ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

VYBRANÁ LEGISLATIVNÍ ÚPRAVA FINTECH V ČESKÉ REPUBLICE A JEHO UŽITÍ V PRAXI

rigorózní práce

2023 Mgr. Huy Ho Ba

ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

Katedra finančního práva a národního hospodářství

Finanční právo

VYBRANÁ LEGISLATIVNÍ ÚPRAVA FINTECH V ČESKÉ REPUBLICE A JEHO UŽITÍ V PRAXI

rigorózní práce

Mgr. Huy Ho Ba

Plzeň, 2023

Prohlášení

„*Prohlašuji, že jsem tuto rigorózní práci zpracoval samostatně, a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem ve vědecké práci obvyklým.*“

Plzeň, červenec 2023

_____

Mgr. Huy Ho Ba

Poděkování

Tímto bych chtěl poděkovat paní JUDr. et Mgr. Silvii Anderlové za rady a připomínky během zpracování této práce. Touto cestou bych chtěl rovněž poděkovat rodičům za neutuchající podporu během celého studia a mé současné koncipientské praxe v advokacii. Také bych chtěl poděkovat všem svým blízkým, přátelům, kamarádům, souputníkům v mém životě, kteří mě neustále inspirují k tomu, abych překonával sám sebe.

Obsah

Seznam použitých zkratek

AMLZ	Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
Nařízení eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 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 RTS	Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace
Občanský zákoník	Zákon č. 89/2012 Sb., občanský zákoník
Směrnice AML	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
Směrnice PSD2	Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu
ZoB	Zákon č. 21/1992 Sb., o bankách
ZoBID	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 (jinak nazýván jako zákon o bankovní identitě)
ZoD	Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů
ZoEI	Zákon č. 250/2017 Sb., o elektronické identifikaci
ZoPS	Zákon č. 370/2017 Sb., o platebním styku
ZoSVD	Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Úvod

FinTech – pojem, jenž poslední roky rezonuje oblastí platebního styku, bankovnictví, bankovního práva a v neposlední řadě i v médiích ve spojení s Bankovní identitou. S FinTech se setkáváme dennodenně, aniž bychom si tuto skutečnost uvědomovali, ať už se jedná o každodenní platby prostřednictvím Revolut karty, využití Moneyback od České spořitelny za účelem ušetření při nákupech a mnoho dalšího, kde dochází ke spojení technologie a finančního sektoru.

Svou diplomovou práci jsem věnoval směrnici PSD2, která přinesla „nový vítr“ do oblasti platebního styku, tím pádem i do sektoru FinTech a celkově bankovního sektoru. Díky výše uvedené zkušenosti jsem si uvědomil, že svět FinTech nepředstavují pouze služby, které přinesly směrnice PSD a směrnice PSD2, ale i zavedené finanční služby používané před účinností směrnic PSD a PSD2. Nebyly pouze regulovány ze strany právních předpisů vnitrostátních či v evropském měřítku. Nemůžeme mít však zákonodárcům za zlé, že ve valné většině ex-post dotváří právní rámec těchto služeb, jelikož tato oblast je velice dynamická a dle mého názoru je zejména potřeba tyto neregulované služby správně pojmout a nadefinovat pro dobro všech stran, a to zejména pro klienty, poskytovatele a potažmo pro regulátory v bankovním světě.

Během výběru tématu pro rigorózní práci se ve mně zrodila myšlenka, že bych se mohl zabývat vybranou legislativní úpravou, která utváří určitý legislativní rámec v České republice pro FinTech. Já, jakožto IT nadšenec, jsem přijal výzvu za svou, když jsem přečetl článek od bývalých kolegů z Deloitte Legal k anketě Zákon roku 2020. V ročníku 2020 drtivě zvítězil zákon o bankovní identitě, jak je nazýván odbornou veřejností, celým názvem pak 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 další podružné zákony. Téma Bankovní identity mě lákalo už během výběru tématu diplomové práce, kdy se teprve diskutovalo o takovém zákoně, který by umožňoval, zejména bankám, realizovat výkon činnosti elektronické identifikace a elektronické autentizace dle nařízení eIDAS, potažmo ZoEI. Daná služba umožňuje obrovskou změnu v přístupu obyvatel České republiky k digitálním službám a dle mého názoru může v následujících letech zcela změnit směr e-Governmentu.

Posun ve FinTech by měl jít ruku v ruce spolu s právní úpravou nových trendů a služeb, které by reflektovaly takové posuny v byznysové sféře. Je však obrovským otazníkem, zda právní řád České republiky, potažmo právo Evropské unie reflektuje takové změny a dokáže připravit půdu novým inovacím. Příliš striktní právní úprava by jim nemusela v mnoha případech svědčit.

Rád bych prostřednictvím této rigorózní práce zjistil, zda je Česká republika a Evropská unie připravena na inovace na půdě FinTech a poskytuje jim dostatečný prostor v právním řádu, zejména z pohledu směrnice PSD2 a ZoBID. Na druhé straně chci reflektovat také to, jak takový právní rámec využívají adresáti těchto právních norem, tedy například banky nebo start-upy.

Vzhledem ke skutečnosti, že obecně k problematice FinTech není dostupná česká právní literatura, kromě komentářů k ZoPS či ZoEL, budu čerpat především ze zákonné úpravy (zejména české a evropské), metodik, směrnic, článků či studií od odborné veřejnosti. Na poznatky z výše uvedených zdrojů, které využiji ke zpracování této rigorózní práce, uplatním následující metody zkoumání, a to zejména analytické a komparativní.

Cílem této rigorózní práce není obsáhnout veškerou legislativní úpravu, která se pojí s FinTech, nýbrž se zaměřit na služby, které s sebou přinesla směrnice PSD2 a jejich praktickou využitelnost, silné ověření uživatele a digitální onboarding ve spojení s Bankovní identitou. Zejména se zaměřím na proces, nástrahy a v čem může pomoci nová služba Bankovní identita během digitálního onboardingu.

Má rigorózní práce je členěna do tří kapitol, přičemž v první kapitole se budu věnovat FinTech a využití novinek v návaznosti na směrnici PSD2. Analyzuji instituce, které se zabývají FinTech v České republice. Neopomenu ani Open Banking standardy, které dle mého názoru stojí za to sledovat v rámci přeshraniční spolupráce mezi bankami ve sdílení dat. V této kapitole se budu zabývat dvěma službami, které směrnice PSD2 přináší, a to služba informování o platebním účtu, jinak zvaná AIS, a dále služba nepřímého dání platebního příkazu, PIS. V závěrečné části první kapitoly uvedu příklady využití těchto služeb v praxi.

Ve druhé kapitole se budu věnovat zvlášť silnému ověření klienta, kde se nejprve zaměřím na prvky ověření daného uživatele, včetně mobilní aplikace Klíč, kterou má v mobilu nainstalovaný nejeden člověk, a to za účelem povolení transakcí či dalších služeb prostřednictvím internetového bankovnictví. Popíši výjimky ze

silného ověření klienta, kterých je na můj vkus mnoho. Na závěr této kapitoly uvedu porušení povinností, které ukládá ZoPS při silném ověření klienta.

Ve třetí a zároveň poslední kapitole plánuji v kostce obsáhnout digitální onboarding a s tím související problémy. Myšleno zejména problémy v návaznosti na „strašáka“ jménem AMLZ, se kterým se setkáváme všichni dennodenně v běžném životě, jak během využívání bankovních služeb, tak například při koupi nemovitosti u notáře či advokáta. V rámci digitálního onboardingu se budu zabývat nařízením eIDAS, který v roce 2014 přinesl průlomové služby, a to elektronickou identifikaci, elektronickou autentizaci a služby vytvářející důvěru. Toto nařízení eIDAS bude sloužit jako předskokan k Bankovní identitě, která je postavena na možnostech nařízení eIDAS a částečně i na AMLZ. U Bankovní identity popíši historický vývoj, právní úpravu a využití Bankovní identity v praxi.

V neposlední řadě chci také poukázat na to, jak nám regulace FinTech a jeho možnosti zlehčují život a umožňují vyřídit některé neodkladné záležitosti rychleji. V návaznosti na FinTech budu rozebírat částečně problematiku e-Governmentu, který je provázán s FinTech v rámci Bankovní identity. Hovoří se o tom, že díky tomuto projektu přibyde mnoho občanů, kteří využijí na dálku služby e-Governmentu, které poskytuje stát, potažmo veřejná správa. Pokud se podíváme optikou skandinávských zemí či pobaltských zemí, domnívám se, že digitalizace veřejné správy je na pořadu dne a je zapotřebí jít vpřed. Problémem nebude dle mého názoru ani to, že veřejná správa v současné době neposkytuje tolik služeb, které se dají zařídit online, ale spíše v tom, že málo občanů ví o takových možnostech, případně se jich zdráhají, a to především v důsledku příliš zdlouhavých procesům při aktivaci přístupu k takovým službám přes internet.

Tato rigorózní práce odpovídá právnímu stavu ke dni 31. července 2023.

1. Novinky ve FinTech v souvislosti se směrnicí PSD2

V dnešní době se pojem FinTech využívá čím dál více ve světě financí a rovněž se často vyskytuje ve slovníku osob pohybujících se v oboru bankovního práva.

Pojem FinTech je složeninou slov finance a technologie. Jde o nové technologie, které se uplatňují ve finančním sektoru, zároveň jde i o společnosti a finanční platformy, které inovují poskytování finančních služeb. Obecně do FinTech spadají inovativní a nové produkty finančního sektoru, které narušují pořádky v tomto sektoru[1].

Souhrnně pojem FinTech pojme například „mobilní platby, kryptoměny, crowdfunding nebo on-line platformy na poskytování mikropůjček“[2]. „Konkrétně se pak z hlediska podnikatelského vztahuje ke společnostem, které využívají sociální sítě, rozšířenou inteligenci (včetně samoučících se programů), mobilní aplikace, distribuované databáze (DLT), jako je především blockchain, datacloudy nebo jiný software, zkrátka moderní technologie k tomu, aby poskytování bankovních, investičních nebo jiných finančních služeb bylo efektivnější. Jedná se buď o samotné poskytovatele těchto služeb (například poskytovatele spotřebitelských úvěrů, platebních či investičních služeb), nebo osoby, které těmto poskytovatelům pomáhají lépe zacílit na zákazníky či rozvíjet jejich podnikání (IT společnosti vyvíjející API, crowdfundingové platformy, účetní cloudy aj.)“[3].

Z hlediska právního nebyly FinTech přímo regulovány českou legislativou, nýbrž legislativou evropskou (pokud nezahrnuji crowdfunding)[4]. Jeden ze zásadních právních předpisů vzniklých z pera evropských legislativců, kterému se budu věnovat v této práci, je směrnice PSD2, která byla přijata dne 25. listopadu 2015, jež plně nahradila směrnici PSD a měla být následně implementována do vnitrostátních právních řádů členských států. Česká republika ji implementovala

[1] FinTech v ČR i ve světě. In: *Deloitte Česká republika* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf, s. 4

[2] ŠOVAR, Jan a Ondřej MIKULA. FinTech v Česku: Legislativní iniciativa míří výlučně z Bruselu. *Právní rádce* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-65872700-fintech-v-cesku-legislativni-iniciativa-miri-vylucne-z-bruselu

[3] Ibid.

[4] ŠOVAR, Jan a Ondřej MIKULA. FinTech v Česku: Legislativní iniciativa míří výlučně z Bruselu. *Právní rádce* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-65872700-fintech-v-cesku-legislativni-iniciativa-miri-vylucne-z-bruselu

pomocí ZoPS, který je platný od 11. října 2017 a účinný od 13. ledna 2018, přičemž uvedené datum bylo mezním termínem, kdy měla být směrnice PSD2 transponována napříč vnitrostátními právními řády členských států Evropské unie.

Ve světle posledních let si nemohu odpustit tu poznámku, že ZoPS neměl za sebou jednoduchý legislativní proces[5], jelikož jeho návrh byl předložen vládou již v březnu 2017, avšak byl schválen až v říjnu 2017, těsně před lhůtou, kdy měla Česká republika mít implementovanou směrnici PSD2 ve svém právním řádu. Podobná zpoždění můžeme spatřit u zákona o ochraně oznamovatelů, který se měl schvalovat už v listopadu 2021[6], kdy nově zvolení poslanci měli v plánu implementovat novým zákonem o ochraně oznamovatelů směrnici Evropského Parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie, o kterém už široká právnická veřejnost hovořila nejméně půl roku předem[7], přičemž moji bývalí kolegové se nad tímto tématem už zabývali na začátku roku 2021[8]. Výše uvedená implementace je platná až od 20. června 2023 a účinnosti nabude 1. srpna 2023[9]. Ale abych se vrátil zpět k tématu, směrnici PSD2 lze pokládat jako jednou z vlaštovek FinTech regulace, pokud nebudeme počítat anti-money laundering (AML) směrnice.

Nejen v právním světě, ale i ve finančním světě se čím dál více rozrůstá disrupce starých pořádků a s příchodem nových technologií, jako jsou například chytré telefony, využívají finanční start-upy, technologické společnosti, ale i banky příležitosti, jak získat zákazníka z pohodlí domova, přes internet.

Z pohledu bank to do budoucna znamená úspory za provoz poboček (při plánovaném postupném zavírání), lidského kapitálu (propouštění pracovníků na pobočkách), ale především snaha neustrnout ve vývoji a přizpůsobovat se současným trendům, které udávají zejména start-upy. V posledních letech můžeme

---

[5] VOJTĚCH, Petr. Nový zákon o platebním styku v platnosti. *Epravo.cz* [online]. 2017 [cit. 2021-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-v-platnosti-106689.html?mail

[6] OTTO, Pavel. Volby poštou, platy učitelů či whistleblowing. Nové poslance čeká spousta nedodělků. E15.cz [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.e15.cz/domaci/volby-postou-platy-ucitelu-ci-whistleblowing-nove-poslance-ceka-spousta-nedodelku-1384711

[7] MALIŠOVÁ, Kristina. Jaké povinnosti přinese nový zákon na ochranu oznamovatelů zaměstnavatelům?. Právní prostor [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/jake-povinnosti-prinese-novy-zakon-na-ochranu-oznamovatelu-zamestnavatelum

[8] Whistleblowing – účinný nástroj pro podporu zdravé a etické firemní kultury. Deloitte Česká republika [online]. [cit. 2022-04-17]. Dostupné z: https://akce.deloitte.cz/akce/21-03-17-whistleblowing-ucinny-nastroj-pro-podporu-zdrave-a-eticke-firemni-kultury/

[9] Zákon č. 171/2023 Sb., o ochraně oznamovatelů

v médiích sledovat zprávy o hromadných propuštěních, jako například v Komerční bance, České spořitelně nebo Československé obchodní bance, které budou redukovat počet poboček a zaměstnanců.[10]

Pro klienta to může být přínosné zejména lepší dostupností finančních služeb, spočívající v jejich přístupnosti v kteroukoliv denní dobu a na kterémkoliv místě, zejména pokud bydlí mimo dosah kamenných poboček bank, například v malé vesnici.

Ruku v ruce jsou tu ale také nevýhody a rizika plynoucí z tohoto způsobu fungování. Hrozí větší kybernetické riziko, odcizení citlivých údajů klientů[11] a nedůvěra konzervativních klientů banky, kteří upřednostňují osobní kontakt s bankéřem na pobočce. V každém případě model uzavírání všech poboček bank není stále na pořadu dne[12], ale pandemie koronaviru COVID-19 uspíšila přechod klientů k bankovním aplikacím dostupným na chytrých telefonech či k internetovému bankovnictví. Jedna z největších tuzemských bank, Česká spořitelna, nedávno přistoupila k videoporadenství, prostřednictvím kterého se na 500 bankéřů věnuje svým klientům přes videohovory způsobem, na který jsou zvyklí z poboček. K tomuto budou využívat aplikaci Microsoft Teams skrze platformu internetového bankovnictví George[13].

Pro start-upy to znamená obrovskou příležitost získat část podílu na trhu od bank, které disponují velkým portfoliem produktů, jenž mohou kombinovat při složení nabídky pro své klienty. Start-upy se zaměřují na určité produkty nebo přímo celé sektory a směrnice PSD2 jim k tomu dává příležitost získat klientelu právě od bank, pomocí otevřeného API (Application Programming Interface). Pro banky nejsou tyto start-upy ztělesněním přímé konkurence, jelikož start-upy se stále zabývají určitými produkty (zejména „niche“ produkty) a některé banky dokonce

[10] ZATLOUKAL, Jiří. Pokračuje propouštění v bankách. Komerčka se zbaví čtvrtiny zaměstnanců. *Seznam Zprávy* [online]. 2021 [cit. 2021-02-22]. Dostupné z: https://www.seznamzpravy.cz/clanek/pokracuje-propousteni-v-bankach-komercka-se-zbavi-ctvrtiny-zamestnancu-142061

[11] FinTech v ČR i ve světě. In: *Deloitte Česká republika* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf, s. 11

[12] BUŘÍNSKÁ, Barbora. Klienti se přesouvají do onlinu, velké banky zavírají pobočky. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://www.novinky.cz/finance/clanek/klienti-se-presouvaji-do-onlinu-velke-banky-zaviraji-pobocky-40340316

[13] VEINBENDER, Kristina. České banky přecházejí na videoporadenství. Přiměli je k tomu mladí zákazníci a pandemie. E15.cz [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.e15.cz/byznys/ceske-banky-prechazeji-na-videoporadenstvi-primeli-je-k-tomu-mladi-zakaznici-a-pandemie-1384331

přímo spolupracují se start-upy. Například Komerční banka, která navázala spolupráci s BudgetBakers.[14]

Dále jako příklad může sloužit český start-up Spendee, který se zabývá správou financí. Díky otevřenému API nemusí jejich uživatel zadávat manuálně všechny platby, které provedl za daný den, ale Spendee si sám stáhne informace od banky přes službu informování o platebním účtu (vizte kapitola 1.4.), která je nově zavedena díky směrnici PSD2 do ZoPS. S takovými možnostmi získává klient do rukou mocné nástroje, které může například využít k lepší finanční správě, ve zmiňovaném Spendee nebo třeba BudgetBakers.

S nástupem směrnice PSD2 se očekávalo, že v České republice bude více FinTechů, které využijí mezery na trhu, avšak opak je pravdou[15]. Jednou z příčin může být zejména zdlouhavý a náročný průběh a zejména podmínky nutné k získání povolení k činnosti od České národní banky (vizte kapitola 1.4.3.)[16].

Výše zmiňované služby nepřímého dání platby a služba informování o platebním účtu jsou uvedeny v ustanovení § 3, odst. 1 ZoPS, v písmenu g), respektive h), které jsou mezi platebními službami. To znamená, že se vztahují na poskytovatele služby nepřímého dání platby a služby informování platebního účtu kritéria platební instituce, která je oprávněna poskytovat platební služby na základě povolení k činnosti platební instituce[17] [18]. V povolení k činnosti platební instituce Česká národní banka uvádí platební služby, na které se povolení vztahuje[19]. To znamená, že platební instituce může požádat o určitý okruh platebních služeb, které bude poskytovat a nemusí v sobě zahrnout všechny možnosti, které ZoPS v ustanovení § 3 udává. Zvláštností je to, že například žádost o povolení k činnosti pro správce informování o platebním účtu se podává pouze elektronicky[20].

---

[14] Komerční banka spolupracuje s BudgetBakers. In: *Komerční banka* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2019/komercni-banka-spolupracuje-s-budgetbakers

[15] HINGAR, Petr. Otevřené bankovnictví, PSD2, open API a BankID aneb Změna paradigmatu ve finančním sektoru. *SystemOnline.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.systemonline.cz/it-pro-banky-a-financni-organizace/otevrene-bankovnictvi-psd2-open-api-a-bankid.htm

[16] VEJVODOVÁ, Alžběta. Platební revoluce se nekoná. O licence na nové služby není v Česku zájem. *Právní rádce* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-66152590-platebni-revoluce-se-nekona-o-licence-na-nove-sluzby-neni-v-cesku-zajem

[17] § 7 ZoPS

[18] § 8 Ibid.

[19] § 10 ZoPS

[20] § 10, odst. 1 Ibid.

Vyhláška č. 1/2022 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku a vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu upravují náležitosti těchto žádostí a podmínky k výkonu činnosti.

Výše se zmiňuji o zdlouhavosti udělení povolení k činnosti, ZoPS udává lhůtu 3 měsíce[21] od zahájení řízení, který je správním řízením[22]. To by se mohlo zdát jako relativně krátká doba, avšak pokud žádost nemá předepsané náležitosti či trpí jinými podstatnými vadami, zastavuje se běh lhůty a obnoví se až po odstranění těchto vad. Často toto řízení zdržuje nedokonalý obchodní plán a nepřizpůsobené vnitřní předpisy těch právnických osob, které se o licenci uchází[23]. Ve výsledku tyto chyby zapříčinily, že některé české společnosti, jmenovitě například Spendee, nestihly nástup konkurence z ostatních zemí v Evropské unii, v důsledku čehož jsou nyní „biti". Mou zkušenost sdílí a potvrzují i kolegové z Deloitte Legal[24].

Samotné požadavky z výše uvedených vyhlášek je dle mého názoru složité splnit a vyžaduje obrovské množství času, úsilí, a hlavně finančních prostředků k zhotovení podání samotné žádosti. Nepočítám ani vynaložení určité části rozpočtu budoucího poskytovatele platebních služeb pro právní zastoupení, jelikož mám za to, že právní laik nemá šanci je splnit a být v souladu se všemi právními předpisy.

1.1. Česká fintech asociace

České fintech společnosti mají vlastní asociaci, ve které se sdružují. Česká fintech asociace vznikla v září 2016. Účelem této asociace je „poskytování obecně prospěšných služeb především v oblasti vedení a propagace odborné diskuse v oblasti rozvoje poskytování finančních služeb za pomoci internetu a moderních informačních a telekomunikačních technologií (dále jen FinTech) mezi zástupci

[21] § 10, odst. 2 ZoPS

[22] BERAN, Jiří. § 10 [Řízení o žádosti o udělení povolení k činnosti platební instituce]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[23] TÓTHOVÁ, Lucia. Jak těžké je získat PSD2 licenci? *#fintechcowboys.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://fintechcowboys.cz/rozhovor-jak-tezke-je-ziskat-psd2-licenci/

[24] FABIÁNEK, Roman a Štěpán KALUHA. Pět zkušeností s licencováním aneb na co se připravit, když si půjdete k ČNB pro licenci. DReport [online]. [cit. 2022-12-26]. Dostupné z: https://www.dreport.cz/blog/pet-zkusenosti-s-licencovanim-aneb-na-co-se-pripravit-kdyz-si-pujdete-k-cnb-pro-licenci/?linkId=183230940

uživatelů, právnických a fyzických osob, organizací akademické, veřejné a neziskové sféry, dále vzdělávání veřejnosti ohledně nových možností a příležitostí, které poskytuje FinTech, a celková podpora odvětví FinTech“[25]. Uvnitř asociace jsou založeny pracovní skupiny pro legislativu a krypto assets[26]. Pořádají vzdělávací semináře, konference a vydávají analýzy.

Jejich řádní členové jsou aktivní v oblasti FinTech[27]. Mezi řádné členy patří výše zmínění BudgetBakers a Spendee. Nelze však opomenout další známé společnosti, jako jsou GoPay, PayU nebo Twisto.

1.2. Česká bankovní asociace

Banky v České republice mají taktéž svou vlastní asociaci, ve které se sdružují. Česká bankovní asociace vznikla v únoru 1992 a má za cíl „rozvoj českého bankovního sektoru, celé naší ekonomiky a finanční gramotnosti Čechů.“[28] Asociace pořádá konference, provozuje vzdělávací projekty jako například Bankéři do škol, #BezpecneBanky[29]. Je součástí Evropské bankovní federace, Evropské rady pro platby, Evropského ústavu pro peněžní trhy. Angažuje se v prevenci kriminality, udržitelnosti a zejména ve snížení uhlíkové stopy během poskytování služeb[30]. Sdružuje 32 bank, což představuje 99 % bankovního trhu[31]. Není třeba více představovat například Českou spořitelnu, Komerční banku a další velké banky.

Česká bankovní asociace je průkopníkem v digitalizaci, což dokazuje projektem Českého standardu pro Open banking (níže v kapitole 1.3.1) a nově průlomovou ZoBID. Tento zákon byl nominován v anketě Zákon roku 2020

[25] Výpis ze spolkového rejstříku - Česká fintech asociace, z.s., L 66392 vedená u Městského soudu v Praze. *Veřejný rejstřík a sbírka listin* [online]. [cit. 2021-03-15]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=944463&typ=PLATNY

[26] Projekty a znalosti. *Česká fintech asociace* [online]. [cit. 2021-03-15]. Dostupné z: http://czechfintech.cz/projekty-a-znalosti/

[27] Stanovy České fintech asociace, z.s., *Česká fintech asociace* [online]. [cit. 2021-03-15]. Dostupné z: http://czechfintech.cz/wp-content/uploads/2018/01/Stanovy_Ceska_fintech_asociace.pdf

[28] Kdo jsme a co děláme. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/co-delame

[29] Naše projekty. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/nase-projekty

[30] Kdo jsme a co děláme. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/co-delame

[31] Členové asociace. *Česká bankovní asociace* [online]. [cit. 2023-07-30]. Dostupné z: https://cbaonline.cz/clenove

pořádané advokátní kanceláří Deloitte Legal. ZoBID v konečném zúčtování danou anketu opanoval[32].

1.3. Open banking standard

Už před příchodem směrnice PSD2 se hodně mluvilo o open banking trendu, který otevírá přístup k datům klientů bank pro třetí strany. Směrnice PSD2 určuje, které služby mají být dostupné pro třetí stranu, jmenovitě služba nepřímé dání platebního příkazu, služba informování o platebním účtu a služba potvrzování zůstatku peněžních prostředků pro vydavatele karetních prostředků (zkráceně CIS), však nevytvořila jednotný standard, který by vyřešil přístup třetích stran k datům o klientech, a proto různé asociace a skupiny vytvořily svůj vlastní open banking standard, jako například v České republice nebo ve Velké Británii.[33] Tyto standardy by měly poskytnout základní technický rámec pro API bank, které se zúčastní daného standardu[34]. Rozdíl v těchto standardech můžeme najít například v tom, že mají: „Jiné sady URL, jiné HTTP metody u semanticky stejných API, jiné struktury JSON request/response objektů.“[35] Což jsou zkrátka technické specifikace pro API, které Evropská unie ve směrnici PSD2 neupravila.

API je zkratkou pro Application Programming Interface, „rozumí se tím rozhraní pro aplikace a jejich programování. Jedná se o balík knihoven, funkcí, procedur, protokolů a tříd, které mohou programátoři používat pro komunikaci se softwarem. Funkce rozhraní jsou na bázi programových celků, které programátoři používají a nemusejí je tak sami programovat. Cílem API je komunikace mezi 2 aplikacemi, kterým je tak umožněna výměna dat. Komunikaci lze nastavit jak jednosměrnou, tak i obousměrnou.“[36]

Přístup přes API je dle mého názoru klíčovým pro FinTech sektor, zejména pro poskytovatele služby informací o platebním účtu a poskytovatele služby přímé dání platebního příkazu, jelikož není třeba vyžadovat od uživatele těchto služeb

[32] Bankovní identita zvítězila v anketě Zákon roku 2020. DReport [online]. 2021, 21. 4. 2021 [cit. 2022-03-11]. Dostupné z: https://www.dreport.cz/blog/bankovni-identita-zvitezila-v-anketezakon-roku-2020/

[33] HINGAR, Petr. Otevřené bankovnictví, PSD2, open API a BankID aneb Změna paradigmatu ve finančním sektoru. *SystemOnline.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.systemonline.cz/it-pro-banky-a-financni-organizace/otevrene-bankovnictvi-psd2-open-api-a-bankid.htm

[34] BARTÁČEK, Václav. Představení PSD2 nejen pro vývojáře. Blíží se otevřené bankovnictví? Udělejte si v tom jasno. *Zdroják.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://zdrojak.cz/clanky/psd2-nejen-pro-vyvojare/

[35] Ibid.

[36] Co je to API (application programming interface)? *Topranker.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://topranker.cz/slovnik/co-je-to-api-application-programming-interface/

jeho přístupové údaje do jeho internetového bankovnictví a přístup přes screen scraping, který je těžkopádný a každá malá změna v internetovém bankovnictví může znehodnotit získaná data. Open banking by měl tuto zastaralou metodu časem zcela nahradit.

Za průkopníka v České republice by se dala pasovat České spořitelna, která už v roce 2015[37], před účinností ZoPS otevřela své API třetím stranám a umožnila jim přístup do klientských dat. Česká spořitelna pořádala v roce 2017 Open banking & WebAPI festival, na kterém proběhly workshopy, kde „účastníci hledali odpovědi na to, jak sestavovat nové aplikace, nasazovat je a snadno dosáhnout jejich vysoké dostupnosti, například při detekci anomálních transakcí na účtu. A nejen to, během hackathonu také vymýšleli způsob, jak platit hlasem nebo pracovat s aplikací, která by hlídala vývoj kurzu Bitcoin.“[38]

Myslím si, že pro případnou novou směrnici PSD3 by bylo velice vhodné harmonizovat open banking standardy napříč celou Evropskou unií a ulehčit tak více FinTech společnostem přístup na nové trhy členských států, jelikož samotné rozdíly mezi standardy jednotlivých států mohou učinit ne jeden problém programátorům a oddálit i případný vstup některých slibných služeb na další trhy členských států. V tomto ohledu si myslím, že zákonodárce byl velmi benevolentní a dal prostor tam, kde podle mého neměl.

1.3.1. Český Open banking standard

Český standard pro Open banking byl představen ke konci roku 2017 Českou bankovní asociací, která jej vypracovala. Tento standard upravuje například API rozhraní pro níže popsané služby v kapitole 1.4 a 1.5, jmenovitě služby nepřímé dání platebního příkazu, služby informování o platebním účtu[39].

V současné době je Český standard pro Open banking ve verzi 6.0, která byla zveřejněna v lednu 2023. Standard je v souladu s doporučeními České národní banky. Někteří členové asociace se však mohou odchýlit od tohoto standardu v určitých jeho částech[40].

---

[37] Jsou otevřená data příležitostí pro banky? Největší festival nad otevřenými daty v ČR. *Česká spořitelna* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2017/11/23-1/nejvetsi-festival-nad-otevrenymi-daty-v-cr

[38] Ibid.

[39] Český standard pro Open banking. *Česká bankovní asociace* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesky-standard-pro-open-banking

[40] Ibid.

Je důležité zdůraznit, že Český standard pro Open banking je nezávazný standard, který je na bázi dobrovolnosti[41] a používají ho někteří členové České bankovní asociace. Jak zmiňuje třeba společnost Spendee, přihodilo se jim například to, že nejmenovaná banka bez oznámení změnila strukturu v API a zapříčinilo to problémy jak společnostem provozujícím aplikaci Spendee, tak i samotným jejím uživatelům[42]. Takovému chování ze strany bank by se předešlo, kdyby tyto standardy byly harmonizovány.

1.3.2. Britský Open banking standard

Velká Británie, jako členský stát Evropské unie do února 2020, v rámci směrnice PSD2 implementovala open banking do svého právního řádu jako všechny ostatní členské státy. Myslím si, že Velká Británie může být vzorem pro ostatní členské státy Evropské unie, s tím jakým způsobem se s open banking vypořádala.

Britský Open Banking je v některých věcech odlišný od kontinentálního open banking. V roce 2017 do britského Open Banking vstoupilo 52 bank, z nichž 9 největších povinně[43]. Jiný přístup spočívá v tom, že britská Competition & Markets Authority může povolit přístup k datům klientů třetím stranám, které nemusí být regulovaným poskytovatelem platebních služeb[44]. Díky tomuto kroku můžou třeba cenové vyhledávače pomoci uživatelům vybrat výhodnější službu přímo na míru pro klienty[45].

Na obrázku 1 situovaném na následující straně můžeme vlevo vidět klasické schéma uzavřeného bankovnictví, které bylo před zavedením směrnice PSD2 a její implementace do vnitrostátních právních řádů členských států, vpravo můžeme názorně vidět, jak funguje open banking ve Velké Británii.

Obrázek 1 *– Porovnání uzavřeného a otevřeného bankovnictví*

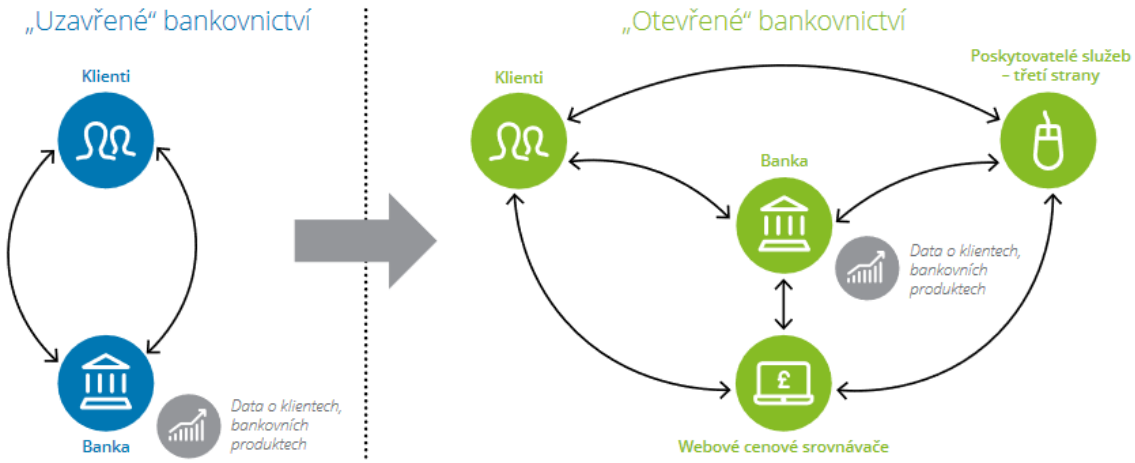
[41] SECHTER, Jakub. Jak jsou české banky s nástupem PSD2 otevřené svým klientům? *Lupa.cz* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.lupa.cz/clanky/jak-jsou-ceske-banky-s-nastupem-psd2-otevrene-svym-klientum/

[42] Ibid.

[43] FAQs. *Open Banking* [online]. [cit. 2021-03-15]. Dostupné z: https://www.openbanking.org.uk/customers/faqs/

[44] Jak prosperovat v nejisté době. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-otevrene-bankovnictvi-a-psd2.pdf, s. 10, 11

[45] Ibid.



Upraveno ze zdroje: Jak prosperovat v nejisté době. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-otevrene-bankovnictvi-a-psd2.pdf, s. 11

1.3.3. NextGenPSD2 a openFinance Framework

Posledním příkladem, který uvedu pro open banking standard, je standard z dílny iniciativy The Berlin Group, která svůj standard nazvala NextGenPSD2. Velkou výhodou tohoto standardu bylo množství účastníků, které přesáhlo přes 70 společností, z tohoto počtu až 75 % evropských bank[46].

Od 1. února 2021 se NextGenPSD2 stala součástí openFinance Framework, která je novou infrastrukturou pro banky a třetí strany. Umožní poskytování dalších služeb, které směrnice PSD2 neupravuje, jako třeba platba půjčkou[47]. Dá se říct, že openFinance Framework poskytne služby, které byly zmíněny v kapitole 1.3.2 a umožní tak FinTech společnosti a další společnosti rozšířit pole působnosti, což bude pouze výhoda pro budoucí uživatele.

V rámci strategie Evropské unie pro digitální finance připravuje Evropská komise návrh nařízení k openFinance Framework (*česky Rámec pro oteveřené financování*). Od května do srpna 2022 bylo období pro zasílání připomínek a veřejné konzultace. „Cílem této iniciativy je umožnit v souladu s pravidly pro ochranu údajů a spotřebitele sdílení údajů a přístup třetích stran do širší škály finančních odvětví a produktů. Vychází se při tom ze zásady, že zákazníci finančních služeb vlastní a kontrolují údaje, které dodávají, a údaje vytvořené jejich

[46] PSD2 Access to Bank Accounts. *The Berlin Group* [online]. [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/psd2-access-to-bank-accounts

[47] PRESS RELEASE - Berlin Group starts new openFinance API Framework. *The Berlin Group* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework

jménem.“[48] Evropská komise plánovalo přijetí nařízení ve druhém čtvrtletí 2023, avšak původně přijetí mělo proběhnout během čtvrtého čtvrtletí 2022. V současné době je daný návrh nařízení v Evropské komisi a je ve fázi období pro zasílání připomínek.[49]

1.4. Služba informování o platebním účtu – AIS

Jednou z novinek směrnice PSD2, která je, troufám si tvrdit, jednou ze stěžejních pro současnou open banking platformu, představuje služba informování o platebním účtu. Již v samotném úvodu této kapitoly jsem nastínil, že služba informování o platebním účtu může mít spoustu funkcionalit, které používáme na denní bázi. Více o praktickém využití v kapitole 1.6, kde se služba informování o platebním účtu nejvíce využívá v rámci multibankingu.

ZoPS přímo definuje službu informování o platebním účtu takto: „služba spočívající ve sdělování informací o platebním účtu prostřednictvím internetu poskytovatelem rozdílným od poskytovatele, který vede daný platební účet“[50]. Služba informování o platebním účtu je jinak známá pod anglickým termínem „Account Information Services“ nebo pod zkratkou AIS nebo ve frankofonních zemích známá jako „Le service d’information sure les comptes“. Ve směrnici PSD2 ji najdeme pod označením služba informování o účtu.

Tato služba je poskytována uživateli a považuji za důležité zdůraznit, že nezahrnuje situace, kdy informace o platebním účtu zpřístupňují jiným osobám, například bance při posuzování úvěruschopnosti klienta, například při spotřebitelském úvěru. Pokud tedy s tím uživatel výslovně nebude souhlasit, že taková data poskytne banka třetí straně k tomuto účelu[51].

Informace z platebních účtů před příchodem směrnice PSD2 a implementace do právních řádů členských států Evropské unie (u nás ZoPS) se čerpaly jinými způsoby než přes API rozhraní bank. Existovaly služby, které fungovaly na bázi nahrávání dat z platebního účtu (například ve strojově čitelném formátu .csv nebo .xml), výpisů v .pdf, přístupem přes internetové bankovnictví

[48] Rámec pro otevřené financování – možnost sdílení údajů a přístupu třetích stran ve finančním odvětví. Evropská komise [online]. [cit. 2022-12-26]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13241-Ramec-pro-otevrene-financovani-moznost-sdileni-udaju-a-pristupu-tretich-stran-ve-financnim-odvetvi_cs

[49] Ibid.

[50] § 2, odst. 1, písm. l) ZoPS

[51] STRNADEL, Dalibor, Tomáš Nýdrle. § 2 Vymezení některých pojmů. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

nebo propojení aplikace s notifikačními e-maily, které zasílala banka uživateli. Šlo zejména o aplikace/služby, které se věnovaly správě financí[52]. Například služba Spendee, o které jsem psal výše v této kapitole 1, stále dává možnost nahrání .xls, .xlsx nebo CSV souboru[53], který vygeneruje v internetovém bankovnictví na příkaz uživatele, který má zájem o zaznamenání transakcí do aplikace a nechce použít službu informování o platebním účtu.

Zajímavostí je, že zákonodárce uvedl službu informování o platebním účtu jako platební službu, která je definovaná v ustanovení § 3 ZoPS, a přitom se tato služba dá těžko nazvat jako platební služba, jelikož není „navázána na žádné převody peněžních prostředků ani platební příkazy k těmto převodům“ [54]. Lze se domnívat, že jde o snahu zjednodušit poskytovatelům služby informování o platebním účtu (*anglicky* Account Information Services Provider, neboli ve zkratce AISP) o snazší přístup na trhy v členských zemích Evropské unie s ohledem na získané povolení k činnosti od České národní banky[55].

1.4.1. Práva a povinnosti poskytovatele, který vede platební účet

Ihned na začátku je zapotřebí si ujasnit práva a povinnosti poskytovatelů, kteří vedou platební účet uživatele, následně práva a povinnosti poskytovatelů služby informování o platebním účtu.

Ze zákona vyplývá, že předtím než poskytovatel, který vede platební účet (typicky banka) poskytne další třetí straně informace (typicky poskytovatel služby informování o platebním účtu), které jsou jinak „přístupné uživateli prostřednictvím internetu“[56], musí získat souhlas uživatele ke sdělení informací o platebním účtu.

Důležitá je interpretace toho, co znamenají informace dostupné uživateli prostřednictvím internetu. Prostřednictvím internetu můžeme přistoupit ke svému platebnímu účtu přes mobilní aplikaci na svých chytrých telefonech nebo

---

[52] STRNADEL, Dalibor, Tomáš Nýdrle. § 2 Vymezení některých pojmů. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[53] How to import data? *Spendee Help Center* [online]. [cit. 2021-02-22]. Dostupné z: https://help.spendee.com/article/121-import-transactions

[54] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[55] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[56] § 191, odst. 1 ZoPS

prostřednictvím internetového bankovnictví na webovém prohlížeči. V aplikaci nebo v internetovém bankovnictví narazíme určitě na zůstatek na platebním účtu a pohyby na účtu (historie transakcí). Autoři komentáře k ZoPS se zabývají problematikou, zda patří do těchto informací rovněž nastavení trvalých příkazů nebo souhlasy s inkasem, které jsou prováděny z účtu nebo informace o přečerpání nebo informace o existenci jiného úvěrového rámce[57]. Dle mého názoru výše, informace, které uvádí autoři komentáře za příklad, patří do tohoto rámce. Musíme vzít na vědomí, jakou funkcionalitu služba informování o platebním účtu poskytuje uživatelům nebo může teoreticky poskytnout, a proto bych informace nad kterými uvažují autoři komentáře, zahrnul mezi sdílené informace, protože se mi nezdá, že by to bylo v rozporu s tím, čeho chtěl zákonodárce tímto ustanovením dosáhnout. Zejména v aplikacích, které spravují finance uživatelům, je záhodno započítávat platby, které mají odejít v příštím měsíci nebo o kterou částku přečerpal uživatel limit svého účtu. Správně autoři komentáře naráží na to, že každý poskytovatel platebního účtu, rozuměje banka, dává uživateli určitý okruh informací, avšak s příchodem open banking standardu si nemyslím, že je toto problém pro sdílení s třetími stranami.

Otazník visí nad tím, co znamená souhlas uživatele, o kterém referuje ustanovení § 191, odstavce 1 ZoPS a čím se uděluje tento souhlas. Jednou z možností může být obsažení daného souhlasu přímo ve smlouvě o poskytování platebních služeb, uzavřené mezi uživatelem a poskytovatelem, který vede platební účet. Tento souhlas má být dle směrnice PSD2 výslovný, avšak v praxi se tento požadavek nevyžaduje. Souhlas by měl být směrován vůči poskytovateli, který vede platební účet, ale může nastat i možnost, kdy souhlas může být dán přes poskytovatele služby informování o platebním účtu[58].

ZoPS zdůrazňuje, že: „Poskytovatel, který uživateli vede platební účet, nesmí činit neodůvodněné rozdíly mezi žádostmi o informace o platebním účtu.“[59] Poskytovatel, který vede platební účet, by tedy neměl diskriminovat a rozlišovat

[57] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[58] Ibid.

[59] § 191, odst. 2 ZoPS

žádosti, které jsou přímo od uživatele (například z internetového bankovnictví) nebo prostřednictvím třetí strany, tedy nepřímo od uživatele[60].

Poskytovatel, který vede platební účet, může ze zákonných důvodů odmítnout sdělit informace o platebním účtu poskytovateli služby informování o platebním účtu. V případě, že nastane jeden či více níže uvedených případů, poskytovatel, který vede platební účet, nemusí přistoupit k odmítnutí sdělit informace poskytovateli služby informování o platebním účtu[61]. ZoPS udává následující důvody:

„a) má-li podezření na neautorizované nebo podvodné použití platebního prostředku, nebo osobních bezpečnostních prvků uživatele,

b) není-li poskytovatel, který žádá o informace, oprávněn poskytovat službu informování o platebním účtu, nebo

c) neosvědčil-li poskytovatel služby informování o platebním účtu svoji totožnost v souladu s § 192 písm. c).“[62]

Prvním důvodem je tedy „podezření na neautorizované nebo podvodné použití platebního prostředku, nebo osobních bezpečnostních prvků uživatele“[63]. Může jít o případ, kdy poskytovatel, který vede platební účet, má podezření, že přístup k informacím o platebním účtu se chce dostat neoprávněná osoba bez souhlasu uživatele[64].

Dalším důvodem, kdy může poskytovatel, jenž vede platební účet odmítnout sdělit informace je tehdy, jestliže poskytovatel požadující informace nemá oprávnění danou službu poskytovat.

Na základě povolení k poskytování platebních služeb mohou banky a spořitelní a úvěrní družstva poskytovat tuto službu jako platební instituce. Platební instituce nebo instituce elektronických peněz musí mít službu informování o platebním účtu přímo uvedenou v povolení k činnosti nebo správci informací o platebním účtu, kteří získali povolení k činnosti[65]. Takoví poskytovatelé se

---

[60] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[61] Ibid.

[62] § 191, odst. 3 ZoPS

[63] Ibid.

[64] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[65] Ibid.

nazývají správci informací o platebním účtu. Seznam těchto poskytovatelů je dostupný na stránkách České národní banky.

Poslední důvod nastane v případě, pokud poskytovatel služby informování o platebním účtu neosvědčí totožnost „při každém dotazu na informace o platebním účtu“[66]. Pro takovou identifikaci „využívají poskytovatelé služby informování o platebním účtu kvalifikované certifikáty pro elektronické pečetě (srov. čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“[67].

Pokud nastane jeden z výše uvedených scénářů, poskytovatel, který vede platební účet, musí informovat uživatele o takové skutečnosti bez zbytečného odkladu. Jelikož pro přístup k těmto informacím na platebním účtu uživatele využívá v dnešní době API rozhraní, dle komentáře k ZoPS bude spíše docházet ke scénáři, kdy bude uživatel informován o odmítnutí sdělení informací poskytovateli služby informování o platebním účtu ex-post[68]. A to z toho důvodu, že informace „jsou poskytovány ve velmi krátkém čase po obdržení žádosti uživatele či třetí strany jednající jménem uživatele“[69].

Tímto ale nekončí informační povinnost poskytovatele, který vede platební účet, jelikož informační povinnost se netýká pouze uživatele, kterému vede platební účet, ale musí informovat bez zbytečného odkladu i Českou národní banku, která vydává povolení k činnosti těmto uživatelům a vykonává nad nimi dohled.

1.4.2. Požadavky pro poskytnutí služby informací o platebním účtu

Poskytovatel služby informování o platebním účtu má ze zákona povinnosti, které musí dodržet při poskytování dané služby. Možná se někteří mohou divit, proč tato skutečnost není uvedena v ZoPS jako požadavek pro správce informací o platebním účtu, ale nesmíme zapomenout na výše uvedená fakta v kapitole 1.4.1, že službu informování o platebním účtu mohou poskytovat jak správci informací o platebním účtu, kteří získali povolení k činnosti od České národní banky za účelem poskytnutí této služby, tak ale i banky a spořitelní a úvěrní družstva mají

[66] § 192, písm. c) ZoPS

[67] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[68] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[69] Ibid.

možnost poskytovat tuto službu dle povolení k poskytování platebních služeb. Mezi požadavky pro poskytovatele patří:

„a) poskytuje službu informování o platebním účtu na základě výslovného souhlasu, který mu uživatel udělil,

b) zpřístupní osobní bezpečnostní prvky uživatele pouze uživateli a tomu, kdo je vydal,

c) při každém dotazu na informace o platebním účtu osvědčí poskytovateli, který uživateli vede platební účet, svoji totožnost,

d) v souvislosti se službou informování o platebním účtu získává a zpracovává pouze informace o platebním účtu, který určil uživatel,

e) nepožaduje citlivé údaje o platbách uživatele a

f) v souvislosti se službou informování o platebním účtu nepožaduje od uživatele, neuchovává a nezpracovává jiné údaje o uživateli, nebo jeho platebním účtu než údaje potřebné k poskytnutí služby informování o platebním účtu.“[70]

Uživatel musí dát souhlas i poskytovateli služby informování o platebním účtu, neliší se to tedy od souhlasu poskytovateli, který vede platební účet. V tomto případě uživatel dává souhlas poskytovateli služby informování o platebním účtu tím, že se uzavře smlouva o platebních službách s tímto poskytovatelem. Každých 90 dnů musí proběhnout silné ověření uživatele, během kterého musí uživatel dát souhlas s tím, aby byly dále poskytovány údaje z platebního účtu tomuto poskytovateli služby informování o platebním účtu[71].

Dalším požadavkem pro zpřístupnění jsou „osobní bezpečnostní prvky uživatele pouze uživateli a tomu, kdo je vydal“[72]. Co je osobní bezpečnostní prvek? Takovým prvkem se rozumí „prvek, který poskytovatel poskytl uživateli za účelem ověření“[73].

Požadavkem osvědčení totožnosti poskytovatele „pro účely identifikace poskytovatelů se využívají kvalifikované certifikáty pro elektronické pečetě (srov.

[70] § 192 ZoPS

[71] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[72] § 192, písm. b) ZoPS

[73] § 2, odst. 3, písm. m) Ibid.

čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“[74].

Poskytovatel služby informování o platebním účtu může získat a zpracovávat pouze ty informace, které uživatel povolí. Myslím si, že je to správný krok, i kvůli tomu, že uživatel může nabýt pocitu, že v dnešním světě má šanci stále ovlivňovat data, která proudí internetem. Já osobně v současné době nevyužívám službu informování o platebním účtu, a kdybych se k tomu někdy uchýlil, nemyslím si, že budu potřebovat více než zůstatek na mém druhém bankovním účtu. S aplikací, která by mi spravovala finance, bych mohl nabýt jiného názoru, ale nemyslím si, že někdy takovou aplikaci využiji. Zejména s ohledem na můj skeptický pocit, že dávám své finanční údaje třetí straně.

Citlivým údajem o platbách uživatele se rozumí „údaj, který může být zneužit k podvodu v oblasti platebních služeb, s výjimkou jedinečného identifikátoru a jména majitele platebního účtu v případě poskytovatele služby informování o platebním účtu nebo služby nepřímého dání platebního příkazu“[75]. V praxi to znamená podle komentáře k ZoPS, že poskytovatel služby informování o platebním účtu nemá možnost přistupovat k účtu prostřednictvím uživatelského rozhraní[76].

Posledním požadavkem je, že poskytovatel služby informování o platebním účtu nesmí uchovávat, zpracovávat ani vyžadovat jiné údaje, které nejsou potřebné k poskytnutí dané služby[77].

Nelze však opomenout povinnost vyplývající z ustanovení § 49, odst. 1 ZoPS, který zavádí informační povinnost a uchovávání dokumentů a záznamů.

Informační povinnost poskytovatele zahrnuje zejména: „finanční situaci, výsledcích svého hospodaření, plnění podmínek výkonu své činnosti“[78]. Vyhláška č. 454/2017 Sb., o informačních povinnostech některých osob oprávněných poskytovat platební služby nebo vydávat elektronické peníze stanoví podrobnější

[74] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[75] § 2, odst. 3, písm. n) ZoPS

[76] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[77] § 192, písm. f) ZoPS

[78] § 30, odst. 1 Ibid.

výkazy, které musí správce informací o platebním účtu sestavovat. Jedná se například o čtvrtletní rozvahu[79] a čtvrtletní výkaz zisku a ztráty[80].

Ohledně uchovávání dokumentů a záznamů, které se týkají plnění povinností se musí uchovávat „alespoň po dobu 5 let ode dne, kdy tyto dokumenty nebo záznamy vznikly“[81].

1.4.3. Povolení k činnosti pro správce informací o platebním účtu od České národní banky

V kapitole 1.4.1 se zmiňuji o tom, že banky, spořitelní a úvěrní družstva mohou jako poskytovatelé platebních služeb poskytovat službu informování o platebním účtu, avšak mezi poskytovatele se mohou zařadit i další, a to správci informací o platebním účtu.

ZoPS definuje správce informací o platebním účtu jako toho, „kdo je oprávněn poskytovat službu informování o platebním účtu na základě povolení k činnosti správce informací o platebním účtu, které mu udělila Česká národní banka.“[82]

Žádost žadatel podává elektronicky, musí splnit podmínky (vizte kapitola 1.4.3.1), které žadatel doloží potřebnou dokumentací.[83] Tato žádost musí splňovat náležitosti zákona č. 500/2004 Sb., správní řád, konkrétně ustanovení § 37 a náležitosti z vyhlášky č. 1/2022 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku, konkrétně ustanovení § 6, mezi které zahrnuje například zakladatelské právní jednání. V souvislosti s podáním žádosti platí žadatel správní poplatek, který je dán zákonem č. 634/2004 Sb., o správních poplatcích, který udává částku 25 000 Kč[84].

V případě, že se v žádosti změní údaje nebo přílohy, musí žadatel nebo správce informací o platebním účtu (pokud už má povolení k činnosti) oznámit tyto změny bez zbytečného odkladu České národní bance.[85]

Česká národní banka dle ZoPS má povinnost do 3 měsíců od zahájení řízení vydat rozhodnutí, avšak v případě neúplnosti žádosti nebo podstatných vad, které

[79] § 4, odst. 4, písm. a) vyhlášky č. Vyhláška č. 454/2017 Sb., o informačních povinnostech některých osob oprávněných poskytovat platební služby nebo vydávat elektronické peníze
[80] Ibid.
[81] § 31, odst. 1 ZoPS
[82] § 41 Ibid.
[83] § 43, odst. 1 ZoPS
[84] Příloha [Sazebník], ČÁST IV, položka 65, písm. p) zákona č. 634/2004 Sb., o správních poplatcích
[85] § 44, odst. 1 ZoPS

brání v pokračování řízení, se lhůta zastaví a započně běžet ode dne jejich odstranění.[86] V médiích proběhly zprávy, kdy si první subjekt s tímto povolením stěžoval, že proces trval dlouho, a tak přišel o konkurenční náskok[87].

Nutno dodat, že správce informací o platebním účtu může poskytovat pouze danou službu a žádnou další platební službu[88].

1.4.3.1. Podmínky pro žadatele

Na samotném začátku této podkapitoly považuji za důležité zmínit, že správcem se může stát jak právnická osoba, tak i fyzická osoba.[89] K tomu, aby se žadatel mohl stát správcem informací o platebním účtu, musí splnit následující zákonné podmínky:

„a) který má sídlo i skutečné sídlo v České republice,

b) jehož obchodní plán, včetně předpokládaného rozpočtu na první 3 účetní období, je podložen reálnými ekonomickými propočty,

c) v jehož prospěch je uzavřena pojistná smlouva nebo poskytnuto srovnatelné zajištění v souladu s tímto zákonem,

d) jehož věcné, technické, personální a organizační předpoklady jsou vhodné z hlediska řádného a obezřetného poskytování služby informování o platebním účtu,

e) jehož řídicí a kontrolní systém splňuje požadavky stanovené tímto zákonem,

f) jehož vedoucí osoby jsou důvěryhodné z hlediska řádného a obezřetného poskytování služby informování o platebním účtu,

g) jehož vedoucí osoby v oblasti poskytování služby informování o platebním účtu jsou odborně způsobilé a mají dostatečné zkušenosti z hlediska řádného a obezřetného poskytování služby informování o platebním účtu,

h) u něhož nenastala skutečnost, která zakládá překážku provozování živnosti podle zákona upravujícího živnostenské podnikání, a

i) který, je-li fyzickou osobou, splňuje všeobecné podmínky provozování živnosti podle zákona upravujícího živnostenské podnikání.“[90]

---

[86] § 43, odst 2 ZoPS

[87] BEDRICH, Vaclav. Český fintech Spendee získal od ČNB jako první licenci k přímému propojení s bankami. *CzechCrunch* [online]. 2018 [cit. 2021-03-09]. Dostupné z: https://www.czechcrunch.cz/2018/12/cesky-fintech-spendee-ziskal-od-cnb-jako-prvni-licenci-k-primemu-propojeni-s-bankami/

[88] § 49, odst. 2 ZoPS

[89] BERAN, Jiří. § 41 [*Správce informací o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[90] § 42, odst. 1 ZoPS

Jak komentář k ZoPS připomíná, podmínky jsou vcelku podobné těm, které jsou dané pro povolení k činnosti platební instituce[91].

První podmínkou ZoPS je to, aby žadatel měl sídlo a skutečné sídlo na území České republiky. Definici sídla nalezneme v Občanském zákoníku, kdy se sídlo podnikatele „určí adresou zapsanou ve veřejném rejstříku“[92]. Veřejným rejstříkem rozumíme dle zákona o veřejných rejstřících právnických a fyzických osob: „spolkový rejstřík, nadační rejstřík, rejstřík ústavů, rejstřík společenství vlastníků jednotek, obchodní rejstřík a rejstřík obecně prospěšných společností.“[93] Sídlem tedy rozumím adresu, kterou můžeme naleznout například třeba u právnické osoby v obchodním rejstříku. Skutečné sídlo je místo „odkud daný podnikatel řídí své obchodní aktivity (NS 29 Cdo 1953/2013), kde je místo správy společnosti (NS 29 Cdo 1680/2009, 29 Cdo 4993/2008), kde se veřejnost může s podnikatelem stýkat (srov. § 19c odst. 2 ObčZ 1964 ve znění účinném do 19. 7. 2009).“[94]

Neméně důležitou podmínkou je obchodní plán žadatele spolu s rozpočtem na první tři účetní období. Obchodní plán je definován ve vyhlášce č. 1/2022 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku. Obchodní plán zahrnuje následující:

„a) marketingový plán zahrnující analýzu konkurenčního postavení žadatele v příslušném segmentu trhu platebních služeb nebo trhu elektronických peněz a popis cílové skupiny uživatelů, propagačních materiálů, distribučních kanálů a zeměpisných oblastí činnosti,

b) finanční výkazy,

c) finanční plán na první 3 účetní období, který obsahuje

1. rozvahu a výkaz zisku a ztráty nebo výkaz o úplném výsledku hospodaření ve struktuře podle účetní závěrky, a to na základě predikce základního i zátěžového scénáře, a základní předpoklady, na nichž jsou tyto predikce založeny, jako jsou alespoň údaje o předpokládaném objemu platebních transakcí a hodnotě platebních transakcí souvisejících

[91] BERAN, Jiří. § 42 [*Podmínky pro udělení povolení k činnosti správce informací o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[92] § 429, odst. 1 Občanského zákoníku

[93] § 1, odst. 1 zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob

[94] ZAPLETAL, Jiří. § 429 [*Sídlo podnikatele*]. In: PETROV, Jan, Michal VÝTISK, Vladimír BERAN. Občanský zákoník: komentář. 2. vydání. V Praze: *C.H. Beck*, 2019. Beckova edice komentované zákony. ISBN 978-80-7400-747-7.. ISBN 978-80-7400-747-7, s. 461.

a nesouvisejících s elektronickými penězi, předpokládaném počtu uživatelů služeb a držitelů elektronických peněz a počtu klientských účtů, tvorbě cen, předpokládané průměrné částce platební transakce a předpokládaném růstu ziskovosti vyjádřené jako podíl výsledku hospodaření po zdanění k úhrnu aktiv a podíl výsledku hospodaření po zdanění k vlastnímu kapitálu,

2. vysvětlení hlavních příjmů a výdajů, závazků a dlouhodobých aktiv a

3. schéma toku peněžních prostředků prováděné platební transakce,

d) v případě platební instituce, instituce elektronických peněz nebo poskytovatele platebních služeb malého rozsahu nebo vydavatele elektronických peněz malého rozsahu podle § 59 odst. 3 a § 100 odst. 3 zákona výši a složení počátečního kapitálu, výši a složení kapitálu podle vyhlášky upravující některé podmínky výkonu činnosti osob povolovaných podle zákona,

e) v případě platební instituce nebo instituce elektronických peněz minimální výši kapitálového požadavku podle vyhlášky upravující některé podmínky výkonu činnosti osob povolovaných podle zákona a návrh přístupu, který bude platební instituce nebo instituce elektronických peněz uplatňovat při výpočtu kapitálové přiměřenosti, a zdůvodnění volby navrhovaného přístupu, a uvedení výpočtů kapitálové přiměřenosti, včetně použitých údajů, podle všech přístupů ve struktuře podle hlášení o kapitálu platební instituce nebo instituce elektronických peněz upraveného vyhláškou o informačních povinnostech některých osob podle zákona,

f) v případě poskytovatele platebních služeb malého rozsahu nebo vydavatele elektronických peněz malého rozsahu vyhodnocení plnění limitů podle § 58 odst. 2 a § 99 odst. 2 a 3 zákona těmito osobami a jejich pověřenými zástupci na prvních 12 měsíců provozování požadovaných činností v členění podle jednotlivých osob a podle jednotlivých měsíců,

g) v případě poskytovatele platebních služeb malého rozsahu nebo vydavatele elektronických peněz malého rozsahu údaje o ovládající osobě a všech osobách ve skupině, které jsou poskytovateli platebních služeb malého rozsahu nebo vydavateli elektronických peněz malého rozsahu poskytujícími platební služby nebo vydávajícími elektronické peníze a uvedení hodnoty platebních transakcí podle § 58 odst. 2 a § 99 odst. 2 a 3 zákona poskytnutých těmito osobami a jejich pověřenými zástupci za poslední 3 roky, a to v členění podle jednotlivých osob a podle jednotlivých měsíců, a

h) popisu opatření k zamezení překročení limitů podle § 58 odst. 2 a § 99 odst. 2 a 3 zákona.“[95].

V návaznosti na obchodní plán je podmínka věcných, technických, personálních a organizačních předpokladů[96], které se posuzují právě v návaznosti na obchodní plán, který předkládá žadatel České národní bance. Obchodní plán má obsahovat plán, jak zajistí právě tyto předpoklady, které by měly být v souladu s řádným a obezřetným poskytováním této služby[97].

Žadatel musí uzavřít pojistnou smlouvu nebo zajištění, které stanoví ustanovení § 46 ZoPS. Povinnost uzavřít pojišťovací smlouvu nebo mít dostatečné zajištění vyplývá z toho, že správci informací o platebním účtu nemusí splňovat kapitálové požadavky z důvodu nepřijetí peněžních prostředků[98]. Pojistná smlouva nebo zajištění má zajistit právo na plnění, pokud správce informací o platebním účtu neoprávněně získá nebo užije informaci o platebním účtu. Vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu stanoví minimální limit pojistného plnění a minimální výši zajištění, který je daný v závislosti na:

„a) rizika, kterým je nebo může být správce informací o platebním účtu vystaven,
b) jiné činnosti správce informací o platebním účtu,
c) vlastnosti srovnatelného zajištění a
d) počet uživatelů služby informování o platebním účtu.“[99]

Řídící a kontrolní systém žadatele musí splnit požadavky, které ZoPS udává v ustanovení § 47, což znamená, že musí vykonávat správu řádně a obezřetně. Tento výklad se dá vyložit jako ustanovení § 19 ZoPS, které nastavuje stejnou povinnost platební instituci. Řádný výkon se dá vyložit jako výkon činnosti „v souladu s požadavky vyplývajícími z právních předpisů“[100], který je dle autorů

[95] Příloha č. 2 k vyhlášce č. 1/2022 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku

[96] § 42, odst. 1, písm. e) ZoPS

[97] BERAN, Jiří. § 9 [*Podmínky pro udělení povolení k činnosti platební instituce*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[98] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

[99] § 46, odst. 2 ZoPS

[100] BERAN, Jiří. § 19 [*Řádný a obezřetný výkon činnosti platební instituce*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI].

komentáře k ZoPS vůdčím principem než povinnost. Obezřetný výkon je zejména minimalizace rizik, vůči kterým správce může být vystaven[101]. Řídící a kontrolní systém je „soubor zásad a postupů“[102], která by měla obsahovat ve vnitřních předpisech žadatele. Předpoklady jsou obsaženy ve vyhlášce č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu.

Vedoucí osoby by měli být důvěryhodné, odborně způsobilé a mít dostatečné zkušenosti. ZoPS udává, že „za důvěryhodnou považuje osoba, jejíž dosavadní činnost dává předpoklad řádného výkonu činnosti“[103]. Česká národní banka ve svém výkladu udává, že obecným kritériem je dodržování právních a etických pravidel, morálního profilu a integrity. Česká národní banka posuzuje i její bezúhonnost. K posouzení používá podklady z veřejně dostupných zdrojů, vlastního zjištění a z podkladů od posuzované osoby[104].

Odbornou způsobilost zkoumá Česká národní banka dle znalostí, odborné praxe na finančním trhu, manažerské praxe a z dosavadního působení na finančním trhu, kterou posuzuje taktéž z výše uvedených zdrojů, jako u důvěryhodnosti[105].

Mezi poslední podmínky z tohoto výčtu patří:

a) požadavek, aby nenastala překážka provozování živnosti, kterou ZoPS odkazuje na zákon č. 455/1991 Sb., o živnostenském podnikání, který v ustanovení § 8 poskytuje výčet překážek provozování živnosti, zejména v souvislosti s prohlášením konkurzu na majetek fyzické či právnické osoby nebo insolvenčním řízením, a

b) v případě fyzické osoby, aby splňovala „všeobecné podmínky provozování živnosti“[106], což znamená opět exkurz do zákona č. 455/1991 Sb., o živnostenském podnikání, který v ustanovení § 6 stanoví plnou svéprávnost a bezúhonnost.

1.4.3.2. Zánik povolení k činnosti

Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[101] BERAN, Jiří. § 19 [*Řádný a obezřetný výkon činnosti platební instituce*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[102] Ibid.

[103] § 261 ZoPS

[104] Úřední sdělení České národní banky č. 18/2020 Věst. ČNB ze dne 5. srpna 2020 k výkladu pojmů důvěryhodnost a odborná způsobilost

[105] Ibid.

[106] § 42, odst. 1, písm. i) ZoPS

Zánik povolení k činnosti od České národní banky může nastat z následujících důvodů:

„a) smrti nebo zrušení správce informací o platebním účtu,

b) nabytí právní moci rozhodnutí o úpadku správce informací o platebním účtu,

c) vykonatelnosti rozhodnutí, kterým Česká národní banka udělila správci informací o platebním účtu povolení k činnosti platební instituce nebo povolení k činnosti instituce elektronických peněz, nebo

d) nabytí vykonatelnosti rozhodnutí o odnětí povolení k činnosti správce informací o platebním účtu.“[107]

1.4.4. Správci informací o platebním účtu v České republice

Vzhledem k tomu, že účinnost ZoPS je od 1. ledna 2018, na trhu se už vyskytli někteří správci informací o platebním účtu, kteří zdárně prošli řízením o žádosti o udělení povolení k činnosti a splnili všechny předpoklady dané ZoPS a souvisejícími prováděcími vyhláškami. Seznam těchto správců je volně dostupný na stránkách České národní banky. Každý uživatel, který má zájem použít službu informování o platebním účtu si může prověřit, zda poskytovatel má povolení k činnosti.

V současné době získaly pouze tři právnické osoby povolení k činnosti a to:

a) SPENDEE a.s.,

b) BudgetBakers s.r.o., a

c) 1. PF Finance, s.r.o[108].

Společnost SPENDEE a.s., IČO: 059 12 890, se sídlem náměstí I. P. Pavlova 1789/5, Nové Město, 120 00 Praha 2, Česká republika byla první společností, která získala povolení k činnosti jako správce informací o platebním účtu. Oprávněním k činnosti disponuje od 28. prosince 2018. Tato společnost provozuje aplikaci Spendee, kterou rozeberu více v kapitole 1.6.2.

Společnost BudgetBakers s.r.o., IČO: 028 82 957, se sídlem Radlická 180/50, Smíchov, 150 00 Praha 5, Česká republika, byla další společností, která získala oprávnění k činnosti od 12. prosince 2019. Provozuje aplikaci Wallet, která bude zmíněna více též v kapitole 1.6.2.

---

[107] § 45 ZoPS

[108] Správci informací o platebním účtu a pobočky zahraničních správců informací o platebním účtu (stav ke dni 29.07.2023). *Základní seznamy subjektů (výsledné sestavy)* [online]. [cit. 2023-07-29]. Dostupné z: https://apl.cnb.cz/apljerrsdad/JERRS.WEB15.BASIC_LISTINGS_RESPONSE_3?p_lang=cz&p_DATUM=29.07.2023&p_hie=HI&p_rec_per_page=25&p_ses_idx=355

Zatím poslední společností, která získala povolení k činnosti správce informování o platebním účtu k 29. července 2020, se stala společnost 1. PF Finance, s.r.o., IČO: 093 73 292, se sídlem Služská 1865/15, Kobylisy, 182 00 Praha 8, Česká republika. Společnost poskytuje ohodnocení bonity žadatele půjčky. Více v kapitole 1.6.3.

1.5. Služba nepřímé dání platebního příkazu – PIS

Další novou platební službou vycházející ze směrnice PSD2 je služba nepřímého dání platebního příkazu, která se využívá nejviditelněji v multibanking aplikacích. Službu nepřímého dání platebního příkazu zařazuji mezi zásadní novinky ze směrnice PSD2, potažmo ZoPS, jelikož se může stát velice žádanou alternativou k platbě kartou[109], například při nakupování na internetových na e-shopech. Výhodou této služby je, že při využití této služby nemusí prodejce hradit poplatek ve výši několika procent z prodejní ceny karetní asociaci (například VISA, Mastercard).

Na začátek musím podotknout, že jsem s příchodem směrnice PSD2 očekával, že služba nepřímé dání platebního příkazu bude žádanou službou a vítanou alternativou k platbě kartou v e-commerce oblasti, ale realita je značně odlišná. Například ve Velké Brátnii, za období od ledna 2018 do dubna 2019, získalo povolení pro poskytování služby informování o platebním účtu 80 poskytovatelů a jenom 30 poskytovatelů získalo povolení k činnosti služby nepřímého dání platebního příkazu[110].

V České republice službu nepřímého dání platebního příkazu „mohou poskytovat pouze banky, družstevní záložny, platební instituce nebo instituce elektronických peněz“[111]. Je zapotřebí zmínit, že platební instituce a instituce elektronických peněz musí rozšířit povolení k činnosti o danou službu, zatímco banky a družstevní záložny nemusí[112].

I tato služba, jako u služby informování o platebním účtu, předběhla legislativu, a služby na podobné bázi už fungovaly před příchodem evropské

[109] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

[110] AIS and PIS – A status update on open banking licenses issued in the UK. *Penser* [online]. 05.2019n. l. [cit. 2021-03-07]. Dostupné z: https://www.penser.co.uk/business/ais-and-pis-a-status-update-on-the-licenses-issued-in-the-uk/

[111] MOSNÁKOVÁ, Michaela. PSD2 a nová platební služba: Nepřímé udělení platebního příkazu. *Epravo.cz* [online]. 2018 [cit. 2021-03-06]. Dostupné z: https://www.epravo.cz/top/clanky/psd2-a-nova-platebni-sluzba-neprime-udeleni-platebniho-prikazu-107127.html

[112] Ibid.

legislativy, potažmo české. Tyto služby třetích stran fungovaly buď na principu screen scrapingu či přesměrování[113].

Na základě přesměrování fungovala služba iDEAL z Nizozemska, která přesměrovala plátce při volbě dané platební metody do jeho internetového bankovnictví. Tam plátce pouze potvrdil platební příkaz, který byl předvyplněný dle obchodníka a následně banka obchodníka informovala obchodníka, že byla platba provedena. Fungoval tu vztah plátce, plátcova banka, obchodník a banka obchodníka, kdy iDEAL měla za úkol oblast technické komunikace mezi bankami[114].

Přes screen scraping, jinak řečeno uživatelské rozhraní, sdílel plátce své přístupové údaje třetí straně, která potom přistoupila do plátcova internetového bankovnictví a zadal příkaz k úhradě[115].

Službu nepřímého dání platebního příkazu můžeme najít pod dalšími termíny, jako Payment Initation Service (anglicky), PIS nebo ve směrnici PSD2 ji najdeme pod názvem služba iniciování platby. Nejvíc zažitá je zkratka PIS, na základě mého úsudku z rešerše na dané téma.

Služba nepřímé dání platebního příkazu je v ZoPS definována, jako „služba spočívající v dání platebního příkazu k převodu peněžních prostředků z platebního účtu jménem plátce poskytovatelem rozdílným od poskytovatele, který pro plátce vede daný platební účet, je-li platební příkaz dán prostřednictvím internetu“[116].

Principiálně to funguje tak, že v této službě figurují tři subjekty. Plátce, poskytovatel, který vede platební účet a poskytovatel nepřímého dání platebního příkazu, který se v literatuře nazývá většinou jako TPP, tedy Third Party Provider neboli třetí strana. Plátce prostřednictvím poskytovateli nepřímého dání platebního příkazu zadá platební příkaz, kterou třetí strana předá poskytovateli, který vede platební účet. Je důležité zmínit, že příkaz, který předává poskytovatel nepřímého dání platebního příkazu poskytovateli, který vede plátci platební účet je stále příkaz

[113] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.
[114] Ibid.
[115] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.
[116] § 2, odst. 1, písm. k) ZoPS

k platbě, který zadal plátce, a zde můžeme spatřit prvek nepřímosti, jelikož příkaz zadal u poskytovatele nepřímé dání platebního příkazu[117].

Způsob dání souhlasu a příkazu plátce poskytovateli nepřímého dání platebního příkazu si dohodnou mezi sebou. Poskytovatel, který vede platební účet plátci má pouze vytvořit platformu k tomu, aby jej poskytovatel nepřímého dání platebního příkazu mohl předat[118].

1.5.1. Práva a povinnosti poskytovatele, který vede platební účet

Poskytovatel, který vede platební účet plátci dle ZoPS má povinnosti, které musí dodržet v případě, že plátce zadá nepřímo platební příkaz přes poskytovatele nepřímého dání platebního příkazu.

Jedna z povinností poskytovatele, který vede platební účet plátci, je ta, že po přijetí tohoto nepřímého platebního příkazu musí sdělit dostupné informace o přijetí a provedení platební transakce. Otázkou je, co znamenají dostupné informace o přijetí nepřímo daného platebního příkazu. Autoři komentáře k ZoPS si myslí, že nejde o sdělení, zda proběhne tato platební transakce, ale mezi informace se řadí to, zda na plátcově platebním účtu je dostatek zůstatku na účtu pro provedení této platební transakce[119]. Provedení samotné platební transakce může zmařit fakt, že poskytovatel, který vede platební účet plátci, může odmítnout transakci z následujících důvodů:

„a) má-li podezření na neoprávněné nebo podvodné použití platebního prostředku nebo osobních bezpečnostních prvků uživatele,

b) byl-li platební příkaz nepřímo dán prostřednictvím osoby, která není oprávněna poskytovat službu nepřímého dání platebního příkazu,

c) neosvědčil-li poskytovatel nepřímého dání platebního příkazu svoji totožnost v souladu s § 162 písm. e), nebo

d) jsou-li splněny podmínky podle § 159 odst. 1.“[120]

Pokud má poskytovatel, který vede platební účet plátci, „podezření na neoprávněné nebo podvodné použití platebního prostředku nebo osobních

---

[117] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[118] Ibid.

[119] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[120] § 161, odst. 3 ZoPS

bezpečnostních prvků uživatele“[121], může platební transakci odmítnout. Taková situace může nastat v případě, že platební příkaz zadá jiná osoba než plátce nebo jím zmocněná osoba. S ohledem na osobní bezpečnostní prvky, které jsou uvedené v ustanovení § 161, odst. 3, písm a) ZoPS se rozumí i případ, kdy se do rozhraní plátce přihlásí jiná osoba než on sám[122].

Další případ může nastat tehdy, pokud je nepřímý platební příkaz dán u osoby, která nemá oprávnění poskytovat tuto službu. Jak jsem zmiňoval v kapitole 1.5, k poskytování této služby jsou oprávněni: „banky, družstevní záložny, platební instituce nebo instituce elektronických peněz“[123]. Z toho vyplývá, že mimo tento okruh, s výjimkou platebních institucí a institucí elektronických peněz, bez povolení k službě nepřímého dání platebního příkazu, nemůže tuto službu poskytovat nikdo jiný a je to důvod k odmítnutí takového příkazu.

I u služby nepřímého dání platebního příkazu, má poskytovatel, který vede platební účet, právo k osvědčení totožnosti poskytovatele služby nepřímého dání platebního příkazu. Ani v tomto případě se nepostupuje jinak a k ověření totožnosti se „využívají kvalifikované certifikáty pro elektronické pečetě (srov. čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“[124].

Pokud nastane odmítnutí transakce na základě výše uvedených 3 případů, musí to bez zbytečného odkladu nahlásit poskytovatel, který vede platební účet České národní bance, která provádí dohled nad finančním trhem. Dle komentáře k ZoPS je taková povinnost snahou odradit poskytovatele od neodůvodněných odmítnutí nepřímo daných platebních příkaz,[125] což se dá vyložit i tímto způsobem, avšak Česká národní banka jako orgán vykonávající dohled by měla mít přehled

[121] § 161, odst. 3, písm. a) ZoPS

[122] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[123] MOSNÁKOVÁ, Michaela. PSD2 a nová platební služba: Nepřímé udělení platebního příkazu. *Epravo.cz* [online]. 2018 [cit. 2021-03-06]. Dostupné z: https://www.epravo.cz/top/clanky/psd2-a-nova-platebni-sluzba-neprime-udeleni-platebniho-prikazu-107127.html

[124] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[125] Ibid.

celkově o takových pochybnostech, navíc přímo směrnice PSD2 v ustanovení článku 68, odst. 6 takové jednání požaduje.[126]

Posledním případem, kdy může poskytovatel, který vede platební účet plátce, odmítnout transakci, je důvod vyplývající z ustanovení § 159 odst. 1 ZoPS, který zní následovně: „Poskytovatel může platební příkaz odmítnout, jestliže není povinen platební transakci provést. Poskytovatel služby nepřímého dání platebního příkazu může platební příkaz odmítnout, jestliže není povinen nepřímo daný platební příkaz předat poskytovateli vedoucímu platební účet.“ [127] Komentář k ZoPS uvádí příklad, kdy má poskytovatel, který vede platební účet, stanovit s uživatelem (budoucím plátcem) důvody a situace, kdy nebude povinen provést platební transakci[128].

V případě, že poskytovatel, který vede platební účet plátci chce z výše uvedených důvodů odmítnout nepřímo daný platební příkaz, „informuje uživatele o důvodech odmítnutí; není-li to možné, informuje uživatele bez zbytečného odkladu po odmítnutí“[129]. To znamená, že před tím, než učiní samotné odmítnutí, musí informovat plátce o tomto úmyslu s odůvodněním, proč tak chce učinit. Povinnost informovat o tomto úmyslu odpadá, pokud by to ohrozilo bezpečnost v oblasti platebního styku[130].

ZoPS udává dále povinnost poskytovateli v ustanovení § 161, odst. 1, písm. b) s tím, že: „nesmí při přijetí nebo odmítnutí platebního příkazu činit neodůvodněné rozdíly mezi nepřímo daným platebním příkazem a ostatními platebními příkazy; to platí i pro provedení související platební transakce“[131]. Poskytovatel, který vede platební účet plátci by neměl diskriminovat nepřímo daný platební příkaz v porovnání s ostatními platebními příkazy, což je logické, jelikož nepřímé dání platebního příkazu měla být alternativou k platbě kartou. Komentář

[126] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[127] § 159, odst. 1 ZoPS

[128] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[129] § 161, odst. 4 ZoPS

[130] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[131] § 161, odst. 1, písm. b) ZoPS

k ZoPS hovoří, že zvýhodnění by mohlo být: „stanovením rozdílné lhůty pro provedení platební transakce, ke které byl dán platební příkaz nepřímo, oproti platebním transakcím, kde byl dán platební příkaz přímo. Zakázána je pak zjevně i diskriminace v reálné lhůtě provádění platebních transakcí. Nestačí tedy jen deklarovat stejné lhůty, ale tyto lhůty je třeba dodržovat.“[132]

Poskytovatel, který vede platební účet, musí umožnit přijetí nepřímo daného platebního příkazu všem poskytovatelům této služby a nesmí podmiňovat přijetí nepřímého platebního příkazu tím, že by poskytovatel této služby měl mít uzavřenou smlouvu s ním. Domnívám se, že v případě nezavedení této podmínky v ZoPS, by mohla nastat taková situace, kdy poskytovatelé, kteří vedou platební účet, mohou danou službu naprosto „pohřbít“, jelikož by mohli preferovat platbu kartou. Otázkou je, zda by to bylo pro ně výhodné.

1.5.2. Práva a povinnosti poskytovatele nepřímého dání platebního příkazu

Poskytovatelem nepřímého dání platebního příkazu může být banka[133] či družstevní záložny[134], jelikož poskytují platební služby, pod které spadá i nepřímé dání platebního příkazu dle ustanovení § 3, odst. 1, písm. g) ZoPS. Dalšími poskytovateli mohou být platební instituce[135] a instituce elektronických peněz[136].

V rámci služby nepřímého dání platebního příkazu poskytovatel:

„a) nepřijímá peněžní prostředky k provedení platební transakce,

b) zpřístupní osobní bezpečnostní prvky plátce pouze plátci a tomu, kdo je vydal,

c) sdílí údaje o plátci, s výjimkou osobních bezpečnostních prvků plátce, pouze s příjemcem a na základě výslovného souhlasu plátce,

d) neuchovává citlivé údaje o platbách plátce,

e) při každém nepřímém dání platebního příkazu osvědčí poskytovateli, který uživateli vede platební účet přístupný prostřednictvím internetu, svoji totožnost,

f) v souvislosti se službou nepřímého dání platebního příkazu nepožaduje od plátce jiné údaje o plátci než údaje potřebné k nepřímému dání platebního příkazu ani takové údaje neuchovává a nezpracovává a

---

[132] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[133] § 1, odst. 3, písm. c) ZoB

[134] § 3, odst. 1, písm. b) zákona 87/1995 Sb., o spořitelnách a úvěrních družstvech a některých opatřeních s tím souvisejících a o doplnění zákona České národní rady č. 586/1992 Sb., o daních z příjmů

[135] § 9, odst. 1, písm. d) ZoPS

[136] § 68, odst. 1, písm. d) Ibid.

g) nemění údaje uvedené v nepřímo daném platebním příkazu.“[137]

Písm. a) je logické, jelikož samotný princip nepřímého dání platebního příkazu spočívá v zprostředkování příkazu plátce k poskytovateli, který vede jeho platební účet a není žádný důvod, aby poskytovatel služby nepřímého dání platebního příkazu přijímal peněžní prostředky k provedení platební transakce. S tím je spojené i písm. g), kdy poskytovatel nepřímého dání platebního příkazu nesmí měnit údaje v platebním příkazu, jelikož z povahy služby má pouze tyto informace předat poskytovateli, který vede platební účet plátce a je vázán vůlí plátce.

Osobním bezpečnostním prvkem uvedeným v písm. b) se rozumí „prvek, který poskytovatel poskytl uživateli za účelem ověření“[138].

Poskytovatel může sdílet údaje o plátci pouze s příjemcem a navíc s výslovným souhlasem plátce a žádným dalším osobám tak učinit nesmí. Tento výslovný souhlas stačí, aby byl uveden ve smlouvě o platebních službách[139].

Dále poskytovatel „neuchovává citlivé údaje o platbách plátce“ [140]. Citlivými údaji o platbách uživatele se rozumí „údaj, který může být zneužit k podvodu v oblasti platebních služeb, s výjimkou jedinečného identifikátoru a jména majitele platebního účtu v případě poskytovatele služby informování o platebním účtu nebo služby nepřímého dání platebního příkazu“[141].

O písm. e) jsem se zmínil již v kapitole 1.5.1, kde jsem uvedl, že k osvědčení poskytovatelů, kteří vedou platební účet, se „využívají kvalifikované certifikáty pro elektronické pečetě (srov. čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“[142].

Vzhledem k tomu, že předání platebního příkazu od poskytovatele služby nepřímého dání platebního příkazu by mělo probíhat přes API rozhraní, které vytvoří poskytovatel, který vede platební účet nebo prostřednictvím screen

[137] § 162 ZoPS

[138] § 2, odst. 3, písm. m) Ibid.

[139] NÝDRLE, Tomáš. § 162 [*Povinnosti poskytovatele nepřímého dání platebního příkazu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[140] § 162 písm. d) ZoPS

[141] § 2, odst. 3, písm. n) Ibid.

[142] NÝDRLE, Tomáš. § 162 [*Povinnosti poskytovatele nepřímého dání platebního příkazu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

scraping, musí poskytovatel služby nepřímého dání platebního příkazu získat určité vstupní údaje od plátce, aby mohl tento příkaz předat. Může jít o přihlašovací údaje, aby mohl poskytovatel předat platební příkaz přes jeho uživatelské rozhraní. Tyto údaje nemá dále uchovávat ani zpracovávat[143].

1.6. Využití v praxi

Výše uvedené novinky, jmenovitě služba informování o platebním účtu a služba nepřímé dání platebního příkazu, jsou dle mého názoru právě služby, které jsou zásadní pro prosazení nové technické vlny v bankovnictví. Tyto služby propojují třetí strany se službami a usnadňují uživateli mít na jednom místě všechny platební účty, které má otevřené u bank a další služby, které mohou být v budoucnu uživateli dostupné. Navíc dává obchodníkům možnost, jak se odklonit od spolupráce s karetními asociacemi při platbě od zákazníka, což bych jako obchodník velmi kvitoval, zejména kvůli poplatkům, které obchodníci musí zaplatit za každou platbu karetní asociaci.

Studie společnosti Deloitte z roku 2018 tvrdí, že uživatelé v České republice jsou konzervativními klienty, jelikož pouze 18 % uživatelů by sdílelo informace o svém platebním účtu za účelem lepších služeb s některou z jiných bank, což v jiných východoevropských zemích činilo až 35 % uživatelů, kteří by byli ochotni za lepší služby poskytnout tato data. Motivovat by je mohly lepší nabídky úvěru nebo kreditní skóre (vizte kapitola 1.6.3).[144]

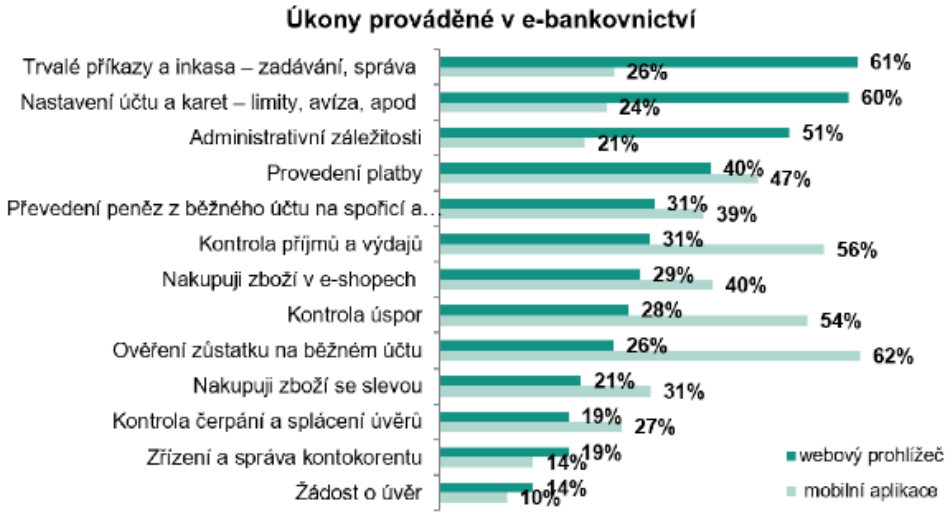
Průzkum Češi a digitalizace 2020, který provedla České bankovní asociace ukázal, že 97 % klientů bank používá internetové bankovnictví, což je 15% nárůst oproti roku 2018[145]. Obrovský nárůst uživatelů si vysvětluji zejména pandemií koronaviru COVID-19, který znemožnil lidem chodit běžně vyřizovat na pobočku standardní záležitosti.

Obrázek 2 *– Úkony prováděné v e-bankovnictví*

[143] NÝDRLE, Tomáš. § 162 [*Povinnosti poskytovatele nepřímého dání platebního příkazu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[144] Studie Deloitte: České banky i uživatelé jsou na PSD2 v regionu nejlépe připraveni. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z:

[145] Češi a digitalizace 2020. *Česká bankovní asociace* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2020



Upraveno ze zdroje: Češi a digitalizace 2020. *Česká bankovní asociace* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2020

Obrázek 2 znázorňuje úkony, které provádí klienti v internetovém bankovnictví. Na obrázku 2 je vidět, ke kterým činnostem klienti používají internetový prohlížeč a ke kterým mobilní aplikaci, avšak to není dle mého názoru v této kapitole důležité. Za důležité považuji právě tu skutečnost, že můžeme spatřit určitý rozptyl služeb, které využívají klienti a z toho můžeme vyvodit, zda jsou spíše konzervativními uživateli, jak zmiňuje výše uvedená studie společnosti Deloitte nebo používají i jiné služby, které jim může nabídnout směrnice PSD2 či služby nad rámec směrnice PSD2 či samotného ZoPS.

Myslím si, že žádost o úvěr, nákup zboží se slevou nebo nákup zboží v e-shopech může být ukazatelem toho, že by tito lidé mohli v budoucnu využít scoring nebo nepřímé dání platebního příkazu. Z výzkumu od České bankovní asociace také vyplývá, že jde hlavně o strach z nedostatku bezpečnosti, který brzdí využití nových služeb. Pokud se poskytovatelé platebních služeb a třetí strany budou snažit v této oblasti zapracovat na veřejném mínění, může jim to do budoucna prospět na českém trhu v podobě zvýšeného zisku klientů.

1.6.1. Multibanking

Jedním z produktů spojení služeb informace o platebním účtu, nepřímé dání platebního příkazu a potvrzování zůstatku peněžních prostředků pro vydavatele karetních prostředků, které jsou nově dostupné ze směrnice PSD2, jsou multibanking aplikace. Multibanking aplikace umožňuje uživatelům připojit do aplikace všechny bankovní účty, se kterými disponují a mají přístup pouze z jedné aplikace, kde nepostrádají základní funkcionalitu.

První českou multibanking aplikací byla již od července 2018 aplikace Richee, kterou spustila Banka CREDITAS[146]. Současný stav je takový, že každá aplikace má omezený počet bank, ke které se může uživatel připojit. V tomto je nejdále Banka Creditas, která umožňuje připojení z 12 bank, například J&T Banka nebo Moneta Money Bank. Některé banky, které sdílí data, nenabízejí vůbec multibanking. Jde například o Fio banku[147] [148].

Otázkou je, jak moc je multibanking využívanou službou napříč uživateli. Z průzkumu Češi a digitalizace 2019 od České bankovní asociace vyplývá, že 47 % dotázaných ve výzkumu uvedlo, že považují multibanking za přínosný ve složení 15 % určitě ano a 47 % spíše ano, což není dle mého názoru moc lichotivý výsledek.[149] Může to být i tím, že mnoho uživatelů nemá více účtů a používá pouze jeden. Já osobně používám dva bankovní účty od dvou bank a nemám potřebu si propojit jednu či druhou aplikaci s účtem od jiné banky. Jednak je to otázka bezpečnosti, o kterou se bojí i další uživatelé, což ve výzkumu od České bankovní asociace potvrdilo 23 % respondentů[150] a jednak je to pro mě řešení na půl cesty. Pokud si chci objednat novou platební kartu, dejme tomu k účtu u České spořitelny, na aplikaci od Komerční banky takovou operaci neuskutečním. Ač to nedělám každý den, chci mít alespoň tu možnost a raději budu mít dvě aplikace na mobilu než jednu.

Nemilou zprávou je to, že 8 % dotázaných se vyjádřilo, že používají multibanking a 8 % respondentů přijde složité manipulovat s multibanking funkcí, a to může být námětem pro banky k tomu, aby zapracovaly na svých aplikacích s mobilním bankovnictví[151].

1.6.2. Správa financí

Aplikací na správu financí je na trhu nespočet, avšak mezi ty nejvíce doporučované se řadí aplikace z českých společností, jmenovitě Spendee, která vyvíjí stejnojmennou aplikaci a BudgetBakers aplikaci Wallet. O těchto

---

[146] První česká multibankovní aplikace Richee. Pro CREDITAS ji vytvořila česká IT společnost Cleverlance. *Cleverlance* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.cleverlance.de/cz/novinky/Stranky/Richee.aspx

[147] Multibanking 2021: Jak funguje a které banky ho podporují? *Skrblík.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://www.skrblik.cz/finance/ucty/multibanking/

[148] Otevřené bankovnictví. *Banka CREDITAS* [online]. [cit. 2023-07-30]. Dostupné z: https://www.creditas.cz/otevrene-bankovnictvi/

[149] Češi a digitalizace 2019. *Česká bankovní asociace* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2019

[150] Ibid.

[151] Češi a digitalizace 2019. *Česká bankovní asociace* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2019

společnostech jsem se už zmínil na začátku kapitoly a není třeba si je více představovat. Aplikace správy financí mají pomáhat uživatelům k tomu, aby měli pod dohledem své měsíční výdaje a příjmy.

Konkrétně tyto dva startupy mají povolení k činnosti jako správce informací o platebním účtu, což znamená, že můžou stahovat data z bankovních účtů uživatelů, kteří k nim mají přístup. Přes API rozhraní se stáhnou data o příjmech a výdajích, které potom zpracovává aplikace a uživatel si může například nechat spočítat, za které položky utratil v měsíci nejvíc nebo kolik utrácí za předplatné. Nutno dodat, že stahování dat z účtu je u obou aplikací dostupné v předplaceném programu.

Z vlastní zkušenosti vím, že zapisování dat z každé útraty do peněženky bylo velmi nekomfortní. Aplikaci jsem navíc příliš nevyužíval i proto, že jsem necítil potřebu platit za to, aby mi aplikace stahovala data z mých bankovních účtů.

1.6.3. Scoring

Scoring je pojem, se kterým se setkáváme zejména v souvislosti s poskytováním úvěrů nebo hypotečních úvěrů. Banka žadatele o úvěr na základě scoringu ověří jeho bonitu, zda splňuje požadavky úvěruschopnosti k tomu, aby mohl daný úvěr získat a zvládat splácet[152]. Ostatně na stránkách Finančního arbitra můžeme narazit na nespočet rozhodnutí arbitra o špatném posouzení úvěruschopnosti žadatele ze strany banky nebo nebankovních poskytovatelů. Dle mého názoru může správné posouzení bonity prostřednictvím využití služby informování o platebním účtu velmi lehce tento problém vyřešit, jestliže tu bude vůle bank a obzvlášť nebankovních poskytovatelů.

V České republice získal povolení k činnosti v roce 2020 zatím poslední správce informací o platebním účtu, a to společnost 1. PF Finance, která se zaměřuje právě na scoring, a která tyto služby poskytuje pro kreditní a leasingové společnosti. Nabízí „soubor významných transakcí, jméno vlastníka účtu, seznam stálých plateb (plateb), maximální příchozí a odchozí platby.“[153]

1.7. Komparace s jinými státy

Kromě Evropské unie a Velké Británie, která se ukázala již během svého členství v Evropské unii jako pokroková země v oblasti FinTech, bych se rád zmínil

[152] Scoring u hypotéky. *Banky.cz* [online]. [cit. 2021-03-16]. Dostupné z: https://www.banky.cz/hypotecni-slovnik/scoring-u-hypoteky/

[153] *1. PF Finance, s.r.o.* [online]. [cit. 2021-03-16]. Dostupné z: https://www.1pffin.cz/

také o dalších dvou státech, na které bychom měli upřít naši pozornost a inspirovat se jimi.

Za zmínku dle mého názoru stojí Austrálie, jakožto země, která je součástí Commonwealthu a je úzce spojena s Velkou Británií, a dále pevninská Čína, která mimo skupinu „asijských tygrů“ (anglicky *Four Asian Tigers*) patří mezi nejvyspělejší ekonomiky světa.

Důležité je na začátku zmínit, že směrnice PSD neboli směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007, o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES a směrnice PSD2, nemá na celém světě v oblasti platebního styku dle mého mínění obdoby. Soubor regulací v jedné právní normě (zejména myšleno směrnice PSD2) s takovým územním dosahem prozatím nemá žádného konkurenta. Navíc na světě není zatím podobné uskupení sui generis jako je Evropská unie. Za podobné uskupení však můžeme považovat například ASEAN (Sdružení národů jihovýchodní Asie), která takovou ambici s platebním stykem zatím nemá. ASEAN je co do počtu členských států zhruba třetinová oproti Evropské unii.

Projekt Bankovní identity (vizte kapitola 3.6.), potažmo skandinávské BankID je spíše evropskou záležitostí, a proto jej nelze přímo porovnat s žádnou další právní úpravou v níže uvedených zemích.

1.7.1. Austrálie

V Austrálii působí v současné době kolem 650 FinTech společností[154], což je extrémně velké množství a takový rozmach můžeme odvíjet buď od výše počtu obyvatel nebo jejich právní regulace. Vzhledem k tomu, že Austrálie má cca 26 milionů obyvatel[155], připisuji v tomto případě zásluhu právní regulaci.

Austrálie nastavila rámec sdílení uživatelských dat do více sektorů v ekonomice a neomezila se pouze u Open banking, tedy sdílení v bankovním sektoru. CDR neboli Competition and Consumer (Consumer Data Right) Rules 2020 (česky *Hospodářská soutěž a spotřebitel (právo spotřebitelských údajů)* v první řadě umožnila sdílení dat v bankovním sektoru, a to v červenci 2020,

[154] TRAN, Kristine. How are Australian Fintechs regulated?. OpenLegal [online]. [cit. 2022-12-29]. Dostupné z: https://openlegal.com.au/how-are-australian-fintechs-regulated/

[155] Australia. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-12-31]. Dostupné z: https://en.wikipedia.org/wiki/Australia

a postupně se zavádí i do ostatních sektorů[156], jako například „energetika, telekomunikace, důchody, pojištění“[157]. Důležitou zásadou CDR je reciprocita, ze které vyplývá, že ten, který použije údaje o uživatel, musí být schopen poskytnout podobně relevantní údaje tomu, který mu je poskytl[158]. Co znamená podobné (ekvivalentní) údaje ukáže až praxe v Austrálii. Problém může nastat zejména při sdílení dat mezi různými sektory.

Uživatel, který sdílí data v rámci CDR, může zvolit, které informace bude sdílet a má možnost kdykoliv zrušit sdílení těchto dat[159].

Myslím si, že Evropská unie by se v budoucnu mohla více zaměřit na sdílení dat i mimo bankovnictví a zejména reciprocitě. Současná regulace se zaměřuje na sdílení uživatelských dat spíše jednosměrně.

1.7.2. Čína

Čína je jedním z největších průkopníků ohledně FinTech na světě, ba dokonce lídrem od roku 2018[160] [161]. Zajímavostí je, že v Číně je přes 200 FinTech společností, které poskytují nebankovní platební služby[162], což je i v celosvětovém měřítku nevídané číslo.

Další zajímavostí je, že se Čína vydala opačným směrem než ostatní státy. Ostatní státy měly potřebu regulovat FinTech, potažmo skoro vnutit Open banking, kvůli větší prostupnosti dat. Čína se paradoxně spoléhala na organický vývoj, avšak v poslední době čínští regulátoři zasahují také do FinTech sektoru po letech volnosti bez větších právních regulací v této oblasti[163]. FinTech v Asii je zaměřena zejména

---

[156] What is the Consumer Data Right?. Office of the Australian Information Commissioner [online]. [cit. 2022-12-29]. Dostupné z: https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right

[157] BUCKLEY, Ross P., Natalia JEVGLEVSKAJA a Scott FARRELL. Open banking and Australia’s data-sharing regime: six lessons for Europe. LSE Business Review [online]. [cit. 2022-12-29]. Dostupné z: https://blogs.lse.ac.uk/businessreview/2022/04/28/open-banking-and-australias-data-sharing-regime-six-lessons-for-europe/

[158] STRACHAN, David. Open Banking around the world. Deloitte [online]. [cit. 2022-12-29]. Dostupné z: https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html

[159] What is the Consumer Data Right?. Office of the Australian Information Commissioner [online]. [cit. 2022-12-29]. Dostupné z: https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right

[160] Open banking’s true story in Asia: emerging markets. Digital Finance [online]. [cit. 2022-12-29]. Dostupné z: https://www.digfingroup.com/open-banking-asia-2/

[161] ZHOU, Qian. A Close Reading of China’s Fintech Development Plan for 2022-2025. China Briefing [online]. [cit. 2022-12-29]. Dostupné z: https://www.china-briefing.com/news/a-close-reading-china-fintech-development-plan-for-2022-2025/

[162] WU, Brendon, Cloud LI, Joanna JIANG a Dimitri PHILLIPS. China: Fintech. The Legal 500 [online]. [cit. 2022-12-29]. Dostupné z: https://www.legal500.com/guides/chapter/china-fintech/

[163] Open banking’s true story in Asia: emerging markets. Digital Finance [online]. [cit. 2022-12-29]. Dostupné z: https://www.digfingroup.com/open-banking-asia-2

na mobilní platby, kdežto v Evropě se zaměřují spíše na uživatelská data klientů. Jedním z důvodů takové skutečnosti je právě prostupnost dat v rámci Open banking. Nic není však ideální a v Číně dohled nad mobilními platbami sdílí více úřadů[164], což není dle mého mínění efektivní.

Myslím si, že jedním z impulzů větších právních regulací FinTech v Číně mohla být událost, která se stala v roce 2017 v provincii Kuang-tung. Pachatel ukradl 90 milionů čínských jüanů (cca 12 milionů Euro) tím, že nahradil QR kódy u prodejců svými QR kódy, které obsahovaly malware[165]. K tomu připočtěme regulaci proti praní špinavých peněz, která příliš nefunguje, jelikož podvodníci a „zprostředkovatelé praní špinavých peněz" využívají díry v zákoně, „kdy využijí špinavé peníze k nákupu zbraní v online hrách a posléze prodají tyto online předměty, z čehož mají zisk"[166]. Bylo na místě zasáhnout, aby nedošlo k podobným událostem a mohlo se efektivněji bojovat proti praní špinavých peněz.

Avšak zpět k Open banking. Čína nemá žádný jednotný systém ke sdílení dat mezi bankami (API rozhraní) a některé banky samy vytvářejí své API rozhraní, přes které mohou sdílet data s ostatními bankami, se kterými spolupracují[167]. To je podle mého jedna z největších slabin čínského Open banking. Pokud budou chtít zabránit budoucím problémům, měli by se zaměřit na danou oblast. V komparaci s čínským přístupem jsem určitě rád, že v České republice se „velcí hráči" na trhu domluvili a nerozdrobili tento systém.

Čína se zaměřuje poslední dobou více na bezpečnost dat, což je deklarováno zejména prostřednictvím Data Security Law (DSL) a Personal Information Protection Law (PIPL) neboli v překladu Zákon o zabezpečení dat a Zákon o ochraně osobních údajů, přičemž oba tyto zákony jsou účinné od roku 2021. Dle čínského plánu na období 2022–2025 pro rozvoj FinTech plánují tyto zákony doplňovat o prováděcí předpisy, zejména za účelem shromažďování a zpracování dat nebo životního cyklu dat za účelem zpětného sledování dat[168].

---

[164] HUANG, Robin Hui. Fintech Regulation in China: Principles, Policies and Practices. Cambridge University Press, 2021. ISBN 978-1-108-73844-6. s. 151

[165] Ibid. s. 147

[166] HUANG, Robin Hui. Fintech Regulation in China: Principles, Policies and Practices. Cambridge University Press, 2021. ISBN 978-1-108-73844-6. s. 148

[167] WU, Brendon, Cloud LI, Joanna JIANG a Dimitri PHILLIPS. China: Fintech. The Legal 500 [online]. [cit. 2022-12-29]. Dostupné z: https://www.legal500.com/guides/chapter/china-fintech/

[168] ZHOU, Qian. A Close Reading of China's Fintech Development Plan for 2022-2025. China Briefing [online]. [cit. 2022-12-29]. Dostupné z: https://www.china-briefing.com/news/a-close-reading-china-fintech-development-plan-for-2022-2025/

2. Silné ověření uživatele

Silné ověření uživatele s postupem času stále považuji za jednu z klíčových úprav vyplývajících z PSD2, kterou členské státy Evropské Unie musely implementovat do svých vnitrostátních právních řádů.

Silné ověření uživatele by mělo chránit uživatele před neautorizovanou platbou a snížit riziko podvodů. Zákonodárce důvod bezpečnosti placení přes internet zdůrazňuje i v důvodové zprávě. Zejména podotýká, že změna oproti stavu před ZoPS spočívá v zákonné povinnosti, jelikož před účinností ZoPS probíhalo silné ověření uživatele na dobrovolné bázi na základě doporučení Evropského orgánu pro bankovnictví[169]. Otázkou je, zda technologický vývoj a technické parametry dané směrnicí PSD2, potažmo nařízení RTS týkající se silného ověření uživatele, budou časem stále dostatečné.

Ustanovení článku 98 směrnice PSD2 určuje, aby regulační technické normy týkající se ověřování a komunikace vypracoval Evropský orgán pro bankovnictví. Po zdlouhavém procesu bylo v listopadu 2017 vydáno v Úředním věstníku Evropské unie nařízení RTS, které vstoupilo v platnost v březnu 2019. Avšak obavy z nereflektování technologického vývoje „rozbíjí“ odstavec 5 článku 98 PSD2: „EBA v souladu s článkem 10 nařízení (EU) č. 1093/2010 regulační technické normy pravidelně přezkoumává a v případě potřeby aktualizuje s ohledem na mimo jiné inovace a technologický rozvoj.“[170] Regulační technické normy „jsou technické povahy a nepředstavují strategická či politická rozhodnutí a jejich obsah je vymezen legislativními akty, z nichž vycházejí.“[171] Regulační technické normy zpracoval Evropský orgán pro bankovnictví, který má pravomoc vydávat dále obecné pokyny a doporučení na základě nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví).

Směrnice PSD ani v ZoPS z 2009 nezahrnovaly technické otázky k zabezpečení při autorizaci platební transakce. Doplňovaly je obecné pokyny od Evropského orgánu pro bankovnictví k bezpečnosti internetových plateb

[169] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

[170] Článek 98, odst. 5 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

[171] Článek 10 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES

EBA/GL/2014/12[172]. Nutno dodat, že obecné pokyny a doporučení od Evropského orgánu pro bankovnictví ovlivňují interpretaci všech úprav v ZoPS a dalších právních úprav v rámci bankovnictví, jak je známo z praxe. V běžné praxi se zachází se všemi doporučení od Evropského orgánu pro bankovnictví a banky jako s obecnými pokyny.

Silné ověření uživatele, někdy se setkáváme s jinými termíny jako silné ověření klienta (terminologie ze směrnice PSD2), v odborných článcích a literatuře pod anglickým termínem Strong Customer Authorization nebo zkratkou SCA. Silné ověření uživatele "je bezpečnostní mechanismus, který si klade za cíl zásadním způsobem snížit riziko vzniku podvodů v důsledku kompromitovaného (uniklého, nebo zneužitého) hesla"[173]. Využívá k tomu kombinaci dvou ze tří prvků, které jsou dané zákonem. Tyto prvky podrobněji rozeberu později v kapitole 2.1.

Ustanovení článku 97 směrnice PSD2 udává, že silné ověření uživatele se použije v případě, pokud uživatel:

„a) využívá on-line přístupu ke svému platebnímu účtu;

b) iniciuje elektronickou platební transakci;

c) prostřednictvím prostředků komunikace na dálku provede jakýkoli úkon, který by mohl vést k riziku platebního podvodu nebo jiných zneužití."[174]

Dále článek 97 směrnice PSD2 uvádí: „Pokud jde o iniciaci elektronické platební transakce uvedenou v odst. 1 písm. b), členské státy zajistí, aby u elektronických platebních transakcí na dálku poskytovatelé platebních služeb uplatňovali silné ověření klienta, jenž zahrnuje prvky dynamicky propojující transakci s konkrétní částkou a konkrétním příjemcem."[175]

Český zákonodárce implementoval ustanovení článku 97 směrnice PSD2 do poněkud jiné formy, která se nijak v zásadě neliší od původní myšlenky, ale přizpůsobuje se české terminologii v ZoPS:

„a) přistupuje ke svému platebnímu účtu prostřednictvím internetu,

---

[172] NÝDRLE, Tomáš. § 223 [Vymezení a použití silného ověření uživatele]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[173] EISELT, Zbyněk. Co znamená silné ověření klienta (SCA) a proč se o něm všude mluví? *GoPay blog* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.gopay.com/blog/co-znamena-silne-overeni-klienta-sca-a-proc-se-o-nem-vsude-mluvi/

[174] Článek 97, odst. 1 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

[175] Článek 97, odst. 2 Ibid.

b) dává platební příkaz k elektronické platební transakci,
c) provádí jiný úkon, který je spojen s rizikem podvodu v oblasti platebního styku, zneužitím platebního prostředku nebo informací o platebním účtu, nebo
d) požaduje informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu."[176]

Dále v odstavci 2 dodává: „Dává-li uživatel platební příkaz prostřednictvím internetu nebo prostřednictvím elektronického zařízení, které lze použít k dálkové komunikaci, nebo dává-li platební příkaz nepřímo, osoba oprávněná poskytovat platební služby použije silné ověření uživatele, které zahrnuje jednorázové prvky propojující platební transakci s přesnou částkou a určitým příjemcem."[177]

Jestliže shrnu předcházející body, které jsou dané ze zákona, plyne z tohoto vzdálený přístup a klient není přímo v kontaktu se svým poskytovatelem služeb.[178]

Znění ustanovení § 223 ZoPS se může zdát jednoznačné, ale při bližším pohledu tomu tak ani zdaleka není, neboť existuje celá řada různých intepretací.

Přístup k platebnímu účtu prostřednictvím internetu není přesněji definován jak v zákoně o platebním styku, tak ani ve směrnici PSD2, a dokonce ani v nařízení RTS. Komentář k danému ustanovení hovoří ve smyslu, že se jedná o: „zpřístupnění uživatelského rozhraní, které uživateli umožňuje získávat informace o platebním účtu (provedené platby, zůstatek, platební prostředky vydané k platebnímu účtu) a popřípadě následně z tohoto rozhraní dávat platební příkazy [179] ". Podle mého mínění jde o klasický přístup do internetového bankovnictví. Žádné další podobné rozhraní, které popisuje přímo komentář v dnešní době neexistuje. Internetové bankovnictví může být dostupné, jak z klasického webového prohlížeče, tak i z mobilní aplikace.

Při dání platebního příkazu je také povinné silné ověření uživatele. Za takový platební příkaz lze považovat každý platební příkaz, který je dán

[176] § 223, odst. 1 ZoPS
[177] § 223, odst. 2 Ibid.
[178] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz
[179] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

elektronickými prostředky (například internetové či mobilní bankovnictví, platbomat nebo platební karta)[180] [181].

Úkon s rizikem podvodu v oblasti platebního styku, který zákonodárce implementoval do písmene c) výslovně neurčuje, že jde o úkon na dálku, avšak dle důvodové zprávy se tak dá dovodit, jak jsem zmiňoval výše. Výklad těchto úkonů není zcela jasný, ale komentář k ZoPS se zmiňuje například o zjištění zůstatku účtu prostřednictvím bankomatu[182].

Jedním z posledních jsou informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu (vizte kapitola 2.4).

V případě, že uživatel zadává platební transakci propojující přesnou částku s určitým příjemcem přes elektronické zařízení nebo prostřednictvím internetu, je rovněž potřeba využít silného ověření uživatele. ZoPS doplňuje oproti směrnici PSD2 povinnost o nepřímé dání platebního příkazu[183], kterému se věnuji v kapitole 1.4.

Od 1. ledna 2021 musí všichni poskytovatelé platebních služeb při placení platební kartou využít silného ověření uživatele. Tato povinnost platí i pro „další subjekty podílející se na zpracování platební transakce (vč. obchodníků a provozovatelů platebních bran, provozovatelů karetních schémat atd.)“[184]

2.1. Prvky ověření

Pojem ověření je definován v ustanovení § 2 odst. 3, písm. l) ZoPS, které znamená „ověřením postup umožňující poskytovateli ověřit totožnost uživatele nebo oprávněné použití platebního prostředku nebo osobních bezpečnostních prvků uživatele[185]“.

---

[180] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[181] SOUKAL, Marek. Silné ověření klienta při poskytování platebních služeb. Epravo.cz [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

[182] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[183] Ibid.

[184] Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021. Česká národní banka [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/

[185] § 2, odst. 3, písm. l) ZoPS

V nařízení RTS se můžeme setkat s následujícími prvky: znalost (*anglicky:* knowledge), držení (*anglicky:* possession) a inherence (*anglicky:* inherence)[186]. Silné ověření uživatele se provádí při ověření ze dvou, ze tří dostupných prvků, jejichž výčet je taxativně uveden v ustanovení § 223, odst. 3 ZoPS:

„a) údaje, který je znám pouze uživateli,

b) věci, kterou má uživatel ve své moci,

c) biometrických údajů uživatele.“[187]

Bližší specifikace těchto prvků je obsažena v nařízení RTS a ve stanovisku Evropského orgánu pro bankovnictví pod označením EBA-Op-2019-06.

V první řadě je třeba zmínit, že tyto prvky „musí být vzájemně nezávislé a prolomení jednoho prvku nesmí ovlivnit spolehlivost prvků ostatních“ [188] s následujícími kritérii:

„a) použití odděleného bezpečného prostředí pro provedení prostřednictvím softwaru nainstalovaného ve víceúčelovém zařízení;

b) mechanismy k zajištění toho, aby software nebo zařízení nebyly pozměněny plátcem nebo třetí stranou;

c) došlo-li ke změnám, mechanismy k zmírnění jejich důsledků.“[189]

2.1.1. Znalost

„Údaje, který je znám pouze uživateli“[190], takto neurčitě je určen prvek znalosti v ZoPS. ZoPS jej nijak dále nevymezuje, avšak směrnice PSD2 se zmiňuje o tom, že prvek znalosti je „to, co ví pouze uživatel“[191]. Výklad ustanovení § 223, odst. 3, písm. a) ZoPS musíme opřít o stanovisko EBA-Op-2019-06, které vydal Evropský orgán pro bankovnictví v polovině roku 2019, jelikož nařízení RTS podobně jako ZoPS v článku 6 neobjasňuje prvek znalosti o něco více.

Nutno dodat, že stanovisko Evropského orgánu pro bankovnictví nenabízí taxativní výčet elementů, které se dají považovat za prvek znalosti a v budoucnosti může být upraven dalším stanoviskem.

Za prvek znalosti se považuje zejména:

---

[186] Článek 4, odst. 1 nařízení RTS

[187] § 223, odst. 3 ZoPS

[188] § 223, odst. 4 Ibid.

[189] Článek 9, odst. 3 nařízení RTS

[190] § 223, odst. 3, písm. a) ZoPS

[191] Článek 4, odst. 30 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

a) heslo[192],

b) PIN[193],

c) otázky založené na předchozí znalosti[194],

d) heslová fráze[195], a

e) memorised swiping path (volně přeloženo jako znak na obrazovce mobilního telefonu[196] nebo zamykací gesto)[197].

Stanovisko Evropského orgánu pro bankovnictví za prvek znalosti nepovažuje:

a) uživatelské jméno[198],

b) e-mailovou adresu[199],

c) údaje na platební kartě (například číslo platební karty, CVV/CVC kód, platnost karty)[200],

d) jednorázové heslo generované nebo přijaté na zařízení (například na mobilním telefonu)[201], a

e) TAN listy (papírové seznamy jednorázových autentizačních kódů)[202].

Neméně důležitý je výklad toho, co znamená pojem „znám pouze uživateli[203]“. Nařízení RTS se zmiňuje o tom, že „poskytovatelé platebních služeb přijmou opatření k zmírnění rizika toho, že prvky silného ověření klienta z kategorie

---

[192] Bod 32, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 8.

[193] Ibid.

[194] Bod 32, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 8.

[195] Ibid.

[196] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[197] Bod 32, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 8.

[198] Bod 34, Ibid.

[199] Ibid.

[200] Bod 33, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 8.

[201] Bod 35, Ibid.

[202] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[203] Ibid.

znalosti jsou použity neoprávněnými stranami.“[204] Z toho lze vyvodit, že pokud dodrží poskytovatel platebních služeb všechna opatření k tomu, aby se k těmto údajům nedostala neoprávněná osoba, nebude poskytovatel platebních služeb odpovědný za to, pokud prvek znalosti uživatel nějakým způsobem, například „jednáním, opomenutím či nedostatečného zabezpečení“[205], poskytne neoprávněné osobě. Nutno také dodat, že při vyzrazení prvku znalosti jej nelze v budoucnosti nadále používat[206].

Pro srovnání, v minulosti podle obecných pokynů od Evropského orgánu pro bankovnictví k bezpečnosti internetových plateb EBA/GL/2014/12 byl akceptován jako prvek znalosti údaje na platební kartě, například CVV/CVC kód. Podle novějšího stanoviska EBA-Op-2019-06 už podle současné úpravy nikoliv[207]. Dle mého názoru je to správný krok, byť je to pro některé krok méně komfortní, na který si mnozí už postupem času zvykli.

2.1.2. Držení

ZoPS definuje prvek držení jako “věci, kterou má uživatel ve své moci”[208]. Na pomoc můžeme k výkladu použít definici věci, která znamená „vše, co je rozdílné od osoby a slouží potřebě lidí“[209]. Směrnice PSD2 popisuje, že držení je „to, co drží pouze uživatel“[210]. Stanovisko EBA-Op-2019-06, které vydal Evropský orgán pro bankovnictví dodává, že nejde pouze o hmotnou věc, nýbrž může jít i o věci nehmotné, například mobilní aplikace[211]. ZoPS se dále podrobněji nezmiňuje o prvku držení, avšak opět ani v případě nařízení RTS, konkrétně v článku 7 nebyl evropský zákonodárce o moc více konkrétní, a tedy neposkytl více podrobností. Poskytovatel platebních služeb má i v prvku držení přijmout opatření

[204] Článek 6, odst. 1 nařízení RTS

[205] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[206] Ibid.

[207] Bod 33, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.8.

[208] § 223, odst. 3, písm. b) ZoPS

[209] § 489 Občanského zákoníku

[210] Článek 4, odst. 30 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

[211] Bod 24, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.6.

k zmírnění rizika použití neoprávněnými osobami[212]. Prvek držení by ve své moci měl mít tedy pouze uživatel a žádná další osoba. Uživatel by měl být natolik odpovědný a i zde by „svým jednáním, opomenutím“[213] neměl umožnit přístup k tomuto prvku další osobě. Z nařízení RTS uživateli přímo vyplývá povinnost opatření k zabránění replikace prvků držení. Odlišnost od prvku znalosti spočívá v tom, že v případě dočasného se zmocnění prvku neoprávněnou osobou a následným navrácením uživateli lze prvek nadále používat k ověření[214].

Stanovisko EBA-Op-2018-04 Evropského orgánu pro bankovnictví určuje, že k tomu, aby zařízení mohlo být použito jako prvek držení „musí existovat spolehlivý prostředek k potvrzení držení prostřednictvím vygenerování nebo přijetí prvku dynamického ověření na zařízení“[215]. Takovým prostředkem pro potvrzení může být jednorázový kód, vygenerovaný softwarem, hardwarem jako token, textová zpráva nebo notifikace[216]. Samotná textová zpráva není prvkem držení, ale SIM karta, která je spojená s telefonním číslem jím je [217]. Generování jednorázového kódu na zařízení může být provedeno přes aplikaci Google Authenticator[218] nebo Microsoft Authenticator, který považuji za velmi intuitivní a zároveň představující nutný základ pro přihlašování k internetovým účtům v dnešní době, kdy se kybernetická bezpečnost stále dosti zlehčuje a přístup k našim internetovým účtům nemáme tak zabezpečený, jak bychom mohli a měli mít.

Za zajímavou považuji skutečnost, že prvek držení může být založen například na aplikaci, kde by měl být provázán se zařízením a uchováván přes šifrování v bezpečnostním čipu[219].

---

[212] Článek 7, odst. 1 nařízení RTS

[213] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[214] Ibid.

[215] Bod 35, European Banking Authority. EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC ze dne 13. června 2018, s.7.

[216] Bod. 25, Ibid., s.6.

[217] Ibid.

[218] SOUKAL, Marek. Silné ověření klienta při poskytování platebních služeb. *Epravo.cz* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

[219] Bod. 26, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019 ,s.6.

Stanovisko EBA-Op-2019-06 Evropského orgánu pro bankovnictví ani v tomto případě není vymezeno taxativním způsobem. Za prvky držení považuje, zejména:

a) zařízení potvrzené jednorázovým kódem, generovaný nebo přijatý na zařízení (hardware nebo softwarový token generátor, textová zpráva s jednorázovým kódem[220],

b) zařízení potvrzené podpisem generovaným zařízením (hardware nebo softwarový token)[221],

c) kartu nebo zařízení potvrzené přes QR kód (nebo fotografií TAN listu) skenovaný externím zařízením[222], a

d) mobilní aplikace nebo webový prohlížeč, jehož držení je navázán na zařízení – například přes bezpečnostní čip v zařízení nebo privátní klíč, který propojuje aplikaci k zařízení nebo propojení webového prohlížeče k zařízení[223].

Za prvek držení se nedá považovat údaje na platební kartě[224] (například CVC/CVV kód), který se nepokládá ani za prvek znalosti (vizte kapitola 2.1.1).

2.1.3. Inherence

Inherencí se rozumí ověření pomocí „biometrických údajů uživatele“[225]. Tento široký pojem se ve směrnici PSD2 definuje jako „to, čím uživatel je“[226].

Troufám si tvrdit, že prvek inherence bude jedním z preferovanějších prvků, které si uživatel zvolí, jelikož díky technologickému pokroku má valná většina uživatelů chytré telefony, které dokážou naše biometrické údaje zaznamenat. Alespoň já osobně prvek inherence využívám nejvíce při silném ověření uživatele v kombinaci s prvkem znalosti. Podle odhadů z roku 2018 mohlo proběhnout v roce 2020 až 126 mld. transakcí v hodnotě kolem 1,1 bilionů USD[227].

---

[220] Table 2, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.6.

[221] Ibid.

[222] Table 2, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.6.

[223] Ibid.

[224] Table 2, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.6.

[225] § 223, odst. 3, písm. c) ZoPS

[226] Článek 4, odst. 30 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

[227] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

Otázkou je, co znamenají biometrické údaje uživatele. Komentář k ZoPS zmiňuje: „Biometrie je vymezena jako biologický vědní obor zabývající se zjišťováním kvantitativních znaků (délky, výšky apod.) organismů (Havránek a kol., 1989, k heslu biometrie). Biometrický údaj lze tedy vymezit jako měřitelný fyzický znak uživatele. Nařízení GDPR vymezuje biometrické údaje jako osobní údaje vyplývající z konkrétního technického zpracování týkajícího se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“[228].

Další zdroj se zmiňuje o tom, že: „Biometrikami rozumíme jedinečné, měřitelné, anatomické, fyziologické nebo behaviorální charakteristiky člověka, přičemž v praxi využíváme ty biometriky, které jsou stálé a které je možné bez nepřiměřených obtíží automatizovaně změřit a naměřená data dále zpracovávat, jako např. otisk prstu, vzor oční duhovky či sítnice, geometrie ruky, charakteristiky tváře či hlasu“[229].

Z toho můžeme dovodit, že tyto údaje jsou anatomicky a fyziologicky dané, jedinečné nebo rozeznatelné ze znaků chování daného uživatele. Je potřeba zdůraznit, že nařízení RTS ukládá povinnost poskytovateli platebních služeb zmírnit riziko, aby nebyly zneužity neoprávněnou osobou, zejména u zařízení a softwaru[230]. Jedno z podobných reálných řešení už se připravuje, a to startup CardioID, který vyvíjí technologii založenou na biometrických údajích, konkrétně na EKG[231]. Tento produkt by měl fungovat v rámci dalšího hardwaru, což si myslím, že by mohla být překážka pro širší využití, především v případě, že funkci EKG už poskytují běžné chytré hodinky, jako jsou Apple Watch. Pro připomenutí, EKG „je základní vyšetřovací metoda v kardiologii. Jejím principem je snímání

[228] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[229] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

[230] Článek 8, odst. 1 nařízení RTS

[231] BREJČÁK, Peter. Místo obličeje vyvíjí brněnští vědci ověření identity pomocí tlukotu srdce. EKG má být unikátnější než otisk prstu. CzechCrunch [online]. 2022 [cit. 2022-03-12]. Dostupné z: https://cc.cz/misto-obliceje-vyviji-brnensti-vedci-overeni-identity-pomoci-tlukotu-srdce-ekg-ma-byt-unikatnejsi-nez-otisk-prstu/ [online]. [cit. 2022-03-12].

elektrické srdeční aktivity a v podobě elektrokardiogramu (časový záznam EKG křivek) umožňuje její hodnocení.“[232]

Stanovisko EBA-Op-2019-06 Evropského orgánu pro bankovnictví uvádí následující příklady toho, co se dá považovat za prvky inherence:

a) sken otisku prstů[233],

b) rozpoznání hlasu[234],

c) rozpoznání žil[235],

d) geometrie ruky a obličeje k identifikaci uživatelova obličeje či ruky[236],

e) skenování sítnice a duhovky[237],

f) dynamika stisknutí kláves[238],

g) srdeční frekvence nebo jiné vzorce pohybu těla[239] (u nositelných zařízení, například Apple Watch), a

h) úhel ve kterém je zařízení držen[240].

Mezi prvky inherence StanoviskoEBA-Op-2019-06 nepokládá memorised swiping path (volně přeloženo jako znak na obrazovce mobilního telefonu nebo zamykací gesto)[241] nebo informace přenášené pomocí komunikačního protokolu, jako například EMV® 3-D Secure[242].

Nejprve je potřeba jeden z těchto prvků zaregistrovat v daném zařízení[243]. Typickým příkladem je mobilní telefon, přičemž já osobně používám Apple iPhone

---

[232] Elektrokardiografie. WikiSkripta [online]. [cit. 2022-03-12]. Dostupné z: https://www.wikiskripta.eu/w/Elektrokardiografie

[233] Bod. 19, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 5.

[234] Ibid.

[235] Bod. 19, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 5.

[236] Ibid.

[237] Bod. 19, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 5.

[238] Ibid.

[239] Bod. 19, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 5.

[240] Table 1, Ibid., s. 35

[241] Bod 20, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 5.

[242] Bod 21, Ibid., s. 5.

[243] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

se zabudovanou technologii FaceID, která rozpoznává obličej uživatele pomocí vyvinuté technologie společností Apple. Tato informace se uloží v šifrovaném úložišti/čipu (záleží na modelu daného telefonu) po registraci tohoto prvku v zařízení. Můžeme zde jen polemizovat o tom, zda je bezpečné svěřit své jedinečné údaje (například oční rohovka a otisk prstu) výrobci, byť s dobrým compliance na uchovávání osobních dat. Obzvlášť v současné době, kdy takřka každý rok se dostane na veřejnost zpráva, která oznamuje velký únik osobních dat. Například únik osobních dat, který se „povedl" americkému Facebooku[244] v roce 2019 nebo britskému BioStar 2[245] v roce 2018, kdy unikly přímo otisky prstů a kontury obličeje. O to horší, že v případě BioStar 2 jej používaly britské banky i metropolitní policie. Ruku v ruce s tím jde také riziko přístupu dalších osob do mobilního telefonu, nýbrž i možného obejití silného ověření uživatele, které mají rovněž nastavený přístup, kromě samotného uživatele. Ze své vlastní zkušenosti mám z důvodu vlastního pohodlí přístup přes TouchID (technologie snímající otisky prstů) do mobilního telefonu svých rodičů, kteří jej však nepoužívají k přístupu do internetového bankovnictví.

V tomto případě nemá banka nad těmito prvky žádnou kontrolu a musí důvěřovat třetí straně. Přínosem je, že neručí za ztrátu těchto dat[246].

2.1.4. Mobilní aplikace „klíč"

Poslední rok a půl zaznamenávám, že banky hledají nové cesty a v praxi už nabízejí nové způsoby, jak dostát požadavku splnění 2 ze 3 prvků při silném ověření uživatele. Je to komfortní v případě, že vlastníte chytrý telefon, který má alespoň snímač otisku prstů (například TouchID od Apple) nebo rozpoznání obličeje (například FaceID od Apple).

Tyto mobilní aplikace se většinou nazývají klíč, například George klíč od České spořitelny nebo KB klíč od Komerční banky. Tyto „klíče" v sobě kombinují 3 prvky[247]:

---

[244] Facebook přiznal obří únik dat. Útočníci se dostali k 50 milionům uživatelských účtů. *INFO.CZ* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://www.info.cz/zpravodajstvi/svet/facebook-priznal-obri-unik-dat-utocnici-se-dostali-k-50-milionum-uzivatelskych-uctu

[245] Otisky prstů i osobní údaje. Bezpečnostní firma nechala na internetu 23 gigabytů nechráněných dat. *IROZHLAS* [online]. [cit. 2021-02-22]. Dostupné z: https://www.irozhlas.cz/veda-technologie/hash-otisky-prstu-rozpoznani-obliceje-unik-dat-databaze-guardian-kauza-vedci_1908160800_mpr

[246] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

[247] Česká spořitelna spouští aplikaci George klíč pro všechny klienty. *Česká spořitelna* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2019/09/11/ceska-sporitelna-spousti-aplikaci-george-klic-pro-vsechny-klienty

a) prvek držení – zařízení,

b) prvek znalosti – PIN, který si nastaví uživatel v aplikaci, a

c) prvek inherence – otisk prstu či rozpoznání obličeje.

Platí zde to, že „musí existovat spolehlivý prostředek k potvrzení držení prostřednictvím vygenerování nebo přijetí prvku dynamického ověření na zařízení“[248], jinak by v tomto případě prvek držení nemohl být uznán.

2.2. Výjimky ze silného ověření klienta

Nařízení RTS udává výjimky, kdy poskytovatel platební služby nemusí provést silné ověření klienta.

2.2.1. Informování o platebním účtu

V článku 10 nařízení RTS je stanovena výjimka, při které se neužije silné ověření uživatele v případě informování o platebním účtu, kdy třetí strana získá přístup k zůstatku na platebním účtu a k platebním transakcím v posledních 90 dnech. Tato výjimka je spjata se službou informování o platebním účtu, kdy uživatel autorizuje přístup aplikace třetí strany ke svému platebnímu účtu. Každých 90 dní musí uživatel potvrdit, že trvá jeho vůle o souhlasu se získáváním těchto výše uvedených údajů[249].

Dle mého názoru je tato lhůta na potvrzování velmi nekomfortní pro uživatele užívající aplikace třetích stran. Tyto aplikace mají usnadňovat každodenní fungování uživatelů. Každé oznámení či potvrzení pouze zdržuje, což mohu potvrdit ze své vlastní zkušenosti. Nechal bych rozhodnutí na každém uživateli, zda chce dále sdílet tato data s poskytovateli služby informování o platebním účtu a spoléhat se na rozumné uvažování těchto uživatelů. Někteří zástupci širší odborné veřejnosti[250] se obávali toho, zda tento model nebude podporovat BFU (běžného Frantu uživatele) k tomu, aby takový uživatel povolil bezhlavě každé aplikaci přístup ke svým datům. Myslím si, že rozumně uvažující člověk bude uvažovat nad tím, komu povolí přístup. Navíc ochrana osobních dat v Evropské unii je již na tak

[248] Bod 35, European Banking Authority. EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC ze dne 13. června 2018, s.7.

[249] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[250] BREJČÁK, Peter. Startupy zbrzdí regulace a další vzniknou jen pro efekt: 6 rizik, které do bankovnictví přináší PSD2. *Tyinternety* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://tyinternety.cz/fastnews/6-rizik-ktere-do-bankovnictvi-prinasi-psd2/

vysoké úrovni, že i kdyby se stalo něco podobného, jak výše prorokovali, tak to nebude mít velké následky.

2.2.2. Bezkontaktní platby v místě prodeje

Výjimka ze silného ověření uživatele v případě bezkontaktní platby v místě prodeje se uplatní, pokud se splní následující podmínky:

„a) jednotlivá částka bezkontaktní elektronické platební transakce nepřesáhne 50 EUR a

b) kumulativní částka předchozích bezkontaktních elektronických platebních transakcí iniciovaných prostřednictvím platebního prostředku s bezkontaktní funkcí ode dne posledního uplatnění silného ověření klienta nepřesáhne 150 EUR, nebo

c) počet po sobě následujících bezkontaktních elektronických platebních transakcí iniciovaných prostřednictvím platebního prostředku nabízejícího bezkontaktní funkci ode dne posledního uplatnění silného ověření klienta nepřesáhne pět.“[251]

Z těchto podmínek můžeme vyčíst, že silné ověření uživatele není potřeba v případě jednotlivé transakce, která nepřesáhne 50 EUR nebo pokud kumulativní částka všech transakcí od posledního silného ověření uživatele nepřesáhne 150 EUR. Můžeme tomu porozumět tak, že při platbě kartou, kdy se zadává PIN kód, který je zároveň prvkem znalosti a platební karta představuje prvek držení (vizte v kapitole 2.1.2) splní požadavky silného ověření uživatele, pokud přesáhne buď jednotlivá transakce hodnoty 50 EUR nebo 150 EUR při více transakcích.

Vydavatelské banky však vyžadují PIN kód při bezkontaktních platbách nad 500 Kč, dále po určitém počtu transakcí bez použití PIN kódu a někdy jej vyžaduje zcela náhodně. Hranice 500 Kč je nastavená skrze konsensus vydavatelských bank v České republice[252] [253]. Ohledně tohoto limitu se vedly diskuse na začátku pandemie koronaviru COVID-19. V konečném důsledku se však limity nezvýšily, navzdory ostatních členských zemí Evropské unie, které tyto limity zvýšily až do výše 50 EUR, jenž směrnice PSD2 povoluje[254].

---

[251] Článek 11 nařízení RTS

[252] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[253] SVOBODA, Jakub. PIN při platbě kartou nad 500 korun zůstává, banky zvýšení limitu odmítly. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://www.novinky.cz/finance/clanek/pin-pri-platbe-kartou-nad-500-korun-zustava-banky-zvyseni-limitu-odmitly-40320375

[254] HOVORKOVÁ, Kateřina. Virus donutil řadu zemí zvýšit limity pro neověřené platby. Česko se však změně brání. *Aktuálně.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z:

S příchodem Apple Pay na český trh[255] a dalších ekvivalentů v podobě například Garmin Pay či Google Pay, nabývám pocitu, že používání klasických platebních karet už není téma na pořadu dne a brzy tato výjimka už nebude ani potřeba.

2.2.3. Terminály bez obsluhy pro jízdné a poplatky za parkování

Silné ověření uživatele se nepoužije v případě samoobslužných terminálů na placení jízdného nebo parkovného bez limitu částky či počtu transakcí, jako například v kapitole 2.2.2.[256] Se samoobslužnými terminály se dá setkat například v plzeňské MHD (která byla mezi prvními v České republice), kde je možnost zaplatit bezkontaktně jízdenku, dále pak v obchodních domech, kde zákazník zaplatí na výjezdu z parkoviště, například v parkovacím domě Rychtářka v Plzni.

2.2.4. Důvěryhodní příjemci

Uživatel dle nařízení RTS zde má možnost zařadit u poskytovatele platebních služeb příjemce na seznam důvěryhodných příjemců, u kterých nebude potřeba uplatnění silného ověření klienta při iniciování platební transakce. Při tvorbě tohoto seznamu je ale silné ověření uživatele zapotřebí[257].

2.2.5. Opakující se transakce

Silné ověření klienta se vždy v těchto případech použije poprvé, kdy uživatel vytváří, změní nebo poprvé iniciuje transakci. Transakce musí mít stejného příjemce a vždy stejnou částku[258].

Typicky opakující se transakce představují trvalé příkazy nebo platba za předplatné některých služeb.

2.2.6. Úhrady mezi účty téže fyzické nebo právnické osoby

V případě, že uživatel má u stejného poskytovatele platebních služeb více účtů, například u stejné banky, silné ověření uživatele se neprovede v případě iniciace úhrady z jednoho účtu na druhý. Tato výjimka platí jak pro fyzické, tak i právnické osoby.

---

https://zpravy.aktualne.cz/finance/rada-zemi-zvysila-limity-pro-platby-kartou-bez-overeni-ceske/r~f9bafb7aac9611ea8b230cc47ab5f122/

[255] MATURA, Jan. PŘEHLEDNĚ: Jak aktivovat Apple Pay a jak jsou platby zabezpečené. *IDNES.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.idnes.cz/mobil/tech-trendy/apple-pay-v-cesku-videonavod.A190219_085956_mob_tech_jm

[256] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[257] Ibid.

[258] Článek 14 nařízení RTS

2.2.7. Transakce týkající se malých částek

V případě, že uživatel iniciuje elektronickou platební transakci na dálku a splní následující podmínky:

„a) částka elektronické platební transakce na dálku nepřesáhne 30 EUR a

b) kumulativní částka předchozích elektronických platebních transakcí na dálku iniciovaných plátcem ode dne posledního uplatnění silného ověření klienta nepřesáhne 100 EUR, nebo

c) počet předchozích elektronických platebních transakcí na dálku iniciovaných plátcem od posledního uplatnění silného ověření klienta nepřesáhne pět po sobě následujících jednotlivých elektronických platebních transakcí na dálku.“[259]

Při elektronické platební transakci na dálku, která je do částky 30 EUR, a tedy je bez silného ověření klienta, si poskytovatel platebních služeb vybere jednu ze dvou možností, které mu nařízení RTS dává.

2.2.8. Zabezpečené platební procesy a protokoly společností

Tato výjimka platí pro uživatele, kteří jsou právnickými osobami a nejsou spotřebiteli. Tyto právnické osoby „iniciují elektronické platební transakce použitím zvláštních platebních procesů nebo protokolů, které jsou zpřístupněny pouze plátcům, kteří nejsou spotřebiteli“[260] což můžeme chápat, jako „korporátní společnosti (nikoliv spotřebitelé) a kde je zabezpečení dosaženo jinými prostředky než autentizací jednotlivé osoby“[261].

2.2.9. Analýza transakčních rizik

Předposlední výjimka, při které poskytovatel platebních služeb nemusí použít silné ověření klienta, nastane v případě, kdy identifikuje transakci s nízkou mírou rizika na základě toho, když bere v potaz rizikové faktory, jako jsou seznamy odcizených či vyzrazených ověřovacích prvků, částky platebních transakcí, scénáře podvodů při poskytování platebních služeb, napadení malwarem při spojení během ověření nebo například neobvyklé použití zařízení nebo softwaru pro přístup[262].

S výše uvedenými případy musí poskytovatel platebních služeb kombinovat také referenční hodnoty pro „elektronické karetní platby na dálku“, resp.

[259] Článek 16 nařízení RTS

[260] Článek 17 Ibid.

[261] HUML, Tomáš. PSD2: Finální verze RTS k SCA – shrnutí zásadních změn. In: *Deloitte Česká republika [*online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/Deloitte_PSD2_Final_RTS_k_SCA_Souhrn_zasadnich_zmen_Technolog_Security.pdf

[262] Článek 2, odst. 2 nařízení RTS

„elektronické úhrady na dálku“ [263] upravené v příloze nařízení RTS o míře podvodů, částky transakce, které nepřesahují stanovenou hodnotu pro výjimku v těchto tabulkách a zda v reálném čase nezjistil během analýzy rizik neobvyklé chování plátce či výdaje, neobvyklé informace o zařízení nebo softwaru plátce, napadení malwarem při spojení během ověření, neobvyklé místo plátce, známé scénáře podvodů při poskytování platebních služeb a vysoce rizikové místo příjemce[264].

2.2.10. Výpočet míry podvodů

Součástí nařízení RTS je pro každý druh transakce v příloze upravená celková míra podvodů, která se vztahuje na platební transakce ověřené silným ověřením uživatele.[265] V případě, že míra podvodů přesáhne referenční hodnoty v příloze, poskytovatel platební služby musí vyrozumět ČNB a pokud překročí ve dvou po sobě jdoucí čtvrtletí, nelze výjimky ze silného ověření uživatele nadále využít[266].

2.3. Porušení povinnosti

Pokud poskytovatel platebních služeb neprovede silné ověření uživatele, ve výše již zmíněných případech, kdy je zapotřebí jej provést při vzniku škody za neautorizovanou platební transakci, pak nese ztrátu poskytovatel platebních služeb v plné výši[267].

Při porušení povinnosti ze strany uživatele, například vyzrazení prvků a faktorů silného ověření uživatele, nese uživatel ztrátu z neautorizované platební transakce[268].

---

[263] Článek 18, odst. 2 nařízení RTS

[264] Článek 18, odst. 2 Ibid.

[265] Článek 19, odst. 1 nařízení RTS

[266] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[267] § 182, odst. 3, písm. c) ZoPS

[268] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

3. Digitální onboarding aneb je Bankovní identita řešením?

FinTech společnosti při poskytování svých služeb klientům mohou narazit na velmi nepříjemný problém, který vězí v uzavírání smluvního vztahu na dálku, zejména v České republice, kde digitalizace veřejné správy a celkově elektronické identifikace osob není tak rozšířená, jelikož nástroje k tomu nejsou v hojné míře rozšířené. Což je pro mě nepochopitelné s tím, jakou rychlostí se adaptovali klienti bank na bezkontaktní platby a následné placení přes Apple Pay, v čem je Česká republika jedním z premiantů v Evropě. Ani západní země nedosahují takové míry plateb bezkontaktním způsobem.

Proces získání klientů na dálku se nazývá digitální onboarding. Tomuto procesu můžeme obecně rozumět jako „možnost potvrdit pravost osoby a zprostředkovat nový smluvní vztah bez nutnosti osobního kontaktu“.[269] Poptávka po tomto způsobu zprostředkování smluvního vztahu se samozřejmě během pandemie koronaviru COVID-19 zvýšila a tím, že banky a FinTech společnosti vycházely klientům vstříc, v postcovidové době si na tento komfortní způsob klienti zvykli. Tento trend digitalizace můžeme brát jako přirozený přechod poskytování služeb v kamenných pobočkách do digitálního prostoru a lze na to nahlížet širší optikou, neboť jsem se už v předchozích kapitolách zmínil, že velké banky, například Česká spořitelna, se chystají uzavírat kamenné pobočky a zaměřovat se na bankovní poradenství přes videokonference. Tento trend nastavuje zejména mladší generace, která není zvyklá na návštěvy poboček těchto bank a raději vše vyřizuje přes Internet. Sám v rámci praxe spatřuji, že i uzavírání velkých smluv je realizovatelné pouhým podpisem přes službu DocuSign, a proto považuji za dosti archaické, aby za účelem založení spořícího účtu musel klient navštívit pobočku své banky, aby podepsal smlouvu o založení účtu a další dokumenty v papírové podobě, například souhlas s poskytováním údajů pro marketingové účely dané banky. Vše lze vyřešit kvalifikovaným podpisem, který tu nabízí nařízení eIDAS, přičemž přitom nemusím vyjít ani z kanceláře nebo ze svého bytu. Ušetřím si tím veliké množství času, byť některé banky vychází vstříc klientům tím, že pošlou smlouvy kurýrní službou. Zatím však ale nejsem prémiovým klientem, abych mohl zprostředkovat takovou zkušenost osobně.

[269] BUCHBAUER, Petr. Vítej na palubě homo digitalis aneb jak na digitální onboarding. Peak.cz [online]. 2019 [cit. 2022-03-12]. Dostupné z: https://www.peak.cz/vitej-palube-homo-digitalis-aneb-digitalni-onboarding/5919/

Dle mých dosavadních praktických zkušenosti je však digitální onboarding stále ještě „v plenkách“. Pokusil jsem se absolvovat digitální onboarding při založení bankovního účtu přes internet u Československé obchodní banky, kde jsem zjistil, že tato banka nevyužívá všechny dostupné nástroje, které nám tu poskytuje dnešní právní rámec v rámci Evropské unie a ani jiné banky nebo FinTech společnosti nejsou na tom o dost lépe.

K tomu, aby mohl proběhnout digitální onboarding, musíme mít k tomuto technické prostředky, jak ověřit osobu na „druhé straně monitoru“, které jsou právně uznatelné na území České republiky či na území členských států Evropské unie. Nabízí se zde zmínit například elektronickou identifikaci dle nařízení eIDAS, které založilo právní rámec pro elektronickou identifikaci, zejména její uznání mezi členskými státy a elektronické podpisy. Nemůžu si však opět odpustit poznámku, že výše uvedená regulace přišla opět trochu pozdě oproti potřebám na trhu, jelikož ve skandinávských zemích, například ve Švédsku, se elektronická identifikace, v souvislosti s jejich systémem e-governmentu, začala realizovat již na začátku milénia, zatímco v Evropské unii to trvalo o něco déle, když elektronickou identifikaci odstartoval až pilotní projekt STORK 2.0.

Definicí elektronické identifikace dle nařízení eIDAS je „postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu“[270]. O elektronické identifikaci se zmíním v kapitole 3.5.1.

V České republice vzniklo v minulosti hodně projektů k identifikaci osob na dálku už v minulosti, můžeme mezi ně zařadit projekt MojeID, které vzniklo pod sdružením CZ.NIC, které bylo mohutně propagováno na začátku desetiletí portálem Seznam.cz a používalo se například k přihlašování na různých diskusních fórech k tomu, aby se členy nestaly anonymní osoby, které by spamovaly fórum. Tento projekt funguje dodnes a je správcem kvalifikovaného systému elektronické identifikace.

V období, kdy jsem si měl vybírat diplomovou práci, příhodně zároveň v době mé pracovní zkušenosti v Deloitte Legal, proběhlo v médiích mnoho zpráv o projektu Bankovní identity, jinak pod označením SONIA či BankID, kterou

[270] Článek 3, odst. 1 nařízení eIDAS

vytvořila Česká bankovní asociace a pracuje na ní od roku 2019[271], která později vyhrála anketu Zákon roku 2020, kterou pořádala právě Deloitte Legal[272].

Myšlenka Bankovní identity, v širším pojmu, nepředstavuje nic nového na scéně identifikace či ověření osob na dálku. Například projekt BankID ve Švédsku je v ostrém provozu již od roku 2003. Obecně skandinávské a pobaltské země jsou dle mého názoru lídrem v tomto oboru.

Myslím si, že tento projekt bude mít zásadní vliv na to, jak bude obyvatelstvo v České republice nahlížet na digitalizaci veřejné správy v rámci e-governmentu a celkově přechod právních jednání do „virtuálního prostoru". Proč si troufám toto tvrdit? Průzkum Češi a digitalizace 2020[273], kterou provedla České bankovní asociace, ukázal, že 97 % klientů bank používá internetové bankovnictví. Cestu k digitalizaci veřejné správy, kterou slibuje ZoD, může Bankovní identita dopomoci účinněji, oproti jiným způsobům přihlášení/přístupu do Portálu občana a dalších služeb pro občany, na které se lze přihlásit přes internet.

Zpět však k digitálnímu onboardingu neboli on-line onboardingu, jak je také nazýván tento proces. Digitální onboarding můžeme obecněji nazvat jako proces, kdy například banka nebo FinTech společnost, získává klienta na dálku, aniž by tento klient musel osobně navštívit pobočku dané instituce. Tento proces se vyznačuje zejména rychlostí, jednoduchostí, bezpečným a garantovaným způsobem[274] [275]. Během tohoto procesu získává daná instituce údaje o svém novém klientovi, během kterého musí potvrdit pravost osoby, uzavřít smlouvu a splní k tomu zákonné požadavky, které musí plnit jako povinná osoba dle AMLZ. O těchto požadavcích dle AMLZ se rozepíši více v kapitole 3.3.

Tento způsob získání klientů je komplexní a vyžaduje splnění jak požadavků zákonných, tak i technických. Existuje však několik technických řešení, která se využívají mimo Bankovní identity nebo MojeID.

---

[271] Bankovní identita umožnila nový rozměr elektronického ověřování totožnosti. Advokátní deník [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://advokatnidenik.cz/2021/02/09/zakon-o-bankovni-identite-umoznil-novy-rozmer-elektronickeho-overovani-totoznosti/

[272] Bankovní identita zvítězila v anketě Zákon roku 2020. DReport [online]. 2021, 21. 4. 2021 [cit. 2022-03-11]. Dostupné z: https://www.dreport.cz/blog/bankovni-identita-zvitezila-v-ankete-zakon-roku-2020/

[273] Češi a digitalizace 2020. *Česká bankovní asociace* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2020

[274] Digital Onboarding: definition, characteristics and how it works. Electronic IDentifiaction [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.electronicid.eu/en/blog/post/digital-onboarding-process-financial-sector/en

[275] Digital onboarding and cost efficiency. PXL Vision [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.pxl-vision.com/en/blog/what-is-digital-onboarding-and-how-to-reduce-business-costs-during-id-verification

Obrázek 3 *– Jedna z variant digitálního onboardingu*

Upraveno ze zdroje: Digitální onboarding klientů. Deloitte Česká republika [online]. 2022 [cit. 2022-04-16]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/financial-services/solutions/digitalni-onboarding-klientu.html

3.1. Způsoby digitálního onboardingu

Digitální onboarding je jedním z mnoha druhů klientského onboardingu, které společnosti využívají při získání klienta. Mimo digitální onboarding se v praxi užívají následující způsoby.

a) On-Site Onboarding – běžný způsob, kdy klient navštíví pobočku nebo sídlo dané společnosti a pracovník ověří jeho totožnost[276] [277].

[276] Digital Onboarding: definition, characteristics and how it works. Electronic IDentifiaction [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.electronicid.eu/en/blog/post/digital-onboarding-process-financial-sector/en

[277] BIELSKAITĖ, Viktorija. Digital Onboarding: Definition, Types and How it Works. IDenfy [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.idenfy.com/blog/digital-onboarding/

b) Semi-On-Site Onboarding – hybrid mezi digitálním onboardingem a On-Site Onboardingem v bodě a). Dokumenty vyplní klient z domova a následně přinese na pobočku nebo sídlo společnosti.[278] [279]

Nevýhody On-Site a Semi-On-Site onboardingu spočívají dle mého názoru v tom, že klienti jsou vázáni na návštěvu pobočky dané společnosti, což je může odradit od toho, aby vůbec danou službu využili. On-Site onboarding je však nejjistějším způsobem, při kterém můžeme uzavřít právní jednání, protože zde není žádné riziko, kromě lidského faktoru, které by způsobilo omyl či přímo podvod při identifikaci osoby, která uzavírá smlouvu. Semi-On-Site je hybridem mezi digitálním onboardingem a On-Site onboardingem, avšak mně osobně takové řešení přijde nešťastné a lze takové řešení nahradit podpisem na dokumentech, které pošle banka kurýrem.

Digitální onboarding je v současné době v Evropské unii regulován nařízením eIDAS a směrnicí AML, která je transponována do české legislativy pod AMLZ. Výhody digitálního onboardingu, které spočívají v rychlosti a dostupnosti pro klienty, jsem již vysvětlil výše.

Průběh digitálního onboardingu můžeme rozdělit do čtyř fází, a to:

a) Fáze před onboardingem – potenciální klient při této fázi zadává společnosti potřebné osobní identifikační údaje a atributy ke KYC[280] pro pozdější ověření a shromáždění informací[281].

b) Fáze ověření – V této fázi se ověřuje:

i) pravost dokumentů k osobní identifikaci potenciálního klienta,

ii) totožnost potenciálního klienta,

iii) proti podvodům, zda dokumenty nesouvisí s podvodnými aktivitami nebo zda potenciální klient není součástí podvodu, pod sankcemi nebo není považován za politicky exponovanou osobu[282].

---

[278] Digital Onboarding: definition, characteristics and how it works. Electronic IDentifiaction [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.electronicid.eu/en/blog/post/digital-onboarding-process-financial-sector/en

[279] BIELSKAITĖ, Viktorija. Digital Onboarding: Definition, Types and How it Works. IDenfy [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.idenfy.com/blog/digital-onboarding/

[280] KYC = poznej svého zákazníka, identifikování a ověření zákazníků, například rámci AML

[281] Study on eID and digital on- boarding: mapping and analysis of existing on- boarding bank practices across the EU [online]. 2018 [cit. 2022-04-16]. ISBN SBN 978-92-79-77867-4. Dostupné z: https://ec.europa.eu/futurium/en/system/files/ged/study_on_eid_digital_onboarding_final_report.pdf

[282] Ibid.

c) Fáze shromažďování – Tato fáze zahrnuje shromažďování a dokumentace atributů ke KYC.

d) Fáze správy – V poslední fázi se atributy spravují.

Fáze shromažďování a správy se v praxi směšuje do jedné aktivity, avšak nahlíží se na ně jako na dvě odlišné fáze.

3.2. Požadavky AMLZ a proč jsou důležité?

AMLZ a jeho opatření, které jsou v něm obsaženy mají smysl a účel v „zabránění zneužívání finančního systému k legalizaci příjmů z trestné činnosti a financování terorismu, uchování stop po přesunech majetku, včetně záznamu o tom od koho, prostřednictvím koho a ke komu se tyto prostředky přemisťovaly.“[283]

Z tohoto pohledu je důležité, aby povinné osoby dle AMLZ provedly identifikaci potenciálního klienta. Mezi povinné osoby patří například banky, spořitelní a úvěrové družstvo, Centrální depozitář cenných papírů, provozovatel hazardních her, osoba, která nakupuje nebo prodává nemovité věci, realitní zprostředkovatel, auditor, advokát, notář a mnoho dalších[284].

Z výše uvedeného výčtu můžeme zpozorovat, že je velice důležité, aby byly pokryty všechny oblasti poskytování služeb, kde se nakládá s majetkem během obchodního vztahu, což nemíjí ani oblast FinTech, kterou se tato rigorózní práce zabývá.

Povinnost provést identifikaci povinné osobě vzniká v následujících případech:

a) kdy je zřejmé, že překročí hodnota obchodu částku 1000 Euro[285],

b) při podezřelém obchodu[286],

c) při vzniku obchodního vztahu[287],

d) během nákupu „nebo přijetí kulturních památek, předmětů kulturní hodnoty, použitého zboží nebo zboží bez dokladu o jeho nabytí ke zprostředkování jejich prodeje anebo přijímání věcí do zástavy“[288],

e) při výplatě „zůstatku zrušeného vkladu z vkladní knížky na doručitele“ [289],

---

[283] Důvodová zpráva k zákonu č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, č. 253/2008 Dz

[284] § 2 AMLZ

[285] § 7, odst. 1 Ibid.

[286] § 7, odst. 2, písm. a) AMLZ

[287] § 7, odst. 2, písm. b) Ibid.

[288] § 7, odst. 2, písm. c) AMLZ

[289] § 7, odst. 2, písm. d) Ibid.

f) kdy osoba není pojistníkem „a má právo na plnění ze životního pojištění, nejpozději v době vyplacení pojistného plnění“ [290],

g) pro jednotlivé typy poskytovaných obchodů povinnou osobou, kterou stanoví na základě hodnocení rizik[291].

3.2.1. Překročení částky 1000 Euro

Povinná osoba provádí identifikaci klienta zejména při jednorázových obchodech, přičemž obchodem rozumíme „jednání povinné osoby jednající v tomto postavení s jinou osobou, pokud takové jednání směřuje k nakládání s majetkem této jiné osoby jednající v tomto postavení nebo k poskytnutí služby této jiné osobě.“[292] Povinnost mu vzniká ve chvíli, kdy je zřejmé, že hodnota transakce daného obchodu překročí částku 1000 Euro. Povinná osoba si však může vnitřně nastavit vlastní hranici, kdy provede identifikaci klienta[293]. V tomto případě rozumím dikci komentáře tak, že si povinná osoba může nastavit nižší hodnotu, při které provede identifikaci klienta. V tomto případě postupuje dle hodnocení rizik, které určuje § 21a AMLZ.

Zajímavostí je, že hranice 1000 Euro se vztahuje k obchodům ve prospěch klienta, jako je třeba výplata vkladu, tak i naopak[294].

3.2.2. Podezřelý obchod

Podezřelým obchodem se rozumí „obchod uskutečněný za okolností vyvolávajících podezření ze snahy o legalizaci výnosů z trestné činnosti nebo podezření, že v obchodu užité prostředky jsou určeny k financování terorismu, nebo že obchod jinak souvisí nebo je spojen s financováním terorismu, anebo jiná skutečnost, která by mohla takovému podezření nasvědčovat“[295].

---

[290] § 7, odst. 3 AMLZ

[291] § 7, odst. 4 Ibid.

[292] § 4, odst. 1 AMLZ

[293] KATOLICKÁ, M. § 7 [Povinnost identifikace] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[294] Ibid.

[295] § 6, odst. 1 AMLZ

Prostředky užité v obchodu znamenají například „finanční prostředky, cenné papíry, nemovitou věc, movitou věc či pohledávku“[296] a nelimituje zde ani výše daných prostředků[297].

Zákon přímo určuje, kdy je daný obchod podezřelý. AMLZ dává za demonstrativní příklady podezřelého obchodu případy, kdy klient provádí převody na jiné účty po hotovostních vkladech, provádí převody majetku bez ekonomického důvodu nebo provádí složité obchody[298], anebo „povinná osoba má pochybnosti o pravdivosti získaných identifikačních údajů o klientovi“[299].

Je nutné dodat, že za podezřelý je obchod považován vždy, když klient je spojen s osobou (v řídící struktuře, skutečný majitel), na kterou se uplatňují mezinárodní sankce podle zákona o provádění mezinárodních sankcí nebo předmětem obchodu má být zboží či služby, na které jsou také uplatněny mezinárodní sankce[300].

3.2.3. Vznik obchodního vztahu

Daná povinnost k provedení identifikace při vzniku obchodního vztahu se vztahuje vždy. Obchodním vztahem dle AMLZ je vždy:

„a) smlouva o účtu,

b) jednorázový vklad,

c) pojistná smlouva,

d) poskytování platebních služeb prostřednictvím elektronických peněz nebo veřejné mobilní telefonní sítě nebo

e) finanční záruka.“[301]

K povinnosti identifikace klienta se nepřihlíží k výši limitu obchodu a tato povinnost má být splněna před první transakcí[302].

---

[296] KATOLICKÁ, M. §6 [Podezřelý obchod] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[297] Ibid.

[298] § 6, odst. 1, písm. a) až h) AMLZ

[299] § 6, odst. 1, písm. i) Ibid.

[300] § 6, odst. 2 AMLZ

[301] § 54, odst. 7 Ibid.

[302] KATOLICKÁ, M. § 7 [Povinnost identifikace] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

3.2.4. Výplata zrušeného vkladu z vkladní knížky na doručitele

Vkladní knížka na doručitele je relikt doby minulé, který byl zrušen k 31. prosinci 2002. Podle dřívější právní úpravy občanského zákoníku, tj. zákon č. 40/1964 Sb., občanský zákoník, bylo možné před 1. srpnem 2000[303] založit vkladní knížku na doručitele nebo na jméno. Výhodou pro některé bylo to, že banka nebo peněžní ústav obecně, při založení vkladní knížky nebo při vybírání, nezkoumala totožnost osoby. Na vkladní knížce byl název, který však nemusel korespondovat s majitelem této vkladní knížky, což by také vlastně odstranilo výhody tohoto typu vkladních knížek. Stačilo tedy jako u některých cenných papírů, předložit vkladní knížku a disponovat s penězi na účtu k nim. Nutno dodat, že při částce vyšší než 100 000 Kč byla potřeba prokázání totožnosti klienta.[304]

Tento druh vkladní knížky byl zrušen v rámci boje proti legalizaci výnosů z trestné činnosti, což podle mě bylo v té době obrovským vstřícným krokem v tomto boji. Omezení každého anonymního vkladu, jak do akcií nebo do vkladních knížek, pouze pomůže v identifikaci původu peněz.

Promlčecí doba pro výše uvedený druh vkladní knížky byla 10 let, a ještě v roce 2016[305] bylo možné vybrat peníze z vkladní knížky na doručitele, nebo jinak tzv. anonymní vkladní knížka.

3.2.5. Plnění ze životního pojištění pro osobu, která není pojistníkem

Životní pojištění jako produkt je upraven v OZ, je „pro případ smrti, dožití se určitého věku nebo dne určeného smlouvou jako konec pojištění“[306].

Pominu-li účel tohoto pojištění, může nastat bohužel situace, kdy toto životní pojištění se vyplácí pro případ smrti a v této chvíli nastává situace, při které je potřeba identifikovat i osobu, která je osobou oprávněnou či obmyšlenou pro plnění ze životního pojištění. Tato povinnost nastává až ve chvíli před výplatou pojistného plnění. Při uzavírání smlouvy není potřeba provedení identifikace[307].

---

[303] Zákon č. 159/2000 Sb., kterým se mění zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů, ve znění zákona č. 15/1998 Sb., a některé další zákony

[304] LIŠKA, Petr. Zánik vkladů na vkladních knížkách na doručitele. Právní rozhledy, 2002, č. 6, s. 255 - 258

[305] Vybrat si peníze z nalezené anonymní vkladní knížky můžete i v roce 2016. Česká spořitelna [online]. 2015 [cit. 2022-04-17]. Dostupné z: https://www.csas.cz/cs/zpravy-z-banky/2015/12/30/vybrat-si-penize-z-nalezene-anonymni-vkladni-knizky-muzete-i-v-roce-2016#

[306] § 2833 Občanského zákoníku

[307] KATOLICKÁ, M. § 7 [Povinnost identifikace] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

3.3. Provádění identifikace dle AMLZ

AMLZ stanoví, že první identifikaci klienta zpravidla provádí povinná osoba následujícími způsoby:

a) v případě fyzické osoby za fyzické přítomnosti identifikovaného[308], a

b) v případě právnické osoby nebo svěřenského fondu za fyzické přítomnosti fyzické osoby, která jedná za klienta[309].

Při identifikaci klienta je tedy nutná fyzická přítomnost identifikovaného, v případě fyzické osoby a v případě právnické osoby by to měl být zpravidla člen statutárního orgánu, který jedná za právnickou osobu. Tato identifikace má proběhnout „nejpozději předtím, než povinná osoba provede první transakci na základě příkazu této konkrétní fyzické osoby (identifikační proces nemusí nutně proběhnout v jeden okamžik)“[310]. V tomto případě nelze identifikovat přes dálkové komunikační systémy, například Skype, MS Teams či jiné platformy[311].

V rámci provádění identifikace je povinná osoba povinna zjistit, zda klient, fyzická osoba jednající za klienta nebo skutečný majitel klienta není politicky exponovanou osobou nebo osobou, vůči níž Česká republika uplatňuje mezinárodní sankce. V případě mezinárodních sankcí se vztahuje dané pravidlo i na osobu, která je ve vlastnické struktuře nebo v řídící struktuře klienta[312].

Politicky exponovaná osoba je zejména fyzická osoba „která je nebo byla ve významné veřejné funkci s celostátním nebo regionálním významem, jako je zejména hlava státu, předseda vlády, vedoucí ústředního orgánu státní správy a jeho zástupce (náměstek, státní tajemník), člen parlamentu, člen řídícího orgánu politické strany, vedoucí představitel územní samosprávy, soudce nejvyššího soudu, ústavního soudu nebo jiného nejvyššího justičního orgánu, proti jehož rozhodnutí obecně až na výjimky nelze použít opravné prostředky, člen bankovní rady centrální banky, vysoký důstojník ozbrojených sil nebo sboru, člen nebo zástupce člena, je-li jím právnická osoba, statutárního orgánu obchodní korporace ovládané státem, velvyslanec nebo vedoucí diplomatické mise, anebo fyzická

[308] § 8, odst. 1, písm. a) AMLZ

[309] § 8, odst. 1, písm. b) Ibid.

[310] KATOLICKÁ, M. § 8 [Provádění identifikace] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[311] Ibid.

[312] § 8, odst. 8 AMLZ

osoba, která obdobnou funkci vykonává nebo vykonávala v jiném státě, v orgánu Evropské unie anebo v mezinárodní organizaci“[313].

Jak je možné vidět výše, definice politicky exponované osoby (anglicky politically exposed person), v odborných článcích jinak uvedena i pod zkratkou PEP, je zde pojímána velice široce a v návaznosti na účel AMLZ je naprosto pochopitelné, proč tomu tak je. Politicky exponovaná osoba je osoba, která už dle samotného pojmenování je velice vlivná a mnoho lobbistů nebo jiných vnějších tlaků bude chtít danou osobu ovlivnit, zejména úplatky. Je podle mého názoru dobře, že na takovou skupinu se AMLZ zaměřuje obzvlášť, v návaznosti na evropskou úpravu směrnice AML. Dle komentáře je výčet funkcí uvedených výše pouze deklaratorní[314].

Zákon nezapomněl ani na osoby, které jsou osobami blízkými k politicky exponované osobě, „společníkem nebo skutečným majitelem stejné právnické osoby, popřípadě svěřenského fondu, jako osoba uvedená v písmenu a), nebo je o ní povinné osobě známo, že je v jakémkoli jiném blízkém podnikatelském vztahu s osobou uvedenou v písmenu a), nebo 3. skutečným majitelem právnické osoby, popřípadě svěřenského fondu, o kterých je povinné osobě známo, že byly vytvořeny ve prospěch osoby uvedené v písmenu a).“[315]

3.3.1. Fyzická osoba

Při identifikaci klienta, kterým je fyzická osoba, má za povinnost povinná osoba učinit následující, a to: „identifikační údaje zaznamená a ověří z průkazu totožnosti, jsou-li v něm uvedeny, a dále zaznamená druh a číslo průkazu totožnosti, stát, popřípadě orgán, který jej vydal, a dobu jeho platnosti; současně ověří shodu podoby s vyobrazením v průkazu totožnosti“[316].

V tomto případě rozumíme identifikačními údaji: „všechna jména a příjmení, rodné číslo, a nebylo-li přiděleno, datum narození a pohlaví, dále místo narození, trvalý nebo jiný pobyt a státní občanství; jde-li o podnikající fyzickou osobu, též její obchodní firma, odlišující dodatek nebo další označení, sídlo a identifikační číslo osoby“[317]. U jmen a příjmení se myslí aktuální, ne rodné

[313] § 4, odst. 5, písm. a) AMLZ
[314] KATOLICKÁ, M. § 4 [Další pojmy] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.
[315] § 4, odst. 5, písm. b) AMLZ
[316] § 8, odst. 2, písm. a) Ibid.
[317] § 5, odst. 1, písm. a) AMLZ

příjmení; místo narození u cizinců stačí stát narození v případě, že je problematické zjistit konkrétní místo narození; pohlaví není nezbytné, pokud vyplývá z příjmení; u státního občanství je potřeba zaznamenat všechna občanství, která má daná osoba[318].

3.3.2. Právnická osoba

Povinná osoba v případě právnické osoby postupuje obdobným způsobem, jako u fyzické osoby, vizte kapitola 3.3.1. Při identifikaci právnické osoby povinná osoba „identifikační údaje zaznamená a ověří z dokladu o existenci právnické osoby získaného z důvěryhodného zdroje a v rozsahu podle písmene a) provede identifikaci fyzické osoby, která za právnickou osobu jedná v daném obchodu nebo při vzniku obchodního vztahu“[319].

U právnické osoby rozumíme identifikačními údaji následující: „základní identifikační údaje právnické osoby, kterými jsou obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, sídlo a identifikační číslo právnické osoby nebo obdobné číslo přidělované v zahraničí“[320]. Obchodní firmou se myslí aktuálním údajem, který je zapsaný v obchodním rejstříku, bez ohledu na historické údaje, kdy byl změněn název nebo byla společnost předmětem projektu fúze[321].

Identifikace fyzické osoby, která je statutárním orgánem právnické osoby se provede podle kritérií, které jsem popsal v kapitole 3.3.1.

3.3.3. Svěřenský fond

Povinná identifikace se vztahuje i na svěřenský fond, kdy „povinná osoba identifikační údaje zaznamená a ověří z dokladu o existenci svěřenského fondu získaného z důvěryhodného zdroje a v rozsahu podle písmene a) provede identifikaci fyzické osoby, která jedná za svěřenský fond v daném obchodu nebo při vzniku obchodního vztahu“ [322].

---

[318] KATOLICKÁ, M. § 5 [Identifikační údaje] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[319] § 8, odst. 2, písm. b) AMLZ

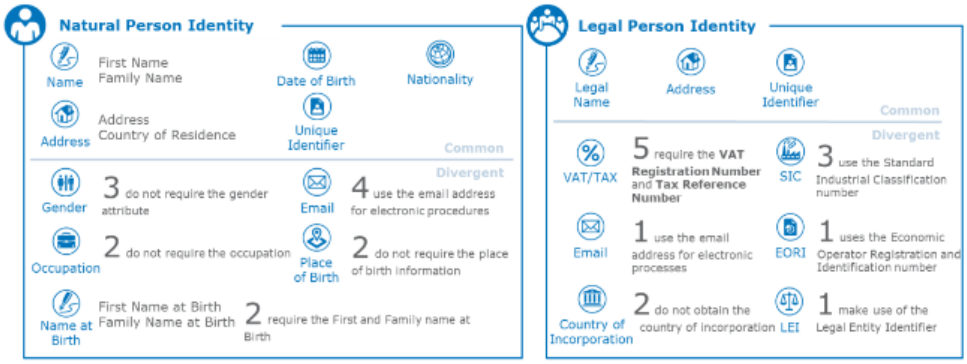
[320] § 5, odst. 1, písm. b) Ibid.

[321] KATOLICKÁ, M. § 5 [Identifikační údaje] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[322] § 8, odst. 2, písm. c) AMLZ

Jedním z identifikačních údajů je vlastní označení svěřenského fondu[323] [324]. V případě svěřenského fondu za něho jedná svěřenský správce, který se bude identifikovat jako fyzická osoba, dle kapitoly 3.3.1. nebo jako právnická osoba, dle kapitoly 3.3.2, avšak v tomto případě se bude identifikovat i jeho statutární orgán[325].

Obrázek 4 *– Přehled údajů k identifikaci fyzických a právnických osob*



Upraveno ze zdroje: Study on eID and digital on- boarding: mapping and analysis of existing on- boarding bank practices across the EU [online]. 2018 [cit. 2022-04-16]. ISBN SBN 978-92-79-77867-4. Dostupné z: https://ec.europa.eu/futurium/en/system/files/ged/study_on_eid_digital_onboarding_final_report.pdf

3.3.4. Výjimky z provádění identifikace

Provádění identifikace klienta, dle výše uvedených kapitol, má být za fyzické přítomnosti identifikovaného nebo osoby jednající za klienta. V tomto případě by však nebyl možný digitální onboarding, o kterém se zmiňuji dříve v kapitole 3 AMLZ nám však dává i jiné možnosti provedení identifikace bez fyzické přítomnosti.

3.3.4.1. Využití prostředku pro elektronickou identifikaci

S příchodem ZoBID, od 1. ledna 2021 umožňuje AML identifikaci klienta využitím prostředku pro elektronickou identifikaci. Prostředkem pro elektronickou identifikaci se rozumí dle AMLZ:

[323] § 1450, odst. 1 Občanského zákoníku

[324] KATOLICKÁ, M. § 5 [Identifikační údaje] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[325] § 1453 Občanského zákoníku

a) „elektronické identifikace pro účely prokazování totožnosti jednající osoby v případech, kdy je to vyžadováno právním předpisem“[326] dle ZoEI, kdy musí jít o „kvalifikovaný systém, je i to, že kvalifikovaný systém umožňuje poskytnutí služby NIA“ [327]. Při využití elektronické identifikace podle ZoEI musí mít prostředek pro elektronickou identifikaci, jinak označen jako PEI, nejvyšší úroveň záruky [328]. Více o elektronické identifikaci a prostředku pro elektronickou identifikaci v kapitole 3.5.

b) Elektronická identifikace, kterou poskytují banky, v rámci projektu Bankovní identita. Více v kapitole 3.6.

3.3.4.2. Zprostředkovaná identifikace

Provedení identifikace lze provést i zprostředkovaně, „na žádost klienta nebo povinné osoby“[329]. Provést zprostředkovanou identifikaci může pouze notář nebo kontaktní místo veřejné správy[330].

Zprostředkovaná identifikace, kterou provede notář nebo kontaktní místo veřejné správy podle podmínek, které jsem vypsal v kapitole 3.3.4.2.

Výsledkem této identifikace je veřejná listina, která dokládá danou identifikaci pro povinnou osobu.

3.3.4.3. Dálková identifikace

Velice podstatnou výjimkou je dálková identifikace, která se využívá zejména ve FinTech oboru a v sektoru bankovnictví obecně. S dálkovou identifikací jsem se setkal například při založení doplňkového penzijního pojištění nebo při založení účtu u služby DEGIRO, kdy jsem si založil obojí během 15 minut, a to z pohodlí domova.

3.3.4.4. S fyzickými doklady

AMLZ umožňuje nahradit fyzické provedení identifikace (vizte kapitola 3.1.3) v případě, že:

a) „klient, který je“[331]:

---

[326] BÉREŠ, J. § 8a [Využití prostředku pro elektronickou identifikaci v rámci identifikace klienta] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[327] PERHÁČOVÁ, M., VESELSKÝ, Š. § 8a In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[328] Ibid.

[329] § 10, odst. 1 AMLZ

[330] Ibid.

[331] § 11, odst. 7, písm. a) AMLZ

i) fyzická osoba nebo fyzická osoba jednající za klienta, rozuměje za právnickou osobu, nebo svěřenský fond „zašle povinné osobě kopie příslušných částí průkazu totožnosti a nejméně jednoho dalšího podpůrného dokladu“[332]. Tyto kopie části průkazu totožnosti musí obsahovat informace, které obsahují údaje, které jsou uvedeny v kapitole 3.3.1. Komentář se zmiňuje také o možnosti zneužití průkazu totožnosti, což je zneužitelné v případě, kdy jsou odcizeny osobní doklady. Pro tento případ je zmínka o podpůrném dokladu, kdy podle komentáře nemá být zvolen dle libovůle klienta k zamezení právě případům zneužití[333],

ii) právnická osoba „zašle povinné osobě doklad o své existenci a své identifikační údaje nebo si povinná osoba existenci a identifikační údaje klienta zjistí z veřejného rejstříku nebo evidence svěřenských fondů“[334]. V praxi se domnívám, že je nejpraktičtější případ, kdy povinná osoba zjistí z veřejného rejstříku, tj. obchodní rejstřík či spolkový rejstřík, údaje a ověří s tím totožnost statutárního orgánu. Nevidím smysl v tom, aby právnická osoba, respektive osoba jednající za ní, posílala například výpis z obchodního rejstříku, kdy udělá samý úkon za povinnou osobu a odradí jí tím více od zařízení služby dálkovým způsobem,

iii) svěřenský fond „zašle povinné osobě doklad o své existenci a své identifikační údaje“. U svěřenského fondu může fungovat to, co v u právnické osoby.

a) povinná osoba prověří údaje a oprávnění dle výše uvedených bodů a nesmí mít žádné pochybnosti o totožnosti klienta nebo osoby jednající za ní[335],

b) povinná osoba a klient uzavřou písemnou smlouvu[336],

c) „klient hodnověrným způsobem prokáže existenci platebního účtu vedeného na jeho jméno u úvěrové instituce nebo u zahraniční úvěrové instituce působící na území členského státu Evropské unie nebo státu tvořícího Evropský hospodářský

[332] § 11, odst. 7, písm. a), bod 1 AMLZ

[333] KATOLICKÁ, M. §11 [Převzetí identifikace] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[334] § 11, odst. 7, písm. a), bod 2 AMLZ

[335] § 11, odst. 7, písm. c) Ibid.

[336] § 11, odst. 7, písm. d) AMLZ

prostor“[337], kdy v tomto případě postačí výpis z účtu, smlouva o zřízení účtu nebo potvrzení úvěrové instituce[338].

d) V návaznosti na prokázání existence platebního účtu v bodu c), provede klient první platbu z daného účtu[339], v praxi se zejména provádí platba 1 Kč nebo 0,01 Euro. Pokud daná platba v platebním systému umožňuje zadat informace o účelu identifikace a označení povinné osoby a hodnocení rizik to povoluje, kopie podpůrného dokladu dle bodu a) nemusí být zaslána[340].

Dálkovou identifikaci mohou provést všechny povinné osoby, kromě povinné osoby uvedené v ustanovení § 2, odst. 1, písm. c) AMLZ a to: „provozovatel hazardní hry podle zákona upravujícího hazardní hry s výjimkou provozovatele peněžité, věcné, okamžité anebo číselné loterie, hry bingo nebo tomboly“.

3.3.4.5. S využitím elektronického podpisu

Kromě dálkové identifikace s fyzickými doklady je možno, aby namísto fyzického provedení identifikace proběhla následujícími způsoby:

a) fyzická osoba k údajům k identifikaci (vizte kapitola 3.3.1) připojí kvalifikovaný elektronický podpis[341], a

b) „povinná osoba ověří u kvalifikovaného poskytovatele služeb vytvářejících důvěru, zda se údaje získané tímto poskytovatelem od této fyzické osoby při vydávání kvalifikovaného certifikátu použitého při vytváření podpisu“[342].

Ani u tohoto způsobu nesmí mít povinná osoba pochybnost o totožnosti fyzické osoby[343].

3.3.5. Kontrola klienta

Identifikací klienta však nekončí naplnění zásady, která se nazývá KYC, nebo-li know your customer. Kontrola klienta dle AMLZ „prohlubuje nástroje identifikace, jednak rozšiřuje požadované informace na ty, které nesměřují výhradně k posouzení klienta, ale k posouzení obchodu nebo obchodního vztahu,

[337] § 11, odst. 7, písm. e) AMLZ
[338] KATOLICKÁ, M. §11 [Převzetí identifikace] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.
[339] § 11, odst. 7, písm. f) AMLZ
[340] § 11, odst. 7, písm. g) Ibid.
[341] § 11, odst. 8, písm. a) AMLZ
[342] § 11, odst. 8, písm. b) Ibid.
[343] § 11, odst. 8, písm. c) AMLZ

který je navazován“[344] a měla by být prvkem, který určí, jestli je obchod obvyklý nebo podezřelý[345]. V případě, že nastane podezření při obchodu nebo obchodního vztahu, může povinná osoba vyžádat „předložení příslušných dokumentů nebo prohlášení (např. na účet klienta jsou připsány finanční prostředky, které neodpovídají jeho majetkovým poměrům, klient je vyzván k doložení jejich původu, načež tvrdí, že tyto prostředky pocházejí z prodeje nemovitosti, povinná osoba ho tedy požádá o předložení kupní smlouvy)“[346]. Klient dané informace a doklady musí poskytnout[347].

Kontrola klienta povinnou osobou neprobíhá vždy, ale pouze v následujících případech, a to:

„a) před uskutečněním obchodu mimo obchodní vztah při naplnění podmínek podle § 7 odst. 1

1. nejpozději v době, kdy je zřejmé, že dosáhne hodnoty 15 000 EUR nebo vyšší,

2. s politicky exponovanou osobou,

3. s osobou usazenou ve třetí zemi, kterou na základě přímo použitelného předpisu Evropské unie[39)] nebo z jiného důvodu je třeba považovat za vysoce rizikovou (dále jen "vysoce riziková třetí země"),

4. s osobou identifikovanou postupem podle § 11 odst. 7,

5. při obchodu v hodnotě alespoň 2 000 EUR, v případě povinné osoby podle § 2 odst. 1 písm. c), nebo

6. při převodu peněžních prostředků v hodnotě 1 000 EUR nebo vyšší,

b) v situacích, na které se vztahuje povinnost identifikace podle § 7 odst. 2 písm. a) a b), a to nejpozději před uskutečněním transakce,

c) v době trvání obchodního vztahu, nebo

d) uvedená v § 2 odst. 2 písm. c) a d) při obchodu v hodnotě 10 000 EUR nebo vyšší.“

Kontrola klienta, dle písmene a), se provede tehdy, když je zřejmé, že hodnota obchodu překročí 1000 Euro, při které je povinná osoba povinna provést

[344] VRÁBLIKOVÁ, Petra. Kontrola klienta a náhradní způsoby identifikace a kontroly klienta podle AML zákona – část druhá. Bulletin advokacie, 2021, č. 5, s. 9-15

[345] KATOLICKÁ, M. § 9 [Kontrola klienta] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[346] Ibid.

[347] § 9, odst. 7 AMLZ

i identifikaci klienta a kontrola klienta pouze zásadu KYC naplňuje. Podle některých názorů: „identifikace a kontrola jsou neoddělitelně spjaty do jednoho procesu, jde tedy o souhrn kontroly klienta, přičemž část této kontroly tvoří zajištění informací o jeho identitě“[348]. Z výše uvedených podmínek nás může zajímat v rámci digitálního onboardingu bod 4., který se zmiňuje o dálkové identifikaci s fyzickými doklady, o kterém jsem se zmiňoval již v kapitole 3.3.4.3.

Písmeno b) míří na podezřelý obchod a vznik obchodního vztahu, který jsem popisoval v kapitolách 3.2.2, respektive 3.2.3.

Samotná kontrola klienta spočívá v:

„a) získání a vyhodnocení informací o účelu a zamýšlené povaze obchodu nebo obchodního vztahu a informací o povaze podnikání klienta,

b) zjištění totožnosti skutečného majitele a přijetí opatření k ověření jeho totožnosti z důvěryhodných zdrojů s tím, že v případě, že klient podléhá povinnosti zápisu do evidence skutečných majitelů nebo obdobného registru, povinná osoba ověří skutečného majitele vždy alespoň z této evidence nebo obdobného registru a jednoho dalšího zdroje, a zjištění, zda skutečný majitel není politicky exponovanou osobou nebo osobou, vůči níž Česká republika uplatňuje mezinárodní sankce podle zákona o provádění mezinárodních sankcí,

c) v případě, že je klientem právnická osoba nebo svěřenský fond, zjištění vlastnické a řídící struktury klienta, a zjištění, zda osoba v této struktuře není osobou, vůči níž Česká republika uplatňuje mezinárodní sankce podle zákona o provádění mezinárodních sankcí,

d) průběžné sledování obchodního vztahu včetně přezkoumávání obchodů prováděných v průběhu daného vztahu za účelem zjištění, zda obchody jsou v souladu s tím, co je povinné osobě známo o klientovi a jeho podnikatelském a rizikovém profilu,

e) přezkoumávání zdrojů peněžních prostředků nebo jiného majetku, kterého se obchod nebo obchodní vztah týká, a

f) v rámci obchodního vztahu s politicky exponovanou osobou též přiměřená opatření ke zjištění původu jejího majetku.“[349]

[348] VRÁBLIKOVÁ, Petra. Kontrola klienta a náhradní způsoby identifikace a kontroly klienta podle AML zákona – část druhá. Bulletin advokacie, 2021, č. 5, s. 9-15

[349] § 9, odst. 2 AMLZ

Úkon uvedený v písm. a) by měl sloužit povinné osobě k tomu, aby dokázala vyhodnotit situaci, zda daný obchod klienta může spadat do kategorie podezřelého obchodu, který je popsán výše v kapitole 3.2.2[350].

U písm. b) se domnívám, že v tomto případě důvěryhodným zdrojem budou veřejné rejstříky, zejména obchodní rejstřík, rejstřík svěřenských fondů, evidence skutečných majitelů, který už je veřejný od 1. června 2021, přičemž se v této evidenci povinná osoba může zjistit i samotnou vlastnickou strukturu klienta dle písm. c), přičemž faktem je, že evidence skutečných majitelů ukazuje pouze na koncovou osobu a nezobrazuje celý řetězec. Zákon č. 37/2021 Sb., o evidenci skutečných majitelů, resp. v prvních návrzích obsahoval i tento požadavek, který však nakonec byl „smeten ze stolu". Zvláště v dnešní době, kdy hodně společností zakládá SPV, neboli special purpose vehicle (*česky volně přeloženo účelově zřízená společnost*[351]) si myslím, že v případech joint-ventures (*česky společný podnik*[352]) se mohou vyskytnout i případy, kdy by povinná osoba mohla narazit ve struktuře na PEP či sankcionované osoby, kterými se zabývá písm. f).

3.4. Technologie umožňující dálkovou identifikaci s fyzickými doklady

K dálkové identifikaci využívají povinné osoby zejména následující technologie, které s oblibou kombinují.

a) OCR softwarem (Optical Character Recognition),

b) automatickým rozpoznáním obličeje, a

c) videopřenos s operátorem.

Dané technologie bývají v balíčku, takový balíček nabízí například slovenská společnost Innovatrics pod balíčkem „Digital Onboarding Toolkit", kterou využívá například Vodafone, ČSOB, O2 a Home Credit[353]. Daný balíček

[350] KATOLICKÁ, M. § 9 [Kontrola klienta] In: BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[351] SPV. Patria.cz [online]. [cit. 2022-04-17]. Dostupné z: https://www.patria.cz/slovnik/591/spv.html

[352] Co je Joint-venture. Peníze.cz [online]. [cit. 2022-04-17]. Dostupné z: https://www.penize.cz/slovnik/joint-venture

[353] BUCHBAUER, Petr. Vítej na palubě homo digitalis aneb jak na digitální onboarding. Peak.cz [online]. 2019 [cit. 2022-03-12]. Dostupné z: https://www.peak.cz/vitej-palube-homo-digitalis-aneb-digitalni-onboarding/5919/

obsahuje OCR software s rozpoznáním průkazu totožnosti a automatické rozpoznání obličeje[354].

3.4.1. OCR software

Technologie OCR neboli anglicky optical character recognition „je technologie umožňující převod různých dokumentů, jako jsou naskenované knihy, PDF soubory nebo dokumenty vyfocené digitálním fotoaparátem, do podoby umožňující úpravy textu a dalšího obsahu“[355]. To znamená, že díky této technologii může daný software převést z obrázku textové části a pracovat dále s těmito údaji[356]. Díky této technologii klient pošle povinné osobě fotografii průkazu totožnosti, resp. její části a z toho vyčte potřebné údaje.

3.4.2. Automatické rozpoznání obličeje

K tomu, aby povinná osoba měla jistotu a splnila compliance s tím, že na dálku se vyskytuje doopravdy klient a průkaz totožnosti a podpůrné doklady nejsou zneužity, využívají software k automatickému rozpoznání obličeje a videopřenos s operátorem. Software pro automatické rozpoznání obličeje z několika fotek, které software náhodně vybere: „například úsměv, mrknutí levým okem, otevřená ústa apod.“[357]

3.4.3. Videopřenos s operátorem

Videopřenos s operátorem je dle mého názoru největší jistota, kdy živý člověk vyhodnotí situaci, zda klient se podobá poskytnutému průkazu totožnosti či nikoliv. Tento způsob je však nákladnější a poskytuje je například poskytovatel IDNow[358].

3.5. Nařízení eIDAS

Praktickým řešením pro digitální onboarding se jeví elektronická identifikace, která byla legislativním procesem zákonodárci z Evropské unie schválena v létě 2014, a to konkrétně nařízení eIDAS, která přinesla elektronickou identifikaci, autentizaci a služby vytvářející důvěru. V českém právním řádu se pro

[354] BUCHBAUER, Petr. Vítej na palubě homo digitalis aneb jak na digitální onboarding. Peak.cz [online]. 2019 [cit. 2022-03-12]. Dostupné z: https://www.peak.cz/vitej-palube-homo-digitalis-aneb-digitalni-onboarding/5919/

[355] MAREK, Tomáš. Jak na rozpáznávání textu zdarma (Free OCR). Cnews.cz [online]. 2012 [cit. 2022-04-17]. Dostupné z: https://www.cnews.cz/jak-na-rozpaznavani-textu-zdarma-free-ocr/

[356] Reading Data From Identity Documents. Innovatrics [online]. [cit. 2022-04-17]. Dostupné z: https://www.innovatrics.com/digital-onboarding-toolkit/reading-data-from-identity-documents/

[357] BUCHBAUER, Petr. Vítej na palubě homo digitalis aneb jak na digitální onboarding. Peak.cz [online]. 2019 [cit. 2022-03-12]. Dostupné z: https://www.peak.cz/vitej-palube-homo-digitalis-aneb-digitalni-onboarding/5919/

[358] Ibid.

adaptaci eIDAS schválil v roce 2017 ZoEI a o rok předtím ZoSVD. K tomu, abychom byli schopni pochopit, na čem je postavená Bankovní identita, je zapotřebí, abychom nejprve pochopili danou tématiku.

3.5.1. Elektronická identifikace a autentizace

Elektronickou identifikací rozumíme dle nařízení eIDAS jako „postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu“[359]. Osobními identifikačními údaji dle eIDAS je „soubor údajů umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující právnickou osobu“[360].

K tomu, abychom pochopili elektronickou identifikaci, musíme pochopit další dva pojmy, a to prostředek pro elektronickou identifikaci a autentizaci.

Prostředkem pro elektronickou identifikaci se rozumí „hmotná či nehmotná jednotka obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line služby“ [361] a autentizace je „elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě“[362].

Tyto pojmy jsou důležité, protože prostředek pro elektronickou identifikaci, jinak nazývaný jako PEI, lze popsat jako věc, díky které se identifikuje osoba v rámci elektronické identifikace. Komentář toto popisuje zdařile jako virtuální průkaz, který je obdobou pro občanský průkaz ve fyzickém světě[363]. PEI může být hmotná či nehmotná, přičemž hmotná je např. USB token, což „je fyzické nebo virtuální zařízení, které usnadňuje uživatelům zabezpečených služeb ověření pro přístup a užívání“[364] a nehmotná jsou například přihlašovací údaje nebo certifikát uložený v souboru.[365] Elektronická identifikace je „elektronický postup předložení

[359] Článek 3, bod 1) nařízení eIDAS
[360] Článek 3, bod 3) Ibid.
[361] Článek 3, bod 2) nařízení eIDAS
[362] Článek 3, bod 5) Ibid.
[363] PERHÁČOVÁ, M., VESELSKÝ, Š. § 1 In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.
[364] Bezpečnostní token. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-04-17]. Dostupné z: https://cs.wikipedia.org/wiki/Bezpe%C4%8Dnostn%C3%AD_token
[365] DOLEČEK, Marek. Využívejte elektronické podpisy a elektronickou identitu. Poradíme, jak na to. BusinessInfo.cz [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.businessinfo.cz/navody/elektronicke-podpisy-elektronicka-identita-ppbi/

tohoto virtuálního průkazu a elektronická autentizace je pak jeho elektronická kontrola“[366].

3.5.1.1. Národní identitní autorita

Pro podporu procesu elektronické identifikace a autentizace se v ZoEI vytvořil Národní identitní autoritu, jinak nazýván jako NIA, který je „informační systém veřejné správy“ [367], který spravovala Správa základních registrů do 31. března 2023. Na základě zákona č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony, spravuje NIA Digitální informační agentura, která byla zřízena 1. ledna 2023. Kromě podpory procesu elektronické identifikace a autentizace má NIA za úkol podle eIDAS v rámci interoperability zajistit napojení na zahraniční systémy elektronické identifikace a autentizace pro účely přeshraničního přístupu k službám veřejného sektoru on-line[368].

Podporou pro proces elektronické identifikace a autentizace můžeme chápat z toho pohledu, že NIA je zprostředkovatel pro poskytovatele služby a poskytovatele identity, který vydá uživateli PEI. Definici poskytovatele identity najdeme v ZoEI pod pojmem kvalifikovaný správce[369], jinak nazývaný v literatuře jako identity provider, a poskytovatele služby jako kvalifikovaný poskytovatel[370], také zvaný jako service provider.

3.5.1.2. Kvalifikovaný správce

Kvalifikovaným správcem může být státní orgán nebo „osoba, které byla udělena akreditace pro správu kvalifikovaného systému“[371]. Takovou osobou může být tedy i soukromoprávní subjekt s akreditací udělenou Ministerstvem vnitra (před 1. dubnem 2023) nebo Digitální informační agenturou.

V současné době má akreditaci udělených 11 soukromoprávních subjektů, a to následující:

a) První certifikační autorita, a. s.,

b) CZ.NIC, z. s. p. o.,

---

[366] PERHÁČOVÁ, M., VESELSKÝ, Š. § 1 In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[367] § 20, odst. 1 ZoEI

[368] PERHÁČOVÁ, M., VESELSKÝ, Š. § 1 In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[369] § 4 ZoEI

[370] § 18, odst. 1 Ibid.

[371] § 20 ZoEl

c) Československá obchodní banka, a. s.,

d) Česká spořitelna, a. s.,

e) Komerční banka, a. s.,

f) Air Bank, a. s.,

g) MONETA Money Bank, a. s.,

h) Raiffeisenbank, a.s.,

i) Fiobanka, a.s.,

j) UniCredit Bank Czech Republic and Slovakia, a.s., a

h) Banka CREDITAS a.s. [372]

Z výše uvedeného seznamu můžeme vypozorovat, že z 11 soukromoprávních subjektů, které získaly akreditaci, jsou z nich v drtivé většině banky. Prvním ze seznamu, který získal akreditaci se stala První certifikační autorita, a. s., se sídlem Podvinný mlýn 2178/6, PSČ 190 00 Praha 9. Tato společnost nabízí hmotnou PEI v podobě čipové karty STARCOS 3.5 ID ECC C1R / STARCOS 3.7, jako jedna z mála kvalifikovaných správců. Po účinnosti ZoBID mohly banky zažádat o akreditaci, a tak se také stalo. Průkopníkem se v tomto případě stala Česká spořitelna, a.s. která získala akreditaci 3. prosince 2020[373]. PEI těchto bank je vesměs jejich mobilní aplikace „Klíč“, o které jsem se zmiňoval v kapitole 2.1.4 a zároveň jejich uživatelské jméno a vstupní heslo do internetového bankovnictví. Záleží však také na úrovni záruky PEI, kterou si popíšeme níže.

Mimo soukromoprávní subjekty uvedené na začátku této podkapitoly, je k 31. červenci 2023 kvalifikovaným správcem také Digitální a informační agentura, která pro prostředek PEI využívá aplikaci Mobilní klíč eGovernmentu a NIA ID[374]. Dále je to Ministerstvo vnitra České republiky, které využívá také fyzické PEI, a to eObčanku[375], která je na všech občanských průkazech vydaných po 1. červenci 2018[376].

[372] Kvalifikovaní správci. Informační web elektronické identity [online]. [cit. 2023-07-29]. Dostupné z: https://info.identitaobcana.cz/KvalifikovaniSpravci.aspx

[373] Oznámení o udělení akreditace pro správu kvalifikovaného systému elektronické identifikace (poskytovatel: Česká spořitelna, a.s.). Ministerstvo vnitra České republiky [online]. [cit. 2022-04-18]. Dostupné z: https://www.mvcr.cz/clanek/oznameni-o-udeleni-akreditace-pro-spravu-kvalifikovaneho-systemu-elektronicke-identifikace-poskytovatel-ceska-sporitelna-a-s.aspx

[374] Kvalifikovaní správci. Informační web elektronické identity [online]. [cit. 2023-07-29]. Dostupné z: https://info.identitaobcana.cz/KvalifikovaniSpravci.aspx

[375] Ibid.

[376] EObčanka. Informační web elektronické identity [online]. [cit. 2022-04-18]. Dostupné z: https://info.identitaobcana.cz/eop/

Důležité je také zmínit to, že výše zmíněný kvalifikovaný správce tvoří kvalifikovaný systém. Kvalifikovaným systémem je dle § 3 ZoEI systém elektronické identifikace:

„a) který spravuje kvalifikovaný správce systému elektronické identifikace (dále jen "kvalifikovaný správce"),

b) který splňuje technické specifikace, normy a postupy alespoň pro jednu z úrovní záruky stanovených přímo použitelným předpisem Evropské unie upravujícím minimální technické specifikace, normy a postupy pro úrovně záruky prostředků pro elektronickou identifikaci[2]) (dále jen "příslušný předpis Evropské unie"),

c) který umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci (dále jen "národní bod"),

d) v jehož rámci jsou osobní identifikační údaje jedinečně identifikující osobu v okamžiku vydání prostředku pro elektronickou identifikaci spojeny s danou osobou v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými příslušným předpisem Evropské unie a

e) v jehož rámci je vydáván a používán pouze prostředek pro elektronickou identifikaci, který je spojen s osobou, kterou identifikuje, v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými příslušným předpisem Evropské unie.“[377]

Dále je kvalifikovaným systémem „systém elektronické identifikace oznámený podle přímo použitelného předpisu Evropské unie upravujícího elektronickou identifikaci[1]), v jehož rámci je vydáván a používán pouze prostředek pro elektronickou identifikaci s úrovní záruky alespoň značnou.“[378]

Příslušným předpisem Evropské unie, který je výše zmíněn, se v tomto případě rozumí nařízení eIDAS.

Kvalifikovaný systém dle ZoEI vychází z nařízení eIDAS, konkrétně z definice systém elektronické identifikace, který je definován jako „systém pro elektronickou identifikaci, na jehož základě jsou fyzickým či právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby vydávány prostředky pro elektronickou identifikaci“[379] Kvalifikovaný systém, potažmo systém elektronické identifikace je systém, na základě kterého jsou fyzickými, právnickými osobami

[377] § 3, odst. 1 ZoEI

[378] § 3, odst. 2 Ibid.

[379] Čl. 3, bod 4) nařízení eIDAS

vydávány PEI, který zahrnuje proces autentizace[380], jehož pojmy jsem podrobněji vysvětlil v předchozí kapitole.

3.5.1.2.1. Udělení akreditace Digitální a informační agenturou

O udělení akreditace pro správu kvalifikovaného systému elektronické akreditace rozhoduje dle ZoEI Digitální a informační agentura (do 31. března 2023 Ministerstvo vnitra). Toto řízení upravuje ZoEI a jde o řízení ve smyslu zákona č. 500/2004 Sb., správní řád.

Žadatel podá písemnou žádost[381], která musí splňovat náležitosti podle § 37, zákona č. 500/2004 Sb., správní řád, a pokud chce být žadatel úspěšný, musí splnit následující podmínky:

„a) skutečnost, že žadatelem o akreditaci vydávaný prostředek pro elektronickou identifikaci a žadatelem o akreditaci spravovaný systém elektronické identifikace splňují technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie,

b) bezúhonnost žadatele o akreditaci,

c) pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému,

d) zpracování plánu ukončení činnosti,

e) skutečnost, že systém elektronické identifikace žadatele o akreditaci umožňuje poskytnutí služby národního bodu, a

f) skutečnost, že žadatel o akreditaci je způsobilý pro správu kvalifikovaného systému z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.“

Těší mě, jakožto uživatele elektronické identity, že Digitální a informační agentura, potažmo zákonodárce myslí i na případ, kdy daný správce kvalifikovaného systému ukončí svou činnost, kvůli různým důvodům, například ztráta akreditace z důvodu nesplnění z podmínek udělení akreditace během své činnosti[382], ztráta podnikatelského oprávnění apod.

Žádost, kterou Digitální a informační agentura musí rozhodnout do 3 měsíců ode dne podání[383], musí obsahovat dále přílohy:

„a) smlouvu o uzavření pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému,

---

[380] Důvodová zpráva k zákonu č. 250/2017 Sb. o elektronické identifikaci, č. 250/2017 Dz

[381] § 5, odst. 1 ZoEI

[382] § 5, odst. 7 Ibid.

[383] § 5, odst. 6 ZoEl

b) doklad o bezúhonnosti, neprokazuje-li se bezúhonnost výpisem z evidence Rejstříku trestů,

c) potvrzení, že žadatelem o akreditaci vydávaný prostředek pro elektronickou identifikaci a žadatelem o akreditaci spravovaný systém elektronické identifikace splňují technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie, a

d) plán ukončení činnosti.“[384]

Tyto přílohy korespondují s výše uvedenými podmínkami udělení akreditace, avšak mě zaráží, že zákonodárce nestanovil minimální hodnotu pojištění odpovědnosti za škodu způsobenou při správě kvalifikovaného systému. Myslím si, že by bylo na místě stanovit její minimální výši přímo v tomto ustanovení ZoEI.

3.5.1.3. Kvalifikovaný poskytovatel

Nelze však opomenout druhou stranu, a to kvalifikovaného poskytovatele neboli service provider. Bez tohoto poskytovatele by nám nedával celý systém smysl, jelikož by například NIA neměla komu zprostředkovávat službu pro druhou stranu. Kvalifikovaným poskytovatelem rozumíme dle ZoEI toho „kdo umožňuje prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace“[385]. Dále se nevymezuje, kdo je považován za takového kvalifikovaného poskytovatele. Dle důvodové zprávy to může být „subjekt či jiné právní uspořádání, tedy jak osoba fyzická nebo právnická, tak například organizační složka státu“[386]. Žádný z těchto uvedených subjektů není povinen umožnit prokázání při přihlašování a využívání jejich služeb využitím elektronické identifikace, neboť se tyto osoby mohou svobodně rozhodnout, zda poskytnou takovou možnost přihlášení uživateli.[387] V případě, že umožní takový způsob přihlášení uživateli, kvalifikovaný poskytovatel přesměruje přihlášení na NIA, přes kterou uživatel vybere PEI, se kterým disponuje. Následně NIA přesměruje na kvalifikovaného správce, který vydal PEI uživateli. Kvalifikovaný správce identifikuje a autentizuje danou osobu. V případě úspěšné identifikace a autentizace se vrátí zpět k NIA, který provede další ověření totožnosti z registru obyvatel a další údaje z informačních systémů veřejné správy. Po odsouhlasení

[384] § 5, odst. 3 ZoEl
[385] § 18, odst. 1 Ibid.
[386] Důvodová zpráva k zákonu č. 250/2017 Sb. o elektronické identifikaci, č. 250/2017 Dz
[387] Ibid.

uživatelem předá NIA tyto údaje kvalifikovanému poskytovateli, který následně uživatele přihlásí[388].

Seznam těchto poskytovatelů lze nalézt na stránkách Identita občana[389].

3.5.1.4. Úroveň záruky systémů elektronické identifikace

Výše v kapitole o kvalifikovaných správcích bylo zmíněno o systému elektronické identifikace. Tento systém se dle nařízení eIDAS dělí do úrovně záruk systémů elektronické identifikace, a to:

a) nízká,

b) značná, a

c) vysoká.

Nízkou úrovní záruky se „označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí omezenou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je snížit riziko zneužití nebo změny totožnosti“[390]

Nízkou úrovní záruky je identifikace pouze jedno-faktorovou autentizací. Typickým příkladem je přihlášení prostřednictvím uživatelského jména a hesla[391].

Značnou úrovní se „označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který nabízí značnou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je značně snížit riziko zneužití nebo změny totožnosti“ [392].

Značnou úrovní je identifikace na základě dvou-faktorové autentizace, kdy se využívá uživatelské jméno, heslo a ověření totožnosti například SMS kódem na zaregistrovaný mobil nebo mobilní aplikací „Klíč“.

Vysokou úrovní záruky se „vysoká úroveň záruky označuje v souvislosti se systémem elektronické identifikace prostředek pro elektronickou identifikaci, který

[388] Důvodová zpráva k zákonu č. 250/2017 Sb. o elektronické identifikaci, č. 250/2017 Dz

[389] Úvod. Portál národního bodu [online]. [cit. 2022-04-18]. Dostupné z: https://www.identitaobcana.cz/Home

[390] Čl. 8, bod. 2, písm. a) nařízení eIDAS

[391] DOLEČEK, Marek. Využívejte elektronické podpisy a elektronickou identitu. Poradíme, jak na to. BusinessInfo.cz [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.businessinfo.cz/navody/elektronicke-podpisy-elektronicka-identita-ppbi/

[392] Čl. 8, bod. 2, písm. b) nařízení eIDAS

nabízí vyšší míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby než prostředek pro elektronickou identifikaci se značnou úrovní záruky a je charakterizován pomocí souvisejících technických specifikací, norem a postupů, včetně technických kontrol, jejichž účelem je předejít zneužití nebo změně totožnosti“[393].

A poslední, vysoká úroveň, je identifikace prostřednictvím PEI, například fyzickou čipovou kartou.

K 31. červenci 2023 soukromoprávní kvalifikovaní správci, kteří získali akreditaci od Ministerstva vnitra České republiky nebo Digitální a informační agentury dosahují se svými PEI úroveň záruky zejména na značné, kdy především banky využívají uživatelské jméno, heslo a SMS klíč nebo mobilní aplikaci „Klíč“, které využívají stejně uživatelé při přístupu do internetového bankovnictví.

Pokud jde o veřejnoprávní kvalifikované správce, Ministerstvo vnitra České republiky disponuje také s PEI, konkrétně s tzv. eObčankou, kterou jsem již popisoval výše. EObčanka má vysokou úroveň záruky, přičemž Digitální informační agentura s PEI NIA ID dosahuje úrovně značná, jako většina soukromoprávních kvalifikovaných správců[394].

3.5.2. Služba vytvářející důvěru

Druhou zásadní službou, kterou přináší nařízení eIDAS, a je neprávem někdy opomíjena odbornou veřejností, je služba vytvářející důvěru.

Služba vytvářející důvěru definuje nařízení eIDAS jako „elektronická služba, která je zpravidla poskytována za úplatu a spočívá:

a) ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo

b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo

c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami“[395].

Tato část nařízení eIDAS se adaptovala do českého právního řádu prostřednictvím ZoSVD, který později doplnil do tandemu ZoEI.

---

[393] Čl. 8, bod. 2, písm. c) nařízení eIDAS

[394] Nejčastější dotazy. Informační web elektronické identity [online]. [cit. 2022-04-18]. Dostupné z: https://info.identitaobcana.cz/faq/

[395] Článek 3, bod. 16 nařízení eIDAS

Jak definuje samotné nařízení eIDAS, službu vytvářející důvěru zastřešují elektronické podpisy, elektronické pečeti a elektronické certifikáty. Myslím si, že tato část nařízení eIDAS je stěžejní pro uzavírání smluv na dálku a již v praxi pozoruji, že služba vytvářející důvěru funguje. Například aplikace DocuSign, prostřednictvím které smluvní strany podepíšou elektronicky přes aplikaci v mobilu nebo na počítači a podpis se pokládá za právně závazný[396], kdy podpis dosahuje úrovně uznávaného elektronického podpisu nebo i kvalifikovaného elektronického podpisu[397]. Zejména při pandemii COVID-19 se hledala různá řešení, která by nahrazovala osobní setkávání a uzavírání smluv, avšak je až s podivem, že možnosti, které nám dávala legislativa, nebyla předtím tolik využívána a až během tohoto období se hlasitě mluvilo o alternativách, které by ušetřily mnoho času pro všechny zainteresované strany. Avšak si nedokážu představit, že by si někdo koupil na dálku například společnost nebo nemovitost bez osobní účasti protistrany (prodejce) a jednal s nimi pouze on-line přes MS Teams. Bylo by však přínosné pro všechny strany, kdyby bylo možné podepsat všechny dokumenty elektronicky.

3.5.2.1. Elektronický podpis

Elektronický podpis ve významu nařízení eIDAS znamená „data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání“[398]. Elektronickému podpisu „nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy“[399]. Tady nařízení eIDAS naprosto jasně vymezuje to, že elektronické podpisy jsou právně závazné, tedy alespoň ty, které jsou uvedené v nařízení eIDAS.

Nařízení eIDAS rozlišuje elektronický podpis na dvě kategorie:

a) zaručený elektronický podpis, a

b) kvalifikovaný elektronický podpis.

[396] The eIDAS Regulation: A primer. DocuSign [online]. [cit. 2022-04-18]. Dostupné z: https://www.docusign.co.uk/learn/eidas-regulation-primer

[397] DocuSign - návod k použití. TechSoup Česká republika [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.techsoup.cz/docusign-navod

[398] Článek 3, bod 10 nařízení eIDAS

[399] Článek 25, bod 1 Ibid.

Zaručený elektronický podpis je podpis, který se dá jednoznačně spojit, identifikovat podepisující osobu, [400] „je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou“ [401] a „je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat“ [402]. Zaručený elektronický podpis garantuje to, „že podpis nemůže být zkopírován a vložen do jiného dokumentu“ [403] . Liší se od kvalifikovaného elektronického podpisu tím, že certifikát není kvalifikovaný a není ověřena tím pádem totožnost osoby, která podepisuje[404].

Kvalifikovaným elektronickým podpisem dle nařízení eIDAS je „zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy“ [405] Kvalifikovaný elektronický podpis má právní účinek v Evropské unii na úrovni vlastnoručního podpisu[406].

Tyto kvalifikované elektronické podpisy musí splňovat technické požadavky, které určuje nařízení eIDAS, a to například „označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis“ [407] ZoSVD upřesňuje, že touto kategorií elektronického podpisu lze podepsat dokument, kterým „činí úkon nebo právně jedná stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem nebo jejich orgán anebo jiná jejich součást (dále jen „veřejnoprávní podepisující“)“ [408] nebo při výkonu jeho působnosti[409].

Kvalifikovaný elektronický podpis je vytvářen kvalifikovaným poskytovatelem služeb vytvářejících důvěru („poskytovatel služeb vytvářejících

[400] Článek 26 nařízení eIDAS
[401] Článek 26 Ibid.
[402] Článek 26 nařízení eIDAS
[403] DOLEČEK, Marek. Využívejte elektronické podpisy a elektronickou identitu. Poradíme, jak na to. BusinessInfo.cz [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.businessinfo.cz/navody/elektronicke-podpisy-elektronicka-identita-ppbi/
[404] Ibid.
[405] Článek 3, bod 12 nařízení eIDAS
[406] Článek 25, bod 2 Ibid.
[407] Příloha I, nařízení eIDAS
[408] § 5, písm. a) ZoSVD
[409] § 5, písm. b) Ibid.

důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele“ [410]) prostřednictvím prostředku pro vytváření elektronických podpisů, tedy programem nebo technickým zařízením k vytvoření elektronického podpisu. Následně poskytne fyzické osobě kvalifikovanou část certifikátu pro elektronický podpis „který použije podepisující, což je zpravidla čipová karta nebo USB token[411]. Kvalifikovaný poskytovatel služeb vytvářejících důvěru umožní ověření tohoto elektronického podpisu. K dnešnímu dni (31. července 2023) je u Digitální a informační agentury uvedeno 6 soukromoprávních společností, které jsou kvalifikovanými poskytovateli služeb vytvářejících důvěru a poskytovatelů kvalifikovaných služeb vytvářející důvěru[412].

Česká právní úprava ZoSVD však povoluje další druh elektronického podpisu, a to uznávaný elektronický podpis, který však nemá právní relevanci v Evropské unii[413].

Obrázek 5 – *Druhy elektronického podpisu*

Typ elektronického podpisu	Brán jako vlastnoruční podpis?	Lze využít při komunikaci s orgány veřejné moci?	Je uznáván v rámci EU?	Speciální požadavky na jeho formu?	Je brán jako uznávaný podpis ve smyslu § 6 odst. 2 ZoSVD ?	Je na úrovni úředně ověřeného podpisu?
Prostý	ano	ne	ne	ne	ne	ne
Zaručený	ano	ne	ne	jakýkoliv certifikát	ne	ne
Zaručený, založený na kvalifikovaném certifikátu	ano	ano	ne	kvalifikovaný certifikát	ano	ne
Kvalifikovaný	ano	ano	ano	kvalifikovaný certifikát + kvalifikovaný prostředek	ano	ne

[410] Článek 3, bod 20 nařízení eIDAS

[411] Kvalifikované elektronické podpisy dle nařízení eIDAS – nový požadavek na obsluhu Czech POINTu. Czech POINT [online]. 2018 [cit. 2022-04-18]. Dostupné z: https://www.czechpoint.cz/public/kvalifikovane-elektronicke-podpisy-dle-narizeni-eidas-novy-pozadavek-na-obsluhu-czech-pointu/

[412] Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. Digitální a informační agentura [online]. [cit. 2023-07-29]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/povinne-zverejnovane-informace/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru/

[413] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra - I. část. Právní prostor [online]. 2020 [cit. 2022-04-18]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/podepisovani-soukromych-listin-vcera-dnes-zitra-i-cast

Upraveno ze zdroje: DOLEČEK, Marek. Využívejte elektronické podpisy a elektronickou identitu. Poradíme, jak na to. BusinessInfo.cz [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.businessinfo.cz/navody/elektronicke-podpisy-elektronicka-identita-ppbi/

3.5.2.2. Elektronická pečeť

Elektronická pečeť jsou „data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu“[414].

Jinak řečeno, elektronická pečeť zaručuje to, od koho daná listina pochází a zda nebyla změněna „na cestě“ k adresátovi. Dle ZoSVD při každém úkonu nebo právním jednání musí veřejnoprávní podepisující zapečetit dokument v elektronické podobě elektronickou pečetí, v kategorii kvalifikovaná.

Elektronická pečeť se dělí také do dvou kategorií dle nařízení eIDAS, a to:
a) zaručená elektronická pečeť, a
b) kvalifikovaná elektronická pečeť.

Úprava elektronické pečeti je analogická k úpravě elektronického podpisu. Jedním z příkladů je, že elektronickým pečetím nesmí být také „upírány právní účinky a nesmí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické pečetě“[415].

Zaručená elektronická pečeť musí být jednoznačně spojena s pečetící osobou a umožní i její identifikaci[416]. Dalšími požadavky je to, že „je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou“ [417] a „je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat“ [418].

Kvalifikovaná elektronická pečeť je „zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť“[419]. V tomto případě to také znamená analogicky s kvalifikovaným elektronickým

[414] Článek 3, bod 25 nařízení eIDAS
[415] Článek 35, bod 1 Ibid.
[416] Článek 36 nařízení eIDAS
[417] Článek 36 Ibid.
[418] Článek 36 nařízení eIDAS
[419] Článek 3, bod 27 Ibid.

podpisem to, že pečeť musí být vydána dle technických požadavků, které požaduje příloha nařízení eIDAS, a poskytuje ho kvalifikovaný poskytovatel služeb vytvářejících důvěru prostřednictvím programu nebo technického zařízení k vytvoření elektronických pečetí.

3.5.2.3. Evidence certifikátů

Výše v kapitolách 3.5.2.1 a 3.5.2.2 jsem psal o certifikátech, které obsahuje například kvalifikovaný elektronický podpis nebo kvalifikovaná elektronická pečeť. Dle ZoSVD tyto certifikáty eviduje Digitální a informační agentura[420].

3.5.3. Budoucnost nařízení eIDAS

Nařízení eIDAS je tu s námi už od poloviny roku 2014 a je zapotřebí, aby Evropská unie držela krok s dobou a dále rozvíjela tak slibný koncept. Je však zapotřebí vyřešit mnoho problémů s regulací eIDAS.

Na půdě Evropské komise se již připravuje delší dobu návrh revize eIDAS, jak někteří z odborné veřejnosti nazývají jako eIDAS 2.0[421]. Výše uvedený návrh z pera Evropské komise předložila do legislativního procesu v červnu roku 2021[422]. Změny, které má přinést návrh Evropské komise, mají být v souladu s vizí a směrováním digitální transformace Evropy do roku 2030 pod názvem „Evropská digitální dekáda“, která byla předložena 3 měsíce před předložení návrhu eIDAS 2.0, v březnu 2021. Tato vize digitální transformace má stavět na čtyřech bodech, a to:

1) dovednostech, kdy 80 % populace v Evropě by si měla osvojit základní digitální dovednosti;
2) zabezpečená a udržitelná digitální infrastruktura, přičemž například internet má zrychlit na rychlost gigabytu a 5G by mělo být primární technologií na území EU;
3) digitální transformace podniků, při které 75 % společností bude využívat AI (umělá inteligence) a bude používat cloud;
4) digitalizace veřejných služeb, kdy klíčové veřejné služby budou dostupné online a lékařská dokumentace bude přístupná pro všechny občany přes internet. Evropská komise chce, aby 80 % občanů používalo digitální

[420] § 15, odst. 1 ZoSVD

[421] KOVÁŘ, Dalibor a Pavel AMLER. Už jste slyšeli o nařízení eIDAS 2.0?. Epravo.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.epravo.cz/top/clanky/uz-jste-slyseli-o-narizeni-eidas-20-113866.html

[422] Revision of the eIDAS Regulation: Findings on its implementation and application. Evropský parlament [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.europarl.europa.eu/thinktank/cs/document/EPRS_BRI(2022)699491

identifikaci[423], což si myslím, že je velice ambiciózní plán, vzhledem k digitální gramotnosti obyvatelstva v Evropské unii.

Výše uvedená vize je velice potřebná pro budoucnost Evropy, pokud chce být technologickým premiantem a bude chtít být v budoucnosti světovým ekonomickým motorem. Dle mého názoru digitalizace nejen veřejné správy, ale tak i společností bude obrovským zefektivněním práce a využitelnosti času.

Zpět k návrhu eIDAS 2.0. Obecným cílem má být „správné fungování ve vnitřním trhu, v souvislosti s poskytováním a užíváním přeshraničních a meziodvětvových veřejných a soukromých služeb, které jsou závislé na dostupnosti a používání vysoce zabezpečených a důvěryhodných řešení elektronické identity“[424]. V tomto smyslu určitě souhlasím a jsem velmi rád, že eIDAS 2.0 bude chtít více regulovat přeshraniční použití elektronické identity, jelikož v dnešní době je využití zahraničních elektronických identit v rámci e-governmentu omezené, což mi přijde jako obrovská škoda nevyužití potenciálu elektronických identit. Proto jsem velmi rád, že specifickým cílem eIDAS 2.0 je i zajistit „rovné podmínky pro poskytování kvalifikovaných důvěryhodných služeb v EU a jejich přijímání“ [425] v rámci Evropské unie.

Dalším cílem tohoto návrhu je zakomponovat i evropskou peněženkou digitální identity, která „by měla mít podobu aplikace na mobilní telefony a jiná zařízení. Založena by měla být na národní elektronické identitě a vydávat ji budou jednotlivé členské státy, popř. z jejich pověření či na základě jejich uznání soukromoprávní subjekt“[426]. Tím pádem tato evropská peněženka digitální identity bude mít identifikační funkci pro obyvatele Evropské unie, kam se mohou zakomponovat i další věci, jako jsou řidičský průkaz nebo rodný list[427].

Myslím si, že s ohledem na výše uvedené se máme na co těšit a rozhodně celou oblast posune tato regulace opět dále, pokud bude účinná v této podobě.

---

[423] Evropská digitální dekáda: digitální cíle pro rok 2030. Evropská komise [online]. [cit. 2022-04-18]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_cs

[424] Revision of the eIDAS Regulation Findings on its implementation and application - BRIEFING. European Parliament [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf

[425] Ibid.

[426] KOVÁŘ, Dalibor a Pavel AMLER. Už jste slyšeli o nařízení eIDAS 2.0?. Epravo.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.epravo.cz/top/clanky/uz-jste-slyseli-o-narizeni-eidas-20-113866.html

[427] Ibid.

3.6. Bankovní identita

Bankovní identita, jedno z rezonovaných témat posledního roku, tedy alespoň na LinkedIn a v mediálním prostoru v oblasti bankovnictví. Banky, respektive jejich joint-venture společnost Bankovní identita, a. s., ve které jsou zainteresované velké banky, hlásí, že Bankovní identita je obrovskou změnou pro „rychlé a bezpečné digitální prokazování totožnosti“[428].

Základem pro myšlenku Bankovní identity v České republice byl projekt digitálního BankID, který se zrodil na počátku milénia ve Skandinávii, konkrétně ve Švédsku v roce 2003, kdy konsorcium velkých bank ve Švédsku vytvořilo danou službu. Díky digitálnímu BankID mohli Švédové už v té době využívat elektronickou komunikaci s veřejnou správou, kromě plateb [429]. Například s „finančním úřadem, veřejným systémem zdravotnictví a městským školním systémem“[430]. Podle statistik z roku 2021[431], které zveřejňuje společnost BankID na svých webových stránkách, ke službě mělo přístup 8 milionů uživatelů a staticky bylo využito 190 krát za jednu sekundu, což je ohromné číslo, o kterém se zatím české službě může zdát, avšak BankID má náskok přes 18 let a společnosti ve Švédsku, potažmo ve Skandinávii jsou už uzpůsobené na takový způsob ověření identity. Zajímavostí je, že dostupnost služby bylo v 99,99 %, což mnoho služeb, jež jsou v cloudu, se může o takové hodnotě pouze nechat zdát.

V současné době švédské BankID provozuje joint-venture společnost Finansiell ID-Teknik BID, kterou vlastní skandinávské banky, a to: Danske Bank, Handelsbanken, Ikano Bank, Länsförsäkringar Bank, SEB, Skandiabanken a Swedbank[432]. Podle statistik, BankID použilo ve Švédsku věkové skupině od 20 do 40 let alespoň jednou a v současné době přes danou službu můžou uživatelé přes

[428] Bankovní identitu za první rok využilo 700 tisíc lidí. Česká bankovní asociace [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://cbaonline.cz/bankovni-identitu-za-prvni-rok-vyuzilo-700-tisic-lidi

[429] HUSZ, Orsi. Bank Identity: Banks, ID Cards, and the Emergence of a Financial Identification Society in Sweden. Cambridge Core [online]. 2018 [cit. 2022-04-18]. Dostupné z: https://www.cambridge.org/core/journals/enterprise-and-society/article/bank-identity-banks-id-cards-and-the-emergence-of-a-financial-identification-society-in-sweden/0D5AF7AE7F3D989ECF542DB5A461C278

[430] Ibid.

[431] BankID in numbers. BankID [online]. [cit. 2022-04-18]. Dostupné z: https://www.bankid.com/en/om-oss/statistik

[432] BankID. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-04-18]. Dostupné z: https://en.wikipedia.org/wiki/BankID

BankID přihlašovat do finančních společností, platebních řešení nebo do rozhraní veřejné správy[433].

Hlasitě hovořit o Bankovní identitě, v té době pod označením Projekt SONIA, se začalo na začátku roku 2019, kdy Česká bankovní asociace začala na konferencích přednášet o tomto projektu a šířit povědomí o něm. Avšak samotný nápad Projektu SONIA vzešel už v roce 2017[434].

Myšlenka byla velice prostá. Bankovní služby využívá většina obyvatel České republiky a z minulé kapitoly už víme, že mnoho z nich využívá i internetové bankovnictví. Banky chtěly vytvořit tzv. soukromoprávní národní identitní autoritu, která by byla alternativou k NIA, kdy by banky mohly prostřednictvím změny legislativy, zejména v ZoB, poskytovat elektronickou identifikaci, autentizaci a zároveň služeb vytvářejících důvěru. Na přípravě zákona se podílela Česká bankovní asociace, ICT unie a advokátní kanceláře Havel & Partners spolu s Rowan Legal.

Zjednodušeně, myšlenkou celé Bankovní identity je zjednodušit komunikaci s úřady a přihlašovat se do různých služeb prostřednictvím internetového bankovnictví. Myslím si, že před tímto projektem například Portál občana nebo další služby, které poskytoval stát, využívalo malé procento obyvatelstva. Zařizování dalšího přihlašovacího účtu nemuselo být pro velké procento občanů pohodlné a byl jsem mezi nimi, který se na danou problematiku díval podobným pohledem. Jak jsem již zmiňoval výše, díky tomuto projektu se elektronická identifikace může dostat k více lidem, a tím splnit i cíle ZoD, který má zdigitalizovat veřejnou správu a úkony, které veřejná správa provádí dnes pouze fyzicky, tak v budoucnu provede i elektronicky. Myslím si, že po pandemii COVID-19 jsme si uvědomili, kde máme v legislativě mezery a i v praktickém životě už jsme poznali pohodlí, kdy nemusíme stát frontu na úřadech k tomu, abychom vyřídili některé maličkosti. Proto vkládám do ZoD, potažmo ZoBID obrovské naděje směrem k digitalizaci a správného směrování do budoucna, čímž bychom měli v této oblasti dohnat i skandinávské země a premianty v pobaltských zemích. V kapitole 3.6.3 se zmíním o některých příkladech, kde se může Bankovní identita používat.

[433] Our history. BankID [online]. [cit. 2022-04-18]. Dostupné z: https://www.bankid.com/en/om-oss/historia

[434] Bankovní identita umožnila nový rozměr elektronického ověřování totožnosti. Advokátní deník [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://advokatnidenik.cz/2021/02/09/zakon-o-bankovni-identite-umoznil-novy-rozmer-elektronickeho-overovani-totoznost

V zásadě mě zaráží to, že Česká republika v tomto směru s digitalizací zaspala dobu a znovu naskakuje do rozjetého vlaku. Je to z důvodu, že Česká republika byla v roce 2009 premiantem v Evropě, i díky projektu Datová schránka, která však nebyla kladně přijata mezi fyzickými osobami, byť dokáže velmi zjednodušit každodenní život.

3.6.1. Bankovní identita, a.s.

Společnost Bankovní identita, a.s., se sídlem Smrčkova 2485/4, Libeň, 180 00 Praha 8 jako joint-venture byla založena v roce 2020, a to konkrétně těmito bankami: Česká spořitelna, a.s., Československá obchodní banka, a.s. a Komerční banka, a.s.

Tato společnost funguje tak, že je prostředníkem „za účelem jednání se soukromými poskytovateli elektronických služeb banky“[435] a funguje tak jako alternativa k NIA v přístupu k údajům uživatelů pro kvalifikované poskytovatele, které může být například třeba pojišťovna. Vůči veřejné správě však každá banka vystupuje jako samostatný kvalifikovaný správce, jelikož zákon jim nedává ani možnost vystupovat ve sdružení, jako ve vztahu se soukromými subjekty.

Zajímavostí je, že k této společnosti se připojily až v průběhu Air Bank, a Moneta Money Bank, kdy Air Bank, Fio banka a Moneta Money Bank založily v listopadu 2020 alianci pro bankovní identitu[436], která měla konkurovat řešení od Bankovní identity, a.s., avšak na začátku roku 2021 se dohodly na jednotném řešení[437]. V případě, že by tyto dvě asociace měly odlišná řešení bankovní identity, mohl by nastat problém pro soukromé subjekty s využíváním takové služby, jelikož by musely platit dva poplatky za přístup, údržbu a třeba registrační poplatek, který je za současného stavu 30 000,- Kč za aktivaci přístupu k Bankovní identitě[438].

3.6.2. Právní úprava

Bankovní identitu upravuje zákon 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

[435] HANZLÍK, Filip. Komentář ČBA k bankovní identitě a vzniku nové aliance. Česká bankovní asociace [online]. [cit. 2022-04-18]. Dostupné z: https://cbaonline.cz/komentar-cba-k-bankovni-identite-a-vzniku-nove-aliance

[436] HEJKRLÍK, Pavel. Air Bank, Fio banka a Moneta zakládají alianci pro bankovní identitu. Marketing & Media [online]. 2020 [cit. 2022-04-18]. Dostupné z: https://mam.cz/zpravy/2020-11/air-bank-fio-banka-a-moneta-zakladaji-alianci-pro-bankovni-identitu/

[437] HOVORKA, Jiří a Petr KUČERA. Bankovní identitu nabídneme společně, dohodly se banky [online]. [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/osobni-ucty/424583-bankovni-identitu-nabidneme-spolecne-dohodly-se-banky

[438] Ceník. BankID.cz [online]. [cit. 2022-04-18]. Dostupné z: https://www.bankid.cz/cenik

terorismu, ve znění pozdějších předpisů, a některé další zákony. Už jenom z názvu je zřejmé, že nejde o lex specialis a mění části relevantních zákonů, a to ZoB, AMLZ. Zajímavostí je, že přizpůsobuje pro účely Bankovní identity i zákony č. 277/2009 Sb., o pojišťovnictví a zákon 168/1999 Sb., zákon o pojištění odpovědnosti z provozu vozidla. Níže se budu věnovat změnám v ZoB. Úpravu AMLZ jsem už obsáhl výše v kapitolách 3.2 a 3.3, což pokládám za dostatečné, jelikož jsem zahrnul i ustanovení § 8a AMLZ, který přinesl tento novelizační zákon.

3.6.2.1. Některé změny v ZoB

ZoB omezuje banky v podnikání tím způsobem, že banky nesmí vykonávat, kromě uvedených činností v § 1, odst. 1, 3 a 4 ZoB. Banky mohou tedy přijímat vklady od veřejnosti a poskytovat úvěry. Aby mohly tyto služby poskytovat, musí získat bankovní licenci, kterou uděluje Česká národní banka. V rámci rozsahu této licence může poskytovat další služby, a to např. směnárenskou činnost, pronájem bezpečnostních schránek nebo poskytování záruk.

Mimo tyto činnosti může banka pouze vykonávat podnikatelské činnosti, které „souvisejí se zajištěním jejího provozu a provozu jí ovládaných jiných bank, spořitelních a úvěrních družstev, obchodníků s cennými papíry, pojišťoven, zajišťoven, finančních institucí a podniků pomocných služeb“[439]. ZoBID umožnil bankám novou podnikatelskou činnost, a to „podnikatelskou činnost spočívající v poskytování elektronické identifikace, autentizace a služeb vytvářejících důvěru, jak jsou definovány přímo použitelným předpisem Evropské unie upravujícím elektronickou identifikaci a služby vytvářející důvěru pro elektronické transakce na vnitřním trhu[35], jakož i souvisejících služeb, zejména poskytování nebo potvrzování osobních identifikačních údajů klienta, informací o klientovi souvisejících s jeho osobními identifikačními údaji, informací o bankovních obchodech klienta a vytváření a uchování elektronických dokumentů (dále jen „identifikační služby“), je-li držitelem příslušného oprávnění, pokud je právními předpisy vyžadováno; na informace získané a zpracovávané při poskytování identifikačních služeb se vztahují ustanovení o bankovním tajemství (§ 38)“[440].

Tato změna je důležitá v tom, že poskytuje bankám možnost poskytovat elektronickou identifikaci, autentizaci a služby vytvářejících důvěru, kterou jsem popisoval v kapitole 3.5, na které závisí provoz celé Bankovní identity. Bankovní identita není nic jiného, než zkompilovaný balíček těchto tří služeb, pod legislativní

[439] § 1, odst. 4 ZoB

[440] § 1, odst. 4, písm. c) Ibid.

zkratkou identifikační služby, kterou poskytují banky a disponují velkým množstvím potencionálních uživatelů, kteří by mohli využít tyto identifikační služby od banky. Myslím si, že nikdy tu nebyla vyšší šance, aby běžný občan využil identifikační služby, kvůli složitým procesům, jak s projektem eObčanka, tak s jinými, které jsem popisoval v minulé kapitole 3.5.

Nezapomínejme však na s tím související zákony, kdy jak u ZoSVD i ZoEI musí požádat banka o akreditaci u Digitální a informační agentury a v tomto případě nestačí pouze to, že ZoB umožňuje bankám podnikat v této oblasti a musí splnit všechny předpoklady, které udává ZoSVD a ZoEI.

Ani pobočka zahraniční banky nepřijde zkrátka ohledně identifikačních služeb, jelikož ZoB umožňuje i těmto pobočkám vykonávat tyto činnosti za stejných podmínek [441] . Avšak za podmínky, že nebude v rozporu s jejím oprávněním, myšleno ekvivalent k bankovní licenci. Zahraniční bankou je dle ZoB: „a) se sídlem v členském státě Evropské unie nebo ve státě, který je smluvní stranou Dohody o Evropském hospodářském prostoru (dále jen „členský stát“), která požívá výhody jednotné licence podle práva Evropské unie (§ 5a), vykonává tyto činnosti prostřednictvím pobočky této zahraniční banky (dále jen „pobočka banky z členského státu“),

b) se sídlem v jiném než členském státě vykonává tyto činnosti prostřednictvím pobočky této zahraniční banky (dále jen „pobočka banky z jiného než členského státu“), pokud jí byla udělena Českou národní bankou licence (§ 5) a pouze v rozsahu udělené licence“[442].

V případě pobočky banky z členského státu jsou to například COMMERZBANK Aktiengesellschaft, pobočka Praha, která sídlí na adrese Jugoslávská 934/1, Praha nebo HSBC Continental Europe, Czech Republic , která sídlí na adrese Na Florenci 2116/15, Praha v kancelářském komplexu Florentinum. V neposlední řadě je to mBank S.A., organizační složka, sídlící v Pernerova 691/42, 186 00 Praha 8. Tato banka je známá zejména mezi retailovými klienty, zatímco Commerzbank a HSBC se v České republice zaměřují na korporátní klientelu. Můžeme se s nimi setkat zejména při financování, jak už při poskytování úvěru jednou bankou či v rámci syndikovaného nebo klubového úvěrování.

Pobočkou banky z jiného než členského státu je například čínská banka Bank of Communications Co., Ltd., Prague Branch odštěpný závod, která sídlí na

[441] § 1, odst. 7 ZoB

[442] § 1, odst. 6 Ibid.

adrese Rohanské nábřeží 693/10, Praha. Tato banka přišla na český trh v roce 2018[443].

V návaznosti na výše uvedené změny, ZoBID přidává 6 paragrafů do ZoB (z nichž jsou 4 paragrafy dle mého názoru relevantní do této práce), konkrétně do Společného ustanovení. První z doplňovaných ustanovení je § 38aa, který se zabývá identifikačními službami a jeho poskytovatelem. Ustanovení zní následovně:

„(1) Banka nebo pobočka zahraniční banky je oprávněna nabízet, poskytovat nebo zprostředkovávat identifikační služby a uzavírat smlouvy o nich též jménem a na účet poskytovatele identifikačních služeb.

(2) Poskytovatelem identifikačních služeb se v tomto zákoně rozumí osoba, která není bankou, je na základě jiného právního předpisu oprávněna poskytovat identifikační služby a ve které mají podíl pouze banky nebo pobočky zahraničních bank; tyto banky nebo pobočky zahraničních bank jsou povinny zajistit, že poskytovatel identifikačních služeb bude zachovávat získané údaje v tajnosti a chránit je před zneužitím."

Z výše uvedeného, zejména odstavec 1 osobně považuji za zbytečný, vzhledem k upravenému § 1, odstavce 4 ZoB, kdy tento odstavec 1 duplikuje možnost banky, potažmo pobočky zahraniční banky, oprávnění k této podnikatelské činnosti a nevidím zde potřebu se znova zmiňovat o tom, že je oprávněna poskytovat identifikační služby. Poskytovatelem identifikačních služeb, který je zmíněn v odstavci 1 a 2 výše, je zmiňovaná společnost Bankovní identita, a.s., ve které mají podíl banky, které se podílejí na Bankovní identitě.

Ustanovení § 38ab ZoBID se zabývá použitím PEI, o kterém jsem se zmínil v kapitole 3.5.1, v rámci a mimo rámec kvalifikovaného systému elektronické identifikace. Níže cituji předmětné ustanovení:

„(1) Banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb jsou v rámci poskytování identifikačních služeb podle § 1 odst. 4 písm. c) oprávněni umožnit používání prostředku pro elektronickou identifikaci[36)] mimo rámec kvalifikovaného systému elektronické identifikace umožňujícího poskytnutí služby národního bodu pro identifikaci a autentizaci podle zákona o elektronické identifikaci (dále jen „kvalifikovaný systém"), pouze pokud je tento prostředek pro

[443] BUKOVSKÝ, Jaroslav. V Česku začíná fungovat další velká čínská banka [online]. [cit. 2022-04-18]. Dostupné z: https://www.e15.cz/byznys/finance-a-bankovnictvi/v-cesku-zacina-fungovat-dalsi-velka-cinska-banka-1354120

elektronickou identifikaci vydán a je umožněno jeho používání také v rámci kvalifikovaného systému.

(2) Banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb nemají povinnost umožňovat v rámci kvalifikovaného systému použití prostředku pro elektronickou identifikaci podle odstavce 1, pokud

a) nastane změna právního předpisu nebo změna na základě právního předpisu, která zásadně ohrožuje plnění povinnosti banky nebo pobočky zahraniční banky postupovat při výkonu své činnosti obezřetně, zejména povinnosti řídit rizika, v souvislosti s používáním tohoto prostředku v rámci kvalifikovaného systému a

b) po bance, pobočce zahraniční banky nebo poskytovateli identifikačních služeb nelze spravedlivě požadovat, aby umožňovali používat tento prostředek v rámci kvalifikovaného systému.

(3) Pokud banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb přestanou podle odstavce 2 umožňovat používat prostředek pro elektronickou identifikaci podle odstavce 1 v rámci kvalifikovaného systému,

a) oznámí tuto skutečnost bez zbytečného odkladu správci národního bodu pro identifikaci a autentizaci podle zákona o elektronické identifikaci (dále jen „správce národního bodu“), Ministerstvu vnitra a České národní bance, pokud podléhají jejímu dohledu; součástí oznámení je jeho odůvodnění,

b) nemají povinnost podle § 16 odst. 1 písm. a) zákona o elektronické identifikaci a nelze je stíhat pro přestupek nebo jim odejmout akreditaci podle zákona o elektronické identifikaci pro neplnění této povinnosti; neplnění této povinnosti se nepovažuje za ukončení činnosti kvalifikovaného správce podle zákona o elektronické identifikaci, a

c) budou vyvíjet veškeré úsilí, které po nich lze spravedlivě požadovat, k tomu, aby obnovili možnost používat prostředek pro elektronickou identifikaci podle odstavce 1 v rámci kvalifikovaného systému.

(4) Pokud pominou okolnosti podle odstavce 2, banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb oznámí tuto skutečnost bez zbytečného odkladu správci národního bodu, Ministerstvu vnitra a České národní bance, pokud podléhají jejímu dohledu.“[444]

V tomto paragrafu se ZoBID zabývá elektronickou identifikací v rámci kvalifikovaného systému (viz kapitola 3.5.1.2) a mimo něho. Zde funguje dle

[444] § 38ab ZoBID

komentáře[445] pravidlo 1:1, které znamená, že vydání PEI v rámci kvalifikovaného systému a jeho následného použití v tomto systému, je možné PEI využít i mimo kvalifikovaný systém. Díky tomuto ustanovení § 38ab je možné, aby to samé vydané PEI v rámci kvalifikovaného systému bylo použito v soukromoprávních vztazích, třeba při přihlašování například do administrace uživatelského účtu u pojišťovny. Funguje to tak, že „bude klient přesměrován ze stránek dotčeného dodavatele energie nikoli na stránky NIA, ale na stránky své banky, pobočky zahraniční banky nebo poskytovatele identifikačních služeb, kde se však přihlásí pomocí stejného PEI, jako používá v rámci kvalifikovaného systému“[446] Dle mého je to velice praktické, a pokud by se muselo vydávat další PEI, vytratila by se jednoduchost celého procesu a mohlo by to odradit a mást uživatele. Jako klasický uživatel nebudu chtít vědět rozdíl mezi PEI v kvalifikovaném systému nebo mimo kvalifikovaný systém, ale bude mě zajímat, zda pod tím samým PEI se budu moci prokázat na co nejvíce službách, bez ohledu na skutečnost, zda jsou ve veřejné správě nebo v soukromoprávním sektoru. Praktickým problémem by taky mohlo být to, že by při správním dohledu mohly nastat komplikace a Ministerstvo vnitra (v současné době Digitální a informační agentura) by nemuselo stíhat takovýto dohled[447].

V dalším odstavci jsou uvedeny výjimky, kdy banky nebo pobočky zahraničních bank nebo poskytovatel identifikačních služeb nemusí umožnit použití PEI, což prolamuje výše uvedené pravidlo 1:1, přičemž podmínky v písmenu a) i b) musí být splněny současně[448]. Odstavec 3 pouze upravuje následné kroky, pokud výše uvedené instituce splní obě podmínky a neumožní použití PEI[449]. Poslední odstavec pouze doplňuje odstavec 2, kdy zavádí povinnost oznámení nesplnění podmínek dle odstavce 2.

ZoBID rovněž upravuje prokázání totožnosti mimo rámec kvalifikovaného systému prostřednictví PEI, a to v paragrafu § 38ac:

---

[445] PERHÁČOVÁ, M., VESELSKÝ, Š. § 38ab In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[446] Ibid.

[447] PERHÁČOVÁ, M., VESELSKÝ, Š. § 38ab In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[448] Ibid.

[449] PERHÁČOVÁ, M., VESELSKÝ, Š. § 38ab In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

„(1) Prostředek pro elektronickou identifikaci podle § 38ab odst. 1 lze rovněž použít pro účely prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, mimo rámec kvalifikovaného systému, pokud

a) splňuje technické specifikace, normy a postupy alespoň pro úroveň záruky značnou stanovené přímo použitelným předpisem Evropské unie upravujícím minimální technické specifikace, normy a postupy pro úrovně záruky prostředků pro elektronickou identifikaci[37)] a

b) banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb, kteří vydali tento prostředek pro elektronickou identifikaci, provedli identifikaci fyzické osoby, která je klientem, nebo fyzické osoby jednající za klienta, je-li klient právnickou osobou nebo svěřenským fondem, případně jiným právním uspořádáním bez právní osobnosti, postupem podle zákona upravujícího některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu

1. za fyzické přítomnosti identifikovaného,

2. s využitím prostředku pro elektronickou identifikaci, který splňuje technické specifikace, normy a postupy pro úroveň záruky vysokou stanovené přímo použitelným předpisem Evropské unie upravujícím minimální technické specifikace, normy a postupy pro úrovně záruky prostředků pro elektronickou identifikaci[37)] a který je vydáván a používán v rámci kvalifikovaného systému, nebo jiného systému elektronické identifikace oznámeného podle přímo použitelného předpisu Evropské unie upravujícího elektronickou identifikaci[35)], nebo

3. s využitím prostředku pro elektronickou identifikaci podle § 38ab odst. 1, který splňuje technické specifikace, normy a postupy podle písmene a), pokud zároveň došlo k ověření totožnosti identifikovaného prostřednictvím národního bodu pro identifikaci a autentizaci nebo v informačním systému veřejné správy a banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb mají k dispozici údaj o tom, kdo provedl identifikaci podle bodu 1 nebo 2.

(2) Podmínka podle odstavce 1 písm. b) bodu 1 je splněna také v případě, kdy identifikaci fyzické osoby, která je klientem, nebo fyzické osoby jednající za klienta a) provedla postupem podle zákona upravujícího některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu za fyzické přítomnosti identifikovaného

1. osoba, která jedná za banku nebo pobočku zahraniční banky nebo poskytovatele identifikačních služeb a je vázána jejich vnitřními předpisy, a banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb nesou odpovědnost za

škodu způsobenou činností této osoby při identifikaci podle zákona upravujícího některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu,
2. úvěrová instituce podle § 2 odst. 1 písm. a) zákona upravujícího některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, pokud náleží do stejné skupiny ve smyslu zákona o finančních konglomerátech jako banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb, nebo
3. osoba, která jedná za úvěrovou instituci podle bodu 2 a je vázána jejími vnitřními předpisy, a příslušná úvěrová instituce podle bodu 2 nese odpovědnost za škodu způsobenou činností této osoby při identifikaci podle zákona upravujícího některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, a
b) informace získané při identifikaci klienta ve smyslu zákona upravujícího některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, včetně kopií příslušných dokladů, pokud byly pořizovány, jsou uloženy u banky, pobočky zahraniční banky nebo poskytovatele identifikačních služeb předtím, než tato banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb vydají příslušný prostředek pro elektronickou identifikaci.
(3) Elektronickou identifikaci prostřednictvím prostředku pro elektronickou identifikaci splňujícího požadavky podle odstavce 1 vydaného bankou nebo pobočkou zahraniční banky je možné provést pouze u
a) banky nebo pobočky zahraniční banky, která tento prostředek vydala nebo
b) poskytovatele identifikačních služeb, pokud je totožnost poskytovateli identifikačních služeb potvrzena bankou nebo pobočkou zahraniční banky, která tento prostředek vydala.“[450]

Odstavec 1 umožňuje, aby PEI, který je vydaný v rámci § 38ab, odst. 1 byl používán i za účely prokázání totožnosti mimo kvalifikovaný systém, který jsem zmiňoval už výše. Podmínky v písmenu a) i b) musí být splněny v obou případech. V případě prokázání totožnosti, jež vyžaduje právní předpis odkazuje ZoBID do soukromoprávní i veřejnoprávní sféry, naopak prokázání totožnosti, jež vyžaduje výkon působnosti odkazuje pouze na veřejnoprávní sféru[451]. V písmenu a) je stanoveno, že je nutné, aby úroveň záruky, v návaznosti na nařízení eIDAS bylo alespoň na značné úrovni, a proto také vidíme, že banky mají ve většině případech

[450] § 38ac ZoBID
[451] PERHÁČOVÁ, M., VESELSKÝ, Š. § 38ac In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

akreditovanou danou úroveň a málokdy nižší. U písmene b) jde o to, aby banky, zahraniční banky nebo poskytovatel identifikačních služeb vydal PEI pouze v případě, že provedli identifikaci osoby, jak fyzické, fyzické podnikající, tak právnické nebo svěřenského fondu dle AMLZ, přičemž lze využít jednu ze tří možností, které toto ustanovení umožňuje.

Odstavec 2 volně navazuje na podmínku identifikace dle AMLZ při zastoupení jinou osobou.

Odstavec 3 už pouze doplňuje to, že elektronickou identifikaci PEI mohou provést pouze banky, pobočka zahraniční banky vydávající dané PEI nebo poskytovatel identifikačních služeb.

Čtvrtým, pro mě posledním zásadním ustanovením, z doplňovaných do ZoB je § 38ad, které má následující znění:

„(1) Přístup do informačního systému veřejné správy nebo elektronické aplikace s využitím prostředku pro elektronickou identifikaci splňujícího požadavky podle § 38ac odst. 1 se považuje za přístup se zaručenou identitou podle zákona o informačních systémech veřejné správy.

(2) Státní orgán a orgán územního samosprávného celku jsou oprávněny použít prostředek pro elektronickou identifikaci vydaný bankou, pobočkou zahraniční banky nebo poskytovatelem identifikačních služeb pro účely prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, pouze prostřednictvím kvalifikovaného systému.

(3) Správce národního bodu poskytne službu národního bodu pro identifikaci a autentizaci při využití kvalifikovaného systému, jehož kvalifikovaným správcem podle zákona o elektronické identifikaci je banka, pobočka zahraniční banky nebo poskytovatel identifikačních služeb, pouze kvalifikovanému poskytovateli podle zákona o elektronické identifikaci, který je státním orgánem nebo orgánem územního samosprávného celku.“[452]

Výše uvedené ustanovení § 38ad se zabývá využití PEI v rámci komunikace s veřejnou správou, kdy odstavec 1 se odkazuje na zákon. č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. Potvrzuje zde pouze to, že PEI vydané bankou či pobočkou zahraniční banky musí mít alespoň zaručenou identitou.

[452] § 38ad ZoBID

Oprávnění využít PEI vydané bankou či pobočkou zahraniční banky státním orgánem a orgánem územního samosprávného celku je zaručenou odstavcem 2. V tomto případě považuji za nešťastné tak úzké vymezení právnických osob, protože využití Bankovní identity k přihlášení by bylo ideální i pro školy zřizované městem jako příspěvková organizace nebo nemocnice[453].

Poslední odstavec pouze zdůrazňuje, že při použití PEI vydané bankou či pobočkou zahraniční banky při přihlašování přes NIA, nelze využít soukromoprávních služeb, což má na starosti Bankovní identita, a.s.[454] [455]

3.6.3. Využití v praxi

Největší otázkou, která vyvstává spolu s Bankovní identitou je ta, jak se projeví nová služba v rámci praxe, respektive v rámci každodenního života. Služby Bankovní identity dle oficiálních dat využilo minimálně jednou alespoň 700 tisíc klientů bank [456], což je ve srovnání se Skandinávii stále kapka v moři, avšak společnosti na českém trhu už dávají šanci tomuto řešení, konkrétně v současné době jejich počet čítá 70[457]. Klíčové dle mého názoru bude také připojení dalších bank do tohoto řešení. Opět zopakuji, že do projektu zatím vstoupily subjekty jako Airbank, Česká spořitelna, Československá obchodní banka, Komerční banka, Raiffeisen Bank a Moneta Money Bank. Mezi poslední připojené se řadí Fio banka [458], překvapivě UniCredit Bank (vzhledem k absenci okamžité platby i v současné době) a Banka CREDITAS, u které jsem velice překvapený, vzhledem k tomu, že byly se svou aplikací Richee premianty v rámci multibankingu. Očekával bych u takové banky, že se připojí do Bankovní identity v první vlně, pokud se chce profilovat jako banka s důrazem na moderní technologie a prozákaznický přístup. Pravdou je, že přístup dalších bank do joint-venture Bankovní identita bude čím dále složitější, vzhledem k vyjednávací pozici vůči

[453] PETERKA, Jiří. Kam všude se s bankovní identitou (přes NIA) nedostanete?. Lupa.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.lupa.cz/clanky/kam-vsude-se-s-bankovni-identitou-pres-nia-nedostanete/

[454] Ibid.

[455] PERHÁČOVÁ, M., VESELSKÝ, Š. § 38ad In: PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

[456] Bankovní identitu za první rok využilo 700 tisíc lidí. Česká bankovní asociace [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://cbaonline.cz/bankovni-identitu-za-prvni-rok-vyuzilo-700-tisic-lidi

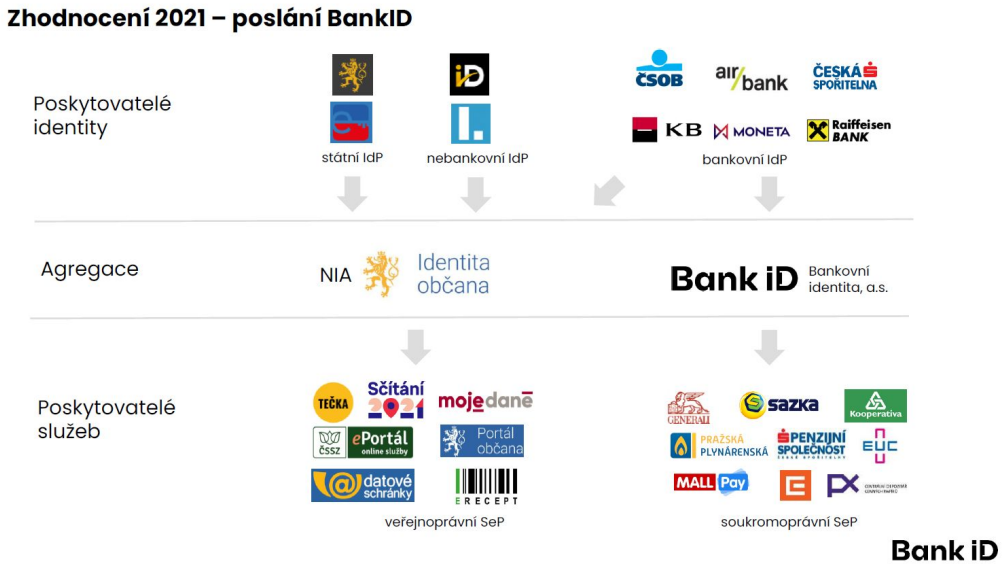
[457] Ibid.

[458] CHVÁTAL, Dalibor Z. Fio banka zpřístupní bankovní identitu, zatím jen na žádost. Měšec.cz [online]. 2022 [cit. 2022-05-31]. Dostupné z: https://www.mesec.cz/aktuality/fio-banka-zpristupni-bankovni-identitu-zatim-jen-na-zadost/

současným bankám, které už jsou v rámci řešení připojené. Myslím si, že to může hrát roli v budoucnosti, avšak doufám, že proklientský přístup zde bude primární, jelikož z toho mohou profitovat všechny banky.

Níže na obrázku můžeme vidět schéma kvalifikovaných správců a poskytovatelů v rámci agregace přes NIA a Bankovní identity. V řádku „Poskytovatelé služeb“ můžeme vidět příklady služeb, které jsou dostupné v tuto chvíli prostřednictvím přihlášení přes elektronickou identifikaci, potažmo Bankovní identitu. V dalších podkapitolách se budu snažit popsat možnosti využití Bankovní identity v praktickém životě.

Obrázek 6 *– Schéma kvalifikovaných správců a poskytovatelů*



Upraveno ze zdroje: ČSOB. [#BankovníIdentita, rychlé a bezpečné digitální prokazování totožnosti...] In: LinkedIn [online] [cit. 2022-3-12]. Dostupné z: https://www.linkedin.com/feed/update/urn:li:activity:6892813344764428288/.

3.6.3.1. Soukromoprávní subjekty

Přihlašování přes Bankovní identitu je jistě velice lákavé pro mnohé soukromoprávní subjekty, a to při výše zmíněném digitálním onboardingu, který může mnoha společnostem ušetřit nemalé náklady na provozu kamenných poboček. Dalším dopadem může být také rychlost získání klienta, kdy stačí zaměřit správně reklamu na potenciálního zákazníka na sociálních sítích či na webových stránkách, na základě cookies, a přes pohodlný digitální onboarding v rámci Bankovní identity je možné získat daného klienta, včetně AMLZ procedur během jednoho dne. Podle mého názoru jde o skvělé využití elektronické identity a s tím související nástroje. Z médií vídáme velice vágní deklaratorní seznam služeb, které by mohly být

využity v souvislosti s Bankovní identitou, a proto níže vypíšu podrobněji alespoň některé z nich.

3.6.3.1.1. Zřízení bankovního účtu

Už v srpnu 2021 jsme mohli zaznamenat, že Česká spořitelna byla první bankou, která umožnila založení bankovního účtu online i bez, léty běžného, nahrávání dvou dokladů[459] (zejména občanský průkaz a řidičský průkaz nebo cestovní pas) a následného OCR skenování dokladů, včetně ověření selfie fotkou. Více v kapitole 3.4.1 ohledně OCR technologie. Vše stačilo nahradit použitím Bankovní identity, díky kterému si myslím, že může dojít i částečně k větší fluktuaci klientů z jedné banky na druhou. Jako příklad z praxe mohu uvést svou zkušenost ze září 2021, kdy jsem byl nemile překvapen se zkušeností s digitálním onboardingem, který jsem popsal dříve v této práci v kapitole 3.1. Po této zkušenosti jsem už ztratil zájem založit účet, kvůli zdlouhavému digitálnímu onboardingu. V případě, že by byla možnost využití Bankovní identity, odpadla by část, kdy by se mohly špatně nahrát fotky z dvou dokladů a OCR technologie by nedokázala přečíst údaje na nich. Proto si myslím, že je velice důležité, přičemž toto zdůrazňuji i ve výše uvedeném textu, že digitální onboarding musí probíhat hladce nebo velice lehce ztratíte potenciálního klienta. V listopadu 2021 možnost zřízení bankovního účtu přes Bankovní identitu umožnila i Komerční banka[460].

Pro zajímavost, přibližně 17 minut má trvat online založení bankovního účtu dle statistik od KPMG[461]. Tato analýza od KPMG ukazuje na slabiny, které jsem výše uvedl, a to strojové čtení údajů z průkazů (OCR technologie), kdy tato technologie není vždy spolehlivá a někdo na centrále musí opravit tato data a následně si je ověřit[462].

---

[459] KUČERA, Petr. První banka založí účet online i bez skenování dokladů. Peníze.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/osobni-ucty/428654-prvni-banka-zalozi-ucet-online-i-bez-skenovani-dokladu

[460] KB nově umožňuje založit účet přes bankovní identitu. Komerční banka [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2021/kb-nove-umoznuje-zalozit-ucet-pres-bankovni-identi

[461] Založení bankovního účtu online trvá 17 minut. Přes aplikaci to umí pouze čtyři banky. E15.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.e15.cz/byznys/finance-a-bankovnictvi/zalozeni-bankovniho-uctu-online-trva-17-minut-pres-aplikaci-to-umi-pouze-ctyri-banky-1381663

[462] Ibid.

3.6.3.1.2. Centrální depozitář cenných papírů

Centrální depozitář cenných papírů v rámci své činnosti poskytuje výpis z nezařazeného účtu cenných papírů, v rámci bývalých účtů Střediska cenných papírů, která zanikla v roce 2011. Dle údajů Centrálního depozitáře cenných papírů je přes 700 tisíc nezařazených účtů[463], a proto je velká pravděpodobnost, že majitelé těchto účtů nebo jejich dědicové mohou nalézt aktiva, která vlastní.

Během minulého roku jsme mohli všichni zaznamenat projekt Zapomenuté miliardy, který se zabývá obchodováním „zapomenutých" akcií z kuponové privatizace[464] a díky tomu se zvedla vlna zájmu o zjišťování současného stavu. Dle projektu Zapomenuté miliardy je více než 10 miliard Kč, které jsou na nezařazených účtech[465].

Od září 2021 umožňuje Centrální depozitář cenných papírů za poplatek 90,- Kč pořídit online výpis, ke kterému se lze dostat přes ověření totožnosti prostřednictvím Bankovní identity a „obejít" tak standardní proces ověření totožnosti žadatele o výpis[466] [467].

Nezařazeným účtem je „účet, který byl převzat ze zaniklého Střediska cenných papírů a jehož majitel dosud neuzavřel s účastníkem centrálního depozitáře smlouvu" [468]. S Centrálním depozitářem cenných papírů se můžeme setkat například při evidenci zaknihovaných cenných papírů.

3.6.3.1.3. Sjednání produktů u dodavatelů energie

V tomto směru byl v září průkopníkem ČEZ[469], který je státem ovládanou společností, jež umožnila ověřování totožnosti nových a stávajících klientů přes Bankovní identitu. Stávající klienti mohou díky této možnosti aktualizovat své

[463] Centrální depozitář usnadní lidem dohledání cenných papírů. Centrální depozitář cenných papírů [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.cdcp.cz/centralni-depozitar-usnadni-lidem-dohledani-cennych-papiru/

[464] Zapomenuté miliardy [online]. [cit. 2022-04-18]. Dostupné z: https://www.zapomenutemiliardy.cz/

[465] Ibid.

[466] Centrální depozitář usnadní lidem dohledání cenných papírů. Centrální depozitář cenných papírů [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.cdcp.cz/centralni-depozitar-usnadni-lidem-dohledani-cennych-papiru/

[467] HOVORKA, Jiří. Akcie z kuponovky najdete snáz. S bankovní identitou. Peníze.cz [online]. [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/burza-cennych-papiru-praha/429129-akcie-z-kuponovky-najdete-snaz-s-bankovni-identitou

[468] Výpis z nezařazeného účtu online. Centrální depozitář cenných papírů [online]. [cit. 2022-04-18]. Dostupné z: https://www.cdcp.cz/nezarazeny-ucet-bankid/

[469] SKALKOVÁ, Olga. ČEZ zjednoduší zařizování. S Bank ID láká i na výhodnější ceny. Peníze.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/spotrebitel/429123-cez-zjednodusi-zarizovani-s-bank-id-laka-i-na-vyhodnejsi-ceny

údaje. Zajímavostí je, že Bankovní identitu využívají i pro předvyplnění formuláře k zaslání výhodnějších podmínek při přechodu od jiného dodavatele energií.

Nutno dodat, že ČEZ není jedinou společností, která umožňuje ověřování identity přes Bankovní identitu, ale dále je jí ještě Pražská plynárenská, která dodává primárně na území Prahy plyn.

Myslím si, že s aktuální situací na trhu s dodávkami energií je jedině dobře, že ověřování identity nových klientů bude takto jednoduché. Mnoho obyvatel České republiky „po pádu" Bohemia Energy je u dodavatelů poslední instance (DPI). Na přelomu října a listopadu 2021 byl znatelný obrovský nápor čekajících nových klientů na pobočkách ostatních dodavatelů energií, kdy ve frontě tito lidé čekali i celý den.

3.6.3.1.4. Lékařské vyšetření na dálku

Zajímavou službou, na kterou jsem narazil už před lety během praxe v jedné advokátní kanceláři v rámci benefitů, byla konzultace s lékařem prostřednictvím internetu. Zda byla daná služba benefit pro zaměstnance a spolupracující mandatáře nebo pouze snaha o zmenšení absencí během pracovní doby prohlídkami u lékaře, ponechám na Vaší fantazii. S obdobím pandemie koronaviru COVID-19 se daná služba pouze rozšířila a troufám si tvrdit, že už je součástí našich životů, což ne každý vítá s otevřenou náručí.

Jedním z poskytovatelů telemedicíny je společnost EUC, která od prosince 2021 umožňuje přihlašování prostřednictvím Bankovní identity[470]. Myslím si, že je to pouze další správný krok, kdy si může poskytovatel služeb být jistý, kdo je na druhé straně, a tak poskytnout zdravotnická data pouze osobě, která by je měla získat.

Telemedicína je „souhrnné označení pro zdravotnické aktivity, služby a systémy, provozované na dálku prostřednictvím informačních a komunikačních technologií za účelem podpory globálního zdraví, prevence a zdravotní péče, stejně jako vzdělávání, řízení zdravotnictví a zdravotnického výzkumu"[471].

[470] Přes bankovní identitu nově i k lékaři. Lékařské vyšetření na dálku bude díky službě BankID rychlejší a bezpečnější. EUC [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://euc.cz/clanky-a-novinky/clanky/pres-bankovni-identitu-nove-i-k-lekari-lekarske-vysetreni-na-dalku-bude-diky-sluzbe-bankid-rychlejsi-a-bezpecnejsi/

[471] Telemedicína Feedback. WikiSkripta [online]. [cit. 2022-04-18]. Dostupné z: https://www.wikiskripta.eu/w/Telemedic%C3%ADna

3.6.3.1.5. Využití v maloobchodě

Pro mě největším překvapením bylo, když řetězec COOP oznámil novinku, v podobě konceptu automatického obchodu, který bude fungovat i mimo otevírací dobu. O takovém konceptu se už hovořilo v červnu 2021[472] v rámci PR článků k Bankovní identitě, avšak jsem neočekával, že realizace takového projektu bude v bližším časovém horizontu. Zvlášť se zkušeností, kdy Amazon teprve v březnu 2021 otevřel v Londýně první kamennou prodejnu Amazon Go Grocery[473], kde můžete zkrátka přijít do obchodu, vzít věci a Amazon Vám automaticky odečte z Vašeho zákaznického účtu za Váš nákup proběhnutý v rámci Amazon Go Grocery.

Díky přihlášení prostřednictvím Bankovní identity v aplikaci od COOP bude zákazník identifikován. Jeho pohyb a bezpečnost zajistí kamerový systém, který je nainstalovaný v tomto obchodu. COOP počítá s tím, že tyto automatické obchody budou fungovat v menších městech, kdy se tyto prodejny zavírají již kolem 18. hodiny[474].

Dokážu si představit, že v dohledné době bude fungovat, i s pomocí Bankovní identity, obchod dle konceptu Amazon Go Grocery, kdy uživatel pouze vezme speciální košík, do kterého vloží zboží a po dokončení nákupu odejde z prodejny bez toho, aby musel přemýšlet nad placením. Budoucnost je v tomto ohledu vzrušující a prodejci se budou dále předhánět v tom, kdo nabídne pohodlnější řešení pro své klienty.

3.6.3.2. eGovernment

eGovernment neboli elektronická veřejná správa je v České republice stále okrajovým pojmem pro fyzické osoby, které nepodnikají nebo nejsou statutáry v právnické osobě. eGovernment „je správa věcí veřejných za využití moderních

[472] MONIOVÁ, Eva. Banky daly Čechům vstupenku do budoucnosti. Pustí vás i do zavřeného obchodu. Seznam Zprávy [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.seznamzpravy.cz/clanek/zapomneli-jste-neco-koupit-obchod-vam-po-zaviracce-muze-odemknout-banka-167823

[473] MANČAŘ, Michal. Amazon otevřel svůj první evropský supermarket bez pokladen. Platba se provede automaticky při odchodu. CzechCrunch [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://cc.cz/amazon-otevrel-svuj-prvni-supermarket-v-evrope-v-londyne-budou-zakaznici-platit-bez-pokladen/

[474] ADAMCOVÁ, Pavla. Coop zpřístupní svůj obchod i po zavíračce. Lidé v něm nakoupí s bankovní identitou. Aktuálně.cz [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://zpravy.aktualne.cz/finance/nakupovani/coop/r~ce3682386f9211eca7d3ac1f6b220ee8/

elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější“[475].

Každoročně Evropská komise vydává index digitální ekonomiky a společnosti (DESI), ve které Evropská komise sleduje „jak se zlepšuje digitální konkurenceschopnost členských států EU v oblasti lidského kapitálu, širokopásmového připojení, integrace digitálních technologií v podnicích a digitálních veřejných služeb“[476]. Je šokující, že v posledním indexu z roku 2021, který čerpal z dat z prvního a druhé čtvrtletí roku 2020, se umístila Česká republika v digitálních veřejných službách v každém indexu této zprávy na posledních místech a nevypadá to, ani se schválením a účinností ZoD, že by se mělo něco změnit, byť nová vláda plánuje dle proklamací z tisku do tří let dokončit digitalizaci veřejné správy[477], tedy splnit 5letý plán od roku 2020, o kterém se hovořilo při schválení tohoto zákona. ZoD slibuje, že v budoucnu budeme moci vyřídit většinu věcí ve veřejné správě přes internet, tedy v rámci eGovernmentu a služby, které budou dostupné přes internet mají být zveřejněny v Katalogu služeb VS[478]. Dle mého názoru je rok 2025 velice těžké splnit a bude to vyžadovat obrovské úsilí, abychom dohnali Pobaltí a Skandinávii. Avšak motivace rozvoje eGovernmentu může pomoci právě Bankovní identita tím, že zesílí uživatelskou základnu a mimo eObčanky a dalších státních PEI poskytne další možnost přihlašování do eGovernmentu. Dle Souhrnné zprávy o digitalizaci veřejné správy z roku 2019 od NKÚ jsou tu bariéry v rozvoji eGovernmentu, například nepřipravenost obecně závazných právních předpisů nebo třeba nedostatečně se využívá institut klíčových služebních míst, při které může mít státní zaměstnanec dvojnásobný platový tarif[479]. Avšak s rostoucí poptávkou z oboru IT si nemyslím, že v tomto případě dvojnásobný platový tarif nebo osobní odměny mohou dostatečně namotivovat příchod těchto zaměstnanců do státní správy bez idealistických myšlenek na

[475] Co je eGovernment?. Ministerstvo vnitra České republiky [online]. 2015 [cit. 2022-04-18]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx

[476] Index digitální ekonomiky a společnosti 2021: digitalizace se celkově zlepšila, ale je třeba vyvinout další úsilí v celé EU. Kurzy.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.kurzy.cz/zpravy/618845-index-digitalni-ekonomiky-a-spolecnosti-2021-digitalizace-se-celkove-zlepsila-ale-je-treba/

[477] ČTK. Vláda chce do tří let dokončit digitalizaci veřejné správy. ITBiz.cz [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.itbiz.cz/zpravicky/vlada-chce-do-tri-let-dokoncit-digitalizaci-verejne-spravy

[478] Katalog služeb VS. PMA3 [online]. [cit. 2022-04-18]. Dostupné z: https://pma3.gov.cz/katalog-sluzeb/info

[479] Nejvyšší kontrolní úřad. Souhrnná zpráva o digitalizaci veřejné správy v ČR [online]. 2019 [cit. 2022-04-18]. Dostupné z: https://nku.cz/assets/publikace-a-dokumenty/ostatni-publikace/zprava-o-digitalizaci-verejne-spravy.pdf

efektivnější veřejnou správu. Níže se zmíním o některých službách, které se dají využít i s pomocí Bankovní identity.

3.6.3.2.1. Datová schránka

Datová schránka byla jedním z pilotních projektů českého eGovernmentu a je v provozu od července 2009. Používá se při komunikaci s orgány veřejné moci a po novele v lednu 2022, předpokládám, že datová schránka se bude používat i více v soukromoprávních vztazích, vzhledem k tomu, že se zde uplatní fikce doručení, na rozdíl od e-mailu, což začínám vídat i v praxi.

Od ledna 2021 umožňuje za pomoci Bankovní identity:

„zřídit datovou schránku fyzické osoby či podnikající fyzické osoby,
zpřístupnit / znepřístupnit datovou schránku,
zneplatnit přístupové údaje, nechat si vydat nové na obrazovku,
přistoupit do datové schránky, číst zprávy, posílat zprávy atd.“[480]

Není to však převratná novinka, vzhledem k legislativě, jelikož jde stále pouze o přihlášení přes NIA s použitím PEI od bank, které jsou v rámci Bankovní identity. Může však pomoci se zjednodušením přihlášení pro nové uživatele, s ohledem automatické zřízení datových schránek všem fyzickým osobám podnikajícím fyzickým osobám a právnickým osobám po 1. lednu 2023, kteří neměli do uvedeného dne zřízenou datovou schránku. Dle odhadů to může být až 2 000 000 osob, které budou mít po tomto datu zřízené datové schránky[481]. Vyvedlo mě z míry, jak moc lidí si zrušilo živnostenské oprávnění, kvůli zřízení datové schránky. Nečekal jsem až tak obrovský odpor k službě, která funguje v České republice už přes 13 let. Ironií je, že takovou věc mohli zařídit přes datovou schránku.

3.6.3.2.2. Portál občana

Současný Portál občana byl spuštěn v červenci 2018 spolu s eObčankami, které se začaly vydávat od 1. července 2018[482]. Portál občana umožňuje uživateli eGovernmentu mít na jednom místě přehled o základních věcech, jako jsou údaje

[480] Co nabízí bankovní identita uživatelům datových schránek?. Datové schránky.info [online]. [cit. 2022-04-18]. Dostupné z: https://www.datoveschranky.info/-/co-nabizi-bankovni-identita-uzivatelum-datovych-schranek-?inheritRedirect=true

[481] TOLLINGEROVÁ, Daniela. Živnostníci, spolky, nadace. Datové schránky musí od příštího roku začít používat na dva miliony lidí. IROZHLAS [online]. [cit. 2022-12-28]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/datove-schranky-info-2023povinnost-osvc_2212261748_ako

[482] HOVORKA, Jiří. Elektronické občanky startují, projděte si průvodce. Jsou povinné a co umí?. Měšec.cz [online]. 2018 [cit. 2022-04-18]. Dostupné z: https://www.mesec.cz/clanky/elektronicke-obcanky-startuji-projdete-si-pruvodce-jsou-povinne-a-co-umi/

ze státních registrů, založení datové schránky nebo přístup na další portály, jako jsou Moje daně, přístup na ePortál České správy sociálního zabezpečení nebo třeba Očkovací portál. Přihlašuje se pomocí PEI, a jak jsem zmínil už u kapitoly 3.6.3.2.1, není nic překvapivého, že s PEI od bank se dá přihlásit do Portálu občana. Je to však obrovský příslib, že občané, kteří ještě nezískali nové eObčanky se budou moci jednoduše přihlásit k Portálu občana.

3.6.3.2.3. Sčítání lidu

Pro mě osobně první setkání s Bankovní identitou proběhlo během projektu Sčítání lidu 2021, které bylo podruhé v historii možné vyplnit elektronicky. Tímto způsobem vyplnilo v roce 2021 87 % obyvatel[483], přičemž v roce 2011 to bylo pouze 25,5 %[484]. Dle mého názoru Bankovní identita v tomto případě přispěla určitou měrou, byť oficiální statistiky zatím nebyly zveřejněny.

3.6.3.2.4. Notářský zápis

V rámci novely zákona č. 358/1992 Sb., Notářského řádu, od září 2021 některé činnosti notářů umožnila provádět dálkovým způsobem, jako například sepsání notářského zápisu. Myslím si, že to ztělesňuje revoluci, která bude potřebovat ještě nějakou dobu, aby ji trh přijal. Například v M&A transakcích, kdy už takové úvahy jsou mezi odbornou veřejností[485].

Notáři mohou od výše uvedeného data využít k ověření totožnosti eObčanku nebo Bankovní identitu[486]. Otevírají se s tím nové možnosti, jako například založení společnosti s ručeným omezením online, bez toho aniž by se zakladatelé společnosti museli osobně dostavit k notáři[487].

---

[483] Zájem o sčítání lidu online překonal očekávání. Výsledky budou na přelomu roku. E15.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.e15.cz/domaci/zajem-o-scitani-lidu-online-prekonal-ocekavani-vysledky-budou-na-prelomu-roku-1376628

[484] Základní údaje o sběru elektronických sčítacích formulářů při sčítání lidu, domů a bytů 2011. SLDB 2011 [online]. [cit. 2022-04-18]. Dostupné z: https://www.czso.cz/csu/sldb/zakladni_udaje_o_sberu_elektronickych_scitacich_formularu_pri_sldb2011

[485] KOVÁŘ, Dalibor a Josef BOUCHAL. Jak se v praxi elektronicky podepisují mezinárodní transakce?. Havel & Partners [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.havelpartners.blog/blog/jak-se-v-praxi-elektronicky-podepisuji-mezinarodni-transakce/304

[486] MORÁVEK, Daniel. Jak založit firmu? Od loňského září klidně online z obýváku. Podnikatel.cz [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.podnikatel.cz/aktuality/jak-zalozit-firmu-od-lonskeho-zari-klidne-online-z-obyvaku/

[487] Založení SRO online - úvodní informace. Notářská komora České republiky [online]. [cit. 2022-04-18]. Dostupné z: https://www.nkcr.cz/sro-online-informace

3.6.4. Budoucnost Bankovní identity

Budoucnost Bankovní identity dle mého názoru závisí na tom, kolik bank a poboček zahraničních bank se bude chtít připojit do tohoto projektu a rozšíří tak uživatelskou základnu, kterou bude potom nabízet soukromoprávním subjektům.

Přínos projektu Bankovní identity vidím v tom, že banky, které se připojily do projektu Bankovní identita, začaly rozvíjet projekt BankID SIGN[488], tedy elektronické podepisování smluv a dokumentů, kdy tyto digitální podpisy jsou zaručenými digitálním podpisy[489]. Od 18. listopadu 2021 je v ostrém provozu a mezi prvními bankami, které se připojily do tohoto projektu jsou České spořitelna, a.s., Československá obchodní banka, a. s. a Komerční banka, a.s.

V zásadě je nyní důležité, aby business model Bankovní identity byl rentabilní a motivoval toto joint-venture bank k většímu rozvoji služeb a zároveň se staral o přibývání dalších bank, které by se připojily do tohoto projektu. Poté dle mého názoru bude mít tento projekt velký úspěch a pomůže i eGovernmentu v České republice získat další uživatele, byť to není primární cíl tohoto projektu.

[488] SKALKOVÁ, Olga. První banka spouští Sign. Smlouvu podepíšete jednoduše online. Peníze.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/osobni-ucty/429350-prvni-banka-spousti-sign-smlouvu-podepisete-jednoduse-online

[489] Zaručený digitální podpis SIGN spouštějí první tři banky. BankID.cz [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.bankid.cz/novinky/zaruceny-digitalni-podpis-sign-spousteji-prvni-tri-banky

Závěr

Cílem této rigorózní práce bylo představit vybranou legislativní úpravu FinTech v České republice a částečně i na území Evropské unie v návaznosti na evropskou legislativu, která danou oblast reguluje, například směrnice PSD2 nebo nařízení eIDAS.

Oproti představám vyplývajícím z mediálního prostoru, diskuze odborné veřejnosti apod. ohledně toho, že je Česká republika průkopníkem v IT oblasti v návaznosti s bankovnictvím, jsem už během zpracování diplomové práce došel k závěru, že tomu tak pravdou úplně není, zejména kvůli právní regulaci a vnímání hráčů na trhu. Dle studie McKinsey & Company z října 2022[490] počet FinTech služeb na jednu osobu v České republice jsou 4, přičemž Irsko, které má o polovinu méně obyvatel, má 30 FinTech služeb na jednu osobu.

Situace se bohužel za necelé dva roky nezměnila, byť je to v této oblasti velmi dlouhá doba. Stále jsme ve FinTech na stejném místě a moc novinek se na trhu a v legislativě neobjevilo, kromě drobných legislativních změn v oblasti platebního styku, které byly spíše kosmetické.

U některých novinek, které přinesla nebo umožnila vůbec vzniknout směrnice PSD2, jsem si já osobně hodně sliboval, například fenomén multibanking. Tento fenomén se na trhu dle mého názoru moc neprosadil, patrně kvůli konzervativnímu přístupu klientů bank, ač na začátku byly obavy, že spíše klienti budou danou službu používat až příliš bez rozmyslu. Multibanking banky nepropagují tak jako dříve a třeba George od České spořitelny už takovou funkci ani nenabízí.

Očekával jsem, že možnosti, které jsme získali díky příchodu směrnice PSD2, jež byla zákonodárci implementována do ZoPS, budou v České republice více využity, ale opak je pravdou. Silné ověření uživatele je však stále dle mého uvážení jedinou zásadní regulací, která ovlivňuje naše každodenní životy a stále si myslím, že je obrovským přínosem pro bezpečnost klientů bank. Dle zákaznické ankety, kterou pořádala společnost Signifyd[491], 53 % respondentů ve Velké Británii

[490] Europe's fintech opportunity. McKinsey [online]. [cit. 2022-12-28]. Dostupné z: https://www.mckinsey.com/industries/financial-services/our-insights/europes-fintech-opportunity

[491] WHITEHEAD, Ed. Why strong customer authentication benefits merchants. FinTech Magazine [online]. [cit. 2022-12-28]. Dostupné z: https://fintechmagazine.com/digital-payments/how-strong-customer-authentication-benefits-merchants

měla povědomí o silném ověření uživatele. O to více šokující je, že méně než jedna třetina uživatelů v Itálii a Francii měla povědomí o silném ověření uživatele.

Vývoj v oblasti silného ověření uživatele mě však těší i z toho pohledu, že u prvku inherence lze zaznamenat počínající vývoj zaměřující se na zaznamenávání individuálních prvků každého člověka, například při měření hodnot EKG. Troufám si tvrdit, že to bude velká výzva z hlediska ochrany osobních údajů a jeho uchováváním, zejména s ohledem na zabezpečení a přístup k těmto datům v budoucnosti.

Na harmonizaci celoevropského Open bankingu stále čekáme a jsem zvědav, jak se s tím popasují příslušné orgány Evropské unie během přípravy směrnice PSD3 nebo v rámci pro otevřené financování, které připravuje Evropská komise.

Velká očekávání jsem vkládal na nově příchozí projekt Bankovní identity, která disponuje extrémně kvalitním PR a marketingem. Mnoho médií se tomuto tématu intenzivně věnuje a týden co týden nás informují o nových přistoupivších projektech a možnostech, které Bankovní identita umožňuje. Velký poprask, co se mého okolí týče, jsem zaznamenal zejména na automatické prodejny COOP.

Částečně si myslím a zároveň doufám, že Bankovní identita přiměje obyvatele České republiky k pravidelnějšímu využívání elektronické identifikace, ale obava z nových technologií (pomineme-li fakt, že legislativa ZoEI je tu s námi již od roku 2017) bude celkově velkou překážkou celkově pro digitální onboarding, byť nás pandemie koronaviru COVID-19 naučila fungovat více prostřednictvím internetu.

Můj názor je postavený na tom, že mnoho „výdobytků“, které jsme získali během této pandemie se postupně, ale jistě vytrácí, například home office nebo videokonference přes MS Teams. Jsem však přesvědčen zejména o tom, že Bankovní identita pomůže obrovským dílem eGovernmentu v České republice, jelikož se jedná o nejjednodušší způsob, jak se dostat k veřejné správě prostřednictvím internetu. Počet potenciálních uživatelů této služby je však obrovský a i ze statistik je patrné, že obyvatelé České republiky začínají používat Bankovní identitu. Přičítám však tomuto trendu tu skutečnost, že použití zkreslilo i první masivnější užití Sčítání lidu přes internet.

Zda mám pravdu s výše uvedenými predikcemi či nemám, ukáže pouze čas, avšak byl bych velice rád, pokud se mé pesimističtější předpovědi nesplní a splní

se pouze ty optimisticky laděné. Netrpělivě čekám na to, co nám přinesou další roky ohledně regulace v oblasti FinTech, jelikož svět se stále mění rychlejším tempem a tato oblast je jednou z těch nejpružnějších v bankovnictví.

Resumé

The subject of this rigorous thesis is “Selected legal framework of FinTech in the Czech Republic and its use in practice”.

The main goal of this thesis is not to cover all legislation related to the FinTech in the Czech Republic or in the European Union, but to slightly cover the services brought by the regulation PSD2 and the digital onboarding, its explanation and regulation in the present time.

This rigorous thesis is divided into three chapters, where the first two chapters are about regulation PSD2 and Open banking and the last chapter is about the new phenomena nowadays in the FinTech, which is digital onboarding and its regulation in the Czech Republic.

The first chapter of this rigorous thesis is about news in Fintech in connection with the regulation PSD2. This chapter introduce the main associations in the Czech Republic, which are making into the spotlight in the FinTech area in the Czech Republic and they are the main movement of the FinTech regulation and new products in this country. The first chapter also describe Open banking standard and its differences in the Czech and British open banking system. In this part the author is also explaining the NextGenPSD2 and openFinance Framework in connection with the Open banking. In addition to the above, this chapter describes the legal framework of the account information services, also known as AIS and payment initiation service, also known as PIS. Based on these last two features, the ending of this chapter is devoted to use in practice of the new features. That describes the multibanking and its use in the Czech Republic, which is basically the product of the account information services and payment initiation service, then money manager that using the account information services and the credit score and its use with these new features that the regulation PSD2 provides.

The second chapter is focusing on the strong customer authentication, which is one of the main feature of the regulation PSD2 as the author claims in this thesis. This chapter explain this procedure of the strong customer authentication, the legal framework of this process and the elements as knowledge, possession and inherence. This chapter also describes mobile applications “Key” (*in Czech: Klíč*). It also contains the exemptions from the strong customer authentication, f. e. payment account information, contactless payments at point of sale, unattended terminals for transport fares and parking fees or credit transfers between accounts

held by the same natural or legal person. At the end of this chapter is dedicated to the breach of the obligations from the strong customer authentication and its sanctions.

The last chapter of this rigorous thesis is devoted to the digital onboarding and the BankID (*in Czech: Bankovní identita*) and consideration of their compatibility. In connection with the digital onboarding the chapter also describe main legal regulations.

In the beginning of the chapter the author describes the methods of the digital onboarding, the On-Site onboarding and the Semi-On-Site Onboarding. With the digital onboarding, the chapter describes the requirements of the Act on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism, also known as AML regulation. In this subchapter the author focuses to the cases, when the liable person have the obligation to identify the client, f. e. the value of the trade up to 1000 EUR, the suspicious trade or the establishment of the business relationship. The next subchapter is about the process of the identification according to the AML regulation in the Czech Republic. The author describes the process of the identification of natural person, legal entity and trust. Also this subchapter contains exceptions from the identification f. e. using the remote identification or using the electronic signature. The last chapter also describe the technologies that made the remote identification possible as OCR software or automatic face detection.

Besides the AML regulation, the last chapter also focus on the eIDAS regulation, which can solve the problem with digital onboarding. This subchapter describes electronic identification, authentication and trust services. About electronic identification and authentication, the reader could discover more about National identity authority (*in Czech: Národní identitní autorita*) and its system. Author also describes in this thesis the trust services, which are electronic signature and electronic seal.

The last part of the last chapter is about the BankID and its company that maintaining this product in the Czech Republic. The introduction of the BankID was based on the legislative changes that allowed this product that this chapter also describes. The main part of this is the use cases that BankID could be use in the practice for private sector and public sector. The private sector could use BankID f. e. for establishing a bank account, remote medical examination or use in the retail.

The public sector could use that heavily in the eGovernment, as for Data box (*in Czech datová schránka*), census or notarial deed.

Seznam použité literatury

Odborné publikace

BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2022-3-12]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

BÉREŠ, J., HLADKÁ, M., KATOLICKÁ, M. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO253_2008CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

GILCHRIST, Alasdair. FinTech Rising: Navigating the maze of US & EU regulations. Amazon, 2017. ISBN 9781549878800.

HUANG, Robin Hui. Fintech Regulation in China: Principles, Policies and Practices. Cambridge University Press, 2021. ISBN 978-1-108-73844-6.

NICOLETTI, Bernardo. The Future of FinTech. Palgrave Macmillan, 2017. ISBN 9783319514147.

PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2022-3-12]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. 2. vydání. V Praze: *C.H. Beck*, 2019. Beckova edice komentované zákony. ISBN 978-80-7400-747-7.

ZAJÍČEK, Zdeněk, KORBEL, František, KOVÁŘ, Dalibor, AMLER, Pavel, DONÁT, Josef, TOMÍŠEK, Jan, ORŠULÍK, David. Zákon o právu na digitální služby. 1. vydání. Praha: C. H. Beck, 2021, ISBN 978-80-7400-822-1

Právní předpisy a podzákonné předpisy

Zákon č. 21/1992 Sb., o bankách

Zákon č. 159/2000 Sb., kterým se mění zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů, ve znění zákona č. 15/1998 Sb., a některé další zákony

Zákon. č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

Zákon č. 500/2004 Sb., o správním řádu (Správní řád)

Zákon č. 634/2004 Sb., o správních poplatcích

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

Zákon č. 89/2012 Sb., občanský zákoník

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

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

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

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

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

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. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony

Zákon č. 171/2023 Sb., o ochraně oznamovatelů

Vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu

Vyhláška č. 1/2022 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku

Úřední sdělení České národní banky č. 18/2020 Věst. ČNB ze dne 5. srpna 2020 k výkladu pojmů důvěryhodnost a odborná způsobilost

Důvodová zpráva k zákonu č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, č. 253/2008 Dz

Důvodová zpráva k zákonu č. 250/2017 Sb., o elektronické identifikaci, č. 250/2017 Dz

Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

European Banking Authority. EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC ze dne 13. června 2018.

European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019.

Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES
Nařízení Evropského parlamentu a Rady (EU) č. 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) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách 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

Elektronické prameny

1. PF Finance, s.r.o. [online]. [cit. 2021-03-16]. Dostupné z: https://www.1pffin.cz/

12. díl: Bankovní identita vám zpřístupní nové možnosti ve světě online služeb. *Průvodce podnikáním - ČSOB* [online]. 2022 [cit. 2022-05-21]. Dostupné z: https://www.pruvodcepodnikanim.cz/clanek/bankovni-identita/

ADAMCOVÁ, Pavla. Coop zpřístupní svůj obchod i po zavíračce. Lidé v něm nakoupí s bankovní identitou. *Aktuálně.cz* [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://zpravy.aktualne.cz/finance/nakupovani/coop/r~ce3682386f9211eca7d3ac1f6b220ee8/

AIS and PIS – A status update on open banking licenses issued in the UK. *Penser* [online]. 05.2019n. l. [cit. 2021-03-07]. Dostupné z: https://www.penser.co.uk/business/ais-and-pis-a-status-update-on-the-licenses-issued-in-the-uk/

An Introduction to China FinTech. *Chambers and Partners* [online]. [cit. 2022-12-29]. Dostupné z: https://chambers.com/content/item/3833

Australia. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-12-31]. Dostupné z: https://en.wikipedia.org/wiki/Australia

BACHURA, Jan. S aplikací George klíč lze nově potvrzovat i platby na internetu. Jak budou moct klienti v roce 2021 potvrzovat platby kartou v eshopech? *Finparáda* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.finparada.cz/6688-S-aplikaci-George-klic-lze-nove-potvrzovat-i-platby-na-internetu.aspx

BankID. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-04-18]. Dostupné z: https://en.wikipedia.org/wiki/BankID

BankID in numbers. *BankID* [online]. [cit. 2022-04-18]. Dostupné z: https://www.bankid.com/en/om-oss/statistik

Bankovní identita umožnila nový rozměr elektronického ověřování totožnosti. *Advokátní deník* [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://advokatnidenik.cz/2021/02/09/zakon-o-bankovni-identite-umoznil-novy-rozmer-elektronickeho-overovani-totoznosti/

Bankovní identita zvítězila v anketě Zákon roku 2020. *DReport* [online]. 2021, 21. 4. 2021 [cit. 2022-03-11]. Dostupné z: https://www.dreport.cz/blog/bankovni-identita-zvitezila-v-ankete-zakon-roku-2020/

Bankovní identitu za první rok využilo 700 tisíc lidí. *Česká bankovní asociace* [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://cbaonline.cz/bankovni-identitu-za-prvni-rok-vyuzilo-700-tisic-lidi

BARANOVÁ, Iva a Linda KOLAŘÍKOVÁ. PSD2: novelizace platebních služeb. *KPMG Česká republika* [online]. 2017 [cit. 2021-03-01]. Dostupné z: https://danovky.cz/cs/psd2-novelizace-platebnich-sluzeb

BARTÁČEK, Václav. Představení PSD2 nejen pro vývojáře. Blíží se otevřené bankovnictví? Udělejte si v tom jasno. *Zdroják.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://zdrojak.cz/clanky/psd2-nejen-pro-vyvojare/

BEDRICH, Vaclav. Český fintech Spendee získal od ČNB jako první licenci k přímému propojení s bankami. *CzechCrunch* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://www.czechcrunch.cz/2018/12/cesky-fintech-spendee-ziskal-od-cnb-jako-prvni-licenci-k-primemu-propojeni-s-bankami/

BERAN, Karel. Tři pilíře moderního bankovnictví pro rok 2020 – digitální onboarding, proaktivní komunikace a empatie. *Bankovní poplatky* [online]. [cit. 2022-05-20]. Dostupné z: https://www.bankovnipoplatky.cz/tri-pilire-moderniho-bankovnictvi-pro-rok-2020-digitalni-onboarding-proaktivni-komunikace-a-empatie-

Bezpečnostní token. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-04-17]. Dostupné z: https://cs.wikipedia.org/wiki/Bezpe%C4%8Dnostn%C3%AD_token

BIELSKAITĖ, Viktorija. Digital Onboarding: Definition, Types and How it Works. *IDenfy* [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.idenfy.com/blog/digital-onboarding/

BOERS, Brooke. Life Hacks: How to Establish a Bank Account and Bank ID in Sweden. *Study in Sweden* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://studyinsweden.se/blogs/2021/03/31/how-to-establish-a-bank-account-and-bank-id/

BOHUSLAV, Tomáš. Na úřadě, v e-shopu i u dodavatele energie. S BankID jsou přihlašování snadná a vaše data v bezpečí. Jak to celé funguje?. *Euro.cz* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://www.euro.cz/byznys/na-urade-v-e-

shopu-i-u-dodavatele-energie-s-bankid-jsou-prihlasovani-snadna-a-vase-data-v-bezpeci-jak-to-cele-funguje

BREJČÁK, Peter. Místo obličeje vyvíjí brněnští vědci ověření identity pomocí tlukotu srdce. EKG má být unikátnější než otisk prstu. *CzechCrunch* [online]. 2022 [cit. 2022-03-12]. Dostupné z: https://cc.cz/misto-obliceje-vyviji-brnensti-vedci-overeni-identity-pomoci-tlukotu-srdce-ekg-ma-byt-unikatnejsi-nez-otisk-prstu/ [online]. [cit. 2022-03-12].

BREJČÁK, Peter. Přichází revoluční PSD2: Jak se změní svět fintech startupů? *Tyinternety* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://tyinternety.cz/startupy-a-byznysy/prichazi-revolucni-psd2-se-zmeni-svet-fintech-startupu/

BREJČÁK, Peter. Startupy zbrzdí regulace a další vzniknou jen pro efekt: 6 rizik, které do bankovnictví přináší PSD2. *Tyinternety* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://tyinternety.cz/fastnews/6-rizik-ktere-do-bankovnictvi-prinasi-psd2/

BUBÁK, Zdeněk. Český standard pro Open Banking je na světě. *Finparáda* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www.finparada.cz/mobile/4722-Cesky-standard-pro-Open-Banking-je-na-svete.aspx

BUCKLEY, Ross P., Natalia JEVGLEVSKAJA a Scott FARRELL. Open banking and Australia's data-sharing regime: six lessons for Europe. *LSE Business Review* [online]. [cit. 2022-12-29]. Dostupné z: https://blogs.lse.ac.uk/businessreview/2022/04/28/open-banking-and-australias-data-sharing-regime-six-lessons-for-europe/

BUCHBAUER, Petr. Dveře pro nové finanční služby se otevírají aneb průvodce tajemnou PSD2. *Peak.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.peak.cz/dvere-nove-financni-sluzby-se-otviraji-aneb-pruvodce-tajemnym-psd2/8841/

BUCHBAUER, Petr. Vítej na palubě homo digitalis aneb jak na digitální onboarding. *Peak.cz* [online]. 2019 [cit. 2022-03-12]. Dostupné z: https://www.peak.cz/vitej-palube-homo-digitalis-aneb-digitalni-onboarding/5919/

BUKOVSKÝ, Jaroslav. V Česku začíná fungovat další velká čínská banka. *E15.cz* [online]. [cit. 2022-04-18]. Dostupné z: https://www.e15.cz/byznys/finance-a-bankovnictvi/v-cesku-zacina-fungovat-dalsi-velka-cinska-banka-1354120

BUŘÍNSKÁ, Barbora. Klienti se přesouvají do onlinu, velké banky zavírají pobočky. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://www.novinky.cz/finance/clanek/klienti-se-presouvaji-do-onlinu-velke-banky-zaviraji-pobocky-40340316

Ceník. *BankID.cz* [online]. [cit. 2022-04-18]. Dostupné z: https://www.bankid.cz/cenik

Centrální depozitář usnadní lidem dohledání cenných papírů. C*entrální depozitář cenných papírů* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.cdcp.cz/centralni-depozitar-usnadni-lidem-dohledani-cennych-papiru/

Co je eGovernment?. *Ministerstvo vnitra České republiky* [online]. 2015 [cit. 2022-04-18]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx

Co je Joint-venture. *Peníze.cz* [online]. [cit. 2022-04-17]. Dostupné z: https://www.penize.cz/slovnik/joint-venture

Co je to API (application programming interface)? *Topranker.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://topranker.cz/slovnik/co-je-to-api-application-programming-interface/

Co nabízí bankovní identita uživatelům datových schránek?. *Datové schránky.info* [online]. [cit. 2022-04-18]. Dostupné z: https://www.datoveschranky.info/-/co-nabizi-bankovni-identita-uzivatelum-datovych-schranek-?inheritRedirect=true

Co PSD1 a PSD2 znamenají a proč jsou důležité? *IBanFirst Blog* [online]. 2018 [cit. 2021-03-16]. Dostupné z: https://blog.ibanfirst.com/cz/co-psd1-a-psd2-znamenaj%C3%AD-a-pro%C4%8D-jsou-d%C5%AFle%C5%BEit%C3%A9

Consumer Data Right. *Treasury.gov.au* [online]. [cit. 2022-12-29]. Dostupné z: https://treasury.gov.au/policy-topics/economy/consumer-data-right

ČERMÁK, Jan. Novinky v oblasti silného ověření uživatele. *Právní prostor* [online]. 2021 [cit. 2021-03-15]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/novinky-v-oblasti-silneho-overeni-uzivatele

Česká spořitelna spouští aplikaci George klíč pro všechny klienty. *Česká spořitelna* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2019/09/11/ceska-sporitelna-spousti-aplikaci-george-klic-pro-vsechny-klienty

Český standard pro Open banking. *Česká bankovní asociace* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesky-standard-pro-open-banking

Češi a digitalizace 2019. *Česká bankovní asociace* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2019

Češi a digitalizace 2020. *Česká bankovní asociace* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2020

Členové asociace. *Česká bankovní asociace* [online]. [cit. 2023-07-30]. Dostupné z: https://cbaonline.cz/clenove

ČSOB. [#BankovníIdentita, rychlé a bezpečné digitální prokazování totožnosti...] In: *LinkedIn* [online] [cit. 2022-3-12]. Dostupné z: https://www.linkedin.com/feed/update/urn:li:activity:6892813344764428288/.

ČTK. Vláda chce do tří let dokončit digitalizaci veřejné správy. *ITBiz.cz* [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.itbiz.cz/zpravicky/vlada-chce-do-tri-let-dokoncit-digitalizaci-verejne-spravy

Digitální onboarding. *Adastra* [online]. [cit. 2022-05-21]. Dostupné z: https://adastra.digital/cs/solutions/digitalni-onboarding/

Digital onboarding and cost efficiency. PXL *Vision* [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.pxl-vision.com/en/blog/what-is-digital-onboarding-and-how-to-reduce-business-costs-during-id-verification

Digital Onboarding: definition, characteristics and how it works. *Electronic IDentifiaction* [online]. 2021 [cit. 2022-04-16]. Dostupné z: https://www.electronicid.eu/en/blog/post/digital-onboarding-process-financial-sector/en

Digitální onboarding klientů. *Deloitte Česká republika* [online]. 2022 [cit. 2022-04-16]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/financial-services/solutions/digitalni-onboarding-klientu.html

DLUBALOVÁ, Klára. Historická chvíle. První klienti budou moci využívat služby veřejné správy přes internetové bankovnictví. *Ministerstvo vnitra České republiky*

[online]. 2020 [cit. 2022-05-21]. Dostupné z: https://www.mvcr.cz/clanek/historicka-chvile-prvni-klienti-budou-moci-vyuzivat-sluzby-verejne-spravy-pres-internetove-bankovnictvi.aspx

DocuSign - návod k použití. *TechSoup Česká republika* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.techsoup.cz/docusign-navod

Do Česka dorazila elektronická identita! Jak na ni?. *Vím, kam klikám* [online]. 2018 [cit. 2022-05-21]. Dostupné z: https://www.vimkamklikam.cz/rady-a-tipy/do-ceska-dorazila-elektronicka-identita-jak-na-ni

DOLEČEK, Marek. Využívejte elektronické podpisy a elektronickou identitu. Poradíme, jak na to. *BusinessInfo.cz* [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.businessinfo.cz/navody/elektronicke-podpisy-elektronicka-identita-ppbi/

DONÁT, Josef. eIDAS a jeho praktické využití v soukromém sektoru [online]. [cit. 2022-05-21]. Dostupné z: https://www.egovernment.cz/soubor/eidas-a-jeho-prakticke-vyuziti-josef-donat/

DONÁT, Josef. Směrnice PSD2 a revoluce v platebních službách. *Epravo.cz* [online]. 2016 [cit. 2021-02-22]. Dostupné z: https://www.epravo.cz/top/aktualne/smernice-psd2-a-revoluce-v-platebnich-sluzbach-102716.html

DOSKOČILOVÁ, Veronika. PSD2 rok poté: multibanking umí 5 bank, API nezpřístupnila polovina. *Měšec.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.mesec.cz/clanky/psd2-rok-pote-multibanking-umi-5-bank-api-nezpristupnila-polovina/

EObčanka. Informační web elektronické identity [online]. [cit. 2022-04-18]. Dostupné z: https://info.identitaobcana.cz/eop/

EIDAS, služby vytvářející důvěru a elektronická identifikace. *Ministerstvo vnitra České republiky* [online]. 2020 [cit. 2022-05-21]. Dostupné z: https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx

EISELT, Zbyněk. Co znamená silné ověření klienta (SCA) a proč se o něm všude mluví? *GoPay blog* [online]. 2019 [cit. 2021-02-22]. Dostupné z:

https://www.gopay.com/blog/co-znamena-silne-overeni-klienta-sca-a-proc-se-o-nem-vsude-mluvi/

Elektrokardiografie. *WikiSkripta* [online]. [cit. 2022-03-12]. Dostupné z: https://www.wikiskripta.eu/w/Elektrokardiografie

Europe's fintech opportunity. *McKinsey* [online]. [cit. 2022-12-28]. Dostupné z: https://www.mckinsey.com/industries/financial-services/our-insights/europes-fintech-opportunity

Evropská digitální dekáda: digitální cíle pro rok 2030. *Evropská komise* [online]. [cit. 2022-04-18]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_cs

Evropský průzkum Deloitte ke směrnici PSD2. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/financial-services/articles/deloitte-european-psd2-surveys.html

FABIÁNEK, Roman a Štěpán KALUHA. Pět zkušeností s licencováním aneb na co se připravit, když si půjdete k ČNB pro licenci. *DReport* [online]. [cit. 2022-12-26]. Dostupné z: https://www.dreport.cz/blog/pet-zkusenosti-s-licencovanim-aneb-na-co-se-pripravit-kdyz-si-pujdete-k-cnb-pro-licenci/?linkId=183230940

Facebook přiznal obří únik dat. Útočníci se dostali k 50 milionům uživatelských účtů. *INFO.CZ* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://www.info.cz/zpravodajstvi/svet/facebook-priznal-obri-unik-dat-utocnici-se-dostali-k-50-milionum-uzivatelskych-uctu

FALTOVÁ, Nikola. Nový zákon o platebním styku a největší změny, které přináší. *Epravo.cz* [online]. 2017 [cit. 2021-03-01]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-a-nejvetsi-zmeny-ktere-prinasi-106626.html

FAQs. *Open Banking* [online]. [cit. 2021-03-15]. Dostupné z: https://www.openbanking.org.uk/customers/faqs/

FinTech v ČR i ve světě. In: *Deloitte Česká republika* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf

FRYDLEWICZ, Jiří. Otevřené bankovnictví se blíží, klienti si ale na nové funkce počkají. *E15.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www.e15.cz/finexpert/investujeme/otevrene-bankovnictvi-se-blizi-klienti-si-ale-na-nove-funkce-pockaji-1341003

GRÖNLUND, Åke. Electronic identity management in Sweden: governance of a market approach. *Identity in the Information Society* [online]. 2010, 3(1), 195-211 [cit. 2022-05-22]. ISSN 1876-0678. Dostupné z: doi:10.1007/s12394-010-0043-1

HAMELE, Thomas a Oliver DATHAN. Next-Generation Client Onboarding [online]. *PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft*, 2018 [cit. 2022-05-22]. Dostupné z: https://www.pwc.de/en/digitale-transformation/pwc-study-next-generation-client-onboarding-2018.pdf

HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *Epravo.cz* [online]. 2020 [cit. 2022-05-21]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

HANZLÍK, Filip. Komentář ČBA k bankovní identitě a vzniku nové aliance. *Česká bankovní asociace* [online]. [cit. 2022-04-18]. Dostupné z: https://cbaonline.cz/komentar-cba-k-bankovni-identite-a-vzniku-nove-aliance

HEJKRLÍK, Pavel. Air Bank, Fio banka a Moneta zakládají alianci pro bankovní identitu. *Marketing & Media* [online]. 2020 [cit. 2022-04-18]. Dostupné z: https://mam.cz/zpravy/2020-11/air-bank-fio-banka-a-moneta-zakladaji-alianci-pro-bankovni-identitu/

HINGAR, Petr. Otevřené bankovnictví, PSD2, open API a BankID aneb Změna paradigmatu ve finančním sektoru. *SystemOnline.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.systemonline.cz/it-pro-banky-a-financni-organizace/otevrene-bankovnictvi-psd2-open-api-a-bankid.htm

HORÁČEK, Jakub. Speciální hesla či biometrické údaje. Začínají platit přísnější pravidla pro platby po internetu. *IROZHLAS* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://www.irozhlas.cz/ekonomika/platby-pres-internet-nakupovani-online-zmena-pravidel_1909140630_kro

HOVORKA, Jiří. Akcie z kuponovky najdete snáz. S bankovní identitou. *Peníze.cz* [online]. [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/burza-cennych-papiru-praha/429129-akcie-z-kuponovky-najdete-snaz-s-bankovni-identitou

HOVORKA, Jiří. Elektronické občanky startují, projděte si průvodce. Jsou povinné a co umí?. *Měšec.cz* [online]. 2018 [cit. 2022-04-18]. Dostupné z: https://www.mesec.cz/clanky/elektronicke-obcanky-startuji-projdete-si-pruvodce-jsou-povinne-a-co-umi/

HOVORKA, Jiří a Petr KUČERA. Bankovní identitu nabídneme společně, dohodly se banky. *Peníze.cz* [online]. [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/osobni-ucty/424583-bankovni-identitu-nabidneme-spolecne-dohodly-se-banky

HOVORKOVÁ, Kateřina. Virus donutil řadu zemí zvýšit limity pro neověřené platby. Česko se však změně brání. *Aktuálně.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://zpravy.aktualne.cz/finance/rada-zemi-zvysila-limity-pro-platby-kartou-bez-overeni-ceske/r~f9bafb7aac9611ea8b230cc47ab5f122/

How to import data? *Spendee Help Center* [online]. [cit. 2021-02-22]. Dostupné z: https://help.spendee.com/article/121-import-transactions

HUANG, Henry a Nicole CHIANG. FinTech in China: overview. *Practical Law* [online]. [cit. 2022-12-29]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/w-019-4896?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_anchor_a205654

HUML, Tomáš. PSD2: Finální verze RTS k SCA – shrnutí zásadních změn. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/Deloitte_PSD2_Final_RTS_k_SCA_Souhrn_zasadnich_zmen_Technolog_Security.pdf

HUSZ, Orsi. Bank Identity: Banks, ID Cards, and the Emergence of a Financial Identification Society in Sweden. *Cambridge Core* [online]. 2018 [cit. 2022-04-18]. Dostupné z: https://www.cambridge.org/core/journals/enterprise-and-society/article/bank-identity-banks-id-cards-and-the-emergence-of-a-financial-identification-society-in-sweden/0D5AF7AE7F3D989ECF542DB5A461C278

CHVÁTAL, Dalibor Z. Fio banka zpřístupní bankovní identitu, zatím jen na žádost. *Měšec.cz* [online]. 2022 [cit. 2022-05-31]. Dostupné z: https://www.mesec.cz/aktuality/fio-banka-zpristupni-bankovni-identitu-zatim-jen-na-zadost/

Identita občana (eIdentita) a přihlášení do Agendového informačního systému MPO. *COVID Portál* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://covid.gov.cz/situace/podnikatelska-cinnost/eidentita-prihlaseni-do-agendoveho-informacniho-systemu-mpo

ILLING, Dawn. The Open Finance API & the requirement for eIDAS Certificates and Qualified Signature Creation Devices. *Utimaco* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://utimaco.com/current-topics/blog/open-finance-api-and-requirement-for-eidas-signtaure-devices

Index digitální ekonomiky a společnosti 2021: digitalizace se celkově zlepšila, ale je třeba vyvinout další úsilí v celé EU. *Kurzy.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.kurzy.cz/zpravy/618845-index-digitalni-ekonomiky-a-spolecnosti-2021-digitalizace-se-celkove-zlepsila-ale-je-treba/

Jak se staví evropské finanční právo k FinTech firmám? *Konečná & Zacha: Advokátní kancelář* [online]. [cit. 2021-02-22]. Dostupné z: https://www.konecna-zacha.com/jak-se-stavi-evropske-financni-pravo-k-fintech-firmam-/

Jak prosperovat v nejisté době. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-otevrene-bankovnictvi-a-psd2.pdf

Jsou otevřená data příležitostí pro banky? Největší festival nad otevřenými daty v ČR. *Česká spořitelna* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2017/11/23-1/nejvetsi-festival-nad-otevrenymi-daty-v-cr

Katalog služeb VS. *PMA3* [online]. [cit. 2022-04-18]. Dostupné z: https://pma3.gov.cz/katalog-sluzeb/info

KB nově umožňuje založit účet přes bankovní identitu. *Komerční banka* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2021/kb-nove-umoznuje-zalozit-ucet-pres-bankovni-identi

Kdo jsme a co děláme. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/co-delame

KLEE, Adrian. Asia is the next frontier in open banking. *Ross Republic* [online]. [cit. 2022-12-29]. Dostupné z: https://rossrepublic.com/asia-is-the-next-frontier-in-open-banking/

Komerční banka spolupracuje s BudgetBakers. In: *Komerční banka* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2019/komercni-banka-spolupracuje-s-budgetbakers

KORBEL, František, Jan TOPINKA, Štěpán ŠTARHA, Dalibor KOVÁŘ a Pavel AMLER. Zákon o právu na digitální služby a zákon o bankovní identitě. *Havel & Partners* [online]. 2019 [cit. 2022-05-21]. Dostupné z: https://www.havelpartners.cz/zakon-o-pravu-na-digitalni-sluzby-a-zakon-o-bankovni-identite/

KOVÁŘ, Dalibor a Pavel AMLER. Už jste slyšeli o nařízení eIDAS 2.0?. *Epravo.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.epravo.cz/top/clanky/uz-jste-slyseli-o-narizeni-eidas-20-113866.html

KOVÁŘ, Dalibor a Josef BOUCHAL. Jak se v praxi elektronicky podepisují mezinárodní transakce?. *Havel & Partners* [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.havelpartners.blog/blog/jak-se-v-praxi-elektronicky-podepisuji-mezinarodni-transakce/304

KŘÍŽ, Lukáš a David ZAJÍC. PSD2: malá revoluce v platebních službách. *Hospodářské noviny* [online]. [cit. 2021-03-16]. Dostupné z: https://ictrevue.ihned.cz/c3-65786220-0ICT00_d-65786220-psd2-mala-revoluce-v-platebnich-sluzbach

KUČERA, David a Aneta PRŮŠOVÁ. Výzvy a milníky nařízení eIDAS. Epravo.cz [online]. 2018 [cit. 2022-05-21]. Dostupné z: https://www.epravo.cz/top/clanky/vyzvy-a-milniky-narizeni-eidas-108441.html

KUČERA, Petr. První banka založí účet online i bez skenování dokladů. *Peníze.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/osobni-ucty/428654-prvni-banka-zalozi-ucet-online-i-bez-skenovani-dokladu

Kvalifikované elektronické podpisy dle nařízení eIDAS – nový požadavek na obsluhu Czech POINTu. *Czech POINT* [online]. 2018 [cit. 2022-04-18]. Dostupné

z: https://www.czechpoint.cz/public/kvalifikovane-elektronicke-podpisy-dle-narizeni-eidas-novy-pozadavek-na-obsluhu-czech-pointu/

Kvalifikovaní správci. *Informační web elektronické identity* [online]. [cit. 2023-07-29]. Dostupné z: https://info.identitaobcana.cz/KvalifikovaniSpravci.aspx

LANGEROVÁ, Jana. Co přinese novela o platebním styku? Žádné revoluční změny. *Podnikatel.cz* [online]. 2020 [cit. 2021-03-16]. Dostupné z: https://www.podnikatel.cz/clanky/co-prinese-novela-o-platebnim-styku-zadne-revolucni-zmeny/#h20

LANGEROVÁ, Jana. Je multibanking výhodou, nebo jen trendem? Zjistěte, kdo ho klientům nabízí. *Podnikatel.cz* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://www.podnikatel.cz/clanky/je-multibanking-vyhodou-nebo-jen-trendem-zjistete-kdo-jej-klientum-nabizi/

LECHNER, Tomáš. Elektronická identifikace od letošního pololetí jen kvalifikovaně. *SystemOnline.cz* [online]. [cit. 2022-05-21]. Dostupné z: https://www.systemonline.cz/sprava-dokumentu/elektronicka-identifikace-jen-kvalifikovane.htm

LEIXNEROVÁ, Lucie. PSD2: z jediné aplikace do všech bank bez rizika. *Světchytře.cz* [online]. 2018 [cit. 2021-03-14]. Dostupné z: https://www.svetchytre.cz/a/iji3L/psd2-z-jedine-aplikace-do-vsech-bank-bez-rizika

LÖRINCZ, Tomáš a Milan BAJÁK. Bankovní identita jako nová „digitální občanka“. Přelomový digitalizační projekt s názvem SONIA. *Český rozhlas Hradec Králové* [online]. 2019 [cit. 2022-05-21]. Dostupné z: https://hradec.rozhlas.cz/bankovni-identita-jako-nova-digitalni-obcanka-prelomovy-digitalizacni-projekt-s-7846983

LUMSDEN, Jaime a Michele LEVINE. FinTech in Australia: overview. *Practical Law* [online]. [cit. 2022-12-29]. Dostupné z: https://uk.practicallaw.thomsonreuters.com/w-015-9782?transitionType=Default&contextData=(sc.Default)&firstPage=true

MALIŠOVÁ, Kristina. Jaké povinnosti přinese nový zákon na ochranu oznamovatelů zaměstnavatelům?. *Právní prostor* [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-

pravo/jake-povinnosti-prinese-novy-zakon-na-ochranu-oznamovatelu-zamestnavatelum

MANČAŘ, Michal. Amazon otevřel svůj první evropský supermarket bez pokladen. Platba se provede automaticky při odchodu. *CzechCrunch* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://cc.cz/amazon-otevrel-svuj-prvni-supermarket-v-evrope-v-londyne-budou-zakaznici-platit-bez-pokladen/

MAREK, Tomáš. Jak na rozpáznávání textu zdarma (Free OCR). *Cnews*.cz [online]. 2012 [cit. 2022-04-17]. Dostupné z: https://www.cnews.cz/jak-na-rozpaznavani-textu-zdarma-free-ocr/

MATURA, Jan. PŘEHLEDNĚ: Jak aktivovat Apple Pay a jak jsou platby zabezpečené. *IDNES.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.idnes.cz/mobil/tech-trendy/apple-pay-v-cesku-videonavod.A190219_085956_mob_tech_jm

MLADĚNKA, Václav. PSD2 a (r)evoluce bankovnictví. *CFOworld.cz* [online]. 2020 [cit. 2021-03-16]. Dostupné z: https://www.cfoworld.cz/clanky/psd2-a-r-evoluce-bankovnictvi/

MONIOVÁ, Eva. Banky daly Čechům vstupenku do budoucnosti. Pustí vás i do zavřeného obchodu. *Seznam Zprávy* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.seznamzpravy.cz/clanek/zapomneli-jste-neco-koupit-obchod-vam-po-zaviracce-muze-odemknout-banka-167823

MORÁVEK, Daniel. Jak založit firmu? Od loňského září klidně online z obýváku. *Podnikatel.cz* [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.podnikatel.cz/aktuality/jak-zalozit-firmu-od-lonskeho-zari-klidne-online-z-obyvaku/

MOSNÁKOVÁ, Michaela. PSD2 a nová platební služba: Nepřímé udělení platebního příkazu. *Epravo.cz* [online]. 2018 [cit. 2021-03-06]. Dostupné z: https://www.epravo.cz/top/clanky/psd2-a-nova-platebni-sluzba-neprime-udeleni-platebniho-prikazu-107127.html

Možné využití bankovní identity nemá hranice. *E15.cz* [online]. [cit. 2022-05-21]. Dostupné z: https://www.e15.cz/byznys/finance-a-bankovnictvi/mozne-vyuziti-bankovni-identity-nema-hranice-1386250

Multibanking 2021: Jak funguje a které banky ho podporují? *Skrblík.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://www.skrblik.cz/finance/ucty/multibanking/

Naše projekty. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/nase-projekty

Nejčastější dotazy. *Informační web elektronické identity* [online]. [cit. 2022-04-18]. Dostupné z: https://info.identitaobcana.cz/faq/

Nejvyšší kontrolní úřad. *Souhrnná zpráva o digitalizaci veřejné správy v ČR* [online]. 2019 [cit. 2022-04-18]. Dostupné z: https://nku.cz/assets/publikace-a-dokumenty/ostatni-publikace/zprava-o-digitalizaci-verejne-spravy.pdf

Next-Generation Client Onboarding. *PwC* [online]. [cit. 2022-05-21]. Dostupné z: https://www.pwc.de/en/next-generation-client-onboarding.html

NOVÁK, Jaromír. Elektronická identita v džungli paragrafů [online]. [cit. 2022-05-21]. Dostupné z: https://www.nic.cz/files/nic/IT21/prezentace/Novak.pdf

NOVÁKOVÁ, Jolana. Otevřené bankovnictví: proč pouštět k penězům na účtu někoho cizího. *IDNES.cz* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.idnes.cz/finance/financni-radce/finance-radce-otevrene-bankovnictvi-bezpeci-ochrana.A180215_124706_viteze_kho

Novela poskytování služeb. *Euro.cz* [online]. [cit. 2021-03-16]. Dostupné z: https://www.euro.cz/archiv/novela-poskytovani-sluzeb-823214

NÝDRLE, Tomáš. Co přináší nový zákon o platebním styku? *Právní rádce* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://pravniradce.ihned.cz/c1-66010790-co-prinasi-novy-zakon-o-platebnim-styku

OCR use-cases: User onboarding with driver license scanning. *Visionify* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://visionify.ai/ocr-use-cases-user-onboarding-driver-license-scanning/

Online onboarding – Vítej nový kliente. *Freefintech.cz* [online]. 2017 [cit. 2022-05-21]. Dostupné z: https://www.freefintech.cz/index.php/2017/11/28/online-onboarding-vitej-novy-kliente/

Open banking's true story in Asia: emerging markets. *Digital Finance* [online]. [cit. 2022-12-29]. Dostupné z: https://www.digfingroup.com/open-banking-asia-2/

Otevřené bankovnictví. *Banka CREDITAS* [online]. [cit. 2023-07-30]. Dostupné z: https://www.creditas.cz/otevrene-bankovnictvi/

Otisky prstů i osobní údaje. Bezpečnostní firma nechala na internetu 23 gigabytů nechráněných dat. *IROZHLAS* [online]. [cit. 2021-02-22]. Dostupné z: https://www.irozhlas.cz/veda-technologie/hash-otisky-prstu-rozpoznani-obliceje-unik-dat-databaze-guardian-kauza-vedci_1908160800_mpr

OTTO, Pavel. Volby poštou, platy učitelů či whistleblowing. Nové poslance čeká spousta nedodělků. E15.cz [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.e15.cz/domaci/volby-postou-platy-ucitelu-ci-whistleblowing-nove-poslance-ceka-spousta-nedodelku-1384711

Our history. *BankID* [online]. [cit. 2022-04-18]. Dostupné z: https://www.bankid.com/en/om-oss/historia

Oznámení o udělení akreditace pro správu kvalifikovaného systému elektronické identifikace (poskytovatel: Česká spořitelna, a.s.). *Ministerstvo vnitra České republiky* [online]. [cit. 2022-04-18]. Dostupné z: https://www.mvcr.cz/clanek/oznameni-o-udeleni-akreditace-pro-spravu-kvalifikovaneho-systemu-elektronicke-identifikace-poskytovatel-ceska-sporitelna-a-s.aspx

PACHOLET, Martin. Stav multibankingu v ČR. *#fintechcowboys.cz* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://fintechcowboys.cz/stav-multibankingu-v-cr/

PETERKA, Jiří. Kam všude se s bankovní identitou (přes NIA) nedostanete?. *Lupa.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.lupa.cz/clanky/kam-vsude-se-s-bankovni-identitou-pres-nia-nedostanete/

PETERKA, Jiří. Přihlašování k službám přes internetbanking? Jak má fungovat SONIA?. *Lupa.cz* [online]. 2019 [cit. 2022-05-21]. Dostupné z: https://www.lupa.cz/clanky/prihlasovani-k-sluzbam-pres-internetbanking-jak-bude-fungovat-sonia/

PETERKA, Jiří. Unijní eIDAS přichází. O co přijdeme u elektronických podpisů?. *Lupa.cz* [online]. 2016 [cit. 2022-05-21]. Dostupné z: https://www.lupa.cz/clanky/unijni-eidas-prichazi-o-co-prijdeme-u-elektronickych-podpisu/

Platby po internetu mají být bezpečnější, nová pravidla schválila vláda. *Aktuálně.cz* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://zpravy.aktualne.cz/finance/platby-po-internetu-maji-byt-bezpecnejsi-nova-pravidla-schva/r~df8c3efe07d911e78af8002590604f2e/

PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra - I. část. *Právní prostor* [online]. 2020 [cit. 2022-04-18]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/podepisovani-soukromych-listin-vcera-dnes-zitra-i-cast

PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra - II. část. *Právní prostor* [online]. 2020 [cit. 2022-05-21]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/podepisovani-soukromych-listin-vcera-dnes-zitra-ii-cast

Podmínky používání NIA ID. *Informační web elektronické identity* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://info.identitaobcana.cz/podminky.aspx

POLÁK, Peter. Komentář: PSD2 jako inovace na úkor bezpečnosti? *Tyinternety* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://tyinternety.cz/technologie/komentar-psd2-jako-inovace-na-ukor-bezpecnosti/

POSPÍŠIL, Lukáš. Elektronické peníze versus Kryptoměna. *Epravo.cz* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicke-penize-versus-kryptomena-107930.html

Postupy „Poznej svého klienta“ (Know Your Customer, KYC). *BitEffect* [online]. [cit. 2022-05-21]. Dostupné z: https://biteffect.net/wp-content/uploads/2019/09/KYC_AML_CZ-1.pdf

PRESS RELEASE - Berlin Group starts new openFinance API Framework. *The Berlin Group* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework

PROCHÁZKA, Jan. PSD2 a GDPR: Harmonie, či disonance? *Právní rádce* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://pravniradce.ihned.cz/c1-65909940-psd2-a-gdpr-harmonie-ci-disonance

Projekt SONIA – příspěvek k rozvoji digitálního Česka [online]. [cit. 2022-05-21]. Dostupné z: http://www.finance-edu.cz/wp-content/uploads/2019/01/V%C5%A0E-konference-1.2.2019-final.pdf

PRŮŠA, Jiří. EIDAS a elektronická identifikace: dlouhá cesta k uznávání elektronických občanek. *Lupa.cz* [online]. 2016 [cit. 2022-05-21]. Dostupné z: https://www.lupa.cz/clanky/eidas-a-elektronicka-identifikace-dlouha-cesta-k-uznavani-elektronickych-obcanek/

První česká multibankovní aplikace Richee. Pro CREDITAS ji vytvořila česká IT společnost Cleverlance. *Cleverlance* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.cleverlance.de/cz/novinky/Stranky/Richee.aspx

Přes bankovní identitu nově i k lékaři. Lékařské vyšetření na dálku bude díky službě BankID rychlejší a bezpečnější. *EUC* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://euc.cz/clanky-a-novinky/clanky/pres-bankovni-identitu-nove-i-k-lekari-lekarske-vysetreni-na-dalku-bude-diky-sluzbe-bankid-rychlejsi-a-bezpecnejsi/

Příležitost s názvem PSD 2. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/legal/articles/psd2.html

PSD2 Access to Bank Accounts. *The Berlin Group* [online]. [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/psd2-access-to-bank-accounts

PSD 2 a nebankovní poskytovatelé po dvou letech – reakce ČNB. *Česká národní banka* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/PSD-2-a-nebankovni-poskytovatele-po-dvou-letech-reakce-CNB

PSD2 – Proč Se Divit. *Freefintech.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www.freefintech.cz/index.php/2017/12/10/psd2-proc-se-divit/

PSD2: What you need to know about Screen Scraping and API's. *Yapily* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.yapily.com/blog/psd2-screenscraping-apis/

RADA, Ivan a František TIKAL. K nové právní úpravě elektronického podpisu. *Epravo.cz* [online]. 2017 [cit. 2022-05-21]. Dostupné z: https://www.epravo.cz/top/clanky/k-nove-pravni-uprave-elektronickeho-podpisu-106077.html

Rámec pro otevřené financování – možnost sdílení údajů a přístupu třetích stran ve finančním odvětví. *Evropská komise* [online]. [cit. 2022-12-26]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13241-Ramec-pro-otevrene-financovani-moznost-sdileni-udaju-a-pristupu-tretich-stran-ve-financnim-odvetvi_cs

Reading Data From Identity Documents. *Innovatrics* [online]. [cit. 2022-04-17]. Dostupné z: https://www.innovatrics.com/digital-onboarding-toolkit/reading-data-from-identity-documents/

REEVES, Peter, Georgina WILLCOCK a Robert O'GRADY. The Financial Technology Law Review: Australia. *The Law Reviews* [online]. [cit. 2022-12-29]. Dostupné z: https://thelawreviews.co.uk/title/the-financial-technology-law-review/australia

Revision of the eIDAS Regulation: Findings on its implementation and application. *Evropský parlament* [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.europarl.europa.eu/thinktank/cs/document/EPRS_BRI(2022)699491

Revision of the eIDAS Regulation Findings on its implementation and application - BRIEFING. *Evropský parlament* [online]. 2022 [cit. 2022-04-18]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf

ROLANDS, Mesters. Europe needs free open banking and here's why. Financial Times [online]. [cit. 2022-12-26]. Dostupné z: https://www.ft.com/partnercontent/nordigen/europe-needs-free-open-banking-and-heres-why.html?utm_source=FB&utm_medium=fintech&utm_content=organic

ROSE, Kristýna. Banky vs. FinTech a nová evropská regulace: Ďábel se skrývá v detailu. *Roklen24.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://roklen24.cz/banky-vs-fintech-a-nova-evropska-regulace-dabel-se-skryva-v-detailu/

RTS and ITS. *Deutsche Börse Group* [online]. [cit. 2021-03-15]. Dostupné z: https://www.mds.deutsche-boerse.com/mds-en/RTS-and-ITS-1339928

Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. *Digitální a*

informační agentura [online]. [cit. 2023-07-29]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/povinne-zverejnovane-informace/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru/

Seznam udělených akreditací pro správu kvalifikovaného systému elektronické identifikace. *Ministerstvo vnitra České republiky* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://www.mvcr.cz/clanek/seznam-udelenych-akreditaci-pro-spravu-kvalifikovaneho-systemu-elektronicke-identifikace.aspx

Scoring u hypotéky. *Banky.cz* [online]. [cit. 2021-03-16]. Dostupné z: https://www.banky.cz/hypotecni-slovnik/scoring-u-hypoteky/

SECHTER, Jakub. Jak jsou české banky s nástupem PSD2 otevřené svým klientům? *Lupa.cz* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.lupa.cz/clanky/jak-jsou-ceske-banky-s-nastupem-psd2-otevrene-svym-klientum/

SKALKOVÁ, Olga. ČEZ zjednoduší zařizování. S Bank ID láká i na výhodnější ceny. *Peníze.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/spotrebitel/429123-cez-zjednodusi-zarizovani-s-bank-id-laka-i-na-vyhodnejsi-ceny

SKALKOVÁ, Olga. První banka spouští Sign. Smlouvu podepíšete jednoduše online. *Peníze.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.penize.cz/osobni-ucty/429350-prvni-banka-spousti-sign-smlouvu-podepisete-jednoduse-online

Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021. *Česká národní banka* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/

SOLTANI, Reza, Uyen TRANG NGUYEN a Aijun AN. A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* [online]. IEEE,

2018, 2018, 1129-1136 [cit. 2022-05-22]. ISBN 978-1-5386-7975-3. Dostupné z: doi:10.1109/Cybermatics_2018.2018.00205

SOUKAL, Marek. Silné ověření klienta při poskytování platebních služeb. *Epravo.cz* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

Správci informací o platebním účtu a pobočky zahraničních správců informací o platebním účtu (stav ke dni 29.07.2023). *Základní seznamy subjektů (výsledné sestavy)* [online]. [cit. 2023-07-29]. Dostupné z: https://apl.cnb.cz/apljerrsdad/JERRS.WEB15.BASIC_LISTINGS_RESPONSE_3?p_lang=cz&p_DATUM=29.07.2023&p_hie=HI&p_rec_per_page=25&p_ses_idx=355

SPV. Patria.cz [online]. [cit. 2022-04-17]. Dostupné z: https://www.patria.cz/slovnik/591/spv.html

Stanovy České fintech asociace, z.s., *Česká fintech asociace* [online]. [cit. 2021-03-15]. Dostupné z: http://czechfintech.cz/wp-content/uploads/2018/01/Stanovy_Ceska_fintech_asociace.pdf

STRACHAN, David. Open Banking around the world. *Deloitte* [online]. [cit. 2022-12-29]. Dostupné z: https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html

Studie Deloitte: České banky i uživatelé jsou na PSD2 v regionu nejlépe připraveni. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/press/articles/cze-tz-ceske-banky-i-uzivatele-jsou-na-psd2-v-regionu-nejlepe-pripraveni.html

Study on eID and digital on- boarding: mapping and analysis of existing on-boarding bank practices across the EU [online]. 2018 [cit. 2022-04-16]. ISBN SBN 978-92-79-77867-4. Dostupné z: https://ec.europa.eu/futurium/en/system/files/ged/study_on_eid_digital_onboarding_final_report.pdf

SVOBODA, Jakub. PIN při platbě kartou nad 500 korun zůstává, banky zvýšení limitu odmítly. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z:

https://www.novinky.cz/finance/clanek/pin-pri-platbe-kartou-nad-500-korun-zustava-banky-zvyseni-limitu-odmitly-40320375

ŠOVAR, Jan a Ondřej MIKULA. FinTech v Česku: Legislativní iniciativa míří výlučně z Bruselu. *Právní rádce* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-65872700-fintech-v-cesku-legislativni-iniciativa-miri-vylucne-z-bruselu

ŠTĚPÁNEK, Pavel a Josef DONÁT. Projekt SONIA: příspěvek bank k rozvoji digitálního Česka [online]. [cit. 2022-05-21]. Dostupné z: https://www.isss.cz/archiv/2019/download/prezentace/cba_dolejsi.pdf

Telemedicína Feedback. *WikiSkripta* [online]. [cit. 2022-04-18]. Dostupné z: https://www.wikiskripta.eu/w/Telemedic%C3%ADna

The eIDAS Regulation: A primer. *DocuSign* [online]. [cit. 2022-04-18]. Dostupné z: https://www.docusign.co.uk/learn/eidas-regulation-primer

TOBIN, Andy. EIDAS 2.0: How Europe can define the digital identity blueprint for the world. *Avast* [online]. 2022 [cit. 2022-05-21]. Dostupné z: https://blog.avast.com/eidas-2.0-avast

TOLLINGEROVÁ, Daniela. Živnostníci, spolky, nadace. Datové schránky musí od příštího roku začít používat na dva miliony lidí. *IROZHLAS* [online]. [cit. 2022-12-28]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/datove-schranky-info-2023povinnost-osvc_2212261748_ako

TOMÁNY, Lubomír. Blog: Bezpečnost a budoucnost digitálního onboardingu. *Banking Software Company (BSC)* [online]. [cit. 2022-05-21]. Dostupné z: https://www.bankingsoftware.company/cs/aktuality/budoucnost-digitalniho-onboardingu/

TOMÁNY, Lubomír. Blog: Digital onboarding v empatickém bankovnictví. *Banking Software Company (BSC)* [online]. 2019 [cit. 2022-05-21]. Dostupné z: https://www.bankingsoftware.company/cs/aktuality/blog-digital-onboarding-v-empatickem-bankovnictvi/

TÓTHOVÁ, Lucia. Jak těžké je získat PSD2 licenci? *#fintechcowboys.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://fintechcowboys.cz/rozhovor-jak-tezke-je-ziskat-psd2-licenci/

TRAN, Kristine. How are Australian Fintechs regulated?. *OpenLegal* [online]. [cit. 2022-12-29]. Dostupné z: https://openlegal.com.au/how-are-australian-fintechs-regulated/

TRNKA, Lukáš. Průvodce světem elektronické identity: Odborníci z MV ČR, NAKIT a AFCEA zveřejnili společně vytvořený dokument „Doporučení pro bezpečné nakládání s e-identitou“. *NAKIT* [online]. 2021 [cit. 2022-05-22]. Dostupné z: https://nakit.cz/pruvodce-svetem-elektronicke-identity/

Úvod. *Portál národního bodu* [online]. [cit. 2022-04-18]. Dostupné z: https://www.identitaobcana.cz/Home

VÁCLAVÍK, Radek. Multibanking: bankovní řešení rok a půl po PSD2. *Trask* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://www.trask.cz/publikace/multibanking-bankovni-reseni-rok-a-pul-po-psd2

VÁCLAVÍK, Radek. Stav PSD2 v českých bankách. *OpenAPI portál* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.apiportal.cz/novinky/stav-psd2-v-ceskych-bankach/

VANĚK, Ondřej. Efektivní digitální onboarding je počátkem dobrého a dlouhodobého vztahu se zákazníkem. *SystemOnline.cz* [online]. [cit. 2022-05-21]. Dostupné z: https://www.systemonline.cz/crm/efektivni-digitalni-onboarding.htm#zdroj01

VEJVODOVÁ, Alžběta. Platební revoluce se nekoná. O licence na nové služby není v Česku zájem. *Právní rádce* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-66152590-platebni-revoluce-se-nekona-o-licence-na-nove-sluzby-neni-v-cesku-zajem

VEINBENDER, Kristina. České banky přecházejí na videoporadenství. Přiměli je k tomu mladí zákazníci a pandemie. *E15.cz* [online]. 2021 [cit. 2022-04-17]. Dostupné z: https://www.e15.cz/byznys/ceske-banky-prechazeji-na-videoporadenstvi-primeli-je-k-tomu-mladi-zakaznici-a-pandemie-1384331

VITÁSEK, Petr. Martin Medek: Bankovní identita je Yetti naruby. *Pražský deník* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://prazsky.denik.cz/podnikani/martin-medek-bankovni-identita-je-yetti-naruby-20210220.html

Vítejte ve světě elektronické identifikace. *Informační web elektronické identity* [online]. [cit. 2022-05-21]. Dostupné z: https://info.identitaobcana.cz/

VOJTĚCH, Petr. Nový zákon o platebním styku v platnosti. *Epravo.cz* [online]. 2017 [cit. 2021-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-v-platnosti-106689.html?mail

VORLOVÁ, Lucie. Digitální právní jednání a písemná forma. *Epravo.cz* [online]. 2021 [cit. 2022-05-21]. Dostupné z: https://www.epravo.cz/top/clanky/digitalni-pravni-jednani-a-pisemna-forma-112802.html

Vybrat si peníze z nalezené anonymní vkladní knížky můžete i v roce 2016. *Česká spořitelna* [online]. 2015 [cit. 2022-04-17]. Dostupné z: https://www.csas.cz/cs/zpravy-z-banky/2015/12/30/vybrat-si-penize-z-nalezene-anonymni-vkladni-knizky-muzete-i-v-roce-2016#

Výpis z nezařazeného účtu online. *Centrální depozitář cenných papírů* [online]. [cit. 2022-04-18]. Dostupné z: https://www.cdcp.cz/nezarazeny-ucet-bankid/

Výpis ze spolkového rejstříku - Česká fintech asociace, z.s., L 66392 vedená u Městského soudu v Praze. *Veřejný rejstřík a sbírka listin* [online]. [cit. 2021-03-15]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=944463&typ=PLATNY

Vyřídit daně a podepsat smlouvy online. BankID šetří firmám čas i peníze, říká předseda představenstva Blažek. *Forbes* [online]. 2022 [cit. 2022-05-21].

What is Digital Onboarding?. In: Youtube [online]. Zveřejněno 09.06.2021 [cit. 2021-05-21]. Dostupné z: https://www.youtube.com/watch?v=EWV45KAU8B4

What is the Consumer Data Right?. *Office of the Australian Information Commissioner* [online]. [cit. 2022-12-29]. Dostupné z: https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right

Whistleblowing – účinný nástroj pro podporu zdravé a etické firemní kultury. *Deloitte Česká republika* [online]. [cit. 2022-04-17]. Dostupné z: https://akce.deloitte.cz/akce/21-03-17-whistleblowing-ucinny-nastroj-pro-podporu-zdrave-a-eticke-firemni-kultury/

WHITEHEAD, Ed. Why strong customer authentication benefits merchants. *FinTech Magazine* [online]. [cit. 2022-12-28]. Dostupné z:

https://fintechmagazine.com/digital-payments/how-strong-customer-authentication-benefits-merchants

WU, Brendon, Cloud LI, Joanna JIANG a Dimitri PHILLIPS. China: Fintech. *The Legal 500* [online]. [cit. 2022-12-29]. Dostupné z: https://www.legal500.com/guides/chapter/china-fintech/

Založení bankovního účtu online trvá 17 minut. Přes aplikaci to umí pouze čtyři banky. *E15.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.e15.cz/byznys/finance-a-bankovnictvi/zalozeni-bankovniho-uctu-online-trva-17-minut-pres-aplikaci-to-umi-pouze-ctyri-banky-1381663

Založení SRO online - úvodní informace. *Notářská komora České republiky* [online]. [cit. 2022-04-18]. Dostupné z: https://www.nkcr.cz/sro-online-informace

Zaručený digitální podpis SIGN spouštějí první tři banky. *BankID.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.bankid.cz/novinky/zaruceny-digitalni-podpis-sign-spousteji-prvni-tri-banky

Zájem o sčítání lidu online překonal očekávání. Výsledky budou na přelomu roku. *E15.cz* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.e15.cz/domaci/zajem-o-scitani-lidu-online-prekonal-ocekavani-vysledky-budou-na-prelomu-roku-1376628

Základní údaje o sběru elektronických sčítacích formulářů při sčítání lidu, domů a bytů 2011. *SLDB 2011* [online]. [cit. 2022-04-18]. Dostupné z: https://www.czso.cz/csu/sldb/zakladni_udaje_o_sberu_elektronickych_scitacich_formularu_pri_sldb2011

ZÁMEČNÍKOVÁ, Inka a Konstantin LAVRUSHIN. FinTech část I. – definice a subjekty. *Epravo.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www.epravo.cz/top/clanky/fintech-cast-i-definice-a-subjekty-106711.html

Zapomenuté miliardy [online]. [cit. 2022-04-18]. Dostupné z: https://www.zapomenutemiliardy.cz/

ZATLOUKAL, Jiří. Pokračuje propouštění v bankách. Komerčka se zbaví čtvrtiny zaměstnanců. *Seznam Zprávy* [online]. 2021 [cit. 2021-02-22]. Dostupné z: https://www.seznamzpravy.cz/clanek/pokracuje-propousteni-v-bankach-komercka-se-zbavi-ctvrtiny-zamestnancu-142061

ZATLOUKAL, Jiří. Rodí se Sonia. Největší banky v Česku chtějí společnou firmou rozhýbat digitalizaci státu. *Euro.cz* [online]. [cit. 2022-05-21]. Dostupné z: https://www.euro.cz/byznys/rodi-se-sonia-nejvetsi-tuzemske-banky-chteji-spolecnou-firmou-rozhybat-digitalizaci-statni-spravy-1434456

ZHOU, Qian. A Close Reading of China's Fintech Development Plan for 2022-2025. *China Briefing* [online]. [cit. 2022-12-29]. Dostupné z: https://www.china-briefing.com/news/a-close-reading-china-fintech-development-plan-for-2022-2025/

Judikatura

Nález Ústavního soudu ze dne ze dne 06.02.2020, sp. zn. I. ÚS 1833/18.

Usnesení Nejvyššího soudu ze dne 24.02.2009, sp. zn. 29 Cdo 4993/2008.

Usnesení Nejvyššího soudu ze dne 26.05.2009, sp. zn. 29 Cdo 1680/2009.

Usnesení Nejvyššího soudu ze dne 19.12.2013, sp. zn. 29 Cdo 1953/2013.

České časopisecké články

KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan, AMLER, Pavel. Elektronická identita při elektronickém (hmotně)právním jednání. Právní rozhledy, 2019, č. 18, s. 626-632.

KORBEL, František, KOVÁŘ, Dalibor. Právní úprava tzv. bankovní identity. Bulletin advokacie, 2021, č. 4, s. 17-23.

SMEJKAL, Vladimír. Kryptografický a dynamický biometrický podpis podle platné právní úpravy. Právní rozhledy, 2019, č. 10, s. 343-351.

TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. Právní rozhledy, 2018, č. 5, s. 160-167.

TRSEK, Jakub. Digitalizace a on-line onboarding. Bankovnictví. 2019, 2019(12).

VRÁBLIKOVÁ, Petra. Kontrola klienta a náhradní způsoby identifikace a kontroly klienta podle AML zákona – část druhá. Bulletin advokacie, 2021, č. 5, s. 9-15.

Seznam obrázků