vztah odpovídá tomu, co jí bylo o klientovi známo, a jaký je původ majetku, jehož se transakce týkají. V případě PEP pak povinná osoba musí zkoumat původ jejího majetku. Kontroly probíhají v rozsahu potřebném pro určení rizikovosti v závislosti na typu klienta, povaze podnikání nebo produktu a s ohledem na hodnocení rizik povinné osoby.[70]

2.1.2. Zjednodušená identifikace a kontrola klienta

Účinná podoba zjednodušené identifikace a kontroly klienta v § 13 AML zákona obsahuje výčet klientů, u nichž je nižší riziko zneužití a u kterých je proto možné provádět zjednodušenou identifikaci a kontrolu. Jedná se například o úvěrové a finanční instituce, ústřední orgány státní správy nebo orgány EU. Ustanovení dále umožňuje provést zjednodušenou identifikaci a kontrolu v závislosti na typu poskytovaného produktu a za tímto účelem uvádí výčet některých pojišťovacích a dalších finančních produktů, pokud pojistné, vklady a maximální hodnoty obchodů nepřesahují určité částky. Navrhovaná podoba zákona dává povinným osobám větší volnost. Nově by mohly samy na základě vlastního hodnocení rizik, národního hodnocení rizik a za předpokladu neuplatnění zesílené identifikace a kontroly určit, že některé kategorie klientů, obchodních vztahů nebo produktů představují nižší riziko. V takovém případě povinná osoba pouze zaznamená splnění těchto podmínek, identifikační údaje klienta a údaje k ověření skutečného vlastníka klienta. K tomu ale navrhovaná podoba zákona v § 13 odst. 2 písm. c) připojuje poměrně vágní ustanovení, podle kterého má povinná osoba navíc „*provádět další úkony v rámci identifikace a kontroly klienta v rozsahu potřebném k účinnému řízení rizik*.“ Přestože obecně by bylo možné pozitivně hodnotit větší svobodu povinných osob, nová podoba ustanovení celkově snižuje jejich právní jistotu a citovaná povinnost působí spíše jako nástroj pro regulátora, kterým může při trestání povinné osoby zpětně argumentovat.

[70] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

Taková povinnost může povinné osoby od aplikace zjednodušené identifikace preventivně odrazovat.[71]

2.1.3. Zesílená identifikace a kontrola klienta

Zesílenou identifikaci a kontrolu klienta provádí povinné osoby na základě vlastního hodnocení rizik a dále vždy ve třech taxativně vymezených případech – obchodní vztah s osobou z vysoce rizikové třetí země, obchod související s vysoce rizikovou třetí zemí a obchod s PEP. Za účelem řízení zjištěného nadstandardního rizika si může povinná osoba vybrat, jakým způsobem bude postupovat. Kromě získání dodatečných informací o povaze obchodního vztahu či původu peněžních prostředků a jejich ověřování z důvěryhodných zdrojů může povinná osoba například požadovat první platbu z účtu vedeného na jméno klienta u finanční instituce, u které jsou zajištěny rovnocenné požadavky na identifikaci jako v EU. Jako vhodné opatření návrh zákona uvádí též požadavek souhlasu k uzavření obchodního vztahu ze strany pověřeného zaměstnance (AML officer).[72]

2.1.4. Výjimky z povinnosti identifikace a kontroly klienta

AML zákon ve svém § 13a vymezuje situace, kdy povinné osoby nemusí provádět identifikaci a kontrolu klienta. Jedná se o elektronické peníze uchovávané na médiu, typicky tedy předplacené karty, a dále o platební služby poskytované v rámci mobilní sítě. To ovšem platí pouze při dodržení poměrně přísných limitů v podobě maximálních částek při dobíjení. Navrhovaná podoba AML zákona na základě implementace článku 12 páté směrnice proti praní špinavých peněz (AMLD5) tyto limity dále snižuje. Nově se bude § 13a týkat pouze předplacených nedobíjecích médií s uchovávanou částkou maximálně 150 EUR a předplacených dobíjecích médií s měsíčním limitem pro dobíjení maximálně 150 EUR. Pozdější vybrání peněz z média bude limitováno částkou 50 EUR. Příkazy z takových platebních prostředků ze třetích zemí budou zpracovávány pouze tehdy, budou-li tyto prostředky splňovat rovnocenná kritéria.

---

[71] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

[72] Tamtéž.

Je pozoruhodné, že v důvodové zprávě k novelizaci AML zákona se o této navrhované změně ve vztahu k dopadům na povinné osoby nehovoří.[73] Podle mého názoru je pravděpodobné, že na základě navrhované novelizace některé tyto služby ukončí činnost, jako se to již dělo v minulosti.[74] Spotřebitelé v předplacených kartách neuvidí tak velký přínos a povinným osobám vzrostou náklady na identifikaci a kontrolu klienta. Taková novelizace by dle mého byla odůvodnitelná pouze vysokým rizikem zneužití.

Výroční zpráva Finančního analytického úřadu (FAÚ) za rok 2019 ve vztahu k formám legalizace výnosů z trestné činnosti uvádí, že stejně jako v předchozích letech se bude v roce 2020 jednat mimo jiné i o „*zneužívání nákupu kryptoměn, elektronických platebních bran a elektronických peněženek*“.[75] Podle informací od státního zastupitelství skončilo v letech 2013-2015[76] v řízení před soudem 199 věcí týkajících se legalizačních trestných činů. U nich způsob legalizace výnosů proběhl ve 13 případech „*novými platebními metodami*.“ Z toho pomocí předplacených karet ani v jednom případě, pomocí mobilní platební služby ve dvou případech, pomocí e-peněz ve dvou případech, zneužitím virtuálních peněz v žádném případě a jiným zneužitím platebních metod v devíti případech. S přehledem nejčastějším způsobem legalizace bylo založení bankovního účtu fyzickou osobou, která provádí platby podle pokynů pachatele. Jednalo se o 111 případů.[77] Státní zastupitelství nepoužívá zákonné definice, vlastní definice těchto pojmů v dokumentu neposkytuje a ani neuvádí výčty konkrétních příkladů zneužití. Mohlo tak dojít ke zkreslení dat při jejich sběru od jednotlivých státních zastupitelství a kvůli absenci definic může dojít i ke zkreslení interpretace dokumentu jeho adresáty.

I přes možná zkreslení dat se na základě výše uvedeného domnívám, že tvrzená vysoká rizikovost předplacených platebních karet není minimálně v případě ČR založena na reálných zkušenostech. Důvodem přísnější regulace přitom dle mého názoru nemůže být jen pouhá

---

[73] Důvodová zpráva In: MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2. Str. 125-126.

[74] Např. COOL karta nebo biip karta. Předplacené platební karty – nabídka 2020. Navigátor úvěrů [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.navigatoruveru.cz/predplacene-platebni-karty/.

[75] FINANČNÍ ANALYTICKÝ ÚŘAD. *Výroční zpráva 2019* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-526990861/1588148007_cs_29042020_vyrocni_zprava_fau_2019.pdf. Str. 10.

[76] V této době byla navíc popularita předplacených karet vyšší než v současnosti.

[77] NEJVYŠŠÍ STÁTNÍ ZASTUPITELSTVÍ. *Národní hodnocení rizik: Podkladové informace k národnímu hodnocení rizik praní peněz a financování terorismu za státní zastupitelství* [online], 2016 [cit. 2020-06-06]. Dostupné z: http://www.financnianalytickyurad.cz/hodnoceni-rizik/narodni-hodnoceni-rizik.html. Str. 69.

potenciální rizikovost, ale i reálná zkušenost se zneužíváním těchto služeb k legalizačním trestným činům.

2.1.5. Dopad povinností na povinné osoby

Z výše uvedeného plyne, že samotné zjištění toho, jaký typ kontroly klienta je třeba v konkrétním případě aplikovat, je na základě různých limitů nebo podmínek u konkrétních transakcí možné poměrně snadno implementovat do vnitřních procesů povinné osoby.[78] V minulých letech byla problémem spíše samotná kontrola klienta, která se dala automatizovat pouze částečně. Jejím základem jsou obecně data z veřejných rejstříků a evidence skutečných majitelů. Překážku představovalo, že OR coby základní zdrojový rejstřík neměl API rozhraní (živnostenský rejstřík ho dosud nemá) a maximální denní počet dotazů z jedné IP adresy byl (a stále je) limitovaný na 5000 požadavků denně nebo 50 požadavků za minutu. V tomto případě tak bylo možné využít pouze omezený *screen scraping*[79] nebo manuální vyhledávání. Z dat OR vychází Administrativní registr ekonomických subjektů (ARES), který provozuje MF. Jeho součástí jsou i data z Registru ekonomických subjektů od Českého statistického úřadu. ARES informace přes API poskytuje a dostal se též na seznam nařízení vlády o seznamu informací zveřejňovaných jako otevřená data.[80] Kompletní sada dat, která je k dispozici volně ke stažení, se aktualizuje jednou měsíčně. Při přístupu přes API ale činí potíže nedostatečná rychlost registru. Zároveň ARES neobsahuje některá data, kterými OR disponuje, například data narození fyzických osob nebo historická data evidovaných subjektů. Z tohoto důvodu nelze snadno vzájemně propojovat data, která jsou přitom pro povinné osoby při kontrole a identifikaci klientů klíčová, jako například informaci, které všechny společnosti konkrétní fyzická osoba vlastní.[81]

Vládní program digitalizace České republiky 2018+ uvádí mimo jiné i že „*cílem je mít všechna klíčová veřejná data publikována způsobem umožňujícím jejich jednoduché strojové*

[78] Samozřejmě pouze pokud vycházíme z předpokladu, že povinné osoby ví, kdo je PEP, kdo je skutečný majitel, co je vysoce riziková třetí země apod., k těmto dílčím otázkám se vyjadřuji dále v této práci.
[79] *Screen scraping* je proces, při kterém dochází k automatickému čtení dat z obrazu původně vzniklého za účelem jejich zobrazení. Poté dojde ke konverzi těchto dat do podoby, která je vhodná pro jejich následné využití.
[80] Nařízení vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data, ve znění pozdějších předpisů.
[81] KOKEŠ, Ondřej. ARES jako otevřená data? Ministerstvo financí šlo cestou nejmenšího odporu. *Lupa* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/ares-jako-otevrena-data-ministerstvo-financi-slo-cestou-nejmensiho-odporu/.

zpracování.“[82] V roce 2019 došlo ze strany MSP ke zpřístupnění dat z OR ve formě pravidelně aktualizovaných otevřených dat.[83] Podle mého názoru se jedná o jeden z velkých kroků ke zjednodušení procesů v rámci kontroly klienta.

2.2. Politicky exponované osoby

Politicky exponované osoby (PEPs) jsou fyzické osoby, které zastávají nebo v minulosti zastávaly významné veřejné funkce. V souvislosti s uplatňováním svěřené moci nebo nakládáním s veřejnými prostředky je u nich nutno preventivně počítat s vyšší mírou rizika z hlediska praní špinavých peněz a financování terorismu. Za PEPs jsou považovány i jejich osoby blízké, jejich společníci a skuteční vlastníci právnických osob vytvořených v jejich prospěch. AML zákon ve svém § 4 odst. 5 uvádí demonstrativní výčet PEPs. Jednotlivé funkce se snaží definovat obecně, aby je bylo možné aplikovat na různé politické systémy. Mimo nejvyšší představitele výkonné moci, zákonodárce, soudce nejvyšších soudů jsou PEPs i vedoucí představitelé samosprávy, vysocí diplomaté nebo členové statutárních orgánů obchodních korporací ovládaných státem.

Určení, zda je klient PEP, je pro povinnou osobu klíčové z hlediska míry uplatňované kontroly. Podle § 9a odst. 2 písm. c) navrhované podoby AML zákona se na obchod s PEP uplatní zesílená identifikace a kontrola klienta vždy.[84] Pro zjištění, zda je klient PEP, může povinná osoba provést vlastní šetření, využít služeb komerčních databází nebo vyžádat od klienta prohlášení.

2.2.1. Vlastní šetření

Jedním ze způsobů, jak zjistit, zda je klient PEP, je vlastní činnost povinné osoby spočívající v rešerši z veřejných zdrojů. Povinná osoba může informacemi disponovat též na základě vlastní nesouvisející činnosti či předchozí zkušenosti. Tyto informace za podmínek § 39 odst. 2 AML zákona nepodléhají mlčenlivosti a lze je za účelem předcházení legalizace výnosů

---

[82] ÚŘAD VLÁDY. *Digitální Česko: Vládní program digitalizace České republiky 2018+* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://i.iinfo.cz/files/lupa/328/digitalni-cesko-informacni-koncepce-ceske-republiky-1.pdf. Str. 5.

[83] Otevřená data Veřejného rejstříku a Sbírky listin [online]. *Ministerstvo spravedlnosti České republiky*, 2020 [cit. 2020-06-06]. Dostupné z: https://dataor.justice.cz/.

[84] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

trestné činnosti a financování terorismu sdílet zejména mezi evropskými úvěrovými a finančními institucemi.[85]

2.2.2. Komerční databáze

Dalším ze způsobů je získání přístupu do specializovaných komerčních databází. Mezi nejznámější databáze patří Refinitiv World-Check, Dow Jones Risk & Compliance nebo LexisNexis WorldCompliance. Tyto databáze jsou vytvářeny a průběžně aktualizovány analytiky po celém světě. Problém představuje nejen cena přístupu do nich, která se může pohybovat v řádech tisíců EUR měsíčně, zejména pokud povinná osoba vyžaduje napojení na vlastní databázový systém a automatizovaný *screening* v reálném čase, ale i neúplnost těchto databází zejména ve vztahu k menším zemím typu ČR. I přesto, že tyto databáze obsahují nejen PEPs, ale i seznamy mezinárodních sankcí, mediální obraz zájmových osob, jejich možné napojení na terorismus nebo pravděpodobný původ jejich majetku, povinná osoba stále musí brát v úvahu, že se jedná pouze o jeden z nástrojů k dosažení souladu s AML pravidly.[86]

2.2.3. Prohlášení klienta

Podle metodického stanoviska FAÚ je možné, aby povinná osoba pouze vyžádala od klienta na počátku obchodního vztahu prohlášení, kde uvede, zda je či není PEP, a smluvně ho zavázala k oznámení případné změny.[87] V zájmu klienta ale není být označen jako PEP, protože se potenciálně vystavuje výzvám k doložení účelu transakce nebo původu svého majetku. Klient si také v některých případech vůbec nemusí uvědomovat, že PEP je. Samozřejmostí je, že pokud by z průběžných kontrol klienta nebo jiné činnosti povinné osoby vyplynulo, že klient je PEP, povinná osoba by ho logicky takto musela označit. Přesto si nejsem jistý, zda není takto benevolentně formulované stanovisko zavádějící. Povinné osoby by z něj mohly získat dojem, že otázku, zda je klient PEP, vyřeší na počátku obchodního vztahu prostřednictvím prohlášení klienta jednou pro vždy. AML zákon přitom v § 9 odst. 2 písm. c) stanoví, že kontrola klienta zahrnuje i „*průběžné sledování obchodního vztahu včetně přezkoumávání obchodů prováděných v průběhu daného vztahu za účelem zjištění, zda obchody jsou v souladu s tím, co*

---

[85] TVRDÝ, Jiří. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. 2. vydání. Praha: C.H. Beck, 2018, 584 s. ISBN 978-80-7400-688-3. Str. 27.

[86] Informace poskytl Andre MARTIROSYAN ze společnosti S-RM Intelligence and Risk Consulting Limited prostřednictvím internetové komunikace ze dne 6. 6. 2020.

[87] FINANČNÍ ANALYTICKÝ ÚŘAD. *Metodický pokyn č. 7: Opatření vůči politicky exponovaným osobám* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-1750233108/1525684379_cs_pep-metodicky-pokyn2018final.pdf. Str. 2.

je povinné osobě známo o klientovi a jeho podnikatelském a rizikovém profilu.“ To v rozsahu potřebném k posouzení rizika v závislosti na typu klienta, obchodního vztahu, produktu nebo obchodu (§ 9 odst. 3 AML zákona). Domnívám se proto, že minimálně v případě naplnění jiných podmínek pro kontrolu klienta ve smyslu § 9 AML zákona, než je status PEP, tedy například u obchodů vyšší hodnoty, by měla povinná osoba přiměřeným způsobem sama aktivně zjišťovat, zda je její klient PEP, a nespoléhat se pouze na klientovo prohlášení. Není však pochyb o tom, že prohlášení klienta je nejjednodušším a nejlevnějším opatřením povinné osoby.

2.2.4. Návrh na vytvoření evropské databáze PEPs

Podle recitálu 23 AMLD5 „*by členské státy měly vydat seznamy konkrétních funkcí, které jsou podle vnitrostátních právních a správních předpisů považovány za významně veřejné funkce*.“ Jedná se zřejmě o opatření směřující k vyšší míře jistoty povinných osob při posuzování statusu PEP u svých domácích i zahraničních klientů. Domnívám se však, že za účelem zjednodušení procesů při zjišťování PEPs by mělo dojít k vytvoření neveřejného centrálního evropského přístupového místa, ze kterého by bylo možné ověřovat identitu klientů povinných osob vůči všem nově vytvořeným národním databázím vybraných PEPs.

Informace z databází by byly přístupné pouze příslušným národním orgánům za účelem jejich činnosti v oblasti předcházení legalizace výnosů z trestné činnosti a financování terorismu a dále všem povinným osobám za účelem plnění povinností plynoucích z AML pravidel. V databázích by nemělo být možné volně listovat nebo filtrovat data. Sloužily by pouze pro ověření konkrétních dotazů. Povinná osoba by zadala identifikační údaje konkrétního klienta a na základě jejího požadavku by přišla pozitivní nebo negativní odpověď. Možnému zneužití spočívajícímu v hromadném sběru dat z databází by zabránil omezený počet dotazů za určité časové období. Neveřejnost a nemožnost hromadného sběru dat by měly minimalizovat riziko zneužití osobních údajů, případně též riziko ohrožení národní bezpečnosti.

Vzhledem k demonstrativnímu výčtu PEPs v AML zákoně (a čtvrté směrnici proti praní špinavých peněz – AMLD4) by takové databáze mohly obsahovat jen fyzické osoby, jejichž zahrnutí je nepochybné a které jsou státu známy. Databáze by proto nikdy nemohly obsahovat kompletní výčet PEPs. Ve zbytku (§ 4 odst. 5 písm. b) AML zákona) by bylo nutné při zjišťování postupovat stávajícím způsobem, tedy prohlášením klienta, vlastní činností povinné osoby nebo s využitím komerčních databází. Databáze by samozřejmě obsahovaly

informace i o osobách, které v posledních 12 měsících měly status PEPs. Po uplynutí této doby by došlo k vymazání záznamu.

Jako vhodným správcem takové národní databáze se v případě ČR jeví ministerstvo vnitra (MV), neboť již v tuto chvíli se jedná o ústřední orgán státní správy například pro evidenci obyvatel, pro sdružování v politických stranách a hnutích, pro volby nebo pro oblast informačních systémů veřejné správy.[88] Pro vytvoření databáze by postačily stávající personální kapacity MV a pro vkládání a aktualizaci seznamu PEPs by mělo postačovat jedno služební místo. Domnívám se, že zřízení takových (byť neúplných) databází s centrálním přístupovým místem by povinným osobám ulehčilo plnění jejich povinností a zlepšilo efektivitu boje proti praní peněz a financování terorismu.

2.3. Evidence skutečných majitelů

Evidence skutečných majitelů je informačním systémem veřejné správy, do kterého rejstříkové soudy zapisují zákonem vyžadované informace o skutečných majitelích právnických osob nebo svěřenských fondů. V současnosti je evidence upravena zákonem o veřejných rejstřících právnických a fyzických osob, avšak po přijetí zákona o evidenci skutečných majitelů se její úprava včetně definice skutečného majitele, která je nyní součástí AML zákona, přesune do tohoto nového zákona.

Definice skutečného majitele se v navrhované právní úpravě nemění. Může jím být pouze fyzická osoba nebo více fyzických osob. Smyslem je zjistit identitu osoby, která má z činnosti právnických osob nebo svěřenských fondů konečný prospěch nebo na ně uplatňuje rozhodující vliv. Jedná se tedy o snahu zachytit skutečný stav a zaznamenat ho do evidence skutečných majitelů. Vychází se z předpokladu, že je povinností právnické osoby znát identitu svého skutečného majitele. V některých případech je ale nutné spokojit se pouze s určitou mírou pravděpodobnosti správnosti zapsaných údajů.[89] Podle návrhu podoby AML zákona je skutečným majitelem i fyzická osoba, za kterou se obchod provádí. Toto ustanovení podle důvodové zprávy míří na případy, kdy tato fyzická osoba sama není součástí vlastnické struktury a ani nemá rozhodující vliv na řízení právnické osoby, která obchod provádí, ale má

[88] § 12 zákona České národní rady č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky, ve znění pozdějších předpisů.
[89] Důvodová zpráva In: MINISTERSTVO SPRAVEDLNOSTI. *Návrh zákona o evidenci skutečných majitelů*. Úřad vlády, 2019. Č. j. 30/2018-LO-SP. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBCZJMEP9. Str. 37.

převážný prospěch z transakce nebo má na její provedení rozhodující vliv.[90] Jedná se tedy o snahu postihnout případy konkrétních transakcí, při kterých by k naplnění standardní definice skutečného majitele nedošlo. Domnívám se, že v případě absence delší klientské historie a tedy širšího kontextu transakcí by pro povinnou osobu bylo mimořádně obtížné existenci takové fyzické osoby zjistit.

Povinné osoby v rámci kontroly klienta provádí zjišťování skutečného majitele svého klienta a zaznamenávají identifikační údaje k ověření jeho totožnosti, jakož i postup vedoucí k jeho zjištění. Identifikační údaje by logicky měly být zaznamenány a uchovány v takovém rozsahu, aby podle nich bylo možné identifikovat konkrétní fyzickou osobu. Účelem této kontroly je zejména zjistit, zda skutečný majitel nepředstavuje PEP a aplikovat v takovém případě související mechanismy.

2.3.1. Automatizovaný sběr dat z evidence skutečných majitelů

Podle vyhlášky ministerstva spravedlnosti[91] (MSP) je přístup do evidence skutečných majitelů povinným osobám umožněn dálkově. Podle § 14c odst. 2 a 3 této vyhlášky ministerstvo oprávněné osobě konkrétní dálkový přístup umožní tak, že po zadání jejího požadavku přijde elektronickou poštou unikátní odkaz, díky kterému lze přistoupit do rozhraní systému, kde se po potvrzení požadavku zobrazí obsah zápisu. Oprávněná osoba se přitom identifikuje svým přiděleným jedinečným identifikátorem. Podrobnější informace o technickém provedení konkrétního přístupu vyhláška neobsahuje. MSP ale na dotaz odpovědělo, že vzhledem k ochraně osobních údajů nelze umožnit automatizované zpracování dat v evidenci a dále, že *screen scraping* dat je technickým provedením úmyslně ztížený, nikoliv však vyloučený. Současně probíhá monitorování neobvyklé aktivity a v případě příliš velkého množství požadavků může dojít k dočasnému omezení nebo zákazu přístupu.[92]

---

[90] Důvodová zpráva In: MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2. Str. 147-148.

[91] Vyhláška ministerstva spravedlnosti č. 323/2013 Sb., o náležitostech formulářů na podávání návrhů na zápis, změnu nebo výmaz údajů do veřejného rejstříku právnických a fyzických osob, evidence svěřenských fondů a evidence údajů o skutečných majitelích a o podrobnostech týkajících se způsobu dálkového přístupu k údajům v evidenci skutečných majitelů a některým údajům v evidenci svěřenských fondů a o zrušení některých vyhlášek.

[92] MINISTERSTVO SPRAVEDLNOSTI. *Odpověď na žádost o informace ze dne 10. 6. 2020*. Č. j. MSP-345/2020-OSV-OSV/4.

Podle návrhu zákona o evidenci skutečných majitelů by povinné osoby na základě § 16 odst. 2 písm. n) opět měly mít dálkový přístup ke všem údajům o skutečném majiteli s tím, že podle § 17 odst. 4 návrhu takový způsob přístupu opět stanoví MSP vyhláškou.[93] Návrh takové vyhlášky ovšem ještě není v době psaní této práce zveřejněn. Podle MSP nicméně dojde ke změně identifikace oprávněných osob, které budou jménem povinných osob požadovat informace o skutečných majitelích. Elektronické ověření jejich totožnosti bude probíhat podle nařízení eIDAS.[94]

MSP v důvodové zprávě k zákonu o evidenci skutečných majitelů uvádí, že do budoucna bude možné uvažovat o poskytování veřejně dostupných informací z evidence ve formě otevřených dat.[95] Na dotaz ale MSP tuto možnost s ohledem na osobní a citlivou povahu evidovaných údajů popřelo, neboť zcela volné nakládání s těmito daty by údajně nebylo proporcionální.[96] Domnívám se však, že tento argument je popřen již samotnou existencí OR, který obsahuje mimo jiné informace o datu narození a trvalém pobytu zapsaných fyzických osob. Nevidím přitom důvod, proč chránit osobní údaje skutečných majitelů více než osobní údaje společníků a statutárních orgánů zapsaných v OR. Tím spíše, pokud jsou tyto osobní údaje součástí otevřených dat, které samo MSP poskytuje. Budoucí možnost strojového zpracování veřejně poskytovaných údajů z evidence skutečných majitelů je z mého pohledu žádoucí a MSP by takové možnosti nemělo bránit nebo o ní „*uvažovat do budoucna*“. Taková funkce by měla být spuštěna současně s připravovaným otevřením veřejného rozhraní evidence. Pokud by v budoucnu ze strany MSP došlo ke zpřístupnění otevřených dat z veřejné části evidence skutečných majitelů, nedávalo by smysl bránit povinným osobám ve strojovém přístupu ke všem údajům z evidence. Potenciálnímu zneužití možnosti hromadného sběru dat by bylo možné snadno zabránit omezením maximálního počtu dotazů.

Nahlížení do evidence skutečných majitelů není jediný způsob, jak zjistit skutečného majitele právnické osoby. Takové povinnosti lze dostát i výpisem z OR. Jak správně uvádí FAÚ, z OR v současnosti lze zjistit společníky obchodních společností. U akciových společností je ale

---

[93] MINISTERSTVO SPRAVEDLNOSTI. *Návrh zákona o evidenci skutečných majitelů*. Úřad vlády, 2019. Č. j. 30/2018-LO-SP. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBCZJMEP9.
[94] MINISTERSTVO SPRAVEDLNOSTI. *Odpověď na žádost o informace ze dne 10. 6. 2020*. Č. j. MSP-345/2020-OSV-OSV/4.
[95] Důvodová zpráva In: MINISTERSTVO SPRAVEDLNOSTI. *Návrh zákona o evidenci skutečných majitelů*. Úřad vlády, 2019. Č. j. 30/2018-LO-SP. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBCZJMEP9. Str. 86.
[96] MINISTERSTVO SPRAVEDLNOSTI. *Odpověď na žádost o informace ze dne 10. 6. 2020*. Č. j. MSP-345/2020-OSV-OSV/4.

možné ve vygenerovaném elektronickém výpisu zjistit pouze jméno, sídlo či adresu místa pobytu akcionáře v případě akciových společností s jediným akcionářem. Pro zjištění údajů o akcionářích akciových společností, které mají alespoň dva akcionáře, je nezbytné zkoumat dokumenty ve sbírce listin OR.[97] Tyto dokumenty jsou ale často naskenované a nejsou strojově čitelné. Případná OCR analýza[98] s využitím umělé inteligence by nezajistila dostatečnou spolehlivost a byla by náročná na výpočetní výkon. Efektivnější by proto bylo zvážit novelizaci § 48 odst. 1 písm. k) zákona o veřejných rejstřících právnických a fyzických osob tak, aby ukládal akciovým společnostem povinnost zveřejňovat výše uvedené údaje o všech jejích akcionářích, jejichž celková jmenovitá hodnota jejich akcií k poměru k celkové jmenovité hodnotě všech akcií společnosti přesáhne určitou, například desetiprocentní hranici. Lze se domnívat, že i přes možné časté změny v osobách minoritních akcionářů by díky existenci takové hranice nedošlo ke způsobení nepřiměřené administrativní zátěže. Zatímco osobní obchodní společnosti a společnosti s ručením omezeným takovou povinnost mají, ekonomicky často silnější akciové společnosti ne. Bylo by též možné zohlednit kritérium určité výše čistého obratu za účetní období tak, aby opatření nepostihovalo ekonomicky slabší společnosti. Akciové společnosti by přitom neměly mít motivaci takovou hranici obcházet, neboť tyto údaje již nyní zveřejňují ve sbírce listin. Navrhované opatření by mohlo do určité míry zefektivnit proces zjišťování skutečných majitelů ze strany povinných osob. MSP o změnách v této oblasti nicméně neuvažuje. Podle ministerstva není veřejná seznatelnost akcionářů s ohledem na práva třetích osob nutná. Pozitivní zpráva je, že v případě dokumentů vkládaných do sbírky listin OR dojde s ohledem na požadavek vyplývající ze směrnice[99] minimálně v případě kapitálových společností k transpozici povinnosti vkládat pouze strojově čitelné listiny.[100]

---

[97] FINANČNÍ ANALYTICKÝ ÚŘAD. *Metodický pokyn č. 3: Zjišťování skutečného majitele povinnými osobami* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-1750233108/1495011685_cs_metodicky_pokyn_c_3_zjistovani_skutecneho_majitele.pdf. Str. 3-4.

[98] OCR, neboli *optical character recognition*, je metoda digitalizace tištěného textu a jeho převedení do strojově čitelné podoby.

[99] Směrnice Evropského parlamentu a Rady (EU) 2019/1151 ze dne 20. června 2019, kterou se mění směrnice (EU) 2017/1132, pokud jde o využívání digitálních nástrojů a postupů v právu obchodních společností. Článek 16 bod 6.

[100] MINISTERSTVO SPRAVEDLNOSTI. *Odpověď na žádost o informace ze dne 10. 6. 2020*. Č. j. MSP-345/2020-OSV-OSV/4.

2.3.2. BRIS

Business Registers Interconnection System (BRIS) je evropská centrální platforma vytvořená na základě článku 22 směrnice o některých aspektech práva obchodních společností.[101] Tato platforma by měla propojovat obchodní rejstříky členských států a prostřednictvím evropského elektronického přístupového místa by k nim měla zajistit veřejný přístup. MSP navrhuje v § 14 odst. 3 zákona o evidenci skutečných majitelů povinnost uveřejnění údajů prostřednictvím systému propojení evidencí, od čehož si slibuje právní zakotvení budoucího napojení veřejné části evidence skutečných majitelů na tento celoevropský systém.[102]

Takové ustanovení ovšem absentuje v § 16 návrhu, který upravuje přístup ke všem údajům o skutečném majiteli. Ten budou využívat povinné osoby při plnění povinností podle AML zákona. Z této skutečnosti usuzuji, že ministerstvo vůbec nepočítá s možností budoucího napojení kompletních údajů z evidence skutečných majitelů na BRIS nebo jinou obdobnou platformu na úrovni EU.

Podle článku 31a AMLD5 přijme Evropská komise postupy nezbytné pro propojení a zpřístupnění informací o skutečných majitelích v systému propojených registrů v závislosti na úrovni přístupu, kterou členské státy poskytnou. Z toho je zřejmé, že samotná centrální platforma sama uchovávat žádná data nebude a bude závislá na kvalitě a způsobu jejich poskytování ze strany členských států. Tímto způsobem tedy během několika let vznikne centrální evropský vyhledavač zpřístupňující v tu dobu již veřejně dostupné údaje o skutečných majitelích.

Je na místě zmínit, že již v současnosti existuje *Open Ownership Register*. Jedná se o iniciativu několika nevládních organizací, která umožňuje snadné a bezplatné vyhledávání ve veřejně přístupných evidencí skutečných majitelů či obdobných rejstřících Velké Británie, Dánska, Slovenska a Ukrajiny, tedy zemí, které (vyjma Ukrajiny) zavedly částečně veřejné evidence skutečných majitelů ještě předtím, než je k tomu donutila AMLD5.[103]

---

[101] Směrnice Evropského parlamentu a Rady (EU) 2017/1132 ze dne 14. června 2017 o některých aspektech práva obchodních společností.

[102] Důvodová zpráva In: MINISTERSTVO SPRAVEDLNOSTI. *Návrh zákona o evidenci skutečných majitelů*. Úřad vlády, 2019. Č. j. 30/2018-LO-SP. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBCZJMEP9. Str. 88.

[103] FAQ. *Open Ownership Register* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://register.openownership.org/faq.

Podle mého názoru by měla tato integrace evidencí postoupit na vyšší úroveň. Evropská komise by ve spolupráci s členskými zeměmi měla zajistit, aby bylo povinným osobám ze všech členských států umožněno skrze BRIS nebo jiný obdobný systém přistupovat ke všem údajům obsaženým v evidencích skutečných majitelů ve všech státech EU, a to způsobem umožňujícím strojové zpracování dat. Ochranu před zneužitím takového přístupu by bylo možné snadno zajistit omezením maximálního počtu přístupů skrze jedinečný identifikátor, který pro své oprávněné osoby povinné osoby získávají již dnes, například v ČR. Takovéto opatření by zefektivnilo postupy povinných osob při zjišťování skutečných majitelů.

2.4. Podezřelý obchod a systém vnitřních zásad

Odhalování podezřelých obchodu, jejich oznamování a vytváření systému vnitřních zásad patří mezi oblasti, ve kterých mají povinné osoby poměrně široké pole působnosti. Tato témata spolu bezprostředně souvisí, neboť odhalování podezřelých obchodů vychází z nastavení vlastního systému vnitřních zásad povinných osob a oznámení o podezřelém obchodu (OPO) je fakultativním výsledkem celého procesu.

2.4.1. Podezřelý obchod

Podezřelý obchod je definován v § 6 AML zákona, kde jsou demonstrativně uvedeny i některé jeho možné znaky. Obecně se jedná o jakýkoliv obchod, který má znaky vyvolávající podezření ze snahy o legalizaci výnosů z trestné činnosti nebo financování terorismu. Příkladem mohou být neobvykle vysoké výběry klienta, finanční operace neodpovídající povaze klientova podnikání nebo pochybnosti o identifikačních údajích. O podezřelý obchod se jedná vždy, pokud jsou proti klientovi, osobě v jeho vlastnické či řídící struktuře nebo jiné na obchodu podílející se osobě uplatňovány mezinárodní sankce. Povinná osoba má povinnost podezřelý obchod oznámit FAÚ. Podle účinného znění AML zákona tak musí učinit nejpozději do 5 dnů, podle navrhovaného znění bez zbytečného odkladu. V případě nebezpečí z prodlení pak podle účinného i navrhovaného znění neprodleně.

2.4.2. Systém vnitřních zásad

AML zákon většině povinných osob ukládá vypracovat a průběžně aktualizovat písemný systém vnitřních zásad, při jehož přípravě musí povinná osoba zohlednit rizika legalizace výnosů z trestné činnosti, která mohou nastat v rámci její činnosti. Zároveň musí brát ohled na národní i nadnárodní hodnocení rizik. Systém vnitřních zásad by měl být jakýmsi vodítkem

pro zaměstnance při plnění povinností vyplývajících z AML pravidel. Tento systém má obligatorní náležitosti jako například podrobný demonstrativní výčet znaků podezřelých obchodů, postupy při provádění kontroly klienta nebo postup v případě zjištění podezřelého obchodu. Povinná osoba má povinnost zřídit nezávislý orgán, který provádí kontrolu dodržování právních předpisů a kontrolu účinnosti přijatých postupů a strategií. Tato povinnost vznikne v případě, že je opodstatněná s ohledem na povahu činnosti povinné osoby a její rozsah. Jedná se zřejmě o povinnost, kterou může plnit oddělení interního auditu povinné osoby. Navrhovaná podoba AML zákona pak přináší i povinnost zřídit vnitřní oznamovací systém umožňující podat anonymní oznámení o porušení AML zákona.[104] Požadavky AML zákona na systém vnitřních zásad pak poměrně robustně doplňuje vyhláška ČNB.[105]

2.4.3. Dopad na FinTech společnosti

V případě FinTech společností přichází pro splnění povinností v úvahu pouze maximálně automatizovaný systém hodnocení rizik analyzující všechny dostupné relevantní informace o klientech a všech probíhajících transakcích, a to nejlépe v reálném čase. Kvalita těchto informací a jejich množství je tak základem pro správné určení míry rizika a včasnost případné reakce v konkrétních případech. Optimálně nastavený systém by měl generovat co nejméně *false positives*, tedy případů, které systém vyhodnotí jako rizikové, přestože objektivně rizikové nejsou.

Zatímco dosud byly komerční systémy pro odhalování podezřelých transakcí zaměřeny převážně na co nejlepší nastavení předdefinovaných pravidel a hranic pro automatické určení podezřelých transakcí, v budoucnu lze očekávat nástup metod strojového učení a pokročilé statistiky. Na základě mnoha faktorů budou automaticky vytvářeny profily obvyklého chování

[104] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

[105] Vyhláška České národní banky č. 67/2018 Sb., o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnost a financování terorismu.

pro konkrétního klienta. Vybočení z takového profilu pak pro systém bude znamenat vyšší riziko. Tyto metody již v současnosti umožňují snižovat množství *false positives*.[106]

Vygenerovaná upozornění musí manuálně přezkoumat pověřená osoba, která zároveň rozhodne o dalším postupu, pokud je nezbytný. Z pohledu mzdových nákladů povinné osoby je samozřejmě ideální minimalizovat manuální činnosti pověřených pracovníků. V současnosti si ale dle mého názoru nelze představit plně automatizované podávání oznámení o podezřelém obchodu. Nadměrný počet nerelevantních OPO by totiž mohl z pohledu regulátora signalizovat, že povinná osoba nemá správně nastavený systém vnitřních zásad. Počty podaných OPO v ČR ostatně nejsou nijak extrémní, podle FAÚ jich bylo podáno 3524 v roce 2017, 4028 v roce 2018 a 3954 v roce 2019.[107] I v případě větších finančních institucí se tak bude jednat pravděpodobně o maximálně desítky OPO ročně. Oznámení může povinná osoba podat vzdáleně a zabezpečeným způsobem prostřednictvím aplikace MoneyWeb od FAÚ.

Problematický aspekt může pro FinTech společnosti představovat absence delší klientské historie. Některé služby jsou využívány i jednorázově a ve větších finančních objemech, jako například měnové konverze skrze P2P FX platformy. V případě zahraničních klientů může problémy navíc představovat ztížená kontrola klienta. Podle § 5 odst. 3 vyhlášky ČNB musí povinná osoba v hodnocení rizik zohlednit mimo jiné i „*rizika spojená s využitím nových technologií při své obchodní činnosti*." Všechny tyto skutečnosti by svědčily ve prospěch obezřetnějšího přístupu k posuzování rizikovosti transakcí, což by FinTech společnosti oproti tradičním institucím znevýhodňovalo.

Další otázka je, do jaké míry lze vytvoření systému nebo i samotný *screening* externalizovat. Samotná tvorba systému vnitřních zásad a jejich implementace do systémů povinných osob od třetích stran je sice záležitost individuální, ale reálná a dokonce nikoliv neobvyklá.[108] Vyhodnocování podezřelých transakcí třetí osobou je pak už méně pravděpodobné. Tyto informace jsou vysoce citlivé jak z pohledu klientů, tak z pohledu povinné osoby. Třetí osoba

---

[106] CHEN, Zhiyuan, Ee na TEOH, Amril NAZIR, Ettikan kandasamy KARUPPIAH a Kim sim LAM. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems* [online]. 2018, **57**(2), 245-285 [cit. 2020-06-06]. DOI: 10.1007/s10115-017-1144-z. ISSN 02191377. Dostupné z: https://link.springer.com/article/10.1007%2Fs10115-017-1144-z. Str. 278.

[107] FINANČNÍ ANALYTICKÝ ÚŘAD. *Výroční zpráva 2019* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-526990861/1588148007_cs_29042020_vyrocni_zprava_fau_2019.pdf. Str. 3.

[108] Např. Anti money laundering and Fraud. *Digital Systems* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.digitalsystems.eu/fraud-risk-and-compliance/#anti-money.

by zároveň měla ve vztahu k případným trestným činům oznamovací povinnost, pokud by nešlo o poskytování právních služeb advokátem.

2.5. Další povinnosti

2.5.1. Školení zaměstnanců

AML zákon vyžaduje každoroční školení zaměstnanců a dalších osob, externistů, podílejících se na činnostech povinné osoby, při kterých se mohou dostat do styku s podezřelými obchody. Obsahem školení jsou požadavky pro identifikaci a kontrolu klientů nebo postupy pro zjišťování jejich rizikovosti a zjišťování podezřelých obchodů.

Tyto požadavky podle mého názoru pro FinTech společnosti nepředstavují nepřiměřené či nedůvodné náklady. V jejich prospěch naopak může svědčit menší počet zaměstnanců, které je nutné školit. Školení je možné provádět online a lze ho částečně pořídit jako hotový produkt od specializovaných společností. Částečně musí odpovídat procesům nastaveným specifickou povinnou osobou. Otázkou může být, zda je nutné poskytovat vyšší úroveň školení odborným zaměstnancům (AML officerům), ale z důvodu absence zákonného požadavku na odlišnou kategorii školení se jedná zřejmě pouze o vhodný preventivní nástroj.

2.5.2. Sankční seznamy

V rámci identifikace klienta povinná osoba zjišťuje, zda proti jejímu klientovi nebo skutečnému majiteli tohoto klienta ČR neuplatňuje mezinárodní sankce. Co se týče sankcí vůči konkrétním osobám, jedná se o jednu z poměrně jednoduše splnitelných povinností. Sankční seznamy jsou veřejné a automatizovaný *screening* lze poměrně snadno zavést. Seznamy jsou i běžnou součástí komerčních databází. Kromě sankcí OSN a EU mohou povinným osobám sloužit jako vodítko pro posouzení rizik i další sankční seznamy, například americký (OFAC) nebo britský (HM Treasury). Problematické mohou být sankce vůči konkrétnímu typu zboží, typicky se bude jednat o obchody se zbraněmi. V takovém případě by jako základní *alert* nejspíš mohlo posloužit územní kritérium.[109]

[109] KATOLICKÁ, Michaela a Ján BÉREŠ. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. Praha: Wolters Kluwer ČR, 2017, 248 s. ISBN 978-80-7552-823-0. Str. 35-37.

3. Vzdálená identifikace

Vzdálená identifikace je výzvou pro většinu FinTech služeb. Absence fyzického kontaktu povinných osob s klienty a snaha o maximálně jednoduché a snadno přístupné služby zde naráží na regulatorní požadavky, které usilují o minimalizaci rizik zneužití identity. Tato rizika nejsou pouze teoretická, v minulosti již došlo například ke zpochybnění procesu vzdálené identifikace v případě německé neobanky N26.[110]

Kromě možností vzdálené identifikace AML zákon upravuje též identifikaci zprostředkovanou, kterou na žádost klienta nebo povinné osoby provádí notář nebo kontaktní místo veřejné správy. Přestože se jedná o možnost, jak povinné osoby mohou přenést administrativní zátěž na třetí osoby, stále je v takovém případě pro identifikaci nezbytná fyzická přítomnost klienta. Z tohoto důvodu se zprostředkovanou identifikací nebudu dále zabývat.

3.1. Stávající typy vzdálené identifikace a jejich novelizace

3.1.1. Převzetí identifikace

Institut převzetí identifikace je založen na předpokladu, že identifikaci klienta již provedla jiná povinná osoba a nejsou pochybnosti o její správnosti či úplnosti. Osoba poskytující identifikaci musí povinné osobě přebírající identifikaci poskytnout všechny potřebné dokumenty o klientovi. Vzhledem k tomu, že se jedná o osobní údaje, je nezbytný souhlas klienta s tímto poskytnutím. Díky souhlasu klienta není porušena ani povinnost dodržovat bankovní tajemství ve smyslu § 38 zákona o bankách (ZOB). Finanční a úvěrová instituce, která identifikaci přebírá, je za ni odpovědná, jako by ji provedla sama. Povinnou osobu, která identifikaci provedla, nelze k součinnosti pro její převzetí nutit. Převzetí identifikace může proběhnout za úplatu.[111]

Převzít identifikaci lze i od některých zahraničních úvěrových a finančních institucí (s výjimkou například osob oprávněných ke směnárenské činnosti nebo některých platebních institucí a všech poskytovatelů platebních služeb malého rozsahu), pokud působí na území státu

[110] Foto-Ident bei N26: BaFin prüft wegen Kontoeröffnungen mit falschen Ausweisen. *Heise Online* [online]. 2018 [cit. 2020-06-06]. Dostupné z: https://www.heise.de/newsticker/meldung/Foto-Ident-bei-N26-BaFin-prueft-wegen-Kontoeroeffnungen-mit-falschen-Ausweisen-4190027.html.
[111] TVRDÝ, Jiří. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. 2. vydání. Praha: C.H. Beck, 2018, 584 s. ISBN 978-80-7400-688-3. Str. 76-78.

se srovnatelnými pravidly pro identifikaci klienta. V tomto ohledu lze předem vyloučit osoby působící v rizikových zemích. Na základě faktorů zeměpisného rizika ve smyslu přílohy č. 2 AML zákona FAÚ průběžně aktualizuje seznam takových zemí. Vychází přitom nejen z uplatňovaných mezinárodních sankcí, ale i ze seznamu vysoce rizikových třetích zemí Evropské Komise[112] nebo tzv. *greylistu* FATF[113,114].

Tento institut má omezené využití nejen z hlediska okruhu institucí, které mohou identifikaci poskytnout. Povinné osoby, které by ji poskytnout mohly, nemají žádnou motivaci přivádět svoje klienty konkurenci, tedy i FinTech společnostem. V případě vyžadování poplatku za takovou službu by pak bylo vhodnější použít jinou, levnější metodu vzdálené identifikace. Tento způsob identifikace si tak lze představit především při kooperaci vzájemně propojených institucí. Navrhovaná novela AML zákona nepřináší v oblasti převzetí identifikace žádné změny, které by tento způsob otevřely širšímu okruhu povinných osob.

3.1.2. Identifikace první platbou

Identifikaci první platbou nalezneme v § 11 odst. 7 AML zákona. Vychází se zde z předpokladu, že identifikaci klienta již provedla jiná povinná osoba, konkrétně domácí nebo evropská úvěrová instituce. Povinná osoba může v tomto případě provést identifikaci klienta bez jeho fyzické přítomnosti, pokud klient zašle povinné osobě kopie průkazu totožnosti, nejméně jednoho dalšího podpůrného dokladu a doklad potvrzující existenci účtu vedeného na jméno klienta u domácí nebo evropské úvěrové instituce. Z tohoto účtu poté musí proběhnout první platba podle uzavřené písemné smlouvy o poskytnutí finančních služeb. Povinná osoba zároveň nesmí mít pochybnosti o skutečné totožnosti klienta.

K potřebě druhého podpůrného dokladu důvodová zpráva k novele AML zákona uvádí, že se jedná o opatření znesnadňující zneužití či padělání ztraceného nebo ukradeného dokladu, neboť

[112] Nařízení Komise v přenesené pravomoci (EU) 2016/1675 ze dne 14. července 2016, kterým se směrnice (EU) 2015/849 Evropského parlamentu a Rady doplňuje o identifikaci vysoce rizikových třetích zemí se strategickými nedostatky.
[113] FATF, neboli *Financial Action Task Force*, česky Finanční akční výbor, je mezinárodní organizace, která vytváří obecně respektované standardy v oblasti boje proti praní špinavých peněz a financování terorismu.
[114] FATF. *Jurisdictions under Increased Monitoring – 21 February 2020* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html.

pachatel by musel k padělání obou dokladů vynaložit „*dvojnásobný objem práce*“.[115] Je vhodné uvést, že typ podpůrného dokladu určuje povinná osoba na základě vlastního hodnocení rizik, může se tak jednat například i o studentský průkaz. Padělat takový doklad je přitom mnohem jednodušší než padělat občanský průkaz nebo cestovní pas. Zároveň se v rámci identifikace první platbou povinné osobě posílají pouze kopie těchto dokladů v elektronické podobě. Není proto nutné padělat samotné doklady, ale postačuje padělání jejich elektronické podoby, což je například v případě uvedeného studentského průkazu triviální záležitost. Nelze proto tvrdit, že takové padělání zákonitě znamená dvojnásobné množství práce. Když pomineme fakt, že v případě krádeže peněženky je vysoce pravděpodobná přítomnost i dalšího podpůrného dokladu, a dále fakt, že pokud pachatel zvládne padělat kopii občanského průkazu nebo cestovního pasu, jistě mu nebude dělat problém padělat i podpůrný doklad s nižší úrovní ochrany, požadavek na další podpůrný doklad je absurdní ještě z dalšího důvodu. I v případě zneužití dokladu totožnosti a dalšího podpůrného dokladu by musel pachatel ještě provést první platbu z platebního účtu vedeného u evropské úvěrové instituce na jméno osoby, jejíž doklady zneužil. Pachatel by tak musel ještě získat přístup do internetového bankovnictví osoby, jejíž identitu zneužívá, a pravděpodobně ještě k jejímu mobilnímu telefonu kvůli potvrzení platby. Z těchto důvodů se domnívám, že požadavek na doložení dalšího podpůrného dokladu je zbytečnou zátěží pro klienty, nemá významný bezpečnostní přínos a MF mělo v novele AML zákona navrhnout jeho zrušení.

AML zákon vyžaduje jak doklad potvrzující existenci účtu vedeného na jméno klienta, tak i první platbu z tohoto účtu. V případě provedení první platby ale příjemce transakce zpravidla získává i jméno plátce. Není tedy zřejmé, proč zákonodárce přidal ještě požadavek na zaslání dokladu potvrzujícího existenci účtu. Zároveň ale ustanovení nelze interpretovat tak, že provedením první platby by došlo i ke splnění požadavku na zaslání dokladu potvrzujícího existenci účtu. Doklad potvrzující existenci účtu nemá zákonnou definici a podle doktríny může mít podobu i pouhého prohlášení klienta.[116] Nedomnívám se, že by takové prohlášení představovalo dodatečnou záruku, a v případech, kdy se příjemce první transakce dozví

[115] Důvodová zpráva In: MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2. Str. 159.

[116] TVRDÝ, Jiří. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. 2. vydání. Praha: C.H. Beck, 2018, 584 s. ISBN 978-80-7400-688-3. Str. 81.

z informací doprovázejících platbu i údaje o plátci, je zcela zbytečné. Podle navrhované podoby AML zákona sice dochází ke změně v tom smyslu, že provedení první platby, která je doprovázená informací o jménu plátce, bude možné (minimálně podle důvodové zprávy)[117] považovat za „*hodnověrný způsob prokázání existence platebního účtu*“, avšak součástí návrhu je i zcela nová povinnost. V rámci provedení první platby bude muset klient uvést doprovodné informace o účelu identifikace, svém jméně a příjmení a bude muset typově označit povinnou osobu.[118] Nabízí se jednoduchá otázka. Pokud by se osoba pokoušející se zneužít identifikaci první platbou dostala k cizímu dokladu totožnosti, případně dalšímu podpůrnému dokladu, dále k přihlašovacím údajům do internetového bankovnictví osoby, jejíž identitu zneužívá, a jejímu mobilnímu telefonu kvůli ověření platby, bude pro ni představovat zadání informací, kterými v tuto chvíli již disponuje, do rozhraní pro zadání platby nepřekonatelný problém? Je pravda, že může teoreticky nastat případ, kdy útočník získá přístup k cizím dokladům a danou osobu nějakým způsobem přesvědčí o tom, aby sama provedla první platbu. Domnívám se ale, že takové případy se mohou týkat hlavně osob blízkých. Cizím svéprávným osobám by muselo připadat provádění bezdůvodných transakcí podezřelé.

Požadavek na provedení první platby by též bylo možno splnit pomocí služby nepřímého dání platebního příkazu a služby informování o platebním účtu ve smyslu ZPS. Povinná osoba by ovšem musela disponovat oběma licencemi zároveň. Novela AML zákona s touto technologií výslovně počítá a s jejím využitím spojuje i nevyžadování kopie podpůrného dokladu, hodnověrného prokázání platebního účtu ani informace o účelu identifikace doprovázející první platbu.[119] V této souvislosti je ovšem třeba zmínit, že podle § 65 odst. 3 a § 106 odst. 4 ZPS

---

[117] Podle důvodové zprávy lze ve většině případů existenci účtu vedeného na jméno klienta hodnověrně doložit prostřednictvím informací doprovázejících kontrolní platbu. Autoři ale neuvádí ani jeden případ, kdy takové informace kontrolní platbu nedoprovází. Důvodová zpráva In: MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2. Str. 160.

[118] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

[119] Důvodová zpráva In: MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2. Str. 163.

nesmí službu nepřímého dání platebního příkazu a službu informování o platebním účtu poskytovat ani poskytovatel platebních služeb malého rozsahu, ani vydavatel elektronických peněz malého rozsahu. Tyto licence jsou přitom mezi FinTech společnostmi velmi rozšířené.[120]

Podle stávajícího i navrhovaného znění je podmínkou identifikace první platbou skutečnost, že povinná osoba nemá pochybnost o skutečné totožnosti klienta. Skepticky je nutno konstatovat, že určité pochybnosti o skutečné totožnosti klienta budou přítomny vždy. Tyto pochybnosti by mohla do určité míry eliminovat limitovaná možnost přístupu povinných osob k základním registrům.

3.1.3. Identifikace podle nařízení eIDAS

Podle § 11 odst. 8 AML zákona lze vzdálenou identifikaci klienta provést, pokud klient povinné osobě sdělí potřebné identifikační údaje a povinná osoba ověří jeho totožnost u kvalifikovaného poskytovatele služeb vytvářejícího důvěru ve smyslu nařízení eIDAS. Povinná osoba přitom nesmí mít pochybnosti o skutečné totožnosti klienta. Toto ustanovení je poměrně obecné, což umožňuje povinným osobám zvolit nejvhodnější způsob identifikace s ohledem na vlastní hodnocení rizik.

Nabízí se tedy otázka, který typ elektronického podpisu je podle tohoto ustanovení dostačující k ověření totožnosti klienta. **Prostý elektronický podpis** podle definice obsažené v článku 3 bodu 10 nařízení eIDAS nepřichází v úvahu, protože nezajišťuje ani identifikaci podepisující osoby, ani autentizaci podepisovaných dat.[121] **Zaručený elektronický podpis** ve smyslu článku 26 nařízení eIDAS sice zajišťuje informace o podepisující osobě a zjistitelnost jakékoliv následné manipulace s daty, ale nezaručuje zjištění identity osoby, která data podepsala. Díky absenci požadavku kvalifikovaného certifikátu si totiž může vlastní certifikát s libovolnými údaji vytvořit kdokoliv.[122] Tento typ elektronického podpisu proto nelze pro identifikaci klienta akceptovat, neboť povinná osoba v takovém případě nemůže nemít pochybnosti o skutečné totožnosti klienta ve smyslu § 11 odst. 8 písm. c) a odst. 9 AML zákona. Jinak je tomu v případě

---

[120] MINISTERSTVO FINANCÍ. *Online identifikace a AML/CFT: Podkladová studie* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/podkladova-studie-financni-technologie-a-31641. Str. 7.

[121] KMENT, Vojtěch. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer ČR, 2018, 417 s. Právní monografie. ISBN 978-80-7552-814-8. Str. 138-139.

[122] PETERKA, Jiří. Jak poznat kvalifikovaný elektronický podpis a kvalifikovanou elektronickou pečeť?. *Lupa*, 2018 [online]. [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/jak-poznat-kvalifikovany-elektronicky-podpis-a-kvalifikovanou-elektronickou-pecet/.

zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronický podpis. Kvalifikované certifikáty vydávají pouze kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří podle článku 24 nařízení eIDAS při vydání certifikátu ověří totožnost osoby, které je certifikát vydáván. Použití kvalifikovaného certifikátu při podpisu dat tedy zajišťuje výrazně vyšší úroveň ověření identity, která by teoreticky mohla pro účely identifikace klienta ve smyslu § 11 odst. 8 AML zákona postačovat. Problém nastává ve chvíli, kdy by měla povinná osoba ověřit totožnost příslušné fyzické osoby u kvalifikovaného poskytovatele služeb vytvářejících důvěru. Nařízení eIDAS nestanoví poskytovatelům služeb vytvářejících důvěru povinnost sdělovat osobní údaje o podepisující osobě jiným subjektům. Zatímco poskytovatel služeb vytvářejících důvěru má povinnost ověřit totožnost osoby, které kvalifikovaný certifikát pro elektronický podpis vystavil, na samotném podpisu může být třeba i pouze jméno a příjmení podepisující osoby.[123] To z pohledu povinné osoby k dostatečné identifikaci klienta nemusí stačit. Tuto situaci nemusí vyřešit ani **kvalifikovaný elektronický podpis** ve smyslu článku 3 bodu 12 nařízení eIDAS, jehož právní účinek je rovnocenný vlastnoručnímu podpisu. Jedná se o elektronický podpis vytvořený kvalifikovaným prostředkem pro vytváření elektronických podpisů, který je založený na kvalifikovaném certifikátu pro elektronické podpisy. Kvalifikovanými prostředky pro vytváření elektronických podpisů mohou být čipová karta nebo token, které má podepisující osoba ve svém držení.[124] Zároveň je třeba připustit, že žádný elektronický podpis nemůže s jistotou vyloučit možnost, že data podepisuje jiná osoba, než ta, které elektronický podpis patří.

Pro doplnění je třeba uvést, že česká legislativa pracuje ještě s pojmem „*uznávaný elektronický podpis*“. Jedná se o legislativní zkratku, kterou nalezneme v zákoně o službách vytvářejících důvěru pro elektronické transakce. Podle § 6 odst. 2 tohoto zákona se uznávaným elektronickým podpisem rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis. Vzhledem k tomu, že přijatá ani navrhovaná novela AML zákona s tímto pojmem nepracuje, nebudu jej dále používat.

---

[123] KMENT, Vojtěch. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer ČR, 2018, 417 s. Právní monografie. ISBN 978-80-7552-814-8. Str. 266.
[124] Tamtéž. Str. 149.

Navrhovaná podoba AML zákona nově v § 11 odst. 8 explicitně vyžaduje kvalifikovaný elektronický podpis a následné ověření poskytnutých údajů u kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo z dokumentu vydaného orgánem veřejné moci opatřeného kvalifikovanou elektronickou pečetí. Povinná osoba stejně jako v současnosti nesmí mít pochybnosti o totožnosti fyzické osoby.[125] Důvodová zpráva k návrhu novely AML zákona podle mého názoru nesprávně uvádí, že již podle účinného znění je k tomuto typu identifikace klienta zapotřebí kvalifikovaný elektronický podpis a tento výklad nijak nezdůvodňuje. Zároveň přiznává, že reálné využití tohoto ustanovení je velmi omezené. Poskytovatel služeb vytvářejících důvěru nemá povinnost s povinnou osobou spolupracovat a v současnosti v ČR nedochází ze strany orgánů veřejné moci ani k vydávání dokumentů opatřených kvalifikovanou elektronickou pečetí, které by přiřadily identifikační údaje klienta ke konkrétnímu kvalifikovanému certifikátu.[126] Nabízí se otázka, proč se autoři návrhu nezamysleli nad zavedením povinnosti spolupráce kvalifikovaného poskytovatele služeb vytvářejících důvěru, když o tomto nedostatku ví. Tato spolupráce by mohla být prováděna za úplatu.

3.1.4. Správní trestání neplnění povinnosti při identifikaci a kontrole klienta

V období od roku 2017 do 1. 5. 2020 udělil FAÚ povinným osobám 39 peněžitých sankcí za přestupky spočívající v neplnění povinností při identifikaci a kontrole klienta ve smyslu ustanovení § 44 AML zákona. Nejvyšší sankce byla 1 000 000 Kč[127], nejnižší pak 20 000 Kč. Průměrná výše sankce převyšovala 135 000 Kč, medián byl 100 000 Kč. Nejčastěji šlo o osoby oprávněné k poskytování platebních služeb nebo vydávání elektronických peněz a dále o osoby oprávněné ke směnárenské činnosti. V roce 2019 byla potrestána osoba poskytující služby spojené s virtuální měnou, a to sankcí ve výši 300 000 Kč. Podrobnosti k tomuto a dalším rozhodnutím o přestupcích odmítá FAÚ poskytovat s odkazem na zvláštní povahu své

---

[125] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

[126] Důvodová zpráva In: MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2. Str. 161-162.

[127] V tomto případě se nejednalo pouze o neplnění povinností při identifikaci a kontrole klienta, ale i nesplnění oznamovací povinnosti a nezajištění proškolení kontaktní osoby. FINANČNÍ ANALYTICKÝ ÚŘAD. *Rozhodnutí o přestupku ze dne 31. 10. 2018*. Č. j. FAU-68073/2018/032. Dostupné z: https://www.financnianalytickyurad.cz/rozhodnuti-o-prestupcich.html.

činnosti.[128] Nelze proto poskytnout podrobnější analýzu. Uvedené informace nicméně mohou naznačovat, že největší problém se splněním povinností při identifikaci a kontrole klienta mají malé finanční instituce.

3.2. Nové možnosti vzdálené identifikace

Zákonem č. 49/2020 Sb. byl do AML zákona s účinností od 1. 1. 2021 vložen § 8a, který přinese dva nové způsoby, jak provést vzdálenou identifikaci fyzické osoby. Tento zákon navržený širokou skupinou poslanců v důvodové zprávě uvádí, že stávající podoba AML zákona je ohledně elektronické identifikace „*zastaralá a významně restriktivní, aniž by pro to byl objektivní důvod*".[129] Zároveň došlo v této souvislosti ke změnám v ZOB, který nově umožní bankám poskytovat identifikační služby. Autoři si od zákona slibují výrazný rozvoj v oblasti eGovernmentu, eCommerce a též posun v digitalizaci finančního sektoru. Tento zákon představuje nezbytný právní základ projektu SONIA (soukromoprávní bod pro identifikaci a autentizaci), který vzešel z iniciativy bank, a týká se bank především. Přijatá podoba zákona ale obsahuje i nový způsob vzdálené identifikace, který budou moci využít všechny povinné osoby.

Důvodová zpráva k tomuto zákonu upozorňuje na § 2 zákona o elektronické identifikaci, podle kterého lze prokázání totožnosti vyžadované právním předpisem umožnit s využitím elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace, což podle autorů vyvolává ve vztahu k AML zákonu právní nejistotu.[130] Domnívám se však, že v tomto případě je zřejmé, že AML zákon poskytuje speciální úpravu vzdálené identifikace a nelze dovozovat obecnou možnost identifikace ve smyslu § 2 zákona o elektronické identifikaci. Takovou možnost by bylo jistě možné dovodit, pokud by AML zákon žádné typy vzdálené identifikace neupravoval a zároveň by vzdálenou identifikaci výslovně nevylučoval.

---

[128] FINANČNÍ ANALYTICKÝ ÚŘAD. *Rozhodnutí o částečném odmítnutí žádosti o informace ze dne 21. 5. 2020.* Č. j. FAU-42153/2020/031. Str. 3-5.
[129] Důvodová zpráva In: KOŘANOVÁ, Barbora, Martin KUPKA, Ivan BARTOŠ a kol. *Návrh poslanců Barbory Kořanové, Martina Kupky, Ivana Bartoše, Pavla Jelínka, Pavla Kováčika, Jana Chvojky, Jana Bartoška, Heleny Langšádlové, Věry Kovářové a dalších na vydání zákona, kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů*. Poslanecká sněmovna Parlamentu České republiky, 2019. Sněmovní tisk 554/0. 8. volební období. Str. 23.
[130] Tamtéž. Str. 23.

3.2.1. Prostředek pro elektronickou identifikaci

Podle § 8a odst. 1 písm. a) bude možné identifikaci klienta nahradit prostředkem pro elektronickou identifikaci, který splňuje standardy pro vysokou úroveň záruky a který je součástí kvalifikovaného systému podle zákona o elektronické identifikaci.

Úrovně záruk prostředků pro elektronickou identifikaci upravuje prováděcí nařízení Evropské komise vycházející z nařízení eIDAS.[131] Rozlišuje se nízká, značná a vysoká úroveň záruky. Tyto úrovně označují míru zabezpečení identifikace a autentizace. **Nízké úrovně záruky** lze dosáhnout požadavkem na přihlašování se uživatelským jménem a heslem. Jedná se o jednofaktorové ověření, při kterém je vyžadován pouze faktor znalosti. Pro **značnou úroveň záruky** je vyžadováno dvoufaktorové ověření, které kromě faktoru znalosti v podobě přihlašovacího jména a hesla vyžaduje i faktor vlastnictví, například mobilního telefonu, na který je zasláno jednorázové heslo. **Vysoká úroveň záruky** je dosažena v případě, že jeden ze dvou požadovaných faktorů je spolehlivě chráněn před vytvořením duplikátu a před zneužitím třetí osobou. Této úrovně lze dosáhnout s využitím jedinečného fyzického nosiče, například USB tokenu nebo čipové karty.[132] Vysoké úrovně záruky v současnosti v ČR dosahují pouze elektronický občanský průkaz (též eObčanka) coby projekt MV a společnost První certifikační autorita se svou čipovou kartou Starcos. Jedná se o kvalifikované prostředky pro vytváření elektronických podpisů. V obou případech jsou dosažena kritéria kvalifikovaného elektronického podpisu a k používání je nezbytná fyzická čtečka.[133]

Na první pohled se nabízí srovnání tohoto ustanovení a navrhované podoby § 11 odst. 8 AML zákona. Toto ustanovení vyžaduje po klientovi sdělení identifikačních údajů, jejich opatření kvalifikovaným elektronickým podpisem a ověření získaných údajů u kvalifikovaného poskytovatele služeb vytvářejících důvěru ze strany povinné osoby. Podle přijatého § 8a odst. 1 písm. a) postačuje pouze provedení identifikace prostřednictvím prostředku pro elektronickou identifikaci, který dosahuje vysoké úrovně záruky (což opět splňuje kvalifikovaný elektronický

---

[131] Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

[132] PETERKA, Jiří. Český eGovernment v roce 2018: Významný milník i příchod elektronických občanek. *Lupa*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/cesky-egovernment-v-roce-2018-vyznamny-milnik-i-prichod-elektronickych-obcanek/.

[133] PETERKA, Jiří. eObčanky ztratily monopol na přihlašování ke službám eGovernmentu. Jak funguje karta Starcos?. *Lupa*, 2020 [online]. [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/eobcanky-ztratily-monopol-na-prihlasovani-ke-sluzbam-egovernmentu-jak-funguje-karta-starcos/.

podpis). V prvním případě je explicitně vyžadována absence pochybností ohledně totožnosti klienta, ve druhém případě ne. Podle mého názoru je možné takovou povinnost dovodit z obecných ustanovení AML zákona. Celkově je zjevné, že navrhovaný § 11 odst. 8 AML zákona je přísnější než přijatý § 8a AML zákona. Z tohoto důvodu lze předpokládat, že pokud bude § 11 odst. 8 AML zákona v této podobě přijat, bude zbytečný. Je třeba připomenout, že legislativní proces je v době psaní této práce teprve na začátku a návrh může doznat podstatných změn. MF v důvodové zprávě k navrhované podobě § 11 odst. 8 AML zákona uvádí, že samotný kvalifikovaný elektronický podpis není pro vzdálenou identifikaci dostatečnou zárukou: „*(…) ze samotného kvalifikovaného certifikátu není možné zjistit všechny identifikační údaje v rozsahu požadovaném AML zákonem, a dokonce lze říci, že z něj není možné ani ověřit totožnost podepisujícího*“.[134] Je tedy pravděpodobné, že zákonodárce přijal ustanovení § 8a AML zákona v rozporu s postojem MF, potažmo FAÚ. Zaměstnanci FAÚ ostatně již v minulosti vyjádřili názor, že i v budoucnu bude představovat jediný plnohodnotný identifikační postup identifikace za fyzické přítomnosti klienta, ačkoliv může dojít k uzákonění metod vzdálené identifikace, které budou oproti těm stávajícím bezpečnější.[135]

Problém pro aplikaci ustanovení § 8a odst. 1 písm. a) AML zákona nebude představovat složitost metody, ale velmi malé rozšíření prostředků pro elektronickou identifikaci dosahujících vysokou úroveň záruky mezi populací. Přijetí tohoto ustanovení ale celkově hodnotím pozitivně. S budoucím rozšířením eObčanek nebo komerčních alternativ může tímto způsobem dojít k výraznému zjednodušení procesu vzdálené identifikace z pohledu povinných osob, a to při zachování vysokých bezpečnostních standardů.

3.2.2. Bankovní identita

Podle § 8a odst. 1 písm. b) AML zákona bude možné provést identifikaci fyzické osoby také pomocí prostředku pro elektronickou identifikaci, který splňuje podmínky podle zákona upravujícího činnost bank. Jedná se o odkaz na přijatou novelu ZOB, která bankám nově umožní podnikání spočívající v poskytování elektronické identifikace, autentizace a služeb

---

[134] Důvodová zpráva In: MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2. Str. 161-162.

[135] HLADKÁ, Michaela a Jiří HYLMAR. Identifikace klienta podle zákona proti praní špinavých peněz – výhled do budoucna. *Bankovnictví*. 4H production, **2018**(8), 20-21. ISSN 1212-4273.

vytvářejících důvěru, a to mimo rámec kvalifikovaného systému ve smyslu zákona o elektronické identifikaci. Díky tomuto prostředku bude pro klienty bank v budoucnu možné využít pro komunikaci se státem (eGovernment) nebo i se soukromými subjekty tzv. bankovní identitu. Ta bude pro klienty bank, tedy přibližně pro 5,5 milionů lidí přístupná zdarma, a to prostřednictvím stejného přístupu, který klienti bank již v současnosti využívají při přihlašování do internetového bankovnictví.[136] Česká bankovní asociace plánuje, že soukromé subjekty by bankám za využití bankovní identity platily poplatky.[137]

Bankovní identita aspiruje pouze na dosažení značné úrovně záruky. Nabízí se proto otázka, proč budou mít všechny ostatní povinné osoby při vzdálené identifikaci podle AML zákona povinnost dosáhnout vysoké úrovně záruky, zatímco v případě bankovní identity postačí značná úroveň záruky. Jako důvod dostatečnosti této úrovně důvodová zpráva uvádí, že banky jsou obecně důvěryhodné, vysoce regulované a dodržují vysoké bezpečnostní standardy.[138] Není přitom zřejmé, z čeho autoři dovozují obecnou důvěryhodnost bank. Banky nepochybně vysoce regulované jsou, nicméně tento fakt automaticky nezaručuje důvěryhodnost vnitřních procesů konkrétní entity.[139] Riziko zneužití identity přitom není primárně sníženo existencí bezpečnostních standardů na straně banky, ale spíše zabezpečením ověřovacích faktorů na straně klienta.

Pro srovnání je však vhodné zmínit, že v současnosti je možné přistupovat do systému datových schránek pomocí jednofaktorového ověření, které zajišťuje pouze nízkou úroveň záruky. Pomocí datové schránky je přitom podle § 18 zákona o elektronických úkonech a autorizované konverzi dokumentů možné provádět vůči orgánům veřejné moci jednání, které má stejné účinky, jako by bylo písemné a podepsané osobou, pro níž byla datová schránka zřízena. V tomto kontextu se zdá, že značná úroveň záruky zajištěná bankovní identitou může být

---

[136] ZATLOUKAL, Jiří. Rodí se Sonia. Největší banky v Česku chtějí společnou firmou rozhýbat digitalizaci státu. *Euro*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.euro.cz/byznys/rodi-se-sonia-nejvetsi-tuzemske-banky-chteji-spolecnou-firmou-rozhybat-digitalizaci-statni-spravy-1434456.

[137] Nejčastější dotazy. Bankovní identita [online]. *Česká bankovní asociace*, 2020 [cit. 2020-06-06]. Dostupné z: https://www.bankovni-identita.cz/faq.

[138] Důvodová zpráva In: KOŘANOVÁ, Barbora, Martin KUPKA, Ivan BARTOŠ a kol. *Návrh poslanců Barbory Kořanové, Martina Kupky, Ivana Bartoše, Pavla Jelínka, Pavla Kováčika, Jana Chvojky, Jana Bartoška, Heleny Langšádlové, Věry Kovářové a dalších na vydání zákona, kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů*. Poslanecká sněmovna Parlamentu České republiky, 2019. Sněmovní tisk 554/0. 8. volební období. Str. 25.

[139] K tomu např. HRUBEŠ, Karel. Nevysvětlených 10 miliard přes J&T. Putovaly po trase Rusko–Česko–Karibik. *iDNES* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.idnes.cz/zpravy/domaci/j-t-rusko-cesko-banka.A191125_192032_domaci_jum.

vnímána v rámci eGovernmentu z hlediska bezpečnosti jako posun vpřed. Zda je taková záruka dostatečná i pro účely AML zákona, se pravděpodobně dozvíme až zpětně po zavedení bankovní identity do praxe.

Podle důvodové zprávy nemá pro banky smysl usilovat o získání akreditace kvalifikovaného správce kvalifikovaného systému elektronické identifikace podle zákona o elektronické identifikaci, neboť v takovém případě by byly povinny zdarma zpřístupnit svůj kvalifikovaný systém elektronické identifikace všem kvalifikovaným poskytovatelům. V takové situaci by banky nemohly kontrolovat, kdo a za jakých podmínek využívá jimi vydaný prostředek pro elektronickou identifikaci. Kromě nákladů na zisk akreditace a následný provoz by se vystavovaly i odpovědnosti za nesprávně provedenou identifikaci nebo za škodu způsobenou při správě kvalifikovaného systému. Podle autorů „*současná situace deformuje tržní prostředí v oblasti poskytování elektronické identifikace ze strany bank*“.[140]

Je poměrně čitelné, že úprava zákona o elektronické identifikaci představuje překážku pro budoucí obchodní model bankovní identity. Zatímco kvalifikovaní správci svým zákazníkům prodávají samotný prostředek pro elektronickou identifikaci a jeho následnou akceptaci ze strany kvalifikovaných poskytovatelů nemohou kontrolovat, bankovní identitu chtějí banky nabízet svým klientům zdarma a o způsobech její akceptace ze strany komerčních subjektů rozhodovat samy, a to za poplatek pro tyto komerční subjekty. Tvrzení, že současná situace deformuje tržní prostředí, je podle mého názoru nesmyslné, neboť samotná absence zákonného zmocnění pro vytvoření obchodního modelu na míru určité skupině subjektů nevytváří aktérům trhu nerovné podmínky. *Ad absurdum* by bylo možné tvrdit, že stávající právní úprava v podobě zákona o elektronické identifikaci deformuje tržní prostředí z pohledu všech osob, které by nechtěly postavit obchodní model na jeho dodržování. Naopak by bylo možné říct, že právní úprava bankovní identity znevýhodní pozici kvalifikovaných správců, jejichž produkty díky přijatým výsadám bankovní identity možná již nebudou tak přitažlivé. V tomto ohledu bude hrát důležitou roli MV, které prostřednictvím katalogu služeb ve smyslu § 2 odst. 4 zákona o právu na digitální služby bude doporučovat, jaká úroveň záruky je pro jaký

[140] Důvodová zpráva In: KOŘANOVÁ, Barbora, Martin KUPKA, Ivan BARTOŠ a kol. *Návrh poslanců Barbory Kořanové, Martina Kupky, Ivana Bartoše, Pavla Jelínka, Pavla Kováčika, Jana Chvojky, Jana Bartoška, Heleny Langšádlové, Věry Kovářové a dalších na vydání zákona, kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů*. Poslanecká sněmovna Parlamentu České republiky, 2019. Sněmovní tisk 554/0. 8. volební období. Str. 10.

účel potřebná. Pokud by s masovým nástupem bankovní identity došlo ke zmírnění doporučovaných úrovní záruky, poškodilo by to ty kvalifikované poskytovatele služeb vytvářejících důvěru, kteří se svými produkty dosáhli na nejvyšší úroveň záruky.[141]

Podnikání spočívající v poskytování identifikace umožní bankám § 1 odst. 4 písm. c) ZOB. Je vysoce pravděpodobné, že některé komerční služby klientům umožní vzájemnou interakci prostřednictvím bankovní identity a za toto zvýšení komfortu pro klienty a snížení vlastní administrativní zátěže budou bankám platit poplatky. Podle mého názoru lze očekávat, že banky neumožní využití bankovní identity ze strany FinTech společností, neboť ty jim v zásadě vytvářejí konkurenci.

Autoři důvodové zprávy dále uvádí, že současná právní úprava bankám neumožňuje přístup do základních registrů, a tato absence je omezuje v efektivním plnění povinností podle AML zákona. To i přesto, že zřízení přístupu údajně předpokládala novela zákona o základních registrech.[142] Tyto výroky jsou podle mého názoru zavádějící. Obecným přístupem do základních registrů nedisponují (vyjma pojišťoven) ani ostatní povinné osoby, nejen banky. Nemůže tak docházet k jejich omezování. Zákon č. 192/2016 Sb., který novelizoval zákon o základních registrech, definoval kategorii „*soukromoprávní uživatel údajů*“. Jedná se o osobu, která není orgánem veřejné moci a je podle jiného právního předpisu oprávněna využívat údaje ze základních registrů. Jedná se tedy o zavedení obecného nástroje, jak poskytovat údaje ze základních registrů soukromým osobám na základě oprávnění stanovených zvláštními zákony. Nelze proto naznačovat, že tato novela předpokládala poskytování informací ze základních registrů bankám pro účely plnění povinností stanovených AML zákonem.

Tento přístup bude bankám umožňovat § 38af odst. 1 ZOB. Na jeho základě budou banky k plnění svých povinností stanovených právním předpisem využívat údaje ze základních registrů. Jedná se o základní registr obyvatel, informační systém evidence obyvatel, informační systém cizinců, informační systém evidence občanských průkazů a informační systém evidence

---

[141] Informace poskytl Roman KUČERA ze společnosti První certifikační autorita prostřednictvím internetové komunikace ze dne 11. 6. 2020.

[142] Důvodová zpráva In: KOŘANOVÁ, Barbora, Martin KUPKA, Ivan BARTOŠ a kol. *Návrh poslanců Barbory Kořanové, Martina Kupky, Ivana Bartoše, Pavla Jelínka, Pavla Kováčika, Jana Chvojky, Jana Bartoška, Heleny Langšádlové, Věry Kovářové a dalších na vydání zákona, kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů*. Poslanecká sněmovna Parlamentu České republiky, 2019. Sněmovní tisk 554/0. 8. volební období. Str. 10.

cestovních dokladů. Trochu vágně působí jak formulace účelu využití údajů („*k plnění svých povinností stanovených právním předpisem*"), tak i povinnost využívání „*jen takových údajů, které jsou v dané věci nezbytné*" v § 38af odst. 8 ZOB. Zatímco banky za účelem ověření identity klienta získají přístup do základních registrů, kvalifikovaní poskytovatelé služeb vytvářejících důvěru při vydání kvalifikovaného certifikátu pro elektronický podpis do základních registrů při ověření totožnosti přistupovat nemohou.[143] Tento stav bude kvalifikované poskytovatele coby konkurenci diskriminovat.

Diskuze ohledně přístupu povinných osob do základních registrů je ovšem zcela legitimní. Je třeba zdůraznit, že již dnes povinné osoby disponují pro účely plnění povinností vyplývajících z AML zákona množstvím osobních údajů o svých klientech. Bylo by vhodné přemýšlet o tom, zda umožnit povinným osobám takový (dobrovolný) přístup k základním registrům, který by byl zabezpečený a nebylo by možné zneužít ho ke hromadnému sběru dat. Jednalo by se bezpochyby o snížení administrativní zátěže povinných osob. Posunem by v této oblasti bylo i samotné potvrzení správnosti údajů, která klient povinné osobě poskytuje, ze strany národního bodu pro identifikaci a autentizaci. Tato opatření by zefektivnila úsilí povinných osob v oblasti předcházení zneužití identity.

Již nyní je zřejmé, že bankovní identita přinese zásadní posun v oblasti eGovernmentu, a to díky iniciativě privátního sektoru. To je jistě pozitivní zpráva. Zavedení mírnějších požadavků AML zákona pouze pro banky, zřízení nepřetržitého online přístupu k základním registrům, kterým ostatní povinné osoby (vyjma pojišťoven) nedisponují[144], a obecně vytvoření právní úpravy identifikačního prostředku na míru, jehož způsoby použití budou určovat banky, ale může působit i jako posilování zákonného bankovního monopolu. V tomto ohledu je možná trochu překvapující poměrně nekritické přijetí novely ze strany odborné veřejnosti.[145] Tím spíše, pokud je návrh zákona doprovázen důvodovou zprávou, kterou lze v některých jejích částech označit za neobjektivní.

---

[143] Informace poskytl Roman KUČERA ze společnosti První certifikační autorita prostřednictvím internetové komunikace ze dne 11. 6. 2020.

[144] Nutno zmínit, že veřejně přístupná je databáze neplatných dokladů na webu MV. Na základě § 77 odst. 6 zákona o hazardních hrách dále existuje služba ověřování existence a plnoletosti hráčů, která dálkovým způsobem ověřuje totožnost a věk osoby žádající o registraci.

[145] To lze demonstrovat na článku, ve kterém autor v zásadě jen argumentačně následuje některé části důvodové zprávy: NOVÁK, Matěj. Návrh zákona upravující podmínky pro vznik bankovní identity [online]. *EPRAVO.CZ*, 2020 [cit. 2020-06-06]. Dostupné z: https://www.epravo.cz/top/clanky/navrh-zakona-upravujici-podminky-pro-vznik-bankovni-identity-110488.html.

3.3. Vzdálená identifikace v zahraničí

3.3.1. Velká Británie

Britský zákon proti praní špinavých peněz a financování terorismu[146] v části o kontrole klienta povinným osobám ukládá, aby klienta identifikovaly v případech, kdy jim není znám. Dále, aby identitu klienta ověřily a posoudily účel a zamýšlenou povahu obchodního vztahu nebo transakce. Povinné osoby musí při identifikaci zvážit rizika vyplývající z vlastního hodnocení rizik a dále rizika vyplývající z konkrétního případu. Bližší podrobnosti stanoví metodika *HM Revenue and Customs*. Podle ní je elektronická identifikace na stejné úrovni jako identifikace za fyzické přítomnosti klienta. Je při ní nezbytné použít širší množství dostupných informací včetně klientské historie, pokud je k dispozici. Informace by měly být získány v rámci delšího časového období a z různých zdrojů. Je potřeba využít i databáze týkající se zneužití identity nebo databáze zemřelých osob. Při posuzování digitální identity poskytované třetí stranou musí povinné osoby zvážit, zda je daná služba důvěryhodná a z jakých zdrojových informací vychází. Výslovně jsou akceptovány prostředky podle nařízení eIDAS a státní digitální identita (GOV.UK Verify). Proces identifikace musí být transparentní a získané informace musí být uchovávány pro účely případné kontroly.[147]

Je zjevné, že povinné osoby mají díky obecně formulovaným ustanovením široké možnosti, jak procesy vzdálené identifikace nastavit. Některé z nich akceptují prosté elektronické kopie dokladů totožnosti. Možnosti vzdálené identifikace využívají v Británii zejména *challenger* banky.[148]

3.3.2. Německo

V Německu oblast AML upravuje *Geldwäschegesetz* (GwG)[149]. Ten ve svém § 12 určuje, jakými způsoby může identifikace klienta proběhnout. Mimo jiné uvádí kvalifikovaný

---

[146] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692).
[147] HM REVENUE & CUSTOMS. *Money service business guidance for money laundering supervision* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/889077/UTF-8__Guidance-for-Money-Service-Businesses-HM-Treasury-approved.docx_.pdf.
[148] EVROPSKÁ KOMISE. *Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions – December 2019*. [online], 2019 [cit. 2020-06-06]. Dostupné z: https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf. Str. 170.
[149] Celým názvem *Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten*.

elektronický podpis nebo elektronický doklad totožnosti. Ustanovení § 13 GwG pak stanoví, že kromě ověření fyzicky předložených dokumentů může dojít i k jinému vhodnému způsobu pro ověření identity, pokud je jeho úroveň bezpečnosti srovnatelná. Zákon dále opravňuje spolkové ministerstvo financí po konzultaci se spolkovým ministerstvem vnitra ke stanovení vhodných metod k provedení identifikace a jejich podrobnějšímu provedení.[150]

Z tohoto ustanovení vychází oběžník 3/2017 (GW), jehož autorem je spolkový ústav pro dohled nad finančními službami. Oběžník upravuje procesy při video identifikaci. Ta může být provedena pouze školenými zaměstnanci povinné osoby nebo třetí strany. V rámci video identifikace, která je prováděna v reálném čase a podle instrukcí zaměstnance, se klient prokazuje takovým dokladem totožnosti, který je dostatečně chráněn před padělaním, je nepoškozený a dobře viditelný na bílém světle. Školený zaměstnanec dále instruuje klienta, aby provedl určité pohyby, například přitiskl prst na doklad totožnosti nebo si přejel rukou přes tvář. V průběhu identifikace zaměstnanec pořizuje snímky klienta s dokladem totožnosti. Celý průběh identifikace je nahrán a musí být povinnou osobou uchován pro účely případné kontroly.[151]

Přestože je tento postup poměrně restriktivní a nelze ho s ohledem na nezbytnou osobní interakci plně automatizovat, domnívám se, že pro účely identifikace poskytuje dostatečné bezpečností záruky. Dále je zřejmé, že tento postup je časově náročnější než by byla identifikace při osobním kontaktu. Pro klienta se ale stále jedná o zásadní zvýšení komfortu, neboť může provést identifikaci odkudkoliv. Nevidím proto důvod, proč by nebylo možné takový způsob zakotvit i v rámci české právní úpravy jako jednu z možných alternativ vzdálené identifikace podobně, jako je tomu ve většině států střední a západní Evropy.[152] Pro případné zvýšení zabezpečení by mohla ještě posloužit možnost povinných osob ověřit doklad totožnosti

---

[150] BAFIN. *Geldwäschegesetz – GwG (Non-binding English Translation)* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8379954#doc7863564bodyText16.

[151] BAFIN. *Circular 3/2017 (GW) – Video Identification Procedures (Non-binding English Translation)* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html.

[152] EVROPSKÁ KOMISE. *Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions – December 2019*. [online], 2019 [cit. 2020-06-06]. Dostupné z: https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf. Str. 104.

dotazem na základní registry. Zavedení tohoto způsobu by ocenili i účastníci konzultace MF.[153] Je velmi pravděpodobné, že podobně jako v Německu by takovou možnost využily nejen FinTech společnosti, ale i tradiční finanční instituce.[154]

3.3.3. Singapur

Vzdálená identifikace pro účely AML může v Singapuru díky poměrně obecným pravidlům proběhnout řadou způsobů.[155] V případě, že klient prokazuje svou identitu pomocí elektronických kopií dokumentů, finanční instituce by měly podle MAS snížit riziko zneužití například tím, že navíc uskuteční ještě videohovor srovnatelný s fyzickým kontaktem, nechají si poslat elektronicky podepsaný dokument nebo využijí technologie využívající biometrické údaje (například otisk prstu, rozpoznávání obličeje či sken oční duhovky). Finanční instituce by měly zajistit, že tyto metody dosahují alespoň stejné spolehlivosti jako fyzický kontakt, a nechat si svůj systém ověřit nezávislým odborníkem.[156]

Pro vzdálenou identifikaci může být dále využit systém MyInfo. Jedná se o systém vyvíjený od roku 2017, který občanům a rezidentům Singapuru zdarma umožňuje využívat svoje státem ověřené a uchovávané osobní údaje pro účely elektronického právního jednání. Kromě případného automatického vyplňování formulářů systém zároveň autentizuje uživatele. Systém je ze strany MAS považován za spolehlivý pro účely AML. Pokud je při identifikaci využit, finanční instituce nemusí získávat žádné další dokumenty nebo fotografie klienta. MyInfo využívá dvoufaktorové ověření. Kromě ID a hesla vyžaduje ověření přes SMS, fyzický token

---

[153] MINISTERSTVO FINANCÍ. *Finanční trh a online identifikace a AML/CFT: Vyhodnocení konzultace* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/financni-trh-a-online-identifikace-a-aml-32102. Str. 3.

[154] EVROPSKÁ KOMISE. *Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions – December 2019*. [online], 2019 [cit. 2020-06-06]. Dostupné z: https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf. Str. 138.

[155] MONETARY AUTHORITY OF SINGAPORE. *Guidelines to MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism* [online] [cit. 2020-06-06]. Dostupné z: https://www.mas.gov.sg/-/media/MAS/resource/legislation_guidelines/aml/CMI-SFA04N02-Guidelines-to-CMS-licensees.pdf?la=en&hash=AED6106BEA86DDE04C47E022A3580B0F81321B2F. Str. 9-10.

[156] MONETARY AUTHORITY OF SINGAPORE. *Use of MyInfo and CDD Measures for Non Face-to-face Business Relations* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf.

nebo otisk prstu skrze mobilní aplikaci. Třetím osobám lze poskytnout pouze takové informace, které uživatel odsouhlasí.[157]

3.4. Působnost AML zákona na přeshraniční služby

Jak již bylo demonstrováno v předchozí podkapitole, regulatorní požadavky vzdálené identifikace se v jednotlivých státech liší. Zároveň je ale často možné využívat zahraničních FinTech služeb i v ČR. Nabízí se proto otázka, zda a do jaké míry musí zahraniční společnosti dodržovat povinnosti vyplývající z českého AML zákona. Pro zodpovězení této otázky je klíčová interpretace § 2 odst. 2 písm. a) a b) AML zákona, tedy zda je zahraniční osoba povinnou osobou.

Podle AML zákona je povinnou osobou rovněž „*zahraniční právnická nebo fyzická osoba uvedená v odstavci 1, která na území České republiky působí prostřednictvím své pobočky, organizační složky nebo provozovny, a to v rozsahu činnosti touto pobočkou nebo provozovnou vykonávané*“ a dále „*na území České republiky působící zahraniční osoba, pokud jako podnikatel vykonává činnosti uvedené v odstavci 1*.“

Navrhovaná podoba AML zákona pouze odstraňuje pojem organizační složka a přidává legislativní zkratku provozovny. Tou se podle návrhu rozumí jiná forma usazení, než je pobočka.[158]

Rovnou můžeme vycházet z předpokladu, že zahraniční osoba, která poskytuje službu dostupnou v ČR, zde pobočku, organizační složku ani provozovnu nemá. Rovněž předpokládejme, že zahraniční osoba vykonává činnosti uvedené v § 2 odst. 1 AML zákona. Zbylá kritéria, tedy zahraniční osoba podnikatelsky působící na území ČR, musí být splněna kumulativně. Podle FAÚ vyžaduje kritérium „*působení na území ČR*“ skutečné působení zástupců zahraničního subjektu na území ČR.[159] MF ale ve své podkladové studii poskytuje jiný pohled. Podle ministerstva může být za „*působení*“ považováno například inzerování

---

[157] FATF. *Guidance on Digital Identity* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf. Str. 76-78.
[158] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.
[159] FINANČNÍ ANALYTICKÝ ÚŘAD. *Rozhodnutí o částečném odmítnutí žádosti o informace ze dne 21. 5. 2020.* Č. j. FAU-42153/2020/031. Str. 3.

služeb v ČR nebo přeložení služby do českého jazyka. MF dále rozlišuje situaci, při které by zahraniční osoba využívání služeb českými klienty na území ČR pouze „*aktivně nebránila*". V takovém případě by bylo možné využít možnosti vzdálené identifikace podle standardů domovské země zahraniční osoby.[160] Katolická k předmětnému ustanovení uvádí: „*Pokud je subjekt zavázán ve svém „domovském" státě alespoň ve stejném rozsahu, v jakém by měl povinnosti podle AML/CFT dle AMLZ, bude své povinnosti zřejmě plnit pouze v místě svého působení. Je ovšem zřejmé, že s ohledem na svou přílišnou obecnost může toto ustanovení způsobovat výkladové problémy a nelze vyloučit ani jiný výklad tohoto ustanovení.*"[161] Je tedy zřejmé, že ustanovení připouští vícero interpretací. Názor FAÚ je zásadní z hlediska správního trestání. Od roku 2017 ale FAÚ žádným povinným osobám ve smyslu § 2 odst. 2 písm. b) AML zákona žádné sankce za přestupky spočívající v neplnění povinností při identifikaci a kontrole klienta ve smyslu § 44 zákona neudělil.[162] Jeho výše uvedené stanovisko tak lze hodnotit jako dlouhodobé. Jako vodítko zde může posloužit i stanovisko ČNB k výkladu pojmu poskytování finančních služeb v ČR. Podle stanoviska je finanční služba poskytována tam, kde je cíleně nabízena a kde může být i využívána. Cílené nabízení je přitom i propagační činnost nebo nabízení služby přes internet. Mezi další znaky poskytování finanční služby v ČR patří například nabídka dálkového uzavření smlouvy, přijímání peněžních prostředků od osob s bydlištěm nebo sídlem na území ČR, překlad služby do češtiny nebo uvedení ČR jako podporované země.[163] Vlastní pohled se na základě uvedeného pokusím demonstrovat na dvou následujících případech.

3.4.1. Případ Revolut

Revolut je neobanka, která vznikla v roce 2015 ve Velké Británii. Službu je možné využívat pouze prostřednictvím mobilní aplikace. V rámci procesu vzdálené identifikace vyžaduje fotografii dokladu totožnosti opatřeného fotografií, fotografii obličeje uživatele, kterou pořídí

---

[160] MINISTERSTVO FINANCÍ. *Online identifikace a AML/CFT: Podkladová studie* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/podkladova-studie-financni-technologie-a-31641. Str. 5.
[161] KATOLICKÁ, Michaela a Ján BEREŠ. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. Praha: Wolters Kluwer ČR, 2017, 248 s. ISBN 978-80-7552-823-0. Str. 9.
[162] FINANČNÍ ANALYTICKÝ ÚŘAD. *Rozhodnutí o částečném odmítnutí žádosti o informace ze dne 21. 5. 2020.* Č. j. FAU-42153/2020/031. Str. 3.
[163] ČESKÁ NÁRODNÍ BANKA. *Stanovisko k výkladu pojmu poskytování finančních služeb v České republice* [online], 2013 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/archiv_stanovisek/k_vykladu_pojmu_poskytovani_financnich_sluzeb_v_cr.pdf. Str. 2-4.

v rozhraní aplikace svým mobilním telefonem, a první platbu z účtu vedeného na jméno uživatele.[164] Revolut nemá v ČR pobočku, organizační složku ani provozovnu.

Revolut poskytuje služby českým občanům na území ČR, jedná se tedy o podporovanou zemi. Služba je přeložená do češtiny, umožňuje na účet dobíjet české koruny, na vyžádání doručuje do ČR fyzické platební karty a svou službu zde propaguje jak v médiích, tak i na veřejných akcích.[165] Za některé služby účtuje poplatky. Na základě uvedeného lze dospět k názoru, že Revolut je zahraniční osoba působící na území ČR, vykonává činnosti uvedené v § 2 odst. 1 AML zákona, vykonává svou činnost podnikatelsky a je tedy povinnou osobou.

Domnívám se, že převzetí identifikace ve smyslu § 11 odst. 2 a 3 AML zákona se v tomto případě neaplikuje, neboť finanční instituce, ze kterých probíhá první platba, po svých klientech, kteří je využijí pro aktivaci služby Revolut, nevyžadují souhlas k poskytnutí informací třetí osobě. Neprobíhá ani identifikace podle § 11 odst. 8 (eIDAS), neboť takovou možnost aplikace Revolut vůbec nepřipouští. Mohlo by se tedy jednat o identifikaci první platbou ve smyslu § 11 odst. 7. Tu lze provést za splnění několika podmínek. Klient musí zaslat povinné osobě kopie průkazu totožnosti a nejméně jednoho dalšího podpůrného dokladu, kopii dokladu potvrzujícího existenci účtu vedeného na jméno klienta, první platba se uskuteční prostřednictvím účtu, jehož existenci klient doložil, a povinná osoba nemá pochybnost o skutečné totožnosti klienta. Pro aktivaci služby ale postačuje pouze jeden doklad. Na základě těchto skutečností lze dovodit, že vzdálená identifikace provedená prostřednictvím aplikace Revolut není v souladu s AML zákonem.

3.4.2. Případ N26

N26 je německá neobanka, která nabízí velmi podobné služby jako Revolut a disponuje evropskou bankovní licencí. Pro vzdálenou identifikaci jiných než německých uživatelů N26 vyžaduje fotografii dokladu totožnosti a fotografii obličeje. Zároveň musí být zapnutá geolokace. Lze využít i identifikaci prostřednictvím videohovoru s operátorem, při kterém uživatel ukáže doklad totožnosti. Při registraci je nutné uvést zemi pobytu a adresu, kam bude

[164] How do I verify my identity?. *Revolut* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.revolut.com/help/getting-started/verifying-identity/how-do-i-verify-my-identity.
[165] Např. David Pavliska z Revolutu: V Česku cílíme na stovky tisíc uživatelů. Chystáme lokalizaci i česká čísla účtů. *CzechCrunch* [online]. 2018 [cit. 2020-06-06]. Dostupné z: https://www.czechcrunch.cz/2018/11/david-pavliska-z-revolutu-v-cesku-cilime-na-stovky-tisic-uzivatelu-chystame-lokalizaci-i-ceska-cisla-uctu/.

doručena fyzická platební karta.[166] ČR není podporovanou zemí, nicméně tento problém lze obejít uvedením rezidenční adresy v podporované zemi, například Slovensku. Na tuto adresu bude doručena platební karta. Aplikace N26 není přeložena do češtiny, nepodporuje platby v českých korunách, nemá na území ČR žádnou pobočku, organizační složku ani provozovnu či zaměstnance a své služby v ČR nepropaguje. Úvaha ohledně způsobu provedení identifikace by byla obdobná jako v případě společnosti Revolut, avšak v tomto případě není zjevné, zda je naplněn požadavek působení na území ČR. Charakter působení je v tomto případě nepochybně nižší intenzity než v případě služby Revolut. N26 své služby v ČR pouze aktivně neblokuje a rovněž počet českých uživatelů služby je oproti službě Revolut minimální. Vezmeme-li v úvahu svobodu pohybu osob v rámci evropského prostoru, je třeba vnímat i fakt, že by pro N26 (a všechny ostatní) bylo mimořádně obtížné blokovat svou službu v některém z nepodporovaných členských států a vyvarovat se přitom diskriminace na základě státní příslušnosti. Blokovala by služba občana ČR, který žije trvale na území Německa a při pobytu na území ČR by chtěl službu použít? Blokovala by Němce, který by zavítal do ČR na krátký pobyt? Blokovala by služba nákup Němce na českém e-shopu? Domnívám se, že v daném případě nelze působení N26 na území ČR považovat za působení v materiálním slova smyslu a nejedná se tak o povinnou osobu ve smyslu AML zákona.

3.4.3. Hodnocení současného stavu

V důsledku stávajícího stavu se zahraničním osobám, které poskytují svoje služby na území ČR, vyplatí nezřizovat zde pobočku, organizační složku ani provozovnu, neboť v takovém případě by na ně FAÚ uplatňoval přísnější kritéria pro vzdálenou identifikaci podle českého AML zákona. Domácím osobám by se tak paradoxně vyplatilo stát se zahraniční osobou a poskytovat služby přeshraničně. Z tohoto hlediska nezbývá než hodnotit postoj FAÚ, tedy jeho nekonání ve vztahu k trestání zahraničních osob, jako přímo diskriminační vůči domácím povinným osobám. Pokud nižší standardy vzdálené identifikace v zahraničí poskytují dostatečnou záruku před jejím zneužitím, na což zřejmě FAÚ spoléhá, měl podle mého názoru ve spolupráci s MF připravit takový návrh novely AML zákona, který by českou úpravu vzdálené identifikace zmírnil nebo poskytl nové alternativy. Přísnější úprava navíc snižuje konkurenceschopnost domácích FinTech společností a brání potenciálnímu vzniku inovací.

[166] How to prove my identity?. *N26* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://support.n26.com/en-eu/account-and-personal-details/verifying-identity/how-to-prove-my-identity.

V tomto ohledu je dále paradoxní, že přestože MF stávající stav v rámci své konzultace kritizovalo[167], v navrhovaných změnách AML zákona se nepokusilo předložit zásadnější úpravy.

[167] MINISTERSTVO FINANCÍ. *Online identifikace a AML/CFT: Podkladová studie* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/podkladova-studie-financni-technologie-a-31641. Str. 19.

4. Působnost AML zákona na vybrané FinTech služby

Některé FinTech služby bezpochyby představují potenciální nástroje pro praní špinavých peněz nebo financování terorismu.[168] To, že mohou představovat zranitelnější místa ve finančním systému ale zároveň neznamená, že k jejich zneužívání za těmito účely dochází. Z mého pohledu je v rámci této problematiky nejdůležitější vymezení osobní působnosti AML zákona.[169] Není totiž vždy zřejmé, do jakých jeho kategorií jednotlivé FinTech služby spadají, jestli v některých případech není jejich zahrnutí do působnosti zbytečné a zda pro některé z nich není možné se této působnosti vyhnout[170].

4.1. Neobanking

Neobanking představuje způsob, jak snadno a rychle realizovat domácí i zahraniční převody peněžních prostředků v různých měnách. Riziko zde může představovat jak zneužití identity, tak i faktická nemožnost zahraničních poskytovatelů finančních služeb zjistit dostatek informací o svých klientech a zamýšlené povaze jejich transakcí. Z důvodu snahy o eliminaci mzdových nákladů v oblasti *compliance* na straně poskytovatelů těchto služeb může docházet k chybám algoritmů, bezdůvodnému blokování účtů nebo věnování nedostatečné pozornosti podezřelým transakcím.[171] Tyto služby jsou často zaměřeny na větší množství drobných klientů, z čehož obvykle vyplývá nutnost provést velký počet identifikací a kontrol klienta, což může snižovat jejich výslednou kvalitu.

V případě využívání zahraničních neobank, které nemají na území ČR pobočku a jejichž součástí je i zřízení zahraničního bankovního účtu, pak může představovat problém i absence informací o těchto účtech v centrální evidenci účtů (§ 2 odst. 1 zákona o centrální evidenci účtů

---

[168] K tomu např. DE SANCTIS, Fausto Martin. *Technology-Enhanced Methods of Money Laundering*. Springer International Publishing, 2019, 174 s. ISBN 978-3-030-18329-5. Str. 136.

[169] Další otázkou by samozřejmě bylo, zda FinTech společnosti v uspokojivé míře AML pravidla dodržují. Wu uvádí, že je mnoho důkazů o jejich nedodržování, mimo jiné i v případě společnosti Ripple. WU, Yen-Te. FinTech Innovation and Anti-Money Laundering Compliance. *National Taiwan University Law Review* [online]. 2017, **12**(2), 201-258 [cit. 2020-06-06]. DOI: 10.3966/181263242017091202002. Dostupné z: http://lawdata.com.tw/tw/doi/?doi=10.3966/181263242017091202002. Str. 233-246.

[170] Vyhýbání se regulaci nebo větší přívětivost dohledových orgánů patří podle tradičních institucí k důvodům, které umožnily vzestup FinTech. PATWARDHAN, Anju. Peer-To-Peer Lending. Handbook of Blockchain, Digital Finance, and Inclusion [online]. *Elsevier*, 2018, 389-418 [cit. 2020-06-06]. DOI: 10.1016/B978-0-12-810441-5.00018-X. ISBN 9780128104415. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/B978012810441500018X. Str. 413-414.

[171] K tomu např. Revolut whistleblower had concerns over CEO conduct and compliance. *BBC*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.bbc.com/news/technology-47751945.

a contrario). Existence takových účtů a jejich souvislost se zájmovými osobami tedy nemusí být orgánům činným v trestním řízení nebo FAÚ známa. I v případě, že by takovými informacemi příslušné orgány disponovaly, musely by další potřebné údaje získávat skrze nástroje mezinárodní spolupráce, která je ze své podstaty pomalejší.

U FinTech služeb označovaných jako P2P FX představuje problém samotná skutečnost, že i přes faktické vyvádění peněžních prostředků do zahraničí dochází pouze k realizaci domácích bankovních převodů a informacemi, které propojují odesílatele a konečného příjemce, disponuje pouze poskytovatel P2P FX služeb. V případě zpětné analýzy převodů peněžních prostředků zájmových osob nebude zřejmé, která z domácích plateb mohla směřovat na účet poskytovatele P2P FX služeb a tedy i fakticky do zahraničí. Dotčené orgány by musely disponovat znalostí o těchto poskytovatelích a o jejich bankovních účtech. Rozkrývání peněžních toků by tak ztěžovala nutnost spočívající ve spolupráci poskytovatele. V případě jeho neochoty by pak bylo mnohdy nutné využít nástrojů mezinárodní spolupráce, neboť tyto služby jsou často poskytovány přeshraničně.

4.1.1. Působnost AML zákona

Neobanking je obvykle realizován pomocí poskytování platebních služeb, vydávání elektronických peněz nebo na základě bankovní licence. Z těchto titulů tyto služby spadají do působnosti AML zákona (§ 2 odst. 1 písm. a) bod 1 a písm. b) bod 5 AML zákona).

V tomto ohledu zasluhuje samostatnou pozornost již zmíněné otevřené bankovnictví. Podle § 2 odst. 1 písm. b) bod 5 AML zákona je povinnou osobou i osoba oprávněná k poskytování platebních služeb. Podle § 3 odst. 1 písm. g) a h) ZPS jsou platebními službami jak služba nepřímého dání platebního příkazu, tak služba informování o platebním účtu. Není tak žádných pochyb o tom, že povinnou osobou jsou i poskytovatelé služeb otevřeného bankovnictví. Je zde ale působnost AML zákona nezbytná? Pro využití těchto služeb musí uživatel projít skrze příslušnou aplikaci stejným procesem jako v případě přihlášení do internetového bankovnictví. V něm zároveň musí potvrdit souhlas s přístupem třetích stran ke svému účtu. Zabezpečení přihlášení a autentizace uživatele jsou tak na stejné úrovni jako bez využití služeb otevřeného bankovnictví. Přes tyto služby žádné peněžní prostředky neprochází, pouze dochází k dání platebního příkazu jménem plátce vůči jinému poskytovateli, který vede platební účet plátce a na kterého již AML pravidla dopadají. Zároveň platí, že podle § 161 odst. 3 písm. a) ZPS má poskytovatel, který vede plátci platební účet, právo na odmítnutí nepřímo daného platebního

příkazu, jestliže má podezření na zneužití platebního prostředku nebo osobních bezpečnostních prvků uživatele. Služba informování o platebním účtu je pak z pohledu praní špinavých peněz zcela irelevantní, neboť jejím prostřednictvím dochází pouze ke sdělování informací o platebním účtu (zůstatek, provedené transakce apod.), což ostatně uvádí i Evropská komise.[172]

4.1.2. Případ TransferWise

TransferWise je britská společnost založená v roce 2010, která se specializuje na levnější měnové konverze a převody peněžních prostředků do zahraničí. Jak již bylo nastíněno, tyto P2P FX služby jsou založeny na párování protijdoucích plateb a faktické mezinárodní převody využívají pouze k občasnému vyrovnávání bilancí. TransferWise disponuje licencí instituce elektronických peněz a licencí poskytovatele platebních služeb. Svým klientům poskytuje multiměnový platební účet elektronických peněz.[173] Jak sama služba uvádí, princip v zásadě odpovídá neformálnímu platebnímu systému *hawala*, avšak na rozdíl od něj se nejedná o vyhýbání se standardnímu finančnímu systému, neboť všechny peníze prochází skrze lokální bankovní účty.[174]

Podle mého názoru lze právně popsat celý proces tak, že převodem peněžních prostředků na lokální bankovní účet vedený na jméno společnosti dochází k vydání elektronických peněz. Ty představují pohledávku vůči společnosti a v okamžiku připsání požadované měny na zahraniční účet pomocí tamějšího bankovního účtu společnosti dojde ke splnění této pohledávky. To sice prostřednictvím peněžních prostředků jiného původu a v jiné měně, ale ve výši odpovídající směnnému kurzu, který je mírně upraven, neboť rozdíl mezi autentickým směnným kurzem a aplikovaným směnným kurzem tvoří odměnu společnosti. Otázkou by mohlo být, zda je v tomto případě naplněno kritérium elektronických peněz obsažené v § 4 odst. 1 písm. d) ZPS, tedy že elektronické peníze jsou přijímány jinou osobou než tím, kdo je vydal. Může se totiž zdát, že nedochází k přijímání elektronických peněz jinými osobami, ale pouze k realizaci pohledávky klienta vůči emitentovi elektronických peněz.

---

[172] EVROPSKÁ KOMISE. *Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1570190003049&uri=CELEX:52019SC0650. Str. 89.

[173] How is the multi-currency account different than a bank account?. *TransferWise* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://transferwise.com/help/17/borderless-account/2736035/how-is-a-borderless-account-different-than-a-bank-account.

[174] How does the Hawala money transfer systém work?. *TransferWise* [online]. 2018 [cit. 2020-06-06]. Dostupné z: https://transferwise.com/gb/blog/what-is-hawala.

V každém případě by TransferWise díky svým licencím povinnou osobou z hlediska AML zákona byl. Vzhledem k tomu, že v ČR nemá tato společnost žádné zastoupení, ale její služby zde využívat lze, se opakuje problém související s působností AML zákona, který jsem již v této práci demonstroval.

4.1.3. Dílčí závěr

I přes zahrnutí poskytovatelů platebních služeb do působnosti AML zákona považuje Evropská komise rizika související s praním špinavých peněz a financováním terorismu za významná. Komise se v této souvislosti bude zabývat společným evropským rámcem pro elektronickou identifikaci a kontrolu klienta. Členským státům doporučuje provádět kontroly systémů vnitřních zásad a hodnocení rizik a zrušit hranice transakcí, při jejichž nedosažení neprobíhá kontrola klienta.[175] Domnívám se však, že v případě nutnosti provádět plnohodnotnou kontrolu klienta ve všech případech by v důsledku došlo k eliminaci malých poskytovatelů platebních služeb.

S ohledem na povahu služeb nepřímého dání platebního příkazu a informování o platebním účtu zastávám názor, že by bylo po vzoru Estonska[176] vhodné těmto službám udělit výslovnou výjimku z působnosti AML zákona. Částečné nebo úplné vynětí služeb otevřeného bankovnictví z působnosti AML zákona podpořila i většina účastníků konzultace MF.[177]

Je třeba zdůraznit, že FinTech platformy, které by provozovaly neformální platební systém *hawala* nebo jiné obdobné systémy, by nemohly být vnímány jako legální, neboť tyto systémy jsou obecně považovány za obcházení regulace platebních služeb.[178] Z hlediska praní špinavých peněz a financování terorismu by problém mohla představovat i taková platforma,

---

[175] EVROPSKÁ KOMISE. *Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1570190003049&uri=CELEX:52019SC0650. Str. 95-96.

[176] MINISTERSTVO FINANCÍ. *Online identifikace a AML/CFT: Podkladová studie* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/podkladova-studie-financni-technologie-a-31641. Str. 21.

[177] MINISTERSTVO FINANCÍ. *Finanční trh a online identifikace a AML/CFT: Vyhodnocení konzultace* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/financni-trh-a-online-identifikace-a-aml-32102. Str. 4.

[178] EVROPSKÁ KOMISE. *Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1570190003049&uri=CELEX:52019SC0650. Str. 86.

která by platební služby sama neposkytovala, ale pouze by propojovala hawaladary[179] navzájem mezi sebou, případně i s jejich stávajícími nebo potenciálními klienty. V konečném důsledku by došlo ke zjednodušení přístupu k tomuto platebnímu systému a jeho zefektivnění, a to mimo působnost AML pravidel, což by samozřejmě bylo nežádoucí.

4.2. Crowdfunding

V případě crowdfundingu největší riziko z pohledu AML představuje možné zneužití platforem k financování terorismu. Teoreticky může skrze crowdfunding docházet i k zastření původu peněz (layering) nebo k jejich investování do legálních činností (integration). Ten, kdo by chtěl crowdfunding pro takové účely zneužít, může být bez vědomí platformy dárcem nebo investorem i vlastníkem financovaného projektu najednou. V takovém případě může docházet například v rámci úvěrového crowdfundingu k investicím špinavých peněz do mnoha malých úvěrů, které slibují nízký úrok (aby odradily skutečné investory) a mají krátkou dobu splatnosti. Takové úvěry si pachatelé vzájemně a koordinovaně financují a získávají své očištěné peníze zpět prostřednictvím splátek jistin a úroků.[180] Rizika obecně mohou narůstat v případě, že projekty lze financovat například pomocí kryptoměn nebo elektronických peněz.

Je potřeba rozlišovat crowdfunding, na který dopadá obecná nebo speciální právní úprava (typicky investiční crowdfunding), a dále neregulovaný crowdfunding. Tato druhá skupina podle Evropské komise zahrnuje i platformy, které crowdfunding samy fakticky neprovádí, ale zprostředkovávají kontakt mezi dárci či investory a vlastníky projektů.[181] Pro demonstraci dopadu AML zákona na crowdfunding v následujícím textu objasním obchodní modely dvou českých crowdfundingových platforem.

4.2.1. Případ Hithit

Hithit je webový portál, na kterém jsou inzerovány projekty poptávající financování od veřejnosti. Přispěvatelé volí výši částky, kterou chtějí zaplatit, a s tím spojené protiplnění,

---

[179] Hawaladar je prostředník, který v rámci platebního systému *hawala* přijímá a vydává hotovost a po určité době vyrovnává vzájemnou bilanci s jinými hawaladary.

[180] XIAO, Zhao, Yuelei LI a Kang ZHANG. Visual analysis of risks in peer-to-peer lending market. *Personal and Ubiquitous Computing* [online]. Springer London, 2018, **22**(4), 825-838 [cit. 2020-06-06]. DOI: 10.1007/s00779-018-1165-y. ISSN 1617-4909. Dostupné z: http://link.springer.com/10.1007/s00779-018-1165-y. Str. 828-829.

[181] EVROPSKÁ KOMISE. *Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1570190003049&uri=CELEX:52019SC0650. Str. 61.

které získají od vlastníka projektu v případě, že je tento projekt po dosažení poptávané částky realizován. Jedná se tedy o odměnový crowdfunding. Při nedosažení cílové částky projektu obdrží přispěvatelé svoje peníze zpět. Vlastníci projektů v případě úspěšného naplnění cílové částky hradí provozovateli portálu provizi ve výši 9 % z celkové částky. Platby přispěvatelů se shromažďují na platebním účtu vedeném společností ComGate Payments. V případě naplnění nebo přesažení cílové částky jsou peníze odeslány na účet vlastníka projektu. Vlastník projektu se zavazuje, že uvedenému poskytovateli platebních služeb poskytne veškerou součinnost pro účely provedení identifikace ve smyslu AML zákona. Provozovatel v obchodních podmínkách uvádí, že nenese žádnou odpovědnost z hlediska AML zákona a není povinen zjišťovat původ finančních prostředků použitých v rámci projektu.[182]

Je zjevné, že společnost Hithit není povinnou osobou z hlediska AML zákona. Přestože se jedná o podnikání, činnost spočívající v inzerování projektů poptávajících financování nebo vzájemné propojování přispěvatelů a vlastníků projektů ve výčtu uvedeném v § 2 AML zákona nenalezneme. Třetí osoba coby poskytovatel platebních služeb ve smyslu ZPS nicméně povinnou osobou podle § 2 odst. 1 písm. b) bod 5 AML zákona je. Nabízí se otázka, zda tato třetí strana disponuje dostatečnými informacemi o přispěvatelích pro účely naplnění povinností stanovených AML zákonem. Zatímco součástí obchodních podmínek je explicitně zdůrazněná povinnost identifikace vlastníka projektu při převádění cílové částky na účet vedený na jeho jméno, o identifikaci a kontrole přispěvatelů Hithit informace neposkytuje. Přispět lze přitom i částkou převyšující 1000 EUR. Při pokusu o zaplacení příspěvku ve výši 150 000 Kč došlo ihned po poskytnutí jména a emailu k přesměrování na platební bránu. Není tak zřejmé, zda identifikace a kontrola přispěvatelů probíhá. Platby přispěvatelů a jejich shromažďování je přitom nutno vnímat jako obchod ve smyslu § 4 odst. 1 AML zákona, neboť jde o jednání poskytovatele platebních služeb, které směřuje k nakládání s majetkem přispěvatelů. Z mého pohledu není rozhodující, zda poskytovatel platebních služeb získá provizi od crowdfundingové platformy nebo od přispěvatelů.

4.2.2. Případ Bankerat

Bankerat je nejstarší platforma úvěrového crowdfundingu v ČR. Vzájemně propojuje osoby poptávající peníze (vydlužitele) a osoby, které jim část nebo celou částku nabízejí (zapůjčitele).

[182] Obchodní podmínky společnosti Hithit s.r.o. *Hithit* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.hithit.com/cs/article/terms.

V případě oboustranného zájmu mezi nimi dojde k uzavření smlouvy o zápůjčce. Platforma získá provizi a administruje vzájemné platby, případně vymáhá jménem zapůjčitele dlužné částky. Zapůjčitel zná identitu vydlužitele a sám ověřuje jeho bonitu. Platforma neposkytuje žádné informace o případných povinnostech vyplývajících z AML zákona.[183]

Jedná se o jednu z nejautentičtějších forem P2P úvěrování. Pro některé konkurenční platformy je typické výrazně větší zapojení do celého procesu. Existují modely, v rámci kterých se investoři nestávají věřitelem dlužníka, ale uzavírají inominátní smlouvu s platformou, kterou na sebe přenášejí riziko vyplývající z možného nesplácení dlužníků, kterým sama platforma nebo její spřízněná osoba poskytla úvěr. Za to jsou investoři odměněni částkou, která odpovídá poměrné části z úroků splácených dlužníkem platformě. Kromě toho existují i modely, které jsou založeny na postupování pohledávek. V takovém případě platforma nebo její spřízněná osoba poskytne standardní úvěr a vzniklou pohledávku nebo její poměrnou část postupuje investorům. Výhodou těchto modelů je výrazně vyšší rychlost celého procesu, neboť k poskytnutí úvěru dojde ihned. Následná participace investorů pak umožňuje platformám širší diverzifikaci úvěrového rizika. Platformy obvykle administrují všechny související platby, posuzují úvěryschopnost dlužníků a mají na starost i vymáhání pohledávek. Věřitelé zpravidla neznají identitu dlužníků z důvodu jejich ochrany.

Jak v případě obchodního modelu, který provozuje společnost Bankerat, tak i u dalších obdobných modelů dochází vždy minimálně k poskytování platebních služeb. V případě, že platforma nebo její spřízněná osoba sama poskytuje úvěry, stává se povinnou osobou i z tohoto důvodu (§ 2 odst. 1 písm. b) bod 6 AML zákona). Teoreticky by mohla vzniknout i taková platforma úvěrového crowdfundingu, která by platební služby neprováděla a pouze by umožnila propojení zapůjčitelů a vydlužitelů (případně úvěrujících a úvěrovaných), kteří by platby prováděli přímo mezi svými platebními účty. V takovém případě by byl pravděpodobně zpoplatněn samotný přístup na platformu. Povinnými osobami by v takovém případě byli poskytovatelé platebních služeb zapůjčitelů i vydlužitelů, nikoliv samotná platforma. Zatím se ovšem takový model neobjevil, nebo je z hlediska své velikosti marginální.

[183] Časté otázky a odpovědi. *Bankerat* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.bankerat.cz/investice/caste-otazky-a-odpovedi/.

4.2.3. Dílčí závěr

I v rámci crowdfundingu lze v některých případech pozorovat trend typický pro tzv. „*sdílenou ekonomiku*“, který se projevuje snahou podnikatelů stát se pouhým zprostředkovatelem služeb, který má minimální odpovědnost a ignoruje aplikovatelnou sektorovou regulaci.[184] Přestože provozovatelé crowdfundingových platforem v některých případech sami o sobě do působnosti AML zákona nespadají, díky povaze souvisejících právních jednání se jí účastníci crowdfundingu zpravidla nevyhnou. Nejčastěji se bude jednat o poskytování platebních služeb, ale může jít i o účast nebankovních poskytovatelů spotřebitelských úvěrů nebo obchodníků s cennými papíry v případě investičního crowdfundingu.

Nutno zmínit také v současnosti připravované nařízení o evropských poskytovatelích služeb skupinového financování pro podniky. To se bude vztahovat na úvěrový crowdfunding (ale pouze v dimenzi P2B) a na investiční crowdfunding. Nařízení přinese pravidla pro licencování a dojde k zavedení některých obezřetnostních požadavků na straně „*poskytovatelů služeb skupinového financování*“. Poskytovatelé budou muset doložit mimo jiné neexistenci záznamů v rejstříku trestů za tresty uložené v souvislosti s porušením předpisů v oblasti boje proti praní peněz u všech osob zapojených do řízení společnosti.[185]

Britské národní hodnocení rizik sice crowdfunding považuje za potenciálně zneužitelný, a to zejména pro financování terorismu, ale takové případy ještě nebyly zaznamenány.[186] Evropská komise vyhodnotila riziko zneužití crowdfundingu k praní špinavých peněz nebo financování terorismu jako středně významné a doporučuje členským státům zvážit, zda nezahrnout poskytovatele neregulovaného crowdfundingu mezi povinné osoby.[187] Takové doporučení jistě nelze jednoduše odmítnout, nicméně dopadem takového kroku by mohlo být ukončení činnosti některých crowdfundingových platforem. Nejdříve by proto mělo dojít k vyhodnocení

---

[184] K tomu např. MATOCHA, Jakub a Jakub SVOBODA. Nevymezený pojem sdílené ekonomiky jako nástroj k obcházení regulace. In: PICHRT, Jan, BOHÁČ, Radim a MORÁVEK, Jakub. *Sdílená ekonomika – sdílený právní problém?*. Praha: Wolters Kluwer ČR, 2017, 336 s. ISBN 978-80-7552-874-2. Str. 222-225.

[185] EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady (EU) 2018/0048 ze dne 8. 3. 2018 o evropských poskytovatelích služeb skupinového financování pro podniky* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0113&from=CS.

[186] HM TREASURY. *National risk assessment of money laundering and terrorist financing 2017* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017. Str. 41.

[187] EVROPSKÁ KOMISE. *Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1570190003049&uri=CELEX:52019SC0650. Str. 65.

dodržování stávajících povinností vyplývajících z AML zákona ze strany platforem a dalších entit, které na celém procesu participují.

4.3. Kryptoaktiva

Jako nejčastější riziko spojené s kryptoměnami se uvádí anonymita účastníků transakcí a plateb.[188] Jednotlivé transakce mezi uživateli ve většině případů anonymní skutečně jsou. Lze nicméně analyzovat veřejně dostupná data o transakcích a na jejich základě vysledovat množinu všech transakcí konkrétního uživatele. V takovém případě postačí, pokud kterýkoliv dotčený účastník transakcí poskytne informace o identitě zájmové osoby. Existují ovšem metody, jak míru anonymity zvýšit.[189] FAÚ již v roce 2013 (tehdy jako Finanční analytický útvar Ministerstva financí) vydal metodický pokyn o přístupu povinných osob k digitálním měnám, kde označil využití digitálních měn nad rámec stanovených limitů pro platby za významný rizikový faktor. Transakce nad 15 000 EUR měla být podle metodického pokynu oznámena vždy jako podezřelý obchod.[190]

V případě stablecoins, které na rozdíl od kryptoměn lépe plní funkci měny coby uchovatele hodnoty, hlavní riziko představuje jejich masové rozšíření.[191] Tím by mohlo dojít ke vzniku nadnárodních alternativních platebních systémů mimo dosah státních orgánů a částečnému nahrazení zákonných měn. Kromě ohrožení v oblastech finanční stability, daňových úniků nebo kyberbezpečnosti by nepochybně došlo i k popření stávající podoby systému boje proti

[188] Např. GOVERNMENT OFFICES OF SWEDEN. *National Risk Assessment of Money Laundering and Terrorist Financing in Sweden* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.government.se/4aed70/contentassets/70c9762f411144dbbaf1020b1a5425b3/swedish-national-risk-assessment-2019-english-20191205-.pdf. Str. 11.
[189] LÁNSKÝ, Jan. *Kryptoměny*. Praha: C. H. Beck, 2018, 160 s. ISBN 978-80-7400-722-4. Str. 57.
[190] MINISTERSTVO FINANCÍ. *Metodický pokyn č. 2 Finančního analytického útvaru Ministerstva financí: O přístupu povinných osob k digitálním měnám* [online], 2013 [cit. 2020-06-06]. Dostupné z: http://www.financnianalytickyurad.cz/download/FileUploadComponent-1133285150/1506340773_cs_1481699516_cs_2-pokyn-mf_c-002_2013-09_metodicky-pokyn-o-pristupu-povinnych-osob-k-digitalnim-menam.pdf.
[191] Takové riziko by představovalo i masové rozšíření kryptoměn, avšak díky jejich cenové volatilitě se v současnosti jedná o nepravděpodobný scénář.

praní špinavých peněz a financování terorismu.[192] Taková rizika představovalo především potenciální rozšíření projektu Libra.[193]

4.3.1. Působnost AML zákona

Povinnou osobou je podle § 2 odst. 1 písm. l) AML zákona i ten, kdo poskytuje služby spojené s virtuální měnou. Podle stejného ustanovení se virtuální měnou rozumí „*elektronicky uchovávaná jednotka bez ohledu na to, zda má nebo nemá emitenta, a která není peněžním prostředkem podle zákona o platebním styku, ale je přijímána jako platba za zboží nebo služby i jinou osobou odlišnou od jejího emitenta*."

Nutno podotknout, že AMLD4 definici virtuálních měn neobsahovala. Tuto definici přinesla až AMLD5, a to v podobě srovnatelné se stávajícím zněním AML zákona. Navrhovaná novela AML zákona ale pojem virtuální měna opouští a zavádí širší pojem virtuální aktivum, čímž následuje doporučení FATF[194] a explicitně zdůrazňuje nejen platební, ale i investiční funkci virtuálních aktiv. Podle definice obsažené v § 4 odst. 9 navrhované podoby AML zákona se virtuálním aktivem rozumí „*elektronicky uchovatelná nebo převoditelná jednotka, která je způsobilá plnit platební, směnnou nebo investiční funkci, bez ohledu na to, zda má nebo nemá emitenta*". Zároveň se nesmí jednat o cenné papíry, investiční nástroje, bankovky, mince, bezhotovostní peněžní prostředky, některé prostředky podle ZPS, kterými lze zaplatit pouze za úzce vymezený okruh zboží nebo služeb (prostředky určené pouze k vnitrostátní platbě, které se týkají stravování poskytovaného zaměstnavatelem, fondu kulturních a sociálních potřeb poskytovaného zaměstnavatelem nebo výplaty dávek pomoci v hmotné nouzi) a nakonec jednotky, pomocí kterých dochází k platbě prováděné poskytovatelem služby elektronických komunikací nebo operátorem, pokud slouží k zaplacení za digitální obsah, hlasové služby

[192] FINANCIAL STABILITY BOARD. *Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fsb.org/wp-content/uploads/P140420-1.pdf. Str. 6.
[193] STATT, Nick. Facebook confirms it will launch a cryptocurrency called Libra in 2020. *The Verge*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.theverge.com/2019/6/18/18682290/facebook-libra-cryptocurrency-visa-mastercard-digital-currency-calibra-wallet-announce.
[194] FATF. *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf. Str. 55-57.

a vstupenky nebo k platbě pro charitativní účely a nepřesahují limity 50 EUR za platbu a celkově 300 EUR měsíčně.[195]

Současně se novelou AML zákona navrhuje i změna definice osoby poskytující služby spojené s virtuálním aktivem. Nově se podle § 4 odst. 8 AML zákona touto osobou rozumí ten, kdo jako předmět své podnikatelské činnosti „*kupuje, prodává, uchovává, pro jiného spravuje, převádí nebo zprostředkovává nákup nebo prodej virtuálního aktiva, poskytuje finanční služby týkající se nabídky nebo prodeje virtuálních aktiv, případně poskytuje jiné obdobné služby spojené s virtuálním aktivem*“. Přibylo „*převádění virtuálních aktiv*“ a taktéž „*poskytování finančních služeb týkajících se nabídky nebo prodeje virtuálních aktiv*“.[196] Pod převáděním jistě můžeme chápat směnu virtuálních aktiv za virtuální aktiva jiné osoby. Poskytování finančních služeb týkajících se nabídky nebo prodeje virtuálních aktiv pak dle mého názoru může zahrnovat například i provozování portálu, který by vzájemně propojoval osoby nabízející virtuální aktiva a osoby poptávající virtuální aktiva, aniž by do probíhajících převodů přímo zasahoval. V této souvislosti se nabízí myšlenka, že takový portál by nemusel být vytvořen jen jako podnikatelský projekt, ale i z altruismu. V takovém případě by do působnosti AML zákona nespadal, ale zprostředkovával by přitom možnost anonymní směny virtuálních aktiv za jiná virtuální aktiva.

Jedná se opět o přijetí definice FATF[197]. Ta u znaků poskytovatele služeb souvisejících s virtuálními aktivy explicitně zmiňuje směnu mezi jednou a více formami virtuálních aktiv a je tak širší než definice obsažená v AMLD5. Podle článku 1 odst. 1 písm. c) AMLD5 se totiž sice doplňuje seznam povinných osob o „*poskytovatele směnárenských služeb mezi virtuálními měnami a měnami s nuceným oběhem*“, avšak z mého pohledu je nutné toto ustanovení interpretovat s ohledem na znění recitálu 8 AMLD5 restriktivně, tedy že směnárenské služby spočívající ve směně virtuální měny za jinou virtuální měnu pod tuto definici nespadají.

---

[195] MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

[196] Tamtéž.

[197] FATF. *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf. Str. 57.

4.3.2. Stablecoins jako elektronické peníze?

Jak již bylo uvedeno, stablecoins jsou pevně navázány na podkladová aktiva nebo algoritmy automatického emitování a odkupování mincí, což by mělo zaručit jejich cenovou stabilitu. Některé stablecoins jsou spjaty přímo s konkrétní zákonnou měnou, nejčastěji s americkým dolarem. Nabízí se proto otázka, zda stablecoins nemohou naplnit definici elektronických peněz. Její zodpovězení může determinovat nejen pod jaký typ povinné osoby ve smyslu AML zákona lze emitenty stablecoins zařadit, ale i zda se nevyhýbají regulaci související s vydáváním elektronických peněz vyplývající ze ZPS.

Podle § 4 odst. 1 ZPS je elektronickými penězi „*peněžní hodnota, která představuje pohledávku vůči tomu, kdo ji vydal, je uchovávána elektronicky, je vydávána proti přijetí peněžních prostředků za účelem provádění platebních transakcí a je přijímána jinou osobou než tím, kdo ji vydal*“.

Posouzení, zda může dojít k naplnění této definice, lze demonstrovat na stablecoins s názvem Tether USD, které jsou navázány na americký dolar v poměru jedna ku jedné. Tokeny jsou uchovávány na blockchainu a je tedy zřejmé, že jsou uchovávány elektronicky. Stablecoins Tether USD jsou vydávány výhradně proti přijetí peněžních prostředků, amerických dolarů, lze je převádět na další osoby a jsou akceptovány například v internetových kryptosměnárnách. Jsou tedy přijímány i jinými osobami. Zpětné vydání amerických dolarů za tokeny je smluvním nárokem zákazníka.[198] Domnívám se, že Tether USD může být považován za elektronické peníze podle ZPS. FCA dokonce přichází se zvláštním pojmem „*e-money tokens*“ pro kryptoaktiva, která naplňují definici elektronických peněz. Zároveň zdůrazňuje, že elektronickými penězi jsou pouze některé stablecoins, a tuto otázku je nutno posuzovat případ od případu.[199]

Pokud by se však někteří emitenti stablecoins chtěli povinnostem souvisejícím s vydáváním elektronických peněz vyhnout, mohli by například přijímáním zákonných peněz a jejich zpětným vydáváním pověřit jinou smluvně zavázanou entitu. Nárok zákazníka na zpětnou výměnu by tak nesměřoval vůči tomu, kdo stablecoins vydal, ale vůči jiné entitě. EBA ale

---

[198] Terms of Service. *Tether Operations Limited* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://tether.to/legal/.

[199] FINANCIAL CONDUCT AUTHORITY. *Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/publication/policy/ps19-22.pdf. Str. 18-19.

ve svém stanovisku uvádí, že jestliže ten, kdo zastupuje vydavatele elektronických peněz, získá peněžní prostředky od zákazníka za účelem jejich výměny za elektronické peníze, má se za to, že tyto prostředky byly přijaty samotným vydavatelem, neboť zmíněný zástupce (distributor) vystupuje jeho jménem.[200] Tento názor lze podle mého názoru analogicky aplikovat i na uplatnění pohledávky při zpětné výměně za zákonnou měnu.

Další otázkou by mohlo být, zda lze za elektronické peníze považovat takové stablecoins, jejichž hodnota může v čase klesat nebo stoupat a jejichž emitent by se zavázal při případné zpětné výměně vracet pouze peníze v takové výši, která odpovídá aktuální hodnotě stablecoins. Jednalo by se sice o pohledávku vůči emitentovi, ovšem ne zcela plnohodnotnou.

4.3.3. Dílčí závěr

Podle Evropské komise představují kryptoaktiva významné riziko v oblasti praní špinavých peněz a financování terorismu.[201] Podle hodnotící zprávy Výboru expertů pro hodnocení opatření proti praní špinavých peněz a financování terorismu Rady Evropy (MONEYVAL) se ale zatím v ČR žádný případ zneužití virtuální měny k praní špinavých peněz neobjevil.[202] Podobně hovoří i britské národní hodnocení rizik, podle kterého je zneužití digitálních měn sice obvyklé v rámci kybernetické trestné činnosti, avšak riziko jejich zneužití pro účely praní špinavých peněž a financování terorismu je nízké.[203] České národní hodnocení rizik v roce 2016 upozorňovalo na vysokou zranitelnost vyplývající z nezahrnutí poskytovatelů služeb s virtuální měnou mezi povinné osoby a v této souvislosti zdůraznilo i možná korupční rizika.[204]

---

[200] EBA. *Opinion of the European Banking Authority on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD)* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/da05ad8a-eed2-410a-bd08-072403d086f3/EBA%20Opinion%20.pdf?retry=1. Str. 6.

[201] EVROPSKÁ KOMISE. *Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1570190003049&uri=CELEX:52019SC0650. Str. 101.

[202] MONEYVAL. *Anti-money laundering and counter-terrorist financing measures: Czech Republic (Fifth Round Mutual Evaluation Report)* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.coe.int/en/web/moneyval/-/combatting-money-laundering-in-the-czech-republic-despite-progress-more-investigations-are-needed-says-council-of-europe-report. Str. 110.

[203] HM TREASURY. *National risk assessment of money laundering and terrorist financing 2017* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017. Str. 40-41.

[204] FINANČNÍ ANALYTICKÝ ÚŘAD. *Národní hodnocení rizik: Zpráva o prvním kole procesu Národního hodnocení rizik praní peněz a financování terorismu (veřejná verze)* [online], 2016 [cit. 2020-06-06]. Dostupné z: http://www.financnianalytickyurad.cz/hodnoceni-rizik/narodni-hodnoceni-rizik.html. Str. 101.

Podle mého názoru je vysoce pravděpodobné, že k rozšíření definice virtuální měny či aktiva by tak jako tak ze strany EU v následující (jistě už připravované) směrnici proti praní špinavých peněz došlo. Navrhovaná podoba AML zákona, která plně přebírá definice z doporučení FATF, tak paradoxně do budoucna může přinést určitou jistotu adresátů normy v tom, že AML zákon se v této věci nebude každé dva roky novelizovat. Kryptoaktiva zahrnují širokou škálu modelů, z nichž některé mohou naplňovat i tradiční zákonné definice (například elektronických peněz nebo investičních nástrojů). Ve zbytku lze s ohledem na rizika praní špinavých peněz a financování terorismu zavedení velmi široké obecné definice virtuálních aktiv považovat za nevyhnutelné. Dále je nutno konstatovat, že i přes zahrnutí osob, které poskytují služby spojené s kryptoaktivy, mezi povinné osoby ve smyslu AML zákona nelze zabránit tomu, že vlastníci kryptoaktiv si budou navzájem vyměňovat přístupové privátní klíče nebo je prodávat bez využití služeb směnáren. Zároveň lze očekávat, že po zavedení souvisejících povinností vyplývajících z AML pravidel dojde ke snížení zájmu o kryptoaktiva celkově, neboť svoboda, soukromí, nezávislost na státu, případně konkurování jeho funkcím patří často mezi důvody, kvůli kterým některá kryptoaktiva vznikla nebo se stala populární.[205]

[205] FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2018, 214 s. ISBN 978-1-108-60970-8. Str. 35.

Závěr

Praní špinavých peněz je inherentní součástí globalizovaného světa a nevyhýbá se ani oblasti FinTech. Snaha o poskytování inovativních, jednoduše přístupných a pro spotřebitele přívětivých finančních služeb často naráží na stále přísnější pravidla sledující prevenci před praním špinavých peněz a financováním terorismu. Cílem této práce proto bylo dopad těchto pravidel objasnit a kriticky je zhodnotit.

Společnosti, které inovace do finančního sektoru přinášejí, jsou přínosem jak pro ekonomiku, tak pro spotřebitele. To si na rozdíl od ČR uvědomují země jako například Velká Británie nebo Singapur, které se snaží inovačním službám usnadnit vstup do vysoce regulovaného odvětví. Přístup zastávající technologickou neutralitu a odmítající nerovný přístup je sice zásadově správný, nicméně v konečném důsledku může zvýhodňovat největší účastníky trhu, kteří těží z úspor z rozsahu a existence bariér pro vstup na trh. FinTech společnosti mají obvykle nadnárodní ambice a méně přívětivý přístup jejich domovského státu je může znevýhodňovat oproti zahraniční konkurenci.

Navrhovaná novela českého AML zákona, která implementuje pátou směrnici proti praní špinavých peněz, přináší změny v oblasti identifikace a kontroly klienta. Dochází ke zpřísnění podmínek zjednodušené identifikace a kontroly klienta a k dalšímu snížení hranic pro výjimky z této povinnosti. Jak jsem však demonstroval na statistikách státního zastupitelství, ke zneužívání předplacených karet, které do těchto výjimek spadají, k legalizačním trestným činům v ČR i přes jejich tvrzenou vysokou rizikovost nedochází. Podle mého názoru tato změna může předplacené karty zcela eliminovat.

Podstatnou součástí procesu kontroly klienta jsou lustrace veřejných rejstříků. Z pohledu FinTech společností, které jsou závislé na co nejvyšší možné míře automatizace procesů, došlo v minulém roce k výraznému posunu, který způsobilo otevření API obchodního rejstříku. Domnívám se, že pokračování ve vzájemném propojování veřejných rejstříků a poskytování otevřených dat je žádoucí, a to nejen z pohledu povinných osob. Celý proces by mohl být ještě efektivnější, pokud by do výpisů z obchodního rejstříku byli od určité hranice podílu na společnosti zapisováni i její akcionáři.

Zjišťování, zda je klient politicky exponovanou osobou, je poměrně nákladné. V této souvislosti nelze souhlasit s názorem FAÚ, že pro účely splnění této povinnosti postačuje

prohlášení klienta. Zájmem kteréhokoliv klienta je totiž nebýt považován za politicky exponovanou osobu. V závislosti na vyhodnocení rizikovosti obchodního vztahu by proto měla povinná osoba tuto skutečnost přiměřeným způsobem zjišťovat sama. V této souvislosti jsem za účelem snížení nákladů povinných osob a zvýšení efektivity boje proti praní špinavých peněz a financování terorismu navrhl zřízení celoevropské neveřejné databáze některých politicky exponovaných osob.

V souvislosti s evidencí skutečných majitelů kriticky hodnotím postoje ministerstva spravedlnosti. Ministerstvo s ohledem na ochranu osobních údajů povinným osobám neumožňuje alespoň do určité míry automatizovaný sběr dat z této evidence. Dále nemá samo jasno v tom, zda v budoucnu, po přijetí zákona o evidenci skutečných majitelů, bude poskytovat data z této evidence ve formě otevřených dat, nebo ne. Podle mého názoru je úsměvné argumentovat citlivou povahou údajů v evidenci skutečných majitelů, pokud vezmeme v potaz připravované otevření většiny dat z této evidence veřejnosti a též samotnou existenci obchodního rejstříku s osobními údaji, které obsahuje. Ty přitom ministerstvo hromadně a volně poskytuje veřejnosti. Nevidím důvod, proč by měla být poskytována skutečným majitelům větší ochrana než společníkům a statutárním orgánům zapsaným v obchodním rejstříku. Do budoucna by podle mého názoru bylo za účelem zefektivnění procesu zjišťování skutečného majitele vhodné skrze evropské centrální místo, například BRIS nebo jinou obdobnou platformu, umožnit povinným osobám pokud možno automatizovaný přístup k evidencím skutečných majitelů všech členských států.

Je nepochybné, že úprava vzdálené identifikace klienta podle účinné podoby AML zákona je pro FinTech společnosti zásadní překážkou. V rámci identifikace první platbou ministerstvo financí trvá i v rámci novely na iracionálním požadavku druhého podpůrného dokladu a navrhuje proces ještě více znesnadnit povinností vyplňovat doprovodné informace při provádění první platby. V rámci identifikace klienta podle § 11 odst. 8 AML zákona, která je reálně nepoužitelná, ministerstvo navrhuje změny, které situaci nezlepšují. Přínosnější jsou v tomto ohledu dva nově schválené, ale ještě neúčinné způsoby vzdálené identifikace.

Identifikace prostředkem pro elektronickou identifikaci, který splňuje standardy pro vysokou úroveň záruky, bude hrát významnější roli ve chvíli, kdy budou v populaci rozšířeny nové elektronické občanské průkazy, neboť vysoké úrovně záruky v současnosti dosahuje pouze jediný komerční produkt. Tento způsob identifikace činí výše uvedený § 11 odst. 8 AML zákona zbytečným. Druhým novým způsobem identifikace klienta bude tzv. bankovní identita.

Ta přinese zcela zásadní posun v oblasti eGovernmentu. Bude ovšem dosahovat pouze značné úrovně záruky, bude mít zvláštní režim mimo kvalifikovaný systém podle zákona o elektronické identifikaci a její použití bude pod výhradní kontrolou bank. Nelze proto očekávat její zpřístupnění pro využití ze strany FinTech společností. Není taky zřejmé, proč v případě bankovní identity postačuje pouze značná úroveň záruky, zatímco konkurenční finanční instituce budou muset provádět identifikaci klienta prostředkem, který zajišťuje vysokou úroveň záruky, jejíž dosažení je výrazně náročnější. Právní úprava bankovní identity bude dále diskriminovat kvalifikované poskytovatele služeb vytvářejících důvěru, neboť ti na rozdíl od bank nebudou moci přistupovat do základních registrů. Je bohužel nutné podotknout, že důvodová zpráva k zákonu, který právní úpravu bankovní identity obsahoval, je nezvykle tendenční.

I přes výše uvedené se domnívám, že by mělo dojít k přijetí dalšího alternativního způsobu vzdálené identifikace klienta, a to video identifikace. Ta by měla být přístupná všem povinným osobám a mohla by mít podobně restriktivní úpravu minimalizující riziko jejího zneužití, jako je tomu v případě Německa. I přes svou administrativní náročnost na straně povinné osoby by představovala výrazné zvýšení komfortu z pohledu spotřebitele.

V této práci jsem rovněž upozornil na problém související s působností AML zákona na zahraniční osoby. Nečinnost FAÚ ve vztahu k zahraničním poskytovatelům služeb, kteří fakticky působí na území ČR, ale právní úpravu vzdálené identifikace obsaženou v českém AML zákoně nedodržují, diskriminuje domácí povinné osoby. Vzhledem k tomu, že česká právní úprava vzdálené identifikace je přísnější než ve většině ostatních členských států, jsou domácí FinTech společnosti oproti své zahraniční konkurenci znevýhodněny. To je může motivovat k přesunu svého působení do zahraničí.

Co se týče působnosti AML zákona na FinTech služby, které jsem zvolil, lze konstatovat, že až na teoretické situace je vymezení povinných osob dostatečné. Jako vhodnou je možné označit též navrhovanou definici virtuálních aktiv. V oblasti služeb otevřeného bankovnictví bych však podpořil jejich úplné vyjmutí z působnosti AML zákona. Určité riziko v oblasti praní špinavých peněz a financování terorismu nelze v případě FinTech popřít, ovšem místo vytváření speciální právní úpravy bych se zaměřil spíše na dodržování plnění stávajících povinností a na hodnocení jejich efektivity ve vztahu k identifikovaným rizikům.

Do budoucna by podle mého názoru nemělo docházet k dalšímu zpřísňování AML pravidel, pokud takové změny nebudou velmi důkladně odůvodněny. Pro zajištění souladu s těmito pravidly je často nutné vytvářet specializované týmy zaměstnanců, což v důsledku zvýhodňuje velké finanční instituce. Cílem tvůrců právních norem by neměla být eliminace FinTech společností, ale spíše minimalizace rizik praní špinavých peněz a financování terorismu v případech, kdy je to nezbytné. Chtěl bych se též vymezit vůči případnému vytváření pravidel na míru určitým skupinám subjektů, posilování zákonných monopolů a diskriminaci obecně, tím spíše, pokud by docházelo ke zvýhodňování nejsilnějších účastníků trhu.

Nepochybně také v budoucnu dojde k diskuzi ohledně přístupu povinných osob do některých základních registrů. Osobně bych takovou možnost podpořil, neboť může zefektivnit boj proti praní špinavých peněz a financování terorismu a zároveň snížit náklady všem povinným osobám. Přístup by ovšem musel být velmi dobře zabezpečen a ochráněn před zneužitím nebo hromadným sběrem dat.

V souvislosti s domácí FinTech scénou bych také rád podotknul, že pokud by byla vyspělá a schopná konkurovat zahraničním službám, situace pro dotčené domácí orgány by mohla být výrazně jednodušší. Domácí spotřebitelé by využívali spíše domácí FinTech služby a dotčené orgány by nemusely tak často využívat nástroje mezinárodní spolupráce.

Na závěr bych chtěl dodat, že podle mého názoru není nutné FinTech služby v oblasti pravidel proti praní špinavých peněz a financování terorismu nějak obecně zvýhodňovat. Místo toho by stačilo, kdyby docházelo k přijímání moderních a efektivních právních norem a kdyby za účelem jejich snadného dodržování došlo k vytvoření takové infrastruktury, která by zajistila, že naplnění požadavků vyplývajících z AML pravidel bude jednoduché a snadné z pohledu všech povinných osob.

Seznam zkratek

AML	Anti-money laundering (boj proti praní špinavých peněz)
AMLD4	Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES
AMLD5	Směrnice Evropského parlamentu a Rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU
AML zákon	Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů
API	Application programming interface (soubor definic pro vzájemnou komunikaci aplikací)
ARES	Administrativní registr ekonomických subjektů
BoE	Bank of England (britská centrální banka)
BRIS	Business Registers Interconnection System
CFT	Countering the financing of terrorism (boj proti financování terorismu)
ČEFTAS	Česká fintech asociace
ČNB	Česká národní banka
ČR	Česká republika
DLT	Distributed ledger technology (technologie distribuovaných záznamů, případně účetních knih)
EBA	European Banking Authority (Evropský orgán pro bankovnictví)
ESMA	European Securities and Markets Authority (Evropský orgán pro cenné papíry a trhy)
EU	Evropská unie
FATF	Financial Action Task Force (Finanční akční výbor)
FAÚ	Finanční analytický úřad
FCA	Financial Conduct Authority (britský finanční regulátor)
FinTech	Finanční technologie

GwG	Geldwäschegesetz (německý AML zákon)
ICO	Initial coin offering (prvotní nabídka kryptoměn)
InsurTech	Insurance technology (pojišťovací technologie)
KYC	Know your customer (poznej svého klienta)
MAS	Monetary Authority of Singapore (singapurská centrální banka)
MF	Ministerstvo financí České republiky
MSP	Ministerstvo spravedlnosti České republiky
MV	Ministerstvo vnitra České republiky
Nařízení eIDAS	Nařízení Evropského parlamentu a Rady (EU) 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
OPO	Oznámení podezřelého obchodu
OR	Obchodní rejstřík
OSN	Organizace spojených národů
P2B	Peer-to-business (člověk – podnikatel)
P2P	Peer-to-peer (člověk – člověk)
P2P FX	Peer-to-peer foreign exchange (zahraniční převody a měnové konverze založené na párování protijdoucích plateb)
PEP(s)	Politically exposed person(s) (politicky exponované osoby)
PSD2	Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu
RegTech	Regulatorní technologie
ZOB	Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů
ZPS	Zákon č. 370/2017 Sb., o platebním styku, ve znění pozdějších předpisů

Seznam použitých zdrojů

1. Seznam použité literatury

Monografie a komentářová literatura

ARJUNWADKAR, Parag. *FinTech: The Technology Driving Disruption in the Financial Services Industry*. CRC Press, 2018, 261 s. ISBN 978-1-138-29479-0.

ARSLANIAN, Henri a Fabrice FISCHER. *The Future of Finance*. Springer International Publishing, 2019, 312 s. ISBN 978-3-030-14532-3.

BLAKSTAD, Sofie a Robert ALLEN. *FinTech Revolution*. Springer International Publishing, 2018, 406 s. ISBN 978-3-319-76013-1.

BOOBIER, Tony. *AI and the Future of Banking*. John Wiley & Sons, 2020, 283 s. ISBN 978-1-119-59613-4.

CUMMING, Douglas a Lars HORNUF, ed. *The Economics of Crowdfunding: Startups, Portals and Investor Behavior*. Springer International Publishing, 2018, 283 s. ISBN 978-3-319-66118-6.

DE SANCTIS, Fausto Martin. *Technology-Enhanced Methods of Money Laundering*. Springer International Publishing, 2019, 174 s. ISBN 978-3-030-18329-5.

FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2018, 214 s. ISBN 978-1-108-60970-8.

GIRASA, Rosario. *Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives*. Palgrave Macmillan, 2018, 274 s. ISBN 978-3-319-78508-0.

HURYCHOVÁ, Klára a Michal SÝKORA. *Compliance programy (nejen) v České republice*. Praha: Wolters Kluwer, 2018. 304 s. ISBN 978-80-7552-667-0.

KARFÍKOVÁ, Marie a kol. *Teorie finančního práva a finanční vědy*. Praha: Wolters Kluwer ČR, 2018, 356 s. ISBN 978-80-7552-935-0.

KATOLICKÁ, Michaela a Ján BÉREŠ. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. Praha: Wolters Kluwer ČR, 2017, 248 s. ISBN 978-80-7552-823-0.

KMENT, Vojtěch. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer ČR, 2018, 417 s. Právní monografie. ISBN 978-80-7552-814-8.

LÁNSKÝ, Jan. *Kryptoměny*. Praha: C. H. Beck, 2018, 160 s. ISBN 978-80-7400-722-4.

LYNN, Theo, John G. MOONEY, Pierangelo ROSATI a Mark CUMMINS, ed. *Disrupting Finance*. Springer International Publishing, 2019, 175 s. ISBN 978-3-030-02329-4.

MARANO, Pierpaolo a Kyriaki NOUSSIA, ed. *InsurTech: A Legal and Regulatory View*. Springer International Publishing, 2020, 401 s. ISBN 978-3-030-27385-9.

NICOLETTI, Bernardo. *Mobile Banking: Evolution or Revolution?*. Palgrave Macmillan UK, 2014, 209 s. ISBN 978-1-349-48166-8.

NICOLETTI, Bernardo. *The Future of FinTech: Integrating Finance and Technology in Financial Services*. Palgrave Macmillan, 2017, 328 s. ISBN 978-3-319-51414-7.

PICHRT, Jan, BOHÁČ, Radim a MORÁVEK, Jakub. *Sdílená ekonomika – sdílený právní problém?*. Praha: Wolters Kluwer ČR, 2017, 336 s. ISBN 978-80-7552-874-2.

TANDA, Alessandra a Cristiana-Maria SCHENA. *FinTech, BigTech and Banks*. Springer International Publishing, 2019, 111 s. ISBN 978-3-030-22425-7.

TVRDÝ, Jiří. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář*. 2. vydání. Praha: C.H. Beck, 2018, 584 s. ISBN 978-80-7400-688-3.

Články a příspěvky ve sbornících

ANG, Adrian, Samuel KWEK a Anil SHERGILL. FinTech in Singapore. *Business Law International* [online]. 2019, **20**(1), 51-62 [cit. 2020-06-06]. ISSN 1467632X. Dostupné z: https://www.ibanet.org/Document/Default.aspx?DocumentUid=5026E3B4-ED5B-4FEE-89A5-693304C7E079.

HLADKÁ, Michaela a Jiří HYLMAR. Identifikace klienta podle zákona proti praní špinavých peněz – výhled do budoucna. *Bankovnictví*. 4H production, **2018**(8), 20-21. ISSN 1212-4273.

CHEN, Zhiyuan, Ee na TEOH, Amril NAZIR, Ettikan kandasamy KARUPPIAH a Kim sim LAM. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems* [online]. 2018, **57**(2), 245-285 [cit. 2020-06-06]. DOI: 10.1007/s10115-017-1144-z. ISSN 02191377. Dostupné z: https://link.springer.com/article/10.1007%2Fs10115-017-1144-z.

PATWARDHAN, Anju. Peer-To-Peer Lending. Handbook of Blockchain, Digital Finance, and Inclusion [online]. *Elsevier*, 2018, 389-418 [cit. 2020-06-06]. DOI: 10.1016/B978-0-12-810441-5.00018-X. ISBN 9780128104415. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/B978012810441500018X.

RINGE, Wolf-Georg a Christopher RUOF. Regulating Fintech in the EU: the Case for a Guided Sandbox. *European Journal of Risk Regulation* [online]. 1-26 [cit. 2020-06-06]. DOI: 10.1017/err.2020.8. ISSN 1867-299X. Dostupné z: https://www.cambridge.org/core/product/identifier/S1867299X20000082/type/journal_article.

WU, Yen-Te. FinTech Innovation and Anti-Money Laundering Compliance. *National Taiwan University Law Review* [online]. 2017, **12**(2), 201-258 [cit. 2020-06-06]. DOI: 10.3966/181263242017091202002. Dostupné z: http://lawdata.com.tw/tw/doi/?doi=10.3966/181263242017091202002.

XIAO, Zhao, Yuelei LI a Kang ZHANG. Visual analysis of risks in peer-to-peer lending market. *Personal and Ubiquitous Computing* [online]. Springer London, 2018, **22**(4), 825-838 [cit. 2020-06-06]. DOI: 10.1007/s00779-018-1165-y. ISSN 1617-4909. Dostupné z: http://link.springer.com/10.1007/s00779-018-1165-y.

2. Seznam použitých internetových zdrojů

Anti money laundering and Fraud. *Digital Systems* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.digitalsystems.eu/fraud-risk-and-compliance/#anti-money.

BAFIN. *Circular 3/2017 (GW) – Video Identification Procedures (Non-binding English Translation)* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html.

BAFIN. *Geldwäschegesetz – GwG (Non-binding English Translation)* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8379954#doc7863564bodyText16.

BANK OF ENGLAND. *Quarterly Bulletin: Embracing the promise of fintech* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2019/embracing-the-promise-of-fintech.pdf?la=en&hash=2445D5B3AF10096FDAA91564BB48F8E5F28486B9.

Cryptoassets. *Financial Conduct Authority* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/consumers/cryptoassets.

Časté otázky a odpovědi. *Bankerat* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.bankerat.cz/investice/caste-otazky-a-odpovedi/.

ČESKÁ FINTECH ASOCIACE. *Standard pro provozování peer-to-peer úvěrových a investičních platforem* [online], 2018 [cit. 2020-06-06]. Dostupné z: http://czechfintech.cz/wp-content/uploads/2018/05/Standardy_P2P_platforem.pdf.

ČESKÁ NÁRODNÍ BANKA. *Stanovisko a odpovědi ČNB na vybrané otázky z konzultačního materiálu Evropské komise „Green Paper – Building a Capital Markets Union“* [online], 2015 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/legislativni_zakladna/stanoviska_cnb/download/capital_market_union_stanovisko_cnb.pdf.

ČESKÁ NÁRODNÍ BANKA. *Stanovisko k obchodování s tzv. převodními tokeny* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/k_obchodovani_s_prevodnimi_tokeny.pdf.

ČESKÁ NÁRODNÍ BANKA. *Stanovisko k výkladu pojmu poskytování finančních služeb v České republice* [online], 2013 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/archiv_stanovisek/k_vykladu_pojmu_poskytovani_financnich_sluzeb_v_cr.pdf.

ČESKÁ NÁRODNÍ BANKA. *Stanovisko k zprostředkování půjček, resp. úvěrů* [online], 2010 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/zprostredkovani_pujcek.pdf.

Členové. *Česká fintech asociace* [online], 2020 [cit. 2020-06-06]. Dostupné z: http://czechfintech.cz/clenove/#clenove.

David Pavliska z Revolutu: V Česku cílíme na stovky tisíc uživatelů. Chystáme lokalizaci i česká čísla účtů. *CzechCrunch* [online]. 2018 [cit. 2020-06-06]. Dostupné z: https://www.czechcrunch.cz/2018/11/david-pavliska-z-revolutu-v-cesku-cilime-na-stovky-tisic-uzivatelu-chystame-lokalizaci-i-ceska-cisla-uctu/.

DĚDEK, Oldřich. Balancing Fintech Opportunities and Risks: Implementing the Bali Fintech Agenda. *Česká národní banka* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/en/public/media_service/conferences/speeches/dedek_20190129_fintech.html.

Definition of fintech in English. *Oxford Dictionaries* [online]. Oxford University Press [cit. 2020-06-06]. Dostupné z: https://en.oxforddictionaries.com/definition/fintech.

DELOITTE & DEPARTMENT FOR INTERNATIONAL TRADE. *Fintech in CEE: Charting the course for innovation in financial services technology* [online], 2016 [cit. 2020-06-06]. Dostupné z: https://www2.deloitte.com/ce/en/pages/about-deloitte/articles/fintech-cee-region.html.

DELOITTE. *FinTech v ČR i ve světě: Vliv nových technologií na finanční sektor* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/financial-services/articles/fintech-v-cr-i-ve-svete.html.

DELOITTE. *Jak prosperovat v nejisté budoucnosti: Otevřené bankovnictví a PSD2* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/legal/articles/psd2.html.

EBA. *Opinion of the European Banking Authority on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD)* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/da05ad8a-eed2-410a-bd08-072403d086f3/EBA%20Opinion%20.pdf?retry=1.

ESMA. *Advice: Initial Coin Offerings and Crypto-Assets* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection.

EVROPSKÁ KOMISE. *Akční plán pro finanční technologie: Za konkurenceschopnější a inovativnější evropský finanční sektor* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0109&from=CS.

EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady (EU) 2018/0048 ze dne 8. 3. 2018 o evropských poskytovatelích služeb skupinového financování pro podniky* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0113&from=CS.

EVROPSKÁ KOMISE. *Report from the Commission to the European parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1570190003049&uri=CELEX:52019SC0650.

EVROPSKÁ KOMISE. *Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions – December 2019* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf.

EVROPSKÝ PARLAMENT – THINK TANK. *Financial technology (FinTech): Prospects and challenges for the EU* [online], 2017 [cit. 2020-06-06]. Dostupné z: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)599348.

EVROPSKÝ PARLAMENT. *Crypto-assets: Key developments, regulatory concerns and responses* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf.

FAQ. *Open Ownership Register* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://register.openownership.org/faq.

FATF. *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

FATF. *Guidance on Digital Identity* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf.

FATF. *Jurisdictions under Increased Monitoring – 21 February 2020* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html.

FCA and Bank of England announce proposals for data reforms across the UK financial sector. *Financial Conduct Authority* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/news/press-releases/fca-and-boe-announce-proposals-data-reforms-across-uk-financial-sector.

FINANCIAL CONDUCT AUTHORITY. *Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/publication/policy/ps19-22.pdf.

FINANCIAL CONDUCT AUTHORITY. *Loan-based ('peer-to-peer') and investment-based crowdfunding platforms: Feedback to CP18/20 and final rules* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/publication/policy/ps19-14.pdf.

FINANCIAL STABILITY BOARD. *Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.fsb.org/wp-content/uploads/P140420-1.pdf.

FINANCIAL STABILITY BOARD. *FinTech and market structure in financial services: Market developments and potential financial stability implications* [online], 2019 [cit. 2020-06-06]. Dostupné z: http://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/.

FINANČNÍ ANALYTICKÝ ÚŘAD. *Metodický pokyn č. 3: Zjišťování skutečného majitele povinnými osobami* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-1750233108/1495011685_cs_metodicky_pokyn_c_3_zjistovani_skutecneho_majitele.pdf.

FINANČNÍ ANALYTICKÝ ÚŘAD. *Metodický pokyn č. 7: Opatření vůči politicky exponovaným osobám* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-1750233108/1525684379_cs_pep-metodicky-pokyn2018final.pdf.

FINANČNÍ ANALYTICKÝ ÚŘAD. *Národní hodnocení rizik: Zpráva o prvním kole procesu Národního hodnocení rizik praní peněz a financování terorismu (veřejná verze)* [online], 2016 [cit. 2020-06-06]. Dostupné z: http://www.financnianalytickyurad.cz/hodnoceni-rizik/narodni-hodnoceni-rizik.html.

FINANČNÍ ANALYTICKÝ ÚŘAD. *Výroční zpráva 2019* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.financnianalytickyurad.cz/download/FileUploadComponent-526990861/1588148007_cs_29042020_vyrocni_zprava_fau_2019.pdf.

Finanční inovace. *Česká národní banka* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/financni-inovace/.

Foto-Ident bei N26: BaFin prüft wegen Kontoeröffnungen mit falschen Ausweisen. *Heise Online* [online]. 2018 [cit. 2020-06-06]. Dostupné z: https://www.heise.de/newsticker/meldung/Foto-Ident-bei-N26-BaFin-prueft-wegen-Kontoeroeffnungen-mit-falschen-Ausweisen-4190027.html.

GOVERNMENT OFFICES OF SWEDEN. *National Risk Assessment of Money Laundering and Terrorist Financing in Sweden* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.government.se/4aed70/contentassets/70c9762f411144dbbaf1020b1a5425b3/swedish-national-risk-assessment-2019-english-20191205-.pdf.

HM REVENUE & CUSTOMS. *Money service business guidance for money laundering supervision* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/889077/UTF-8__Guidance-for-Money-Service-Businesses-HM-Treasury-approved.docx_.pdf.

HM TREASURY. *National risk assessment of money laundering and terrorist financing 2017* [online], 2017 [cit. 2020-06-06]. Dostupné z: https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017.

How do I verify my identity?. *Revolut* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.revolut.com/help/getting-started/verifying-identity/how-do-i-verify-my-identity.

How does the Hawala money transfer systém work?. *TransferWise* [online]. 2018 [cit. 2020-06-06]. Dostupné z: https://transferwise.com/gb/blog/what-is-hawala.

How is the multi-currency account different than a bank account?. *TransferWise* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://transferwise.com/help/17/borderless-account/2736035/how-is-a-borderless-account-different-than-a-bank-account.

How to prove my identity?. *N26* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://support.n26.com/en-eu/account-and-personal-details/verifying-identity/how-to-prove-my-identity.

HRUBEŠ, Karel. Nevysvětlených 10 miliard přes J&T. Putovaly po trase Rusko–Česko–Karibik. *iDNES* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.idnes.cz/zpravy/domaci/j-t-rusko-cesko-banka.A191125_192032_domaci_jum.

Initiative of the year: Bank of England's FinTech Accelerator. *CENTRAL BANKING* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.centralbanking.com/awards/3333176/initiative-of-the-year-bank-of-englands-fintech-accelerator.

KOKEŠ, Ondřej. ARES jako otevřená data? Ministerstvo financí šlo cestou nejmenšího odporu. *Lupa* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/ares-jako-otevrena-data-ministerstvo-financi-slo-cestou-nejmensiho-odporu/.

MINISTERSTVO FINANCÍ. *Finanční trh a online identifikace a AML/CFT: Vyhodnocení konzultace* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/financni-trh-a-online-identifikace-a-aml-32102.

MINISTERSTVO FINANCÍ. *Inovace na finančním trhu a ochrana spotřebitele: Veřejná konzultace* [online], 2020 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/o-ministerstvu/verejne-diskuze/2020/verejna-konzultace-inovace-na-financnim-37490.

MINISTERSTVO FINANCÍ. *Koncepce rozvoje kapitálového trhu v České republice 2019-2023* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/aktualne/tiskove-zpravy/2019/ministerstvo-financi-predstavilo-koncepc-34656.

MINISTERSTVO FINANCÍ. *Metodický pokyn č. 2 Finančního analytického útvaru Ministerstva financí: O přístupu povinných osob k digitálním měnám* [online], 2013 [cit. 2020-06-06]. Dostupné z: http://www.financnianalytickyurad.cz/download/FileUploadComponent-1133285150/1506340773_cs_1481699516_cs_2-pokyn-mf_c-002_2013-09_metodicky-pokyn-o-pristupu-povinnych-osob-k-digitalnim-menam.pdf.

MINISTERSTVO FINANCÍ. *Online identifikace a AML/CFT: Podkladová studie* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/bankovnictvi-a-platebni-sluzby/platebni-sluzby-a-vyporadani-obchodu/aktuality/2018/podkladova-studie-financni-technologie-a-31641.

MONETARY AUTHORITY OF SINGAPORE. *Fintech Regulatory Sandbox Guidelines* [online], 2016 [cit. 2020-06-06]. Dostupné z: http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines%2019Feb2018.pdf.

MONETARY AUTHORITY OF SINGAPORE. *Guidelines to MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism* [online]. [cit. 2020-06-06]. Dostupné z: https://www.mas.gov.sg/-/media/MAS/resource/legislation_guidelines/aml/CMI-SFA04N02-Guidelines-to-CMS-licensees.pdf?la=en&hash=AED6106BEA86DDE04C47E022A3580B0F81321B2F.

MONETARY AUTHORITY OF SINGAPORE. *Use of MyInfo and CDD Measures for Non Face-to-face Business Relations* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf.

MONEYVAL. *Anti-money laundering and counter-terrorist financing measures: Czech Republic (Fifth Round Mutual Evaluation Report)* [online], 2019 [cit. 2020-06-06]. Dostupné z: https://www.coe.int/en/web/moneyval/-/combatting-money-laundering-in-the-czech-republic-despite-progress-more-investigations-are-needed-says-council-of-europe-report.

MORA, Marek. FinTech pohledem centrální banky [online]. *Česká národní banka*, 2018 [cit. 2020-06-06]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/verejnost/.galleries/pro_media/konference_projevy/vystoupeni_projevy/download/mora_20181011_bankovni_forum.pdf.

Nejčastější dotazy. Bankovní identita [online]. *Česká bankovní asociace*, 2020 [cit. 2020-06-06]. Dostupné z: https://www.bankovni-identita.cz/faq.

NEJVYŠŠÍ STÁTNÍ ZASTUPITELSTVÍ. *Národní hodnocení rizik: Podkladové informace k národnímu hodnocení rizik praní peněz a financování terorismu za státní zastupitelství* [online], 2016 [cit. 2020-06-06]. Dostupné z: http://www.financnianalytickyurad.cz/hodnoceni-rizik/narodni-hodnoceni-rizik.html.

New Bank Start-up Unit launched by the financial regulators. *Financial Conduct Authority* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/news/press-releases/new-bank-start-unit-launched-financial-regulators.

NONNEMANN, František. Regulatory sandbox: možnosti a meze nástroje pro chytrou regulaci [online]. *EPRAVO.CZ*, 2019 [cit. 2020-06-06]. Dostupné z: https://www.epravo.cz/top/clanky/regulatory-sandbox-moznosti-a-meze-nastroje-pro-chytrou-regulaci-109048.html.

NOVÁK, Matěj. Návrh zákona upravující podmínky pro vznik bankovní identity [online]. *EPRAVO.CZ*, 2020 [cit. 2020-06-06]. Dostupné z: https://www.epravo.cz/top/clanky/navrh-zakona-upravujici-podminky-pro-vznik-bankovni-identity-110488.html.

Obchodní podmínky společnosti Hithit s.r.o. *Hithit* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.hithit.com/cs/article/terms.

On the Frontline: Fintech vs Money Laundering. *The Economist Intelligence Unit* [online]. 2019 [cit. 2020-06-06]. Dostupné z: https://eiuperspectives.economist.com/sites/default/files/money-laundering-exposed-fintech-wp-uk_1.pdf.

Otevřená data Veřejného rejstříku a Sbírky listin [online]. *Ministerstvo spravedlnosti České republiky*, 2020 [cit. 2020-06-06]. Dostupné z: https://dataor.justice.cz/.

PERRY, Michelle. Taking the next step in sandbox evolution [online]. *Raconteur*, 2020 [cit. 2020-06-06]. Dostupné z: https://www.raconteur.net/finance/fca-sandbox-fintech.

PETERKA, Jiří. Český eGovernment v roce 2018: Významný milník i příchod elektronických občanek. *Lupa*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/cesky-egovernment-v-roce-2018-vyznamny-milnik-i-prichod-elektronickych-obcanek/.

PETERKA, Jiří. eObčanky ztratily monopol na přihlašování ke službám eGovernmentu. Jak funguje karta Starcos?. *Lupa*, 2020 [online]. [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/eobcanky-ztratily-monopol-na-prihlasovani-ke-sluzbam-egovernmentu-jak-funguje-karta-starcos/.

PETERKA, Jiří. Jak poznat kvalifikovaný elektronický podpis a kvalifikovanou elektronickou pečeť?. *Lupa*, 2018 [online]. [cit. 2020-06-06]. Dostupné z: https://www.lupa.cz/clanky/jak-poznat-kvalifikovany-elektronicky-podpis-a-kvalifikovanou-elektronickou-pecet/.

Předplacené platební karty – nabídka 2020. *Navigátor úvěrů* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.navigatoruveru.cz/predplacene-platebni-karty/.

Regulatory sandbox. *Financial Conduct Authority* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

Revolut whistleblower had concerns over CEO conduct and compliance. *BBC*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.bbc.com/news/technology-47751945.

STATT, Nick. Facebook confirms it will launch a cryptocurrency called Libra in 2020. *The Verge*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.theverge.com/2019/6/18/18682290/facebook-libra-cryptocurrency-visa-mastercard-digital-currency-calibra-wallet-announce.

Terms of Service. *Tether Operations Limited* [online]. 2020 [cit. 2020-06-06]. Dostupné z: https://tether.to/legal/.

TĚTEK, Josef. Stable coins (VŠE, CO CHCETE VĚDĚT) – Svatý grál kryptoměn?. *Alza*, 2018 [online]. [cit. 2020-06-06]. Dostupné z: https://www.alza.cz/stable-coins.

ÚŘAD VLÁDY. *Digitální Česko: Vládní program digitalizace České republiky 2018+* [online], 2018 [cit. 2020-06-06]. Dostupné z: https://i.iinfo.cz/files/lupa/328/digitalni-cesko-informacni-koncepce-ceske-republiky-1.pdf.

What is Fintech?. *Investopedia* [online]. 2019 [cit. 2020-06-06]. Dostupné z: https://www.investopedia.com/terms/f/fintech.asp.

ZATLOUKAL, Jiří. Rodí se Sonia. Největší banky v Česku chtějí společnou firmou rozhýbat digitalizaci státu. *Euro*, 2019 [online]. [cit. 2020-06-06]. Dostupné z: https://www.euro.cz/byznys/rodi-se-sonia-nejvetsi-tuzemske-banky-chteji-spolecnou-firmou-rozhybat-digitalizaci-statni-spravy-1434456.

3. Seznam použitých právních předpisů (v platném znění)

Nařízení Evropského parlamentu a Rady (EU) 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Nařízení Komise v přenesené pravomoci (EU) 2016/1675 ze dne 14. července 2016, kterým se směrnice (EU) 2015/849 Evropského parlamentu a Rady doplňuje o identifikaci vysoce rizikových třetích zemí se strategickými nedostatky.

Nařízení vlády č. 210/2008 Sb., k provedení zvláštních opatření k boji proti terorismu.

Nařízení vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data.

Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES.

Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES.

Směrnice Evropského parlamentu a Rady (EU) 2017/1132 ze dne 14. června 2017 o některých aspektech práva obchodních společností.

Směrnice Evropského parlamentu a Rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU.

Směrnice Evropského parlamentu a Rady (EU) 2019/1151 ze dne 20. června 2019, kterou se mění směrnice (EU) 2017/1132, pokud jde o využívání digitálních nástrojů a postupů v právu obchodních společností.

The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544).

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692).

Vyhláška České národní banky č. 67/2018 Sb., o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnost a financování terorismu.

Vyhláška ministerstva spravedlnosti č. 323/2013 Sb., o náležitostech formulářů na podávání návrhů na zápis, změnu nebo výmaz údajů do veřejného rejstříku právnických a fyzických osob, evidence svěřenských fondů a evidence údajů o skutečných majitelích a o podrobnostech týkajících se způsobu dálkového přístupu k údajům v evidenci skutečných majitelů a některým údajům v evidenci svěřenských fondů a o zrušení některých vyhlášek.

Zákon č. 111/2009 Sb., o základních registrech.

Zákon č. 117/2001 Sb., o veřejných sbírkách a o změně některých zákonů (zákon o veřejných sbírkách).

Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

Zákon č. 186/2016 Sb., o hazardních hrách.

Zákon č. 192/2016 Sb., kterým se mění zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, a některé další zákony.

Zákon č. 21/1992 Sb., o bankách.

Zákon č. 250/2017 Sb., o elektronické identifikaci.

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Zákon č. 300/2016 Sb., o centrální evidenci účtů.

Zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřenských fondů.

Zákon č. 370/2017 Sb., o platebním styku.

Zákon č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a některé další zákony.

Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí.

Zákon České národní rady č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky.

4. Seznam ostatních zdrojů

EVROPSKÁ KOMISE. *Creating FinTech opportunities for SMEs*. Luxembourg, 2019. ISBN 978-92-76-02901-4.

FINANČNÍ ANALYTICKÝ ÚŘAD. *Rozhodnutí o částečném odmítnutí žádosti o informace ze dne 21. 5. 2020.* Č. j. FAU-42153/2020/031.

FINANČNÍ ANALYTICKÝ ÚŘAD. *Rozhodnutí o přestupku ze dne 31. 10. 2018.* Č. j. FAU-68073/2018/032. Dostupné z: https://www.financnianalytickyurad.cz/rozhodnuti-o-prestupcich.html.

Informace poskytl Andre MARTIROSYAN ze společnosti S-RM Intelligence and Risk Consulting Limited prostřednictvím internetové komunikace ze dne 6. 6. 2020.

Informace poskytl Roman KUČERA ze společnosti První certifikační autorita prostřednictvím internetové komunikace ze dne 11. 6. 2020.

KOŘANOVÁ, Barbora, Martin KUPKA, Ivan BARTOŠ a kol. *Návrh poslanců Barbory Kořanové, Martina Kupky, Ivana Bartoše, Pavla Jelínka, Pavla Kováčika, Jana Chvojky, Jana Bartoška, Heleny Langšádlové, Věry Kovářové a dalších na vydání zákona, kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů*. Poslanecká sněmovna Parlamentu České republiky, 2019. Sněmovní tisk 554/0. 8. volební období.

MINISTERSTVO FINANCÍ. *Návrh zákona, kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů, a další zákony související s těmito zákony a zákonem o evidenci skutečných majitelů*. Úřad vlády, 2020. Č. j. MF-11223/2019/32-15. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBDJKEVE2.

MINISTERSTVO SPRAVEDLNOSTI. *Návrh zákona o evidenci skutečných majitelů*. Úřad vlády, 2019. Č. j. 30/2018-LO-SP. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNBCZJMEP9.

MINISTERSTVO SPRAVEDLNOSTI. *Odpověď na žádost o informace ze dne 10. 6. 2020*. Č. j. MSP-345/2020-OSV-OSV/4.

Abstrakt a klíčová slova

FinTech a AML z právní perspektivy

Tématem této práce je dopad pravidel proti praní špinavých peněz a financování terorismu na oblast FinTech. Cílem práce je tato pravidla analyzovat a poskytnout k nim kritický pohled, který reflektuje technologický vývoj ve finančním sektoru a vnímá nákladnost dodržování těchto pravidel. Za tímto účelem je v první kapitole nejprve definován samotný pojem FinTech, jsou objasněny jeho specifika a uvedeny typické případy finančních služeb, které lze v současnosti tímto způsobem označit. V druhé kapitole jsou poté vysvětleny jednotlivé povinnosti vyplývající z AML zákona a jsou vyhodnoceny jejich dopady na povinné osoby. Následně jsou v samostatné kapitole podrobeny kritice stávající i budoucí možnosti vzdálené identifikace jakožto nejjednoduššího způsobu získání klienta. V poslední kapitole je zkoumána působnost AML zákona ve vztahu k neobankingu, crowdfundingu a kryptoaktivům. V závěru práce jsou shrnuty získané poznatky, formulovány názory na stávající stav problematiky a prezentovány podněty do budoucna.

Je nepochybné, že praní špinavých peněz a financování terorismu jsou škodlivé společenské jevy, které dopadají i na oblast FinTech. Neustálé zpřísňování AML/CFT pravidel, které je v poslední době trendem, ale musí být doprovázeno i veřejnou infrastrukturou a zákonnými normami, které reflektují digitální dobu. Bez nich se budou zvyšovat tržní bariéry pro vstup malých společností do finančního sektoru, což bude bránit vzniku inovací, které mohou mít přínos pro spotřebitele a celou ekonomiku. Zároveň je nutné věnovat pozornost tomu, aby přijetím přísnějších domácích pravidel nedocházelo k nedůvodné diskriminaci FinTech společností, které vznikají v České republice a mají nadnárodní ambice. V budoucnu by taktéž nemělo docházet k vytváření právní úpravy, která v určitých ohledech privileguje vybrané skupiny subjektů. Místo toho by více pozornosti zasluhovalo pokračování v budování bezpečné a moderní infrastruktury, která by umožnila snadnější plnění zákonných požadavků všem povinným osobám.

Klíčová slova: FinTech; AML; Neobanking; Crowdfunding; Kryptoaktiva

Abstract and keywords

FinTech and AML from a legal perspective

The subject matter of this thesis is the impact of regulations preventing money laundering and terrorism financing in the field of FinTech. The goal is to analyse these regulations and to offer a critical standpoint which would reflect the technological development in the financial sector and take into consideration the cost of adhering to these regulations. With this objective in mind, the first chapter defines the concept of FinTech, breaks down its specifics and provides typical examples of the financial services currently fitting this definition. In the second chapter, the obligations stemming from the AML/CFT rules are defined along with an evaluation of their impact on obliged persons. The current and future possibilities of remote identification which represents the simplest way of acquiring a client are further evaluated in a separate chapter. In the last part, this paper analyses the applicability of the AML/CFT Act in relation to neobanking, crowdfunding and crypto-assets. The paper concludes by summarizing the findings, formulating views on the current state of the topic, and presenting suggestions for future development.

Money laundering and terrorism financing are detrimental social phenomena affecting the FinTech sector. The constant tightening of the AML/CFT regulations, however, must be accompanied by the appropriate public infrastructure and legal rules reflecting the nature of the digital age. Without these measures, the market entry barriers for small companies in the financial sector will grow, potentially preventing innovation that would otherwise be beneficial for the consumer and the entire economy. Furthermore, it is important to prevent unreasonable discrimination of Czech FinTech companies with transnational ambitions, which may face more restrictive domestic regulations compared to other states. Future legal amendments that would selectively promote certain groups of market participants should also be avoided. Instead, Czech officials should focus towards developing a secure and modern infrastructure that would ensure that meeting legal requirements is accessible to all obliged persons.

Keywords: FinTech; AML; Neobanking; Crowdfunding; Crypto-Assets