ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

Bankovní podvody

Banking Frauds

Daniela Platzová

Plzeň 2022

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma

„Bankovní podvody“

vypracoval/a samostatně pod odborným dohledem vedoucí/vedoucího diplomové práce za použití pramenů uvedených v přiložené bibliografii.

Plzeň/Cheb dne .....

podpis autora/autorky

Poděkování

Tímto bych ráda poděkovala paní Ing. Janě Šturcové, Ph.D., za odborné vedení, poskytnuté konzultace a ochotu, které přispěly k vypracování celé práce.

Obsah

Úvod

Při vyslovení pojmu banka mnohým vyvstanou na mysli peníze, vklady a úvěry. I když se může zdát, že banky existují jen proto, aby získávaly co největší sumy finančních prostředků od svých klientů, jejich působnost je ve skutečnosti mnohem větší. Zvláštní charakteristikou bankovního sektoru je jeho schopnost přelévat se do celého finančního trhu, ale i daleko za jeho hranice do dalších sektorů. V tržním hospodářství zastává bankovnictví mimořádně významnou pozici, neboť jeho podoba do značné míry ovlivňuje stabilitu celé ekonomiky státu a určuje dynamiku hospodářského vývoje.

Stejně tak jako jsou podvody a nelegální aktivity přítomny ve všech odvětvích národního hospodářství, nevyhýbají se ani bankovnímu sektoru. Ba naopak, pravděpodobně neexistuje odvětví, které by bylo atraktivnějším cílem kriminálníků. Tato skutečnost je dána už samotnou povahou tohoto sektoru – vše v něm se točí okolo peněz.

Vzhledem k tomu, že je bankovní systém velmi fragilní a citlivý na řadu vnitřních i vnějších vlivů, přičemž jeho narušení může mít devastující účinky až na národní úrovni, o důležitosti a aktuálnosti tématu není pochyb. A navíc, jedná se o systém, do kterého se nějakým způsobem zapojuje každý jeden z nás.

Autorka nejprve provedla literární rešerši, na jejíž základě přináší čtenáři přehled o uvedeném tématu. Za účelem objasnění problematiky bankovních podvodů je nejprve proveden úvod do bankovnictví se zaměřením na jeho specifika. Následně autorka vysvětlí problematiku bankovní regulace a dohledu. Významněji se bude autorka věnovat konkrétně systému regulace a dohledu bank v České republice. V závěru kapitoly pak nastíní tématiku bankovní unie.

Zvláštní pozornost je věnována kapitole o podvodných jednáních v bankovním sektoru. Budou představeny nejčastější druhy bankovních podvodů ve členění na podvody páchané bankou, podvody páchané vůči bance, podvody páchané na klientech banky a nové formy podvodů páchaných na klientech banky.

V poslední části práce bude představen vlastní výzkum autorky, jehož bodem zájmu je chování klientů bank ve vztahu k bezpečnosti v bankovním styku na příkladu České republiky a Francie. Na závěr bude provedena sumarizace zjištěných poznatků a odhad budoucího vývoje.

Cíl práce a použitá metodika

Předložená diplomová práce vychází z předpokladu systematického zpracování teoretických východisek pro vytvoření vlastní práce. Teoretická východiska jsou zpracována na základě rešerše odborné literatury zaměřené na problematiku definice základních témat samostatného výzkumu.

Zpracováním teoretické části práce je upřesněn cíl diplomové práce a jeho následné dosažení v praktické části práce.

Při psaní teoretické části práce byla využita metoda dedukce, u které se vychází z obecnějších závěrů k méně obecným. Mimo metody dedukce je v práci použita také metoda dotazníkového šetření.

Hlavním cílem předložené práce je objasnit chování klientů bank ve vztahu k bezpečnosti v bankovním styku na příkladu České republiky a Francie.

Dílčí cíle, jejichž prostřednictvím bude dosaženo hlavního cíle, jsou:

- vymezit pojmy, které se vztahují k problematice bankovních podvodů;
- posoudit, jak se klienti bank orientují v problematice podvodných činností v bankovním styku;
- zhodnotit zodpovědnost chování klientů bank v bankovním styku;
- zjistit, jakými způsoby se klienti bank angažují do zajištění bezpečnosti jejich bankovních aktivit;
- porovnat postoje a chování klientů bank v českém a francouzském prostředí.

1 Úvod do bankovnictví

Autorka nejdříve stručně charakterizuje finanční trh a představí jeho základní dělení. Do kontextu finančního trhu dále zasadí právě sektor bankovnictví, který je pro účely této práce stěžejní problematikou. Představí specifika sektoru, vymezí pojem banka a jmenuje základní funkce banky. V závěru kapitoly se autorka bude věnovat bankovní soustavě se zaměřením na centrální banku.

1.1 Charakteristika finančního trhu a jeho dělení

Ještě před tím, než se autorka ponoří do sektoru bankovnictví, považuje za důležité čtenáři představit jemu nadřazený finanční trh.

Autorka nejprve uvádí definici Bakeše a Karfíkové (2012, s. 102), podle kterých lze finanční trh vymezit jako „systém vztahů, nástrojů, subjektů a institucí, umožňující shromažďování, soustřeďování, rozdělování a rozmisťování dočasně volných peněžních prostředků na základě nabídky a poptávky “.

Pro porovnání autorka dále cituje definici Revendy, Mandela, Kodery, Musílka a Dvořáka (2012, str. 71): „Finanční trhy můžeme vymezit jako systém institucí a instrumentů zabezpečujících pohyb peněz a kapitálu prostřednictvím různých finančních instrumentů mezi ekonomickými subjekty na základě nabídky a poptávky“.

Na takovém finančním trhu dle Zrůsta (2019, s. 9) dochází k přelévání finančních prostředků od těch, jež jich mají přebytek, k těm, jež jich mají nedostatek. Dochází tak k procesu směny, přičemž na straně nabídky tedy stojí přebytkové subjekty a na straně poptávky ty deficitní. K této činnosti obě strany potřebují finanční instrumenty. Finanční trh je tu zjednodušeně od toho, aby přebytkové subjekty byli motivování k tvorbě úspor a na druhou stranu deficitní subjekty měly motiv k získávání financí pro své investiční či spotřební výdaje prostřednictvím půjček.

Z uvedených definic je zřejmé, že finanční trh umožňuje pohyb kapitálu jakožto jednoho z výrobních faktorů, a proto Bakeš a Karfíková (2012, s. 102) doplňují, že jej tedy lze postavit hned vedle trhu práce a trhu zboží a služeb.

Podle Poloučka, Fraita, Skaunice, Stavárka a Vodové (2013, str. 7) mají finanční instituce dvě základní funkce: **transakční** a **zprostředkovatelskou**. Tato informace je zcela v souladu s výše uvedenou definicí. Transakce totiž představuje platbu, jež vede

k vyrovnání subjektů obchodu (pomocí finančních instrumentů) a zprostředkování pak kolekci vkladů jakožto úspor a jejich transformaci na investice. Autoři zde mluví o finančních institucích, ale stejně se dle nich mohou přetvářet úspory i na finančních trzích. Čtenář by nyní mohl být překvapen a tápat, z jakého důvodu jsou tyto termíny oddělené. Pro objasnění lze zhlédnout přílohu A.

Také Zrůst (2019, s. 9) ve své publikaci pojednává o funkcionalitě trhu financí, konkrétně z hlediska ekonomického. Finanční trh dle něho zajišťuje **determinaci ceny** (na základě střetu nabídky a poptávky), **redukci transakčních nákladů** (tedy vyhledávacích a informačních nákladů) a **likviditu** (deficitní i přebytkové subjekty mohou relativně rychle reagovat na změny a měnit své portfolio).

Revenda et al. (2012, s. 71) tvrdí, že se finanční trh nejčastěji člení na **trh peněžní, kapitálový a úvěrový**. Nezapomínají však zmínit, že tato segmentace není zdaleka ta jediná. Jednotlivé dílčí trhy od sebe totiž nejsou jednoznačně oddělené. Na národním trhu je jejich prolínání způsobeno zejména vstupováním stále nových finančních produktů, které figurují ve více různých částech finančních trhů zároveň. Na mezinárodní úrovni je poté řeč o prolínání z důvodu globalizace národních trhů.

Nejednoznačnost členění finančního trhu dokazuje například odlišná segmentace Rejnuše (2014), podle něhož ho lze rozdělit následovně:

- **trh peněz** (trh úvěrů a trh cenných papírů krátkodobého časového horizontu);
- **kapitálový trh** (trh úvěrů a trh cenných papírů dlouhodobého časového horizontu);
- **trh s cizími měnami** (trhy valutové a trhy devizové);
- **trh drahých kovů** (nejvýznamnější je trh zlata a trh stříbra).

Jak si čtenář může snadno všimnout, v každém segmentu se objevuje banka jakožto jeden z hlavních aktérů.

1.2 Charakteristika sektoru bankovnictví

Jako se sektor financí významně liší od ostatních sektorů ekonomiky, liší se v jeho rámci i banky od ostatních finančních subjektů.

1.2.1 Specifika sektoru

Skutečnosti, které podle Revendy a dalších (2012, s. 263-265) bankovnictví odlišují od ostatních sektorů ekonomiky, jsou následující:

- vydávání peněz (nabídka peněz je důležitým makroekonomickým aspektem);
- zajišťování platebního styku (nezbytného pro každé hospodářství);
- disponování cizími prostředky (velká rizikovost poškození vkladatelů);
- zvláštní struktura majetku (velký podíl krátkodobých pasiv a dlouhodobých aktiv);
- vysoká ziskovost (větší náchylnost k podvodům);
- extrémní dopady na celou ekonomiku v případě krachu.

Mnoho autorů vyzdvihuje **informační asymetrii** (více viz Kapitola 2.2).

Srovná-li se banka s nějakou firmou provádějící podobné aktivity, lze najít další zásadní rozdíly. Jeden z nich je patrný z výroku Zrůsta (2019, s. 24): „Je důležité si uvědomit, že banky neobchodují jen s penězi, ale v převážné míře i s riziky“. Tato rizika však nejsou hrozbou pouze pro banky samotné, ale také pro celé hospodářství země. Zatímco banky jsou vzájemně propojené platebním systémem, nebankovní subjekty se této systémové integraci vyhýbají. Jsou tak ve značné míře osvobozeny od kritického **systémového rizika** (Jurošková, 2012, stránky 14-15).

Termínem často skloňovaným právě v sektoru bankovnictví je tzv**.** „**run na banku**“. Představuje to situaci, kdy si klienti náhle začnou vybírat své vložené prostředky z důvodu strachu z nesolventnosti banky. Ocitne-li se totiž jedna banka ve finanční tísni, snadno se kvůli vzájemné provázanosti platebního systému v problémech ocitnou i ty další. Klienti jsou si tohoto řetězového efektu dobře vědomi (Zrůst, 2019, str. 25).

Tento fenomén úzce souvisí s **existencí velké míry důvěry**. Banka totiž spoléhá na to, že nedojde k vybrání depozit velkého množství vkladatelů ve stejný časový okamžik. Na tomto základě si tvoří rezervy pouze z malé části vkladů, tedy pouze v takovém objemu, který je nezbytný k uspokojení současných klientských potřeb (Zrůst, 2019, str. 26). Jurošková (2012, s. 15) se k témuž vyjadřuje ve své publikaci a uvádí, že „Fungování bank je tak založeno na iluzi, že vkladatelé mají okamžitý přístup ke svým penězům, ačkoli ve skutečnosti jsou jejich peníze půjčovány dále a budou splaceny někdy v budoucnu“, což dále doplňuje o výrok Goodharta (1999), „Občas se stane, že tato iluze rozplyne […] a domeček z karet se zhroutí“.

Typickým znakem bankovního sektoru je dle Zrůsta (2019, s. 25) také to, že jeho struktura vykazuje znaky **oligopolu**. To znamená, že výsadní postavení na trhu zaujímá pouze několik málo bank. Tento typ struktury vytváří nevýhodné prostředí pro bankovní klienty (vysoké poplatky apod.). Reakcí na tento trend však v posledních letech začaly na trh

vstupovat nové banky, které vsadily na nabídku klientsky atraktivnějších bankovních produktů (Air Bank, Fio banka apod.).

Další skutečností charakteristickou pro sektor bankovnictví je dle Mejstříka, Pečené a Teplého (2008, s. 164) **mimořádně nízký podíl vlastního kapitálu na celkových pasivech banky** (více viz Kapitola 2.2).

Jurošková (2012, s. 15) v otázce specifik bankovnictví pojednává také o velmi omezené možnosti zpeněžení majetku banky. Půjčky, jež tvoří obrovskou část jejích aktiv, nelze jednoduše prodat.

Bankovní systém je dále charakteristický **platbami uskutečňovanými i daleko přes hranice státu**, ve kterém banka primárně působí. Transakce klidně může být zadána v pravomoci jedné země, řízena ve druhé a skutečně provedena opět v jiné. To vše navíc může zvládnout sám klient a banka tedy do tohoto procesu ani nemusí zasáhnout (Zrůst, 2019, str. 25).

Vzhledem k podstatě banky jako takové a faktu, že se vše v ní točí okolo finančních nástrojů a nemalých sum finančních prostředků, se jedná o velmi **lákavé prostředí pro nelegální obchodní praktiky** (Zrůst, 2019, str. 25).

Na základě výše uvedených skutečností není překvapivé, že je žádoucí bankovní sektor důsledně regulovat a dohlížet na něj. Rizika plynoucí z bankovních aktivit je možné tímto způsobem redukovat nebo je přinejmenším lépe řídit (Zrůst, 2019, str. 26).

Pro lepší úvod do sektoru bankovnictví mimo výše zvýšená specifika sektoru lze v příloze B zhlédnout základní definice banky a její funkce.

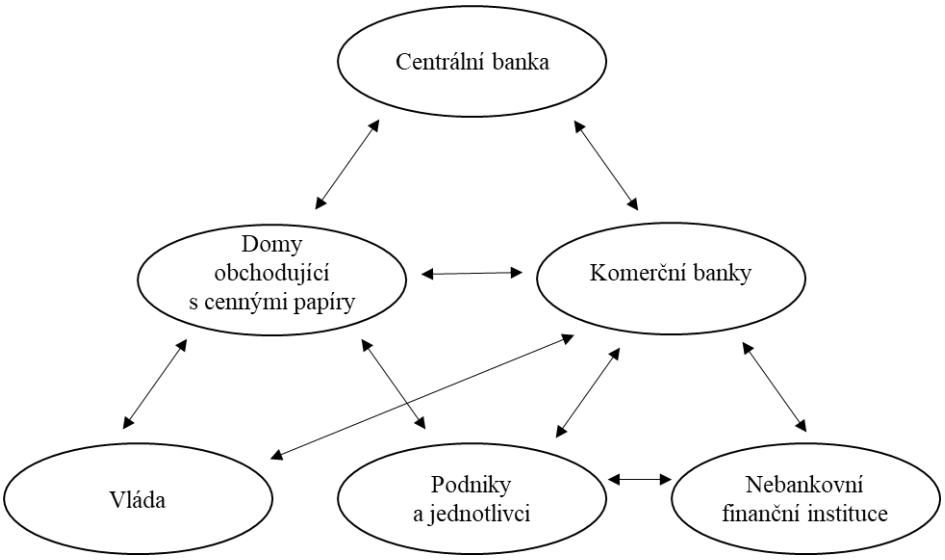
1.3 Bankovní soustava se zaměřením na centrální banku

Bankovní soustava se skládá z centrální banky a komerčních bank v dané zemi operujících. Pozice bank v České republice je definována v zákonu o bankách. Každá banka vystupuje na trhu financí jako jedna z částí bankovního systému, který je vysoce náročný na regulaci (Zrůst, 2019, str. 21). Revenda a další (2012, str. 88) navíc do soustavy započítávají i vztahy bank k ostatním subjektům, tedy domácnostem, státu, firmám apod.

Takto postavený bankovní systém se nazývá dvoustupňovým a je přítomen v každé rozvinuté ekonomice. „**Dvoustupňový bankovní systém** spočívá na institucionálním

oddělení makroekonomické funkce, kterou zabezpečuje centrální banka, a mikroekonomické funkce, která je doménou sítě komerčních bank“ (Revenda et al., 2012, s. 88). Postavení centrální banky a komerčních bank na trhu peněz znázorňuje následující schéma.

Obr. č. 1: Postavení centrální banky a komerčních bank na trhu peněz



Zdroj: Choudhry (2012, s. 24), zpracováno autorkou

Centrální banky jsou mimořádně důležitým prvkem nejen bankovního systému, ale i celého finančního trhu. Její politika má vliv na množství peněz v ekonomice, úrokové sazby a množství nabízených úvěrů. Všechny tyto faktory působí na makroekonomické ukazatele, jejichž příkladem může být inflace, hrubý domácí produkt apod. V korespondenci centrální banky je široká škála činností, pro zjednodušení autorka uvádí základní členění Mejstříka (2008, s. 102). Dvě **základní funkce centrální banky** podle něho jsou:

- vykonávání měnové politiky;
- regulace bankovních a dalších finančních institucí.

Seznam pravomocí centrálních bank tak, jak jich postupně přibývalo, uvádí Janáček (2020). Jejich výčet doplněný o kritický pohled na makroobezřetnostní politiku centrální banky lze najít v Příloze C. Tento autor dále hovoří o tzv. trilematu centrálního bankovnictví (viz příloha D).

Statut centrální banky má v České republice Česká národní banka (dále jen ČNB). Jak zdůrazňuje Mejstřík a další (2008, s. 56), existují různé druhy bank, ale na ČNB je třeba pohlížet separátně. V České republice fungují také zahraniční banky ve formě poboček,

které k témuž získají povolení od ČNB. Banky působící v rámci EU jsou od povinnosti získání licence oproštěny.

Nahlédnutím do Zákona č. 6/1993, o České národní bance, lze výše uvedené pravomoci centrální banky ověřit. Dle tohoto zákona mezi úkoly ČNB patří:

- určování a provádění monetární politiky;
- emitování bankovek a mincí;
- řízení platebního styku, peněžního oběhu a zúčtování bank (a dalších subjektů v zákoně specifikovaných, např. spořitelen) – zajišťování plynulosti, bezpečnosti, spolehlivosti, účinnosti a hospodárnosti;
- dohlížení na subjekty účinkující na trhu financí;
- sledování rizikového prostředí, diagnostika rizik, hodnocení vlivu rizik na finanční stabilitu, prevence vzniku rizik a jejich redukce;
- další činnosti v tomto zákoně a jiných právních předpisech uvedených.

Janáček (2020, stránky 75-79) se ve své publikaci zabývá otázkou, zda jsou centrální banky stále tak důležité a efektivní, jako tomu bývalo dříve. Uvádí několik problematických okolností, se kterými se v současnosti banky musejí potýkat. Jejich výčet je k dispozici v příloze E.

Revenda a další (2012, str. 88) z hlediska účelu rozlišují centrální banku od komerční tak, že centrální banka usiluje o cenovou a měnovou stabilitu a komerční banka usiluje o dosažení zisku.

Revenda a další (2012, s. 88) dále uvádějí dva modely používané v bankovnictví, přesněji řečeno **model univerzálního bankovnictví** a **model odděleného bankovnictví**. Aktuálně ve světových ekonomikách jasně převládá první z uvedených. Jeho princip spočívá v tom, že banky provádějí celou škálu aktivit, tedy jak služby typické pro komerční banky, tak i služby typické pro investiční banky. Ve výčtu produktů univerzální banky tím pádem lze najít poskytování úvěrů, zajišťování platebního styku, přijímání vkladů, obchodování s emisemi, stejně tak jako správu majetku, nákup a prodej investičních instrumentů (cenných papírů), jejich úschovu (depotní služby) a fúze a akvizice.

2 Bankovní regulace a bankovní dohled

„Finanční trhy jsou stroje, ve kterých se rozhoduje o velké části lidského blaha; přesto víme více o tom, jak fungují motory našich aut než o tom, jak funguje náš globální finanční systém. Potácíme se od krize ke krizi. V propojeném světě se chaos na jednom trhu okamžitě šíří na všechny ostatní – a máme jen mlhavé představy, jak se to děje nebo jak to regulovat.“ (Mandelbrot & Hudson, 2004, s. 255, vlastní překlad)

Aby čtenář získal přehled o tom, jak funguje systém regulace a bankovního dohledu, předkládá mu autorka následující kapitolu. Nejprve budou vymezeny hlavní cíle regulace a představeny základní články tohoto složitého systému. Následně autorka představí důvody pro regulaci bank, nevynechá však ani nejznámější argumenty proti regulaci. Objasněna bude také problematika bankovního dohledu. Autorka se poté zaměří na systém regulace a dohledu, jež funguje v České republice. Závěr kapitoly poskytne úvod do tématiky bankovní unie.

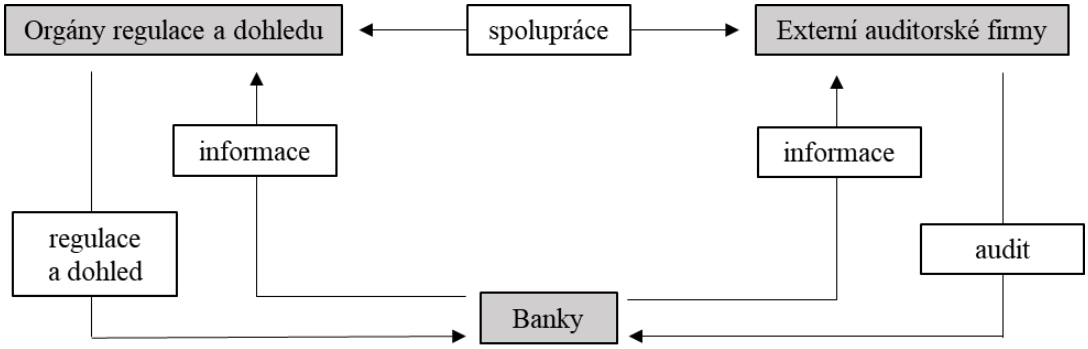
2.1 Obecné cíle, základní články systému

Hlavním cílem nejen bankovní regulace, ale i bankovního dohledu, je jak na úrovni České republiky tak i Evropské Unie „chránit stabilitu celého bankovního systému a přispívat ke stabilitě celého finančního systému“ (Mejstřík, 2008, s. 166).

Blahová (2018, s. 18) ve své publikaci tvrdí: „Regulace bank by měla přispívat k zabezpečení spolehlivosti a efektivnosti bankovního systému. Přestože aplikaci regulatorních pravidel ve stále větší míře předchází analýza jejich potenciálních dopadů, nedaří se vždy tohoto optimálního cíle dosáhnout.“

Do procesu regulace a dohledu se dle Revendy (2012, s. 247) zapojují tři třídy subjektů. Které to jsou a jaké jsou mezi nimi vazby lze vidět na následujícím schématu.

Obr. č. 2: Články procesu regulace a dohledu bank



Zdroj: Revenda et al. (2012, s. 248), zpracováno autorkou

Orgány regulace jsou centrální banky, které mohou, ale nemusí současně zastávat i pozici supervizora. Orgány bankovního dohledu pak mohou, ale nemusejí být totožné s orgány dohledu nad celým finančním trhem. V případě, že bankovním dohledem není pověřena centrální banka, ujímá se této zodpovědnosti jiná specializovaná instituce (nebo i více institucí najednou), která však s centrální bankou musí minimálně kooperovat. Na místě bank v uvedeném schématu je možné si představit i spořitelny či mezinárodní bankovní holdingy. Externí auditorské firmy kontrolují, zda jsou bankovní výkazy korektní, pravdivé, obsahují vše nezbytné a zabývají se managementem rizik banky (Revenda, 2012, s. 247-248).

2.2 Důvody pro regulaci bank

Podle Juroškové (2012, s. 18) lze za hlavní důvod regulatorních zásahů do fungování bank považovat existenci tržních selhání, se kterými se musejí ekonomiky potýkat. Regulace je tu od toho, aby těmto selháním předcházela, či v případě jejich vzniku zmírňovala jejich dopady.

Jak je tomu známo u každého jiného odvětví, za vznikem selhání stojí podle Blahové (2018, s. 13) zpravidla jeden, nebo více ze tří faktorů:

- **existence externalit;**
- **asymetričnost informací;**
- **zneužití tržní síly** (dle Zrůsta (2019, s. 55) se jedná zejména o insider dealing a manipulaci s trhem, jež blíže popisuje kapitola 3.2.1)

Ochrana banky před **negativními externalitami** spočívá v ochraně věřitelů v případě krachu banky, přičemž věřiteli jsou zejména její vkladatelé, ale i další subjekty, jako

například držitelé dluhopisů vydaných bankou (Blahová, 2018, s. 13). Negativní externality souvisejí především se systémovým rizikem, jinak řečeno dominovým efektem. Je důležité si uvědomit, že případné selhání banky neohrožuje pouze věřitele banky, ale následně také ostatní úvěrové instituce, a v konečném důsledku celý bankovní sektor (Jurošková, 2012, s. 19).

Oproti tomu Revenda a další (2012, s. 263-265) dělí důvody pro regulaci bankovního sektoru do následujících čtyř skupin:

- **odlišnost bankovních aktivit** (jmenovány v kapitole 1.1.1);
- **zpomalení procesu poklesu zprostředkování** (proces poklesu je omezován zvýhodňováním bank nad ostatními články finančního oběhu, např. v podobě pojištění vkladů a spolehnutí se na podporu od centrální banky v případě potřeby);
- **provádění měnové politiky centrální bankou** (což bez doprovodu regulace a dohledu není reálné);
- **vysoký stupeň informační asymetrie** (viz dále).

Autorka pro úplnost lépe vysvětlí problematiku **asymetrie informací**.

Polouček a další (2013, str. 14) vysvětlují, že asymetrie informací vychází zejména ze dvou skutečností. Tou první je, že kromě veřejných informací existují také informace soukromé, tedy takové, ke kterým nemá přístup každý. Držitelé soukromých informací tuto výhodu mohou při uzavírání smluv zužitkovat ve svůj prospěch. Druhou skutečností pak je, že chování účastníků obchodu není vždy možné důsledně sledovat. Vysvětlená informační nerovnováha významně křiví okolnosti hospodářské soutěže.

Aby autorka vztáhla asymetričnost informací konkrétně na bankovnictví, uvádí tvrzení Mejstříka et al. (2008, s. 164): „Zásadním problémem v bankovnictví je vyhrocenější informační asymetrie v tzv. problému principála a agenta (kdy muže jít o vztah věřitele a dlužníka, vkladatele a banky, vlastníků a managerů banky, ústředí a poboček banky“.

Jak tvrdí Revenda a další (2012, s. 264), „Především drobní vkladatelé nemají ve srovnání s bankami příliš možností dostatečně dobře „monitorovat“ zdraví banky a rizikovost jejich vkladů roste“.

Pod asymetrií informací si čtenář může mylně představit nedostatek informací pouze na straně klientů banky. Ve skutečnosti se však jedná o asymetrii oboustrannou. Jak ale tvrdí Zrůst (2019, s. 25), větší míra znevýhodnění je na straně klienta. Klient nemá veškeré

informace o bance, jen těžko posuzuje míru rizik, kterým banka čelí, chybně přistupuje k rozložení svého majetku, či nedostatečně chápe charakteristiky jednotlivých bankovních produktů. Na straně banky vzniká asymetrie informací z toho důvodu, že banka je zcela závislá na platební schopnosti klientů, přičemž právě sami klienti o sobě tento zásadní údaj poskytují (Blahová, 2018, s. 14). Navíc největší míru úvěrového rizika bance přináší ti, kteří o úvěr žádají nejčastěji a nejúporněji (Mejstřík, 2008, s. 166). V případě uzavření kontraktu mezi oběma stranami vzniká bance povinnost vynakládat finanční prostředky na kontinuální sledování situace klienta, aby byla schopna včas identifikovat jeho možnou neschopnost splácení dluhu (Blahová, 2018, s. 14).

Rejnuš (2014, s. 702) mezi důvody nutnosti bankovní regulace řadí také **zneužití dominantního postavení na trhu**, jež je dle něho jeden z faktorů selhání trhu. Jeho existence totiž negativně ovlivňuje hospodářskou soutěž, neboť způsobuje, že subjekt v dominantním postavení získává konkureční výhodu.

Mejstřík, Pečená a Teplý (2008, s. 164) pro vyjádření fragility bankovnictví a vyzdvižení nutnosti regulace také konstatují, že „Rizika nesolvence a nelikvidnosti, ale i nestability bankovního sektoru prohlubuje **mimořádně nízký podíl vlastního kapitálu na celkových pasivech banky**.“ Je však pravdou, že v porovnání s podniky v jiných odvětvích jsou aktiva banky více likvidní a diverzifikovaná, některá dokonce zcela bezriziková (vládní dluh). Naprostá většina zdrojů, se kterými banka disponuje, je cizího původu. Až 90 % těchto zdrojů, které bance umožňují být podnikatelsky činnou, je tvořeno vklady veřejnosti. Banka je tak vystavena nadměrně vysokému riziku zkrachování (Zrůst, 2019).

2.2.1 Rizika v bankovní praxi se zaměřením na provozní riziko

Nutná existence regulatorních pravidel úzce souvisí s riziky, která v bankovní praxi vyvstávají. Riziko se objevuje zejména v důsledku nejednoznačnosti v průběhu činností, které se odehrávají jak uvnitř, tak i vně banky, a v důsledku proměnlivosti dosahovaných výsledků (někdy také požadovaných výsledků vůbec nemusí být dosaženo) (úvod do problematiky bankovních rizik poskytuje příloha H).

Pro účely této diplomové práce se autorka blíže zaměří na provozní rizika banky, neboť právě v této kategorii se lze setkat s problematikou bankovních podvodů.

Pro vysvětlení autorka nejdříve uvádí definici Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky, která popisuje operační riziko jako „[…] riziko ztráty, které vyplývá z nedostatků či selhání vnitřních procesů, osob a systémů nebo z vnějších událostí, a zahrnuje právní riziko“. Riziko právní pro banku představuje riziko ztráty z důvodu nerespektování právní normy.

Podle Choudhryho (2012, str. 44) se pod operačním rizikem skrývají záležitosti nefinančního charakteru, jako jsou etika, podvody, selhání systému či náhodné události a nehody. Operační riziko lze snížit definováním a prosazováním přesných protokolů pro všechny části obchodních funkcí banky, a to od front office až po back office. Každé oddělení banky by mělo jmenovat styčného pracovníka pro operační riziko, který bude fungovat jako hlavní kontaktní osoba pro vedoucího oddělení operačního rizika.

V porovnání s ostatními riziky vyjmenovanými výše, provozní riziko je velmi specifické z několika důvodů. Nalezení a vymezení operačního rizika není zdaleka snadné, stejně tak jeho měření, k němuž je potřeba využití zvláštních metod. Vyskytuje se navíc napříč všemi činnostmi, které v bance probíhají. V závislosti na tom je nezbytné, aby i řízení tohoto rizika probíhalo na všech úrovních banky a nemůže být efektivní bez zapojení celého personálu. Na to, jak provozní riziko vypadá, má značný vliv rychle rostoucí rozvoj informačních technologií, který přetváří řadu systémů, jež jsou bankami využívány. Inovace mají dopad například na podobu prováděných bankovních obchodů, platebních operací i zavádění nových produktů (Blahová, 2018, s. 176).

Podle Mejstříka, Pečené a Teplé (2014) tvoří provozní riziko 5-30 % všech bankovních rizik.

Blahová (2018, s. 179) identifikuje následujících sedm kategorií událostí, které lze považovat za provozní rizika:

- **interní podvod** – ztráty, jež jsou důsledkem zpronevěry majetku nebo neplnění předpisů, interních zásad banky či legislativy, a to za účasti nejméně jedné osoby z vnitřního prostředí banky;
- **externí podvod** – ztráty, jež jsou důsledkem zpronevěry majetku nebo neplnění legislativy, a to za účasti nejméně jedné osoby z vnějšího prostředí banky;
- klienti, produkty, obchodní postupy;
- škody na hmotném majetku;

- postupy při zaměstnávání, bezpečnost na pracovišti;
- transakce, dodávky, procesní řízení;
- přerušení obchodní činnosti, selhání systému (vysvětlení viz příloha E).

Základem pro efektivní řízení rizik banky je jasné oddělení kompetencí a odpovědností. I když se organizace oddělení řízení rizik v bankách liší, za osvědčené postupy lze dle Choudhryho (2012, stránky 44-45) považovat následující:

- existence samostatného oddělení odpovědného za vypracování detailní rizikové politiky banky a její výslovné vyhlášení, jakož i za stanovení limitů obchodování a definování oblastí trhu, na kterých firma působí;
- jmenování vedoucího oddělení rizik (Chief Risk Officer – CRO), který poskytuje pravidelné reporty nezávislému senior manažerovi;
- dohlížení nad rozdělením odpovědnosti mezi front, middle a back office, často ve spojení s funkcí interního auditu;
- podávání zpráv vrcholovému vedení týkající se dodržování celkové rizikové politiky společnosti ze strany front office;
- obeznámení shareholderů s riziky a nastavenou rizikovou strategií.

2.3 Argumenty proti bankovní regulaci

Regulace však má i své odpůrce, jež často poněkud agresivně argumentují svými názory.

Zajímavý přístup ve své publikaci poskytuje Revenda (2012). Mezi hlavní argumenty odpůrců regulace bankovnictví patří narušování přirozeného tržního prostředí, podpora oligopolní struktury, vznik dodatečných nákladů na bankovní dohled (více viz Příloha F).

Zastáncem volného bankovnictví je například Dowd (1999). Diskutuje o tom, z jakého důvodu se naprostá většina společnosti shoduje na tvrzení, že liberální obchod je v pořádku, ba i velmi žádoucí, ale liberální bankovnictví nikoli. Způsob, kterým své argumenty prosazuje, je obsažen v Příloze F.

Autorka zastává názor Juroškové (2012, str. 17), podle které „Tyto argumenty ale nejsou v dnešní době obhajitelné. Na banky již nelze nahlížet jako na rozumné subjekty, ale jako na subjekty hnané touhou po zisku“.

Stejně tak se autorka ztotožňuje se slovy Blahové (2018, str. 17), podle které zcela liberální bankovnictví nemůže v současnosti dostát fungování. Regulace je zkrátka nutná, diskutabilní je spíše míra jejího užití.

Jak se své publikaci zmiňují Revenda a další (2012, s. 263), popularity se takzvaná deregulace bankovnictví dočkala v 70. letech 20. století. Tento trend však postupně oslaboval a od ekonomické krize v prvním desetiletí 21. století lze pozorovat převážně podporu regulace.

2.4 Bankovní dohled

Kromě výše diskutované regulace je nutné si vysvětlit pojem bankovního dohledu. Obě tyto oblasti jsou si velmi blízké, ale kromě jejich vzájemných vztahů je nezbytné na ně pohlížet také odděleně a stejně tak je i hodnotit. Bankovní dohled je vykonáván vládními orgány v rámci jedné země, a to na základě zákonů a předpisů stanovenými ve vnitrostátní legislativě. Na rozdíl od toho regulace je napříč zeměmi Evropské unie (EU) jednotná a řídí se směrnicemi EU (Blahová, 2018, s. 18).

Autorka uvádí definici Rejnuše (2014, s. 699) podle kterého si lze pod dohledem představit „[…] kontrolu dodržování obecně závazných pravidel a případné vynucování jejich plnění“.

Rejnuš (2014, s. 700) dále uvádí na pravou míru, že „Úkolem dohledové činnosti není zabraňovat krachům jednotlivých finančních institucí, ale včas rozpoznat jejich problémovost a minimalizovat případné ztráty“. Za tyto instituce (a za jejich úspěchy, nezdary a následky jejich podnikání) tedy stále nesou odpovědnost jejich vlastníci a vedoucí pracovníci a není přípustné, aby orgány dohledu zastupovaly jejich místo. Zároveň dohled nesmí nahrazovat výkon národních regulačních orgánů a orgánů činných v trestním řízení.

Mejstřík a další (2008, s. 172) vyzdvihují, že bankovní dohled „[…] působí jak preventivně (ex ante), tak i průběžně monitoruje problémy a podílí se na jejich nápravě.“

V současnosti je bankovní dohled vykonáván příslušnými orgány ve dvou úrovních, mikro a makro.

Jak vysvětluje Blahová (2018, s. 20), **mikro úroveň** je zastoupena Evropským systémem orgánů finančního dohledu. Ten se skládá ze tří orgánů na evropské úrovni a z národních dohledových autorit a jeho cílem je, aby všechny tyto orgány fungovaly koordinovaně

jako celek. Třemi orgány na evropské úrovni jsou myšleny Evropský orgán pro bankovnictví (EBA), Evropský orgán pro cenné papíry (ESA) a Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění (EIOPA). Každý z těchto orgánů má právní subjektivitu. Činnosti EBA blíže specifikují Haentjens a Gioia-Carabellese (2015, s. 95) a Blahová (2018) (viz příloha I).

Na **makro úrovni** bankovního dohledu vystupuje Evropský výbor pro systémová rizika (ESRB). Jeho cílem je kontrolovat makroekonomický vývoj a vývoj finančního systému jako celku a určit faktory, které by mohly vést ke vzniku finanční nerovnováhy. Za cílem zajištění finanční stability byla zřízena Rada pro finanční stabilitu. Důležitou úlohu v bankovním dohledu na makro úrovni plní jak Evropská centrální banka (ECB), tak i centrální banky jednotlivých států. Jsou to totiž právě ony, které mají zajistit finanční stabilitu státu (Blahová, 2018, s. 20). Maastrichtská dohoda z roku 1992 nařídila zřízení Evropského systému centrálních bank (ESCB), jehož členy jsou ECB a centrální banky všech členských zemí EU. ESCB je řízen rozhodovacími orgány ECB (Haentjens & Gioia-Carabellese, 2015, s. 95).

Blahová (2018, s. 21) dále uvádí, že finanční dohled v České republice provádí Česká národní banka (ČNB), odpovídající legislativa je v rukou Ministerstva financí České republiky (MF ČR). Naše země se řadí mezi ty ze členských států, které bez problémů dokáží řešit různá témata a diskutovat z jednoho místa. Je nutné říci, že regulace i dohled jednoho státu EU jsou jiné od druhého a zdá se téměř nemožné dosáhnout shody. Každá národní ekonomika disponuje vlastní podobou finančního trhu a stanovuje si pravidla, která právě s konkrétními vlastnostmi daného systému korespondují. Tento fakt závažně ovlivňuje výsledky snahy o efektivní přeshraniční spolupráci.

Mejstřík a kol. (2008, s. 172) doplňují, že bankovní dohled je „[…] poskytován na konsolidovaném základě (§ 26c-h Zákona o bankách)“. Tito autoři dále tvrdí, že činnosti dohledu probíhají dvěma způsoby:

- na místě, tzv. „on-side“ – jedná se zejména o kontroly přímo v samotných bankách;
- vzdáleně, tzv. „off-side“ – jedná se zejména o kontroly finančního výkaznictví a kontroly plnění pravidel obezřetnosti.

Janovec (2018) se ve své monografii také zabývá dohledem nad finančním trhem, přesněji řečeno integrací dohledu. Vysvětluje, že „[…] dohled nad finančním trhem je dohledem nad bankovním sektorem, družstevními záložnami, kapitálovým trhem, pojišťovnictvím,

penzijními společnostmi, fondy penzijních společností, směnárnami a dále také dohledem nad institucemi v oblasti platebního styku.“ Vzájemné propojování dohledových činností nad všemi těmito oblastmi ve světě probíhá již více než 30 let, v rámci Evropy byla integrace poprvé zaznamenána v Norsku v roce 1986. Důvodem je charakter finančního trhu jako takový, jeho měnící se struktura a princip fungování a stále intenzivnější snaha o odstraňování překážek na tomto trhu. Jistým předpokladem sjednocování dohledu je také existence velkých skupin peněžních institucí, jejichž působnost mnohdy přesahuje národní měřítko. Pravidla podnikání těchto skupin je nutné harmonizovat.

Přestože se ČNB aktivně zapojuje do procesu propojování dohledu a má zájem o udržování rovnováhy a transparentnost bankovního trhu, je známá spíše negativním k pohotovému vstupu do bankovní unie či eurozóny. „Tím hlavním, proti čemu se ČNB staví, a co kritizuje, je v rámci přijímání nového systému evropského dohledu postupné přesunování pravomocí národních dohledových orgánů směrem na úroveň EU, kdy autority na úrovni EU neponesou odpovědnost za přijatá rozhodnutí“ (Janovec, 2018, str. 122). To však neznamená, že ČNB odmítá spolupráci s dohledovými autoritami a centrálními bankami ostatních států, ba naopak. V procesu dohledu nad trhem financí má své nezastupitelné místo a je v těsné kooperaci s ESBR a ESA.

2.5 Regulace a dohled v České republice

Bankovní sektor je pod stále silnějším vlivem vnějších, v tomto případě přeshraničních, faktorů. V Evropě se konkrétně jedná o politické vlivy a zákonodárství v Evropské unii, které značně formují podobu finančních trhů jednotlivých zemí. Sektor bankovnictví je předmětem mnoha směrnic a opatření EU. V české právní úpravě se většina z nich začala uplatňovat ještě před vstupem ČR do EU (Polouček et al., 2013, s. 40).

Bankovní sektor v ekonomikách s klasickým dvoustupňovým systémem je obvykle regulován alespoň dvěma zákony. Jedním je zákon o centrální bance a druhým zákon o finančních institucích/službách (Polouček et al., 2013, s.7).

Mejstřík a kol. (2008, s. 168-172) ve své publikaci představují hlavní kategorie regulace bank v České republice. Jedná se o tyto:

- pravidla obezřetného podnikání;
- formulace základních cílů regulace v zákoně o České národní bance č. 6/1993 Sb., v platném znění;

- pravidla stanovená v zákoně o bankách č. 21/1992 Sb., v platném znění;
- bankovní tajemství a jeho uvolnění;
- fond pojištění vkladů;
- úvěry centrální měnové instituce v rámci její funkce věřitele poslední instance;
- pravidla proti nelegálním bankovním praktikám (zejména proti „praní špinavých peněz“).

Pravidla obezřetného podnikání budou vzhledem k jejich důležitosti vysvětlena v samostatné podkapitole. Zbývajícími kategoriemi regulace se zabývá následující text.

- **Zákon o České národní bance**

Pozici České národní banky v České republice upravuje zákon č. 6/1993, o České národní bance. V §1 odst. 1 tohoto zákona lze najít základní charakteristiku toho orgánu: „Česká národní banka je ústřední bankou České republiky, orgánem vykonávajícím dohled nad finančním trhem a orgánem příslušným k řešení krize“. Stěžejním je vymezení **hlavního cíle ČNB**, kterým je „[…] **péče o cenovou stabilitu**. Česká národní banka dále pečuje o finanční stabilitu a o bezpečné fungování finančního systému v České republice.“ Pro celistvost je toto vymezení je dále doplněno tím, že „Česká národní banka podporuje obecnou hospodářskou politiku vlády vedoucí k udržitelnému hospodářskému růstu a obecné hospodářské politiky v Evropské unii se záměrem přispět k dosažení cílů Evropské unie.“

Důležitý je §1 odst. 3, ve kterém stojí, že „České národní bance jsou svěřeny kompetence správního úřadu v rozsahu stanoveném tímto zákonem a jinými právními předpisy“ (Zákon o České národní bance, 1992). Příklady zmíněných jiných právních předpisů uvádí Janovec (2018, str. 107) (viz příloha G).

- **Zákon o bankách**

Jurošková (2012, str. 21) mezi nejpodstatnější oblasti regulace a dohledu řadí **regulaci vstupu do bankovní sféry**. „Regulace vstupu do odvětví je centrálním pilířem obezřetnostní regulace bankovnictví, která vychází z přesvědčení, že důkladná kontrola instituce před vstupem do odvětví může předejít pozdějším problémům“. Výhodu institutu prvotního souhlasu ke vstupu do bankovnictví lze spatřit především v omezení nekorektních, nedostatečně finančně stabilních a nezpůsobilých subjektů stát se bankovní

institucí a tím ohrozit ekonomiku země. Pro dosažení tohoto musí subjekt získat bankovní licenci.

Problematika bankovního licencování v ČR je postižena právě ve výše jmenovaném zákonu o bankách. Lze v něm najít informaci, že rozhodnutí o **udělení licence** vydává ČNB, tedy právě té je předkládaná příslušná žádost. Tou nejzákladnější podmínkou k získání licence je složit základní kapitál v minimální výši 500 000 000 Kč, který minimálně v této výši musí být tvořen peněžitými vklady. Bez specifického citování zákona další požadavky zahrnují sídlo v ČR, existenci minimálně 3 zaměstnanců, transparentnost základního kapitálu a čestnost jeho původu, úplné splacení ZK, odbornou způsobilost a důvěryhodnost hlavních zasvěcených osob, nároky z hlediska organizačního a technického, a další (Zákon o bankách, §4, odstavce 1, 2 a 5). Podstatnou kapitolou toho zákona je i **princip jednotné licence.** Spočívá ve zbavení povinnosti zahraničních bank získat bankovní licenci od ČNB. Pro provoz své pobočky na území ČR jim postačí pouze prokázání oprávnění k výkonu činnosti ze své domovské země (Zákon o bankách, §5c).

Zákon o bankách č. 21/1992 byl do začátku roku 2022 již více než sedmdesátkrát novelizován. Podle Poloučka a dalších (2013, str. 39) to značí, že potřebám bank v České republice nepříliš vyhovuje. Již v roce nadcházejícím po nabytí jeho účinnosti byly v českém parlamentu nadneseny návrhy na zavedení nového zákona o bankovnictví. S přihlédnutím k ostatním zemím světa a Evropské unie lze dojít ke zjištění, že takto nastavená legislativa není běžná. Mnohem častěji se zahraniční bankovní sektor řídí zákonem o finančních službách. Řada českých bankovních specialistů doporučuje následování tohoto příkladu.

„Tento zákon zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis Evropské unie a upravuje některé vztahy související se vznikem, podnikáním a zánikem bank se sídlem na území České republiky, včetně jejich působení mimo území České republiky, a dále některé vztahy související s působením zahraničních bank na území České republiky“ (Zákon č. 21/1992, o bankách, §1, odst. 1).

Polouček a další (2013, str. 39) objasňují nedokonalosti zákona o bankách. Největším problémem je, že se vztahuje jen a výhradně na bankovní subjekty. V současnosti však na finančním trhu působí spousta dalších investicí, které poskytují stejné služby jako banky. Na tyto nebankovní subjekty se však práva a povinnosti zákona o bankách již

neaplikují. Zákon pouze vymezuje rozsah činností, které nikdo jiný kromě banky nemůže provozovat, nelze však zabránit jeho obcházení např. prostým přejmenováním činností.

- **Bankovní tajemství**

Bankovním tajemstvím se dle Jílka (2013, str. 388) rozumí „[…] právní institut, podle něhož banky nesmí poskytnout informace o svých klientech (například orgánům činným v trestním řízení), pokud nejsou splněny určité podmínky“. Podle ČNB (2022) bankovní tajemství dotýká uzavíraných obchodů bank, bankovních finanční služeb, zůstatků na účtech, ale také dalších souvisejících informací. Příkladem mohou být soukromé informace o situaci klienta a jeho finančních poměrech, osobní údaje (rodné číslo apod.), obrazové záznamy klienta a tak dále. Jílek (2013, s. 388) dále tvrdí, že se úroveň bankovního tajemství liší stát od státu. Vysoká míra bankovního tajemství je typická pro země s velmi nízkým daňovým zatížením a také například pro Švýcarsko, Hongkong, Lucembursko, Rakousko, Belgii a Singapur.

- **Fond pojištění vkladů**

Klient, který se rozhodne v bance uložit své úspory, se může obávat ztráty svých prostředků. Aby vkladatelé měli větší pocit bezpečí a nebyla narušena stabilita sektoru bankovnictví, existuje po celém světě fond pojištění vkladů. Jedná se o „odškodnění vkladatele při neschopnosti banky vyplácet vklady“ (Zrůst, 2019, str. 297). Podmínky pojištění pohledávek z vkladů jsou ukotveny v zákoně č. 21/1992 Sb., o bankách (§ 41a - § 41s), odpovědnost za fond pojištění vkladů převzal v roce 2016 Garanční systém. Do fondu jsou povinny přispívat všechny banky (včetně stavebních spořitelen a družstevních záložen) sídlící na území ČR a pobočky těch bank, které působí na území ČR, ale sídlí v zemi mimo EU. Vydá-li ČNB oznámení, že není v silách banky dostát svým závazkům, nebo rozhodne-li soud o úpadku banky, přichází vkladatelům na pomoc právě Garanční systém finančního trhu, který vyplatí „[…] z Fondu všem fyzickým a právnickým osobám 100 % jejich vkladů, a to včetně úroků, až do výše ekvivalentu částky 100 000 EUR, přičemž novou legislativou je umožněno ve výjimečných případech získat náhradu za vklad přesahující tento limit“ (Garanční systém, 2022).

- **Věřitel poslední instance**

Pro případ, kdy se solventní banka ocitne v problémech s likviditou, slouží také princip věřitele poslední instance, jehož funkci v ČR zastává ČNB. Jak pro objasnění uvádí

Jurošková (2012, s. 39), „[…] likviditou rozumíme schopnost banky dostát v každém okamžiku svým splatným závazkům“, zatímco „[…] solventnost vyjadřuje stav, kdy výše bankovních aktiv je větší než hodnota jejich závazků“. Věřitel poslední instance takové bance poskytne na přechodnou dobu finanční prostředky, není to však jeho povinností. Činí tak v zásadě v těch případech, kdy hrozí, že nelikvidní banka kvůli systematickému riziku poškodí celý bankovní sektor (Polouček, 2013, s. 307).

- **Pravidla proti nelegálním bankovním praktikám**

Jak je již zřejmé, rozsah působení orgánů regulace a dohledu je velmi široký. Jejich zásahy jsou žádoucí i v případech, kdy nejsou schopné spolehlivě pomoci. Právě nelegální praktiky bank a jejích klientů jsou oblastí, kterou není snadné korigovat. Jak tvrdí Polouček a další (2013, s. 392), „Je zřejmé, že absolutní ochrana před nelegálními a podvodnými operacemi bank, pracovníků ve vedení bank i ostatních pracovníků bank, stejně jako klientů, není možná“. Podle těchto autorů však prostřednictvím bankovní regulace a dohledu, legislativních požadavků, ale i veřejného mínění lze před kriminální aktivity v bankovnictví postavit překážky. Podobně smýšlejí Revenda a další (2012, s. 255), podle kterých regulující a dohledové autority svou proaktivitou mohou identifikovat protiprávní operace a podvody a vzájemně mezi sebou kooperovat napříč zeměmi. Spolupráce má v této oblasti zvláštní význam, neboť je zde znatelná tendence přesunu kriminálních činností ze zemí s pečlivě nastaveným systémem pravidel k těm liberálnějším. Autoři rozlišují dva základní typy nekalých praktik, které je třeba regulovat, a to **důvěrné obchody** (insider trading) a **praní špinavých peněz** (money laudering) (více viz kapitola 3.2.1).

2.5.1 Základní pravidla činnosti bank

Základní pravidla činnosti bank, neboli **pravidla obezřetnostního podnikání,** dle Mejstříka a dalších (2008, str. 170) vycházejí především z basilejských standardů a směrnic EU. Ta základní lze najít i v zákoně o bankách. Podobné požadavky a některé navíc dále detailně popisují i vyhlášky a informační prostředky ČNB.

Jurošková (2012, str. 25) a Zrůst (2019, str. 78) o témže hovoří jako o základních pravidlech činnosti bank. která se zaměřují na následující:

- **kapitálová přiměřenost;**
- **úvěrová angažovanost;**

- **likvidita;**
- **správa a management bank;**
- **povinnost sdělovat informace** (Jurošková, 2012, str. 25)

Zrůst (2019, str. 80) i Revenda a další (2012, str. 255) tuto kategorizaci doplňují ještě o **povinné minimální rezervy**. Také Jílek (2013, str. 175) o nich pojednává, tentokrát jako o rezervních požadavcích.

ČNB (2021) je definuje jako „[…] povinnost komerčních bank držet určité množství likvidních prostředků ve formě rezerv na účtu u centrální banky. Toto množství je stanoveno jako procentuální podíl (tzv. sazba PMR) z určité základny, která je určena závazky bank vůči nebankovním subjektům“. Pod komerční banky jakožto souhrnný pojem ČNB řadí i stavební spořitelny, pobočky zahraničních bank a družstevní záložny. Podmínky tvorby povinných minimálních rezerv obsahuje vyhláška č. 253/2013 Sb. k zákonu č. 6/1993 Sb., o České národní bance, podle které jejich výše činí „pro banky a pobočky zahraničních bank 2 % ze základu pro výpočet stanovené výše povinných minimálních rezerv s výjimkou závazků z repo operací, pro které činí 0 %“, přičemž stejné platí i pro družstevní záložny (vyhláška č. 232/2013 Sb.).

Molnár (2021) uvádí, že tento nástroj měnové politiky centrálních bank patří k těm tradičním, které v posledních letech ztrácejí na důležitosti, a to zejména v rozvinutých ekonomikách. Sazby se snižují (např. ECB 1 %), byť se dokonce zcela ruší (např. Bank of England, Bank of Canada). „V rozvinutých zemích s režimem cílování inflace pak již PMR nehrají v měnové politice těchto centrálních bank zásadní roli. Mohou však pomáhat stabilizaci sazeb na mezibankovním trhu a usnadňovat průběh platebního styku“ (Molnár, 2021).

- **Úvěrová angažovanost**

Jak vysvětlují Revenda a další (2012, s. 252), pod pravidly úvěrové angažovanosti si lze představit stanovování úvěrových limitů, ale i limitování ostatních bankovních pohledávek za účelem zajištění různorodosti aktivních položek v majetku banky. Tím je pak dosaženo snížení kumulace investičních a obchodních rizik. Limity se liší v závislosti na charakteru dlužníka (rozdílné jsou stropy u dlužníků institucionálních, vládních apod.). Angažovanost banky vůči jednomu klientovi obvykle nesmí být vyšší než 25 % kapitálu banky. Velkou úvěrovou angažovanost musí banka ohlásit orgánům pro to učeným (Polouček, Frait, Skaunic, Stavárek, & Vodová, 2013, str. 227).

- **Likvidita**

Mejstřík, Pečená a Teplý (2008, str. 146) likviditu banky vysvětlují jako její „[…] schopnost dostát svým krátkodobým (hotovostním nebo platebním) závazkům v odpovídající objemové a časové struktuře“.

Pravidla likvidity se zakládají na přesně stanovené struktuře aktiv a pasiv banky, jakož i jejich vzájemných vztahů. Přesněji řečeno, banky mají povinnost třídit položky jejich majetku na základě jejich doby splatnosti, předpokládaného vývoje, úrovně zajištění rizikových aktiv prostřednictvím rezerv, vedené měny a dalších kritérií. To vše přispívá účelu existence těchto pravidel – diverzifikaci rizika bankovních operací (Zrůst, 2019, s. 79). Likviditu lze tedy vést v částkách domácí měny, nebo lze hovořit o devizové likviditě (Revenda et al, 2012, s. 253).

Mejstřík, Pečená a Teplý (2008, str. 146) doplňují, že zajištění likvidity je podporováno také minimálními rezervami u centrálních bank. Pravidla likvidity nastavuje ČNB proto, že likvidita aktiv souvisí s jejich rentabilitou. Vzhledem k tomu, že se komerční banky snaží o co nejvyšší ziskovost, mohou na likviditu snadno zapomenout a tíhnout k podstupování nadměrného rizika (Zrůst, 2019, s. 79).

- **Informační povinnost**

Dle zákona o bankách je každá banka povinna na pravidelné bázi sdělovat informace o svých aktivitách příslušné dohledové autoritě. Podrobné informace lze najít ve Vyhlášce č. 346/2013 Sb., o předkládání výkazů bankami a pobočkami zahraničních bank České národní bance, která „[…] upravuje obsah, formu, lhůty a způsob sestavování a předkládání výkazů České národní bance bankami a pobočkami zahraničních bank, a to jak výkazů v návaznosti na přímo použitelné předpisy Evropské unie, tak i dalších výkazů k zabezpečení úkolů České národní banky“. Požadavky na obsah a periodicita hlášení závisí na konkrétním druhu výkazu, příkladem může být následující: „Banka a pobočka zahraniční banky za každý obchodní den sestavuje a nejpozději do osmé hodiny pracovního dne následujícího po tomto obchodním dni předkládá […] „Denní výkaz o nezajištěných jednodenních vkladech“ (Vyhláška č. 346/2013 Sb., § 1). Cílem této povinnosti je udržovat finanční trh v rovnováze prostřednictví jeho transparentnosti. „Informační povinnost směřuje do oblasti změny vlastnické struktury, majetkové účasti či změny stanov“ (Zrůst, 2019, s. 80).

- **Správa a řízení bank**

Pod pravidly správy a řízení bank si lze dle Juroškové (2012, s. 28) kromě obecných požadavků na správu a management bank představit také pravidla týkající se kompetentnosti vedení bank k získání licence. Cílem je, aby v představenstvech bank působili jen lidé s odpovídajícími dovednostmi a znalostmi. Důraz je dále kladen na vysokou efektivnost interní kontroly a řízení rizik.

- **Pravidla kapitálové přiměřenosti**

Největší pozornost je napříč dostupnou literaturou věnována pravidlům kapitálové přiměřenosti, které nařizují, v jaké minimální výši musejí banky držet svůj kapitál. Tato problematika je velmi těsně spjata s otázkou výše vlastních rezerv, jež představují hlavní zdroj financování ztrát v případě zrodu problémů banky se solventností (Zrůst, 2019, str. 78).

V porovnání s pravidly likvidity, která představuje schopnost banky dostát svým závazkům v době jejich splatnosti, pravidla kapitálové přiměřenosti se soustřeďují na způsobilost banky krýt ztráty z činnosti tak, aby nebyli negativně ovlivněni její vkladatelé (Revenda et al, 2012, s. 253).

Důležitost tématu je umocněna těmito skutečnostmi:

- disponování s kapitálem má bezprostřední vliv na akcionáře banky (jedná se totiž o vlastní zdroj krytí) – pro doplnění lze uvést tvrzení Revendy a dalších (2012, s. 252), že „Kapitál je navíc zdroj, který je dražší než cizí zdroje, neboť akcionáři nesou nejvyšší riziko ztrát při problémech banky, a proto požadují vyšší relativní výnosy než například vkladatelé“;
- pro kapitál je význačná jeho přímá měřitelnost;
- držba kapitálu je spojena se vznikem dodatečných nákladů (dopad do naceňování služeb banky, vliv na její konkurenceschopnost apod.)
- „Nákladnost akciového kapitálu při neexistenci pravidel by ve snaze zvýšit rentabilitu mohla vést k jeho relativnímu snižování“ (Zrůst, 2019, str. 78);
- vliv skladby vlastního kapitálu na operace banky (ke krytí ztrát nelze použít jakoukoli složku vlastního kapitálu).

2.6 Bankovní unie

Bankovní sektor je pod stále silnějším vlivem vnějších, v tomto případě přeshraničních, faktorů. V Evropě se konkrétně jedná o politické vlivy a zákonodárství v Evropské unii, které značně formují podobu finančních trhů jednotlivých zemí. Sektor bankovnictví je předmětem mnoha směrnic a opatření EU. V české právní úpravě se většina z nich začala uplatňovat ještě před vstupem ČR do EU (Polouček et al., 2013, s. 40).

Jak uvádějí Haentjens a Gioia-Carabellese (2015, s. 94), evropští zákonodárci se snaží vytvořit bezpečnější a stabilnější finanční sektor pro EU již od začátku globální finanční krize v roce 2007. Jakožto odpověď na krizi došlo na popud Evropské komise ke zrodu velkého množství iniciativ s cílem revitalizovat sektor financí. Činnosti těchto iniciativ se soustředily zejména na tvorbu striktnějších pravidel obezřetnosti bank, dále na důslednější péči o spotřebitele (vkladatele, investory) a v neposlední řadě na požadavky pro management bank, které mají problém se solventností. Byl vytvořen tzv. „Single Rulebook“, tedy soubor pravidel, jež byl stěžejní pro vznik bankovní unie. Bankovní unie je aktuálně nejvyšším stupněm integrace bankovního dohledu v EU (Janovec, 2018, str. 2).

Jedním z kroků podniknutých k dosažení tohoto cíle bylo vytvoření Evropského systému finančního dohledu (ESFS), pod jehož záštitou byly založeny tři evropské orgány dohledu včetně EBA. Jak se však krize prohlubovala a vyústila v dluhovou krizi eurozóny v letech 2010–2011, bylo zřejmé, že vystoupení z bludného kruhu mezi bankami a národními financemi bude pro země sdílející euro jakožto společnou měnu vyžadovat značné úsilí, a to právě z důvodu jejich vzájemné provázanosti. Následkem toho se v červnu roku 2012 představitelé hlav států a vlád dohodli na založení bankovní unie, která měla doplnit ekonomickou a monetární unii. Bankovní unie měla vést k centralizovanému uplatňování pravidel pro banky působící v EU, a to jak v členských zemích eurozóny, tak i v ostatních evropských zemích, které se chtěly zapojit (Haentjens & Gioia-Carabellese, 2015).

Haentjens a Gioia-Carabellese (2015, s. 94) dále vysvětlují, že základem bankovní unie je nový regulatorní rámec obsahující základní pravidla pro banky všech členských zemí EU. Tato pravidla v první řadě mají pomoci předcházet bankovním krizím. Středem pozornosti je nejnovější legislativní soubor kapitálových požadavků, tedy Směrnice o kapitálových požadavcích (CRD IV a CRD V) a Nařízení o kapitálových požadavcích (CRR I a CRR II) (Evropská unie, 2021a). Pro případ, že by banka trpěla finančními

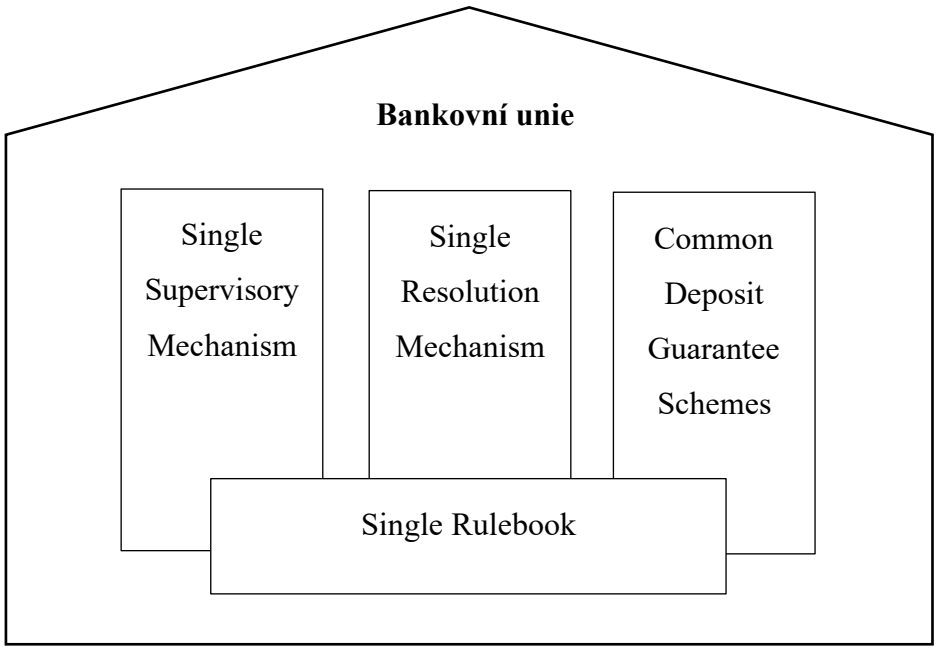
problémy i navzdory dodržování těchto pravidel dohledu, byl vytvořen obecný rámec pro jejich řešení a zotavení banky. Tento rámec je k nalezení ve Směrnici pro ozdravné postupy a řešení krize úvěrových institucí a investičních podniků (BRRD) (Evropská unie, 2021b). Tato pravidla dále zajišťují, že vklady maloobchodníků z EU do 100.000 € za jednoho vkladatele (a banku) jsou chráněny kdykoli a kdekoli v EU.

Bankovní Unie stojí podle (Haentjens & Gioia-Carabellese, 2015) na dvou hlavních pilířích:

- **jednotný mechanismus pro řešení problémů** (SRM – Single Resolution Mechanism) a
- **jednotný mechanismus dohledu** (SSM – Single Supervisory Mechanism).

Janovec (2018, str. 49) mezi základní pilíře řadí ještě společný systém ochrany vkladů (Common Deposit Guarantee Schemes). Tyto pilíře jsou postaveny na několika směrnicích a nařízeních EU a po jejich boku stojí již zmíněný Single Rulebook.

Obr. č. 3: Bankovní unie a její pilíře



Zdroj: Janovec (2018, s. 51), zpracováno autorkou

3 Podvodná jednání v bankovním sektoru

Ačkoli s sebou globalizace přináší zejména výhody, které pomáhají ekonomikám růst, na straně druhé také otevírá možnosti pro nelegální ekonomické činnosti. Kriminalita se objevuje ve všech oblastech našich životů a všech ekonomických odvětvích, přičemž sféra financí a bankovnictví samozřejmě není výjimkou. Kriminální činy ve finanční sféře s sebou přinášejí obrovské peněžní ztráty, zpomalují ekonomický i sociální růst, oslabují alokační efektivnost a další (Kantnerová, 2016, s. 190). Není tedy pochyb, že je více než žádoucí věnovat tomuto tématu dostatečnou pozornost.

Podle Poloučka a dalších (2013, str. 392) je finanční sféra vystavena kriminálním aktivitám zejména kvůli její komplikované a heterogenní povaze. Počet těchto aktivit nelze s přesností určit, neboť znatelná část z nich není součástí statistik. Pravděpodobně i proto, že se jedná o „[…] společensky, ekonomicky i politiky velice citlivou a delikátní oblast“. Je typické, že banky, ostatní finanční instituce, dohledové a policejní orgány a další autority se jistým způsobem vyhýbají poskytování detailních zpráv veřejnosti.

Autorka nejdříve provede teoretický úvod do hospodářské kriminality, načež se přenese hlouběji do problematiky bankovních podvodů. Představeny budou podvody páchané samotnou bankou, podvody páchané vůči bance, podvody páchané na klientech banky a nové formy podvodů páchaných na klientech.

3.1 Hospodářská, ekonomická a finanční kriminalita

Dříve než se autorka ponoří do problematiky bankovních podvodů, považuje za důležité vysvětlit pojmy jim nadřazené.

Za obecnější rovinu, do které spadá problematika bankovních podvodů, lze považovat hospodářskou a ekonomickou kriminalitu. Jak uvádějí Chmelík a Bruna (2015, s. 11), „Hospodářskou kriminalitou rozumíme zaviněné (společensky škodlivé) jednání popsané ve zvláštní části zákoníku, poškozující nebo ohrožující hospodářský pořádek, systém ekonomických a souvisejících právních vztahů, jejich fungování, práva a oprávněné zájmy subjektů těchto vztahů.“

Institut pro kriminologii a sociální prevenci v Praze (2004, s. 9) definuje ekonomickou kriminalitu jako „protiprávní ekonomické jednání, kterým byl dosažen finanční nebo jiný prospěch na úkor konkrétního ekonomického subjektu (stát, obchodní společnost, fond,

fyzická osoba apod.), které naplňuje zákonné znaky skutkových podstat konkrétních trestných činů“.

O něco specifičtějším pojmem je kriminalita finanční, která je páchána výhradně ve finančním sektoru. Chmelík a Bruna (2015, s. 16) kladně hodnotí a uvádějí definici Šámala, který finanční kriminalitu vysvětluje jako „[…] trestnou činnost směřující proti fungování bankovního systému, kapitálového trhu a finančních institucí, zejména bank, burzy, investičních společností a investičních fondů, penzijních fondů, pojišťoven a dalších finančních institucí, jež mají v rámci tržního hospodářství mimořádně významnou roli, neboť do značné míry určují dynamiku hospodářského vývoje“.

Laure (2020) tvrdí, že firma na poli finanční kriminality může vystupovat třemi způsoby:

- jako manipulátor trhu (porušením právních předpisů);
- jako aktivní oběť (žalováním jiného účastníka trhu za jeho údajné kriminální jednání, zatímco skutečným pachatelem je žalobce);
- jako pasivní oběť.

Chmelík a Bruna (2015, s. 16) člení problematiku finanční kriminality do čtyř základních kategorií:

a) zločiny v bankách a jiných finančních institucích;
b) zločiny na trhu s kapitálem, neodvádění sociálního a zdravotního pojištění;
c) neodvádění daní a jiných povinných plateb;
d) padělání a pozměňování bankovek, šeků a dalších platebních nástrojů.

Pojmem často skloňovaným ve finanční kriminalitě je kriminalita bílých límečků, při které bankéři, makléři a vrcholní manažeři jiných finančních organizací značně profitují prostřednictvím podvodů, obchodování zasvěcených osob, zpětného datování opcí, podvodů s cennými papíry, chybných finančních zpráv a dalších nezákonných nebo kriminálních činů (Freeman, 2010).

Kriminální aktivity ve finanční sféře jsou jedinečné tím, že se týkají peněz – je jednoduché je získat, byť protiprávně, a obratem znovu použít na trhu. Pachatelé takto disponují s cizími prostředky jako se svými vlastními (Chmelík & Bruna, 2015, s. 17).

3.2 Druhy bankovních podvodů

Bankovních podvodů je obrovská škála a není proto možné je v rámci této práce vyjmenovat všechny, natož potom podrobněji je vysvětlovat. Autorka se proto rozhodla zabývat těmi nejznámějším a nejvíce diskutovanými, přičemž je rozdělila do čtyř kategorií a jim odpovídajících podkapitol: podvody páchané bankou, podvody páchané vůči bance, podvody páchané na klientech a nové formy podvodů páchaných na klientech.

Těmi nejčastěji skloňovanými nelegálními činnostmi, které se svou nějakým způsobem dotýkají bankovnictví, jsou podle Kantnerové (2016, s. 190) „[…] úvěrové podvody (těch je nejvíce), krádeže zaměstnanců bank, padělání dokumentů a finančních nástrojů, financování terorismu, praní peněz pocházejících z kriminálních aktivit, manipulace s trhem, podplácení, falšování účtů a podvody s kreditními kartami“.

Před představením konkrétních druhů podvodů se autorka rozhodla stručně vysvětlit kriminální čin, jímž je krádež identity. Dle názoru autorky je totiž velmi složité jej kategorizovat, neboť se prolíná celou řadou níže uvedených podvodů. „Krádež identity je kriminální čin, kdy útočník podvodným jednáním získá citlivá data oběti a poté se za oběť vydává. Motivací je samozřejmě finanční zisk.“ (ESET, 2022) Varovným signálem, který jedinci může napovědět, že se stal obětí krádeže identity, může být například dostávání bankovních dopisů nebo dopisů od vymahačů dluhů, o kterých adresát nic neví (Citizents Advice, 2022). Bank of America (2022) pak poukazuje především na neautorizované pohyby na bankovním účtu, upozornění na přihlášení z jiného zařízení, zúčtování za zdravotní péči, kterou dotyčný neobdržel, absence e-mailových zpráv od banky a některé další.

3.2.1 Podvody páchané bankou

V rámci podvodů, ve kterých vystupuje sama banka, jsou nejčastějším předmětem diskuse praní špinavých peněz a insider trading. Tyto praktiky jsou vysvětleny v následujícím textu, přičemž zmíněné jsou i příliš riskantní či nákladné obchody. Někteří autoři zmiňují také korupci, dle Poloučka (2012) však v sektoru bankovnictví v současnosti nepředstavuje závažný problém. Autorka se proto rozhodla se jí nezabývat.

- **Zneužití trhu, insider trading**

Současná literatura v problematice bankovních podvodů často diskutuje o situaci, kdy se do nečestných praktik zapojují sami zaměstnanci bank nebo jiné osoby disponující

informací z vnitřního prostředí banky. Janovec (2018, s. 134) tento fenomén vztahuje ke **zneužití trhu**.

Nařízení Evropského parlamentu a Rady (EU) č. 596/2014, o zneužívání trhu (nařízení o zneužívání trhu) tento pojem vymezuje jako činnost, která „[…] sestává z obchodování zasvěcené osoby, nedovoleného zpřístupnění vnitřní informace a manipulace s trhem. Takové jednání snižuje úplnou a řádnou průhlednost trhu, která je předpokladem pro operace všech hospodářských subjektů na integrovaných finančních trzích.“ Otázka manipulace s trhem se týká situace, kdy zasvěcená osoba šíří lživá nebo klamavá sdělení. K takovým aktivitám může využívat masmédií, poskytovat tyto informace benchmarkům a využívat je ke uzavírání výhodných obchodů (Janovec, 2018, s. 135).

Problematika obchodování a uzavírání smluv na základě informací, které nejsou dostupné všem, je také známá pod pojem **insider trading**. Z vysvětlení již může být čtenáři patrná určitá souvislost s informační asymetrií. Insider trading se v naprosté většině případů týká obchodování s cennými papíry (Polouček et al, 2013, s. 394). Tuto techniku si lze vysvětlit na názorném příkladu, kdy si je jedinec na manažerské úrovni v podniku vědom toho, že se v důsledku plánované akvizice zvýší cena akcií a provede proto obchod ve prospěch svůj či nějakého třetího článku (Janovec, 2018, s. 134).

- **Legalizace výnosů z trestné činnosti**

Jak je známo, při hotovostní platbě získává prodávající peněžní prostředky okamžitě a s finální platností. V této formě je může ihned využít pro své účely, a to bez jakéhokoli dalšího zpracování a přeměny. Velkým benefitem plateb v hotovosti je jejich anonymita. Technologové v posledních letech usilovně pracují na vývoji nových řešení s co nejvyšším stupněm anonymity i u elektronických plateb. Tato výhoda však jde ruku v ruce s problémy jako je zastírání transakce před orgány právní moci (např. transakce plyne z nelegální činnosti) či před správci daně (Mann, 2016, str. 4).

Legalizace výnosů z trestné činnosti, běžně známá pod pojmem **praní špinavých peněz** „[…] představuje proces proměny příjmů (výnosů, majetku) získaných trestnou činností na legální majetkové hodnoty prostřednictvím využití legálního finančního systému“ (Chmelík & Bruna, 2015, s. 62-63).

Polouček a další (2013, s. 407) doplňují, že pod pojmem špinavé peníze bývají chápány také peněžní prostředky pocházející z legálních aktivit, které však nebyly řádně zdaněny.

Cílem legalizace výnosů trestné činnosti je vyvolat domnění, že finanční prostředky plynoucí z nějakého protizákonného obchodu, mají ve skutečnosti původ ve zcela legální obchodní aktivitě. Konkrétními případy, které si vyžadují proces legalizace výnosu, jsou obchody s bílým masem, falešné hry a sázky, racketeering (vyděračství, např. vymáhání peněz za ochranu), ilegální přemisťování migrantů, majetková kriminalita (zpronevěry uměleckých děl, aut apod.), prostituce, obchod s drogami, násilná trestná činnost na zakázku a mnohé další. Pokud by pachatelé těchto činů příjmy z nich plynoucí neočistili, čelili by vysokému riziku odhalení, jehož následkem jsou velmi vysoké trestní postihy (Chmelík & Bruna, 2015, s. 63).

S ohledem na to, že předmětem diskuze je kriminální aktivita, není překvapením, že tu nejzásadnější roli v boji s touto problematikou zastává policie (legalizace výnosů z trestné činnosti je předmětem § 216 trestního zákoníku (Prezidium ČR)). I bankovní instituce však mohou být nápomocné. Jejich úlohou je snížit možnosti nabytí legálního původu takto získaných peněz. Jako příklad lze uvést zákaz zřizování anonymních bankovních účtů, zavedení povinnosti bankám hlásit všechny nestandardní transakce, stanovování stropů pro platby v hotovosti apod. (Revenda et al., 2012, s. 255).

Pro účely boje bank proti legalizaci výnosů z trestné činnosti slouží zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Tento zákon stanoví, že „Povinná osoba provede identifikaci klienta nejpozději tehdy, kdy je zřejmé, že hodnota obchodu překročí částku 1000 EUR, pokud tento zákon dále nestanoví jinak.“ Povinnou osobou je myšlena banka, spořitelní a úvěrní družstvo a další finanční instituce v zákoně definované. Povinnost identifikace klienta se dle tohoto zákona nehledě na zmíněný limit vztahuje také na:

a) *podezřelý obchod,*
b) *vznik obchodního vztahu,*
c) *nákup 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, nebo*
d) *výplatu zůstatku zrušeného vkladu z vkladní knížky na doručitele* (Zákon č. 253/2008, § 7, odst. 1 a 2).

Uvedená problematika je postižena také ve vyhlášce ČNB č. 67/2018 Sb., o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu.

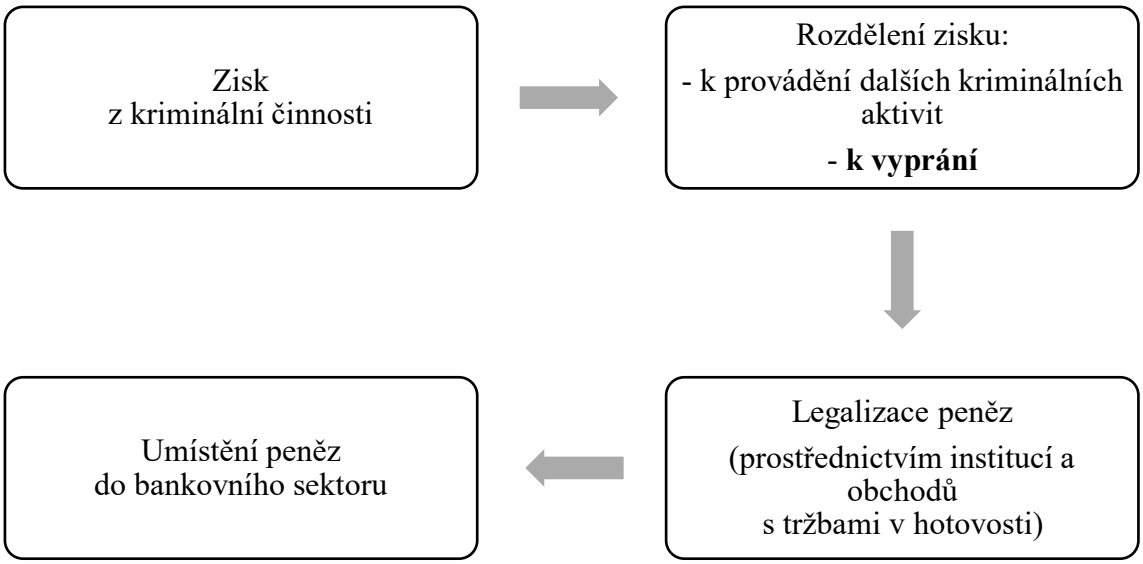
Autorka si v souvislosti s tématikou praní špinavých peněz vybavila pasáž ze seriálu Ozark, který od roku 2017 vysílá streamovací služba Netflix. Marty Byrde, hlavní postava seriálu, v americkém státě Missouri pere špinavé peníze pro drogový kartel. Podstatu této protiprávní činnosti Marty v jednom z prvních dílů vysvětluje, a to s jistou nadsázkou a způsobem, kterému dokáže porozumět i naprostý laik. Právě z důvodu odlehčené interpretace, snadnosti pochopení a výstižnosti textu se autorka rozhodla pasáž zakomponovat do této práce v rámci přílohy J.

Česká národní banka (2020) vysvětluje, že metod, které pachatelé k legalizaci špinavých peněz využívají, je mnoho. Princip ale bývá stejný – pachatelé většinou vynakládají veškeré úsilí na vytvoření co nejdelšího a nejkomplikovanějšího toku těchto peněz, aby znemožnili zjištění jejich původu. Proces praní peněz pocházejících z kriminálních aktivit má v obecném pojetí následující tři fáze:

1) placement – zavedení hotovosti do bankovního systému;
2) layering – vrstvení velkého množství akcí a převodů peněz;
3) integration – uvedení očištěných peněz do užívání.

Koloběh nelegálně nabytých peněžních prostředků zobrazuje následující schéma:

Obr. č. 4: Koloběh nelegálně nabytých peněžních prostředků



Zdroj: Polouček et al. (2012, s. 411), zpracováno autorkou

Česká národní banka (2020) však uvádí na pravou míru, že kromě těchto nejzávažnějších činů může jít také o „pouhou“ krádež. ČNB vyzdvihuje závažnost výše popsaných činů, neboť jimi dochází k porušování základních lidských práv (např. obchod s lidmi), nelegálnímu obchodování se zvířaty (např. prodej vzácných druhů), ohrožování systémů státní správy (např. daňová kriminalita) apod.

Praní špinavých peněz někdy bývá zaměňováno s problémem **financování terorismu**. V kontrastu s praním špinavých peněz, financování terorismu zajišťuje tok prostředků v opačném směru. Výnos, tentokrát obvykle legálního původu, putuje k teroristům pro účely financování jejich zločinné činnosti. Tento problém se dle Kantnerové (2016, s. 197) začal prohlubovat až po roce 2010. Na poli řečených zločinů paradoxně často vystupují například dobročinné a nadační spolky, u kterých se snáze ztratí převody z účtů mimo rámec jejich hlavní činnosti. Děje se tak zejména ve státech islámského světa.

- **Příliš riskantní či nákladné obchody**

V tomto případě je hlavním aktérem zaměstnanec banky, který nerespektuje limity pro spekulativní transakce bankou stanovené. V momentě, kdy pracovník zjistí, že obchod nebyl výhodný, usiluje o znovuzískání prodělečné částky uskutečňováním dalších obchodů. Světově známým případem takového jednání jsou obchody Nicka Leesona (Kantnerová, 2016, s. 194). Nick stál za pádem Barings, nejstarší obchodní banky Spojeného království. Leesonovy ztráty činily 827 milionů GBP, což představovalo dvojnásobek dostupného obchodního kapitálu Barings, a po neúspěšném pokusu o záchranu banka v roce 1995 vyhlásila bankrot (Beattie, 2020).

3.2.2 Podvody páchané vůči bance

- **Krádeže a defraudace**

Trestné činy krádeže, loupeže a podvodu (včetně padělání peněz a dalších nelegálních činností) mohou být v bankách páchány jak jejími klienty, tak i jejími zaměstnanci. Pro tyto situace mají banky stanovené postupy, jejichž osvojení musejí prokázat už při získávání bankovní licence. Jedná se zejména o dodržování systému bezpečnosti s pomocí nejrůznějších zabezpečovacích technologií, trezorů, najmutím bezpečnostní agentury apod., ale také např. o stanovování limitů pro použití hotovosti. Pro ochranu před podvody zaměstnanců, které představují větší hrozbu než klienti, slouží spíše bankovní regulace a dohled. Osoby na vedoucích pozicích musejí mít dostatečné profesní

zkušenosti a splňovat požadavky na jejich morální profil. Dále musí být dodržován princip čtyř očí, jež spočívá v povinnosti vést odpovědnost za jednu bankovní operaci dvěma zaměstnanci banky (všechny dokumenty banky obsahují dvě signatury). V ČR došlo k milionovým zpronevěrám z řad zaměstnanců např. v Komerční bance či České spořitelně (Polouček, 2013, s. 435-436).

Kantnerová (2016, s. 197) doplňuje, že bankovní loupeže jsou jedním z nejstarších zločinů v bankovní sféře (první záznam je z roku 1831). Přesto, že dodnes nedošlo k jejich úplnému zániku, ani zdaleka nejsou v popředí kriminální scény.

– **Úvěrové podvody**

Jednou ze základních činností bank je poskytování úvěrů. Za účelem vzniku úvěrového vztahu mezi klientem a bankou prochází tyto dva subjekty několika etapami:

1. osobní schůzka (informativní charakter – banka nabízí možnosti úvěru a poskytuje detaily s ním související, zjišťuje stav klientovo majetku apod.);
2. předložení žádosti o úvěr v písemné formě (osobní údaje o žadateli a informace, které bance pomáhají ověřit možnost klienta dluh splácet, údaje o jeho závazcích, informace o konkrétním druhu úvěru apod.; příloha žádosti obsahuje finanční výkazy, znalecké posudky, výpisy z katastru nemovitostí apod.)
3. zhodnocení žádosti věřitelem – bankou;
4. uzavření smlouvy o úvěru;
5. kontrola plnění podmínek stanovených úvěrovou smlouvou;
6. dostání závazků ze smlouvy plynoucích (Chmelík & Bruna, 2015, s. 59).

Okamžik, ve kterém je podána písemná žádost o úvěr, je zásadní z pohledu spáchání úvěrového podvodu.

Podvodu tohoto typu se obvykle dopouští klient nacházející se ve špatné ekonomické situaci. Pro takového klienta, kterého už například jiné banky registrují jako problémového dlužníka, je téměř nemožné získat nový úvěr. „Klient-podvodník žádá o úvěr a snaží se zastřít svoji finanční historii, používá falešné či pozměněné osobní údaje, aby nebylo možné zjistit jeho nesplacené úvěry u jiných bank“ (Kantnerová, 2016, s. 196). Po zdařilém získání úvěru klient padá do platební neschopnosti, v případě podniku dochází k bankrotu.

Chmelík a Bruna (2015, s. 60) popisují princip této kriminální aktivity tak, že pachatel v krátkém časovém intervalu uzavře hned několik úvěrových smluv. Pachatel, jemuž se přezdívá bílý kůň, je motivován příslibem vysokého výdělku prostřednictvím provize. Autoři vyzdvihují skutečnost, že existence spolupachatele zločinu je v tomto případě zcela nezbytná. Nic neobvyklým není ani organizovaná forma tohoto zločinu.

V § 211 Trestního zákoníku stojí, že „Kdo při sjednávání úvěrové smlouvy nebo při čerpání úvěru uvede nepravdivé nebo hrubě zkreslené údaje nebo podstatné údaje zamlčí, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti“.

Chmelík a Bruna (2015, s. 60) jmenují jeden konkrétní peněžní ústav, který se s tímto problémem musel často potýkat, a to Českou spořitelnu, a. s. Obětmi organizátorů byli zejména obyvatelé nacházející se ve finanční tísni či nepřizpůsobiví občané, od nichž pomocí nejrůznějších taktik získali potřebné doklady a podpisy. Organizátoři jsou za dobře odvedenou práci následně odměněni nemalým podílem na celkové sumě úvěru.

K diskutované problematice bankovních podvodů se autorka rozhodla zařadit i **použití prostředků banky k jinému než sjednanému účelu.** Klient, který žádá o úvěr (nebo uskutečňuje nějakou obchodní transakci), musí bance sdělit, jak získávané finance použije. Banky tak poskytují klientům prostředky pouze pro účely vymezené v uzavřené smlouvě. Nelegálního jednání se klient dopustí tehdy, použije-li tyto peníze k jinému než předem dohodnutému záměru. Častým případem je nákup cenných papírů prostředky získanými v rámci podnikatelského úvěru. Pro obchody s cennými papíry stanovují americké zákony poměry vlastních zdrojů na celkové sumě nákupu konkrétního druhu cenného papíru, kdy např. nákup akcií je nutné financovat alespoň z poloviny vlastními prostředky. Pokud investor uvedené hranice překročí, podstupuje zvýšené riziko a v případě neúspěchu jeho obchodu ohrožuje nejen sebe, ale i jeho banku, a tedy i celý bankovní sektor (Polouček, 2013, s, 434-435).

Prezidium ČR však nezanedbává ani opačnou situaci, kdy se podvodu v souvislosti s úvěry dopouští sami zaměstnanci bank. Takovým případem může být schválení úvěru proti všem opatřením. Poškozenou je i v tomto případě banka (Prezidium ČR, 2022).

- **Padělání hotovostních peněz**

Padělání platidel je nejstarší formou finančního zločinu, k němuž docházelo ještě před vznikem bank (Kantnerová, 2016, s. 195). Penězokazectví představuje náročný proces, jehož jednotlivé fáze jsou v trestním zákoníku vymezeny jako samostatné trestné činy.

Prvním stupněm padělání platidel je výroba potřebného náčiní, následuje výroba samotných padělků, a celý proces končí uvedením padělané hotovosti do oběhu. K vyhotovení padělaných papírových peněz jsou zapotřebí tiskárny vysoké kvality, xerografická zařízení a nejrůznější výpočetní technika. Zhotovení padělaných mincí zahrnuje činnosti odlévání a ražby, a to prostřednictvím matric jak vlastními silami zhotovených, tak i těch nelegálně získaných. Kromě vlastní výroby padělků však někdy pachatelé pouze pozměňují hodnotu peněz v oběhu. Chemickými a mechanickými postupy odstraňují z pravých bankovek text a číslice, načež je nahrazují údaji vyšší hodnoty. V případě mincí pachatelé obrušují jejich povrch (Chmelík & Bruna, 2015, s. 48).

Na základě údajů od Prezidia ČR se právě popsané problematice v České republice z hlediska legislativy věnuje trestní zákoník č. 40/2009 Sb., konkrétně Hlava VI: Trestné činy hospodářské, Díl 1: Trestné činy proti měně a platebním prostředkům; a to v následujícím složení:

- Padělání a pozměnění peněz (§ 233);
- Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234);
- Udávání padělaných a pozměněných peněz (§ 235);
- Výroba a držení padělatelského náčiní (§ 236);
- Neoprávněná výroba peněz (§ 237);
- Společné ustanovení (§ 238);
- Ohrožování oběhu tuzemských peněz (§ 239) (Trestní zákoník, Hlava VI, Díl 1).

Chmelík a Bruna (2015, s. 48) připomínají, že to však nejsou jen bankovky a mince, kterými lze platit, ale také šeky nebo platební karty. Riziko padělání se tedy samozřejmě vyskytuje i u těchto. S rapidním zdokonalováním technologických postupů, a tedy zvyšováním bezpečnosti ochranných prvků je padělání pro zločince stále větší výzvou. Přesto se ale této nelegální činnosti ve značné míře daří. „Mnoho lidí považuje přijímání a vydávání peněz za stereotypní každodenní činnost a nevěnuje pozornost té možnosti, že obdrží padělek. Je pravda, že poznat zdařilý padělek není vždy až tak jednoduché.“ (Chmelík & Bruna, 2015, s. 49).

3.2.3 Podvody páchané na klientech banky

- **Podvody bank na klientech**

Polouček a další (2013, s. 437) neopomíjejí ani podvody klientů bank páchané samotnými bankami, respektive jejími pracovníky. Dochází k nim zejména z důvodu existence informační asymetrie a dominantní pozice některých bank v bankovním sektoru (tyto jevy jsou blíže identifikovány v kapitole 2.2) K vážnému prohřešku došlo mezi 11 investičními bankami banky v USA v roce 2003, kdy tyto banky publikovaly falešné analýzy cenných papírů a nabádaly tak ke koupi akcií, jež samy pokládaly za zcela nevýhodné. Agentura SEC si po těchto bankách vyžádala celkem 1,4 mld. dolarů. Posláním SEC (U. S. Securities and Exchange Commission) je chránit investory, zajišťovat čestnost, spořádanost a efektivitu trhů a umožňovat tvorbu kapitálu. SEC usiluje o to, aby si tržní prostředí zasloužilo důvěru veřejnosti (SEC, 2016).

Na základě informací od Prezidia ČR autorka zmiňuje také zneužívání informací o klientech banky s cílem vylákat z klienta peněžní prostředky (př. § 255 tr. zákoníku – Zneužití informace a postavení v obchodním styku).

Autorka vidí souvislost této problematiky i s článkem Bidrmanové (2022), která bankovní klienty varuje před platbou zbytečně vysokých bankovních poplatků. Podle jejích údajů se jedná o každého druhého klienta, který platí víc, než je nezbytně nutné. K tomuto dochází z toho důvodu, že „Bankéř nebo finanční poradce vám skoro nikdy nedá o hypotéce či úvěrů všechny informace. Někdy ani ty, co jsou ze zákona povinné. A navíc zkoušejí různé manipulace.“

- **Subjekty vydávající se za banku**

Tento druh podvodu se objevuje zejména v rozvojových zemích, nicméně i rozvinuté ekonomiky jej znají. Jde o subjekty, které se tváří jako banka, ale nemají bankovní licenci, bez které se bankou zkrátka nemohou nazývat. V zemích, které se neřadí mezi vyspělé, se navíc vyskytují fiktivní směnárny zahraniční měny na domácí měnu (Kantnerová, 2016, s. 195).

- **Podvody se směnkami a šeky**

Mann (2016, s. 5) vysvětluje, že procesy související s papírovými šeky jsou oproti elektronicky zpracovávaným procesům nákladné a pomalé. Pro verifikaci je v šekovém systému nutný manuální podpis či prokázání totožnosti odpovídajícím průkazem

s fotografií. Ke zjištění, zda bude šek nakonec bankou (na kterou je vystaven) proplacen, je obvykle potřeba několika dní. Právě tyto prodlevy brání systému v jeho efektivnosti. Papírové platební systémy jsou navíc náchylnější ke vzniku podvodů. Doba od okamžiku vkladu do okamžiku, kdy banka potvrdí splnění závazku z šeku plynoucího, je dostatečně dlouhá k poskytnutí příležitosti podvodníkům. V minulosti vznikla řada kreativních schémat, jak v tomto období zpronevěřit peníze banky, do které byl šek vložen. Nejen výše zmíněné vlastnosti tohoto typu placení vedly k obrovskému propadu v jejich užití.

- **Podvody s platebními kartami**

Jak uvádí Jílek (2013, s. 529), podvody s platebními kartami spočívají v nakládání s cizí platební kartou, přičemž cílem může být pořízení produktu či služby bez placení nebo získání peněžních prostředků na kartě přítomných.

Kantnerová (2016) objasňuje, že platebních karet lze zneužít několika způsoby – pomocí bankomatu, platebních terminálů, internetového bankovnictví či samotným odcizením karty. A nejsou to jen hotovostní peníze, které se dají padělat, zločinci totéž umějí i s platebními kartami.

Mann (2016, s. 34-44) v souvislosti s podvody s platebními kartami zmiňuje také chybné transakce, ovšem jak sám tvrdí, chybování nepředstavuje závažný problém, neboť se nejedná o úmyslné jednání. Větší závažnost lze přisoudit neoprávněným transakcím, které se navíc dotýkají autorkou zkoumané problematiky bankovních podvodů. Neautorizované platby jsou vlastně pokusy podvodníků o obdržení zboží či služeb bez úplaty. Přestože k těmto prohřeškům dochází stále méně často, ztráty z nich plynoucí pořád nabývají významných hodnot. Pouze v USA se v průměru jedná o miliardu dolarů ročně.

K podvodu s platební kartou může dle Jílka (2013) dojít dvěma způsoby:

a) **s přítomností karty** (card present transaction) – méně nebezpečná varianta pro vlastníka karty, neboť si je odcizení jeho fyzické karty velmi rychle vědom;
b) **bez přítomnosti karty** (card not present transaction – CNP) – mnohem nebezpečnější, neboť na tuto skutečnost vlastník přijde většinou až s určitým časovým odstupem.

V prvním případě se tedy jedná o krádež fyzické karty, zatímco v druhém případě dochází ke zneužití údajů na kartě uvedených nebo zneužití údajů o účtu, jež je ke kartě veden.

Podle čl. 69 směrnice Evropského parlamentu a Rady (EU) 2015/2366, ze dne 25. listopadu 2015, o platebních službách na vnitřním trhu, má uživatel platebních služeb povinnost oznámit poskytovateli těchto služeb ztrátu, krádež, zneužití prostředku placení nebo platbu bez autorizace, a to bez jakéhokoli prodlení po zaznamenání vzniku této události. Směrnice dále uvádí, že uživatelé platebních prostředků jsou k nahlášení takových skutečností podněcováni stanovením velmi nízké úrovně odpovědnosti, konkrétně ve výši 50 EUR. Pokud však nebylo pro uživatele možné se o takové situaci dozvědět, jeho odpovědnost je nulová.

Mann (2016, s. 67) také uvádí několik opatření, které mají za cíl snížit ztráty z podvodů s platebními kartami. Prvním příkladem jsou specifická pravidla, která slouží k prevenci nevyžádaných emailů o aktivaci karty a také zasílání PIN kódu odděleně od karty. Tímto způsobem je možné omezit podvody s ukradenými kartami, k nimž došlo bez vědomí jejich majitele. Druhým opatřením je autorizace žádosti podané bance obchodníkem a odpověď banky v zašifrované podobě, což způsobuje relativně obtížné získání prostředků prostřednictvím přenosu falešných zpráv. Třetím nástrojem k zastavení podvodníků je software, který je součástí PIN pads (elektronická klávesnice k zadávání osobních identifikačních čísel při platbě platební kartou (Netinbag, n. d.) v místě prodeje. Ten je navržený tak, aby zabránil krádeži šifrovacího protokolu jeho zničením v případě, že někdo s PIN pads manipuluje.

Na tématiku podvodů s platebními kartami je navázáno v Kapitole 3.2.4.

3.2.4 Nové formy podvodů páchaných na klientech

Kantnerová (2016, str. 189) ve své publikaci tvrdí, že nejčastějším předmětem diskusí z hlediska bankovních podvodů jsou v posledních letech klamavé e-maily. Na vzestupu jsou v počtech případů pokusy hackerů o obcházení bezpečnostních systémů bank. Z tohoto důvodu banky vynakládají značně vysoké finanční prostředky do stále novějších metod zabezpečení svých systémů.

Dle mínění autorky je důležité čtenáře v krátkosti seznámit s kybernetickou kriminalitou, která v současnosti stojí za řadou bankovních podvodů. Podle Chmelíka a Bruny (2015, s. 91) se spolu s organizovaným zločinem dokonce jedná o nejzávažnější druh kriminální činnosti. Tento trestný čin je význačný využitím počítače a vysokou mírou sofistikovaností. Formu využití počítače a tím pádem i kybernetickou kriminalitu lze rozdělit do tří základních skupin:

a) počítač jako předmět útoku – jeho napadení s cílem vytěžení jeho dat (obvykle doprovázeno snížením důvěryhodnosti poškozeného, vydíráním apod.);
b) počítač jako nástroj útoku – např. falšování dokumentace, penězokazectví, šíření pornografie či informací zakládajících protiprávní aktivitu;
c) počítač jako pomocný nástroj útoku – např. příprava dokumentů ke spáchání podvodu.

V roce 2020 byl podle Petříčka (2021) zaznamenán nárůst v intenzitě útoků s cílem odcizení finančních prostředků klientů. Autor podotýká, že ve většině případů mohou sami klienti útoku zabránit, problému však nevěnují pozornost a nenahlížejí na něj s dostatečnou mírou závažnosti.

– **Phishing**

Phishing podle Petříčka (2021) aktuálně představuje největší hrozbu pro klienty bank.

Kantnerová (2016, str. 190) vysvětluje phishing jako útoky, které „[…] se pomocí podvržených mailů snaží od klientů získat hesla a další přístupy k účtům.“ Phishing obvykle vypadá tak, že uživateli přijde e-mail, jehož odesílatel se tváří jako banka či známý elektronický obchod.

Pojem phishing vychází z anglického *fishing*, v překladu rybaření. Místo ryb jsou však z obětí vytahovány důvěrné informace. Phishing je označením pro scam (podvod), který zahrnuje podvodné získávání a používání osobních nebo finančních údajů jednotlivce (UcadaVelez, 2004).

Prvním terčem tohoto kriminálního činu u nás byla banka CitiBank v roce 2006 (ČTK, 2006). Klientům jmenované banky bylo slíbeno převedení částky v zahraniční měně na jejich účet, ovšem až po udělení údajného souhlasu vyplněním osobních údajů. Nenásledovalo nic jiného než odčerpání peněz z úču. S phishingem se nejvíce potýkají Spojené státy americké, konkrétně zejména „lídři“ internetového prodeje (např. Amazon) či největší banky (např. Citibank) (Kantnerová, 2016, str. 190-191).

Podle Europolu (2018) kyberkriminálnící spoléhají na to, že většina lidí je velmi zaneprázdněna a došlé korespondenci nevěnuje příliš pozornosti. Phishingové e-maily se obvykle opravdu velmi důvěrně podobají zprávám banky. Mohou být natolik profesionální z hlediska jejich tónu, designu, a dokonce i použití loga banky, že odhalení jejich nečestného původu může být velmi komplikované. Útočníci obvykle vyzývají

příjemce e-mailu ke stažení nějaké přílohy nebo k otevření přiloženého odkazu, a vyvolávají pocit naléhavosti

Podobně o tyto e-maily popisuje i Kantnerová (2016, s. 192), která provádí výčet často používaných frází v podvodných e-mailech, po jejichž existenci by měl příjemce okamžitě zbystřit, a to:

- *Ověřte svůj účet* (o přístupové a osobní údaje firmy/banky přes e-mail nežádají);
- *Pokud neodpovíte do 48 hodin, váš účet bude zrušen* (navození pocitu urgentnosti);
- *Vážený a milý zákazníku* (neadresnost zprávy – bez oslovení jménem);
- *Klepnutím na níže uvedení odkaz získáte přístup ke svému účtu* (odkazování na jiný web).

ČBA (2022) varuje před tzv. bazarovým phishingem, jakož novým způsobem páchání této trestné činnosti. Obyčejně vypadá tak, že kupující pošle prodejci odkaz, kde má prodejce potvrdit přijetí peněz vyplněním údajů na kartě. „Protože jsou klienti oslovováni údajným kupcem jejich zboží, nepředpokládají, že se z nich někdo snaží získat přístupové údaje k jejich účtům, do jejich internetového bankovnictví“. Možná právě kvůli jejímu ošidnému charakteru je tato strategii z hlediska útočníků natolik úspěšnou. V únoru 2022 došlo k desetinásobnému nárůstu výskytu tohoto podvodu, a to zejména na bazaru VINTED.

Značné obavy přinášejí tzv. **phishingové toolkity**, tedy „systém nástrojů, které umožňují velmi jednoduše vytvořit webové stránky bez znalosti HTML“ (Kantnerová, 2016, str. 191).

Phishingové toolkity lze získat velmi snadno. K nalezení na internetu jsou hotové webové stránky i texty e-mailových zpráv, a to konkrétně pro určitou bankovní instituci. Příkladem takového toolkitu může být volně přístupný SniperPhish, který umožňuje vytvářet a plánovat phishingové e-mailové kampaně, vyvíjet webový a e-mailový sledovací kód, tvořit vlastní sledovací obrázky, kombinovat phishingové stránky s e-mailovými kampaněmi pro centrální sledování, sledovat reakce na phishingové zprávy, vytvářet reporty a další (Zorz, 2021).

- **Vishing**

Obdobou phisingu je vishing, ten se však odehrává po telefonu. „Vishing je technika založená na vyvolání strachu a zpanikaření oběti. Klientovi útočník často volá v neobvyklý čas a vydává se za bankéře, případně policistu.“ (ČBA, 2021b).

Vishingu útočníci využívají méně častěji než phishingu, škody na finančním majetku jsou však mnohdy velmi znatelné. „Současně se jedná o metodu, o které mezi veřejností ještě není tak široké povědomí, navíc velmi zákeřnou, neboť útočníci používají různé manipulační techniky, které navíc neustále vylepšují“ (Česká bankovní asociace, 2021b).

Pachatelé volají klientům bank a žádají po nich citlivé údaje, aby zabránili údajným únikům financí z jejich účtů. Předseda Komise České bankovní asociace pro bankovní a finanční bezpečnost Petr Barák však apeluje na to, že „Přihlašovací prvky do internetového bankovnictví či informace o platebních kartách jsou informace, které banky vůbec nepotřebují k tomu, aby dokázaly zablokovat účty. Pokud mě někdo vyzývá, abych mu sdělil tyto bezpečností prvky, tak je to vždycky podvod“ (Česká televize, 2021).

Výsledkem nátlaku a vyvolaného strachu se sami klienti jaksi podvolují podvodníkovi. Tímto způsobem vishing pomáhá prakticky obejít všechny bezpečnostní překážky bank. Právě z toho důvodu je natolik zákeřnou technikou, které je možné zabránit zejména zvýšením povědomí o jejím výskytu (Havlíková, 2021).

- **Smishing**

Také smishing používá telefon jako hlavní nástroj ke zpronevěře peněz obětí. Jeho parketou jsou však výhradně SMS zprávy. Kantnerová (2016, s. 194) mluví o smishingu jako o praktice existující prozatím pouze ve Spojených státech amerických, nicméně nyní už na ni upozorňuje i Hodačová (2021b), podplukovnice Policie České republiky: „Znáte už nový trik podvodníků? Citlivé údaje jako rodná čísla nebo přístupová hesla k bankovním službám lákají prostřednictvím SMS.“

Europol (2018) informuje, že smishingová SMS opět obvykle obsahuje odkaz nebo telefonní číslo. Jednu z možností má adresát využít k údajnému ověření, aktualizaci či znovuobnovení účtu. Odkaz však oběť navede na falešnou internetovou stránku a telefonní číslo k podvodníkovi, který se vydává za legitimní podnik či banku.

Všechny tyto praktiky (a mnohé další), lépe řečeno phishing, vishing i smishing, bývají umocněny metodami **spoofingu**. Právě pomocí spoofingu podvodníci imitují webové

stránky, e-mailové adresy a telefonní čísla reálných důvěryhodných subjektů (Cavaglieri, 2021).

- **Pharming**

Kantnerová (2016, s. 193) vysvětluje pojem pharming jako techniku, jejíž „principem je napadení sysému domén a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu po napsání URL banky do prohlížeče“. Podvodné webové stránky jsou nerozeznatelné od těch oficiálních, což pachateli opět zajistí, že o sobě oběť zcela nevědomě poskytne přístupové údaje ke svému účtu

- **Malware**

Termín malware se původem skládá ze dvou slov, a to z anglického *malicious*, což znamená škodlivý a *software*. „Autoři škodlivého kódu jsou při hledání cestiček, jak infikovat zařízení, velmi kreativní a efektivní. Většinou se snaží útočit z více směrů např. přes neznámé zranitelnosti, s použitím phishingu, skrýváním v paměti nebo imitací legálních procesů v počítači.“ (ESET, 2022)

Bankovní malware je druhem podvodu, který Kantnerová (2016, str. 192) vysvětluje jako „útok na klientské účty prostřednictvím škodlivých virů“. Podle téže autorky se s malwarem potýkají firmy všech velikostí a odvětví.

Petříček (2021) uvádí počítačové viry, se kterými se lze v českém bankovnictví setkat nejčastěji. Jedná se například o Ramnit virus, neboli počítačový červ, který kromě bankovního sektoru významně zasahuje také sociální síť Facebook. Jeho předností je schopnost získání přístupových hesel. Dalším příkladem je TrickBot trojan, jinak řečeno bankovní trojský kůň. I tento se specializuje na krádeže přihlašovacích údajů, avšak z kompromitovaných počítačů. Oproti tomu malware Spy.Zbot trojan pomáhá pachateli na dálku ovládat napadený počítač. Bankovní malware ClipBanker trojan se zaměřuje na odcizování citlivých dat z historie internetového prohlížeče, účtů s kryptoměnou, Skypu nebo Outlooku.

- **Podvody s platebními kartami na internetu**

Problematika podvodů s platebními kartami je pro lepší pochopení vysvětlena již v Kapitole 3.2.3. Nyní je pozornost soustředěna na elektronické platby.

Stejně jako po dobu několika desítek let stabilně klesá finanční náročnost elektronického zpracování transakcí platebními kartami, elektronické platby se také stávají rychlejšími,

efektivnějšími a zvyšuje se i jejich bezpečnost. Vzhledem k tomu, že informace poskytnuté na platební kartě mohou být čteny elektronicky, systém je schopný ověřit autentičnost karty v reálném čase. Ani tento systém samozřejmě není vůči podvodům zcela odolný (Mann, 2016).

S rostoucí globalizací a růstem digitálního světa jsou ale stále častější zejména podvody při CNP transakcích. Jedná se tedy o vzdálené transakce – přes mobilní telefon, fax, internet nebo e-mail. Vzhledem k povaze těchto plateb obchodník jen těžko prověří, zda platbu provádí skutečný majitel karty. Podvodníci z karet obvykle kradou informace jako CVV kód a fakturační adresa (Kantnerová, 2016, s. 193 & Galante, 2017).

Jak uvádí Kantnerová (2016, s. 193), „Mnoho bankovních organizací proto instaluje antiscrinningová zařízení zabraňující skenování karet, neoprávněné stahování jejich dat a dále zkvalitňuje bezpečnost bankomatů a především bezpečnost internetových aplikací."

Galante (2017) uvádí možnosti autentizace online transakcí. Jsou jimi verifikační čísla CVN (která jsou umístěna na zadní straně karty), zřizování černých listin, systém ověření adres AVS (porovnání fakturační adresy poskytnuté klientem s adresou založenou v bance poskytovatele karty).

Také Bradley (2021) uvádí možnosti detekce a prevence podvodů s platebními kartami.

- **3D Secure**
  Jedná se o finanční protokol, který přidává další vrstvu zabezpečení mezi kupujícím, obchodníkem a vydavatelem karty. Při provádění online transakcí tato technika nutí plátce k dodatečnému ověření, čímž se minimalizuje nebezpečí podvodu. Podle Raiffeisenbank (2022) je služba 3D Secure aktuálně nejefektivnější možnou ochranu dat platební karty při platbách na internetu.
- **Dvoufaktorové ověření**
  Při použití dvoufaktorové autentizace mají neoprávněné subjekty výrazně obtížnější přístup k cizím zařízením. Autentizace může být provedena třemi způsoby, tedy heslem, kódem nebo autentizační aplikací. Chce-li klient přistupovat ke svému účtu pomocí dvoufaktorového ověřování, musí zadat alespoň dva z nich.
- **Otisky prstů** (vestavěné snímače otisků prstů má v dnešní době má mnoho zařízení)
- **Strojové učení**

Pokrok ve strojovém učení je nejlepším způsobem ochrany před podvody v elektronickém obchodování. Lze pomocí něho analyzovat miliardy datových bodů a odhalit „podezřelé“ aktivity na účtech.

- **Systémové propojení obchodníků**
  Tvorba sítí, v jejichž rámci dochází ke shromažďování a vyhodnocování objednávek a jejichž členové jsou chráněni, pokud je u jednoho obchodníka detekován podvodný čin.
- **Najímání analytiků** (jejichž doménou jsou podvodná jednání)
- **Záruky zpětného zúčtování**
  Tyto záruky umožňují kompletní vrácení peněz za nákupy, jež byly zajištěny zárukou, ale ukázalo se, že byly podvodné**.**

- **Skimming**

Skimming, na rozdíl od předchozích forem podvodů, nemůže být úspěšný bez faktické přítomnosti platební karty. Jedná se totiž o „Postup, při kterém jsou originální údaje z magnetického proužku karty elektronicky zkopírovány na jinou kartu bez vědomí právoplatného držitele karty“ (Kantnerová, 2016, s. 193). „Nová“ karta může bez jakýchkoli dalších prodlev a úkonů uvedena do užívání.

Policie ČR (2022) uvádí dvě formy skimmingu, a to u bankomatů a u obchodníků, přičemž první je rozšířenější. K bankomatům podvodníci připojují speciální čtecí zařízení a získaná data dále používají k výrobě padělků. Druhá forma spočívá v tom, že kopírování údajů provádí obchodník před navrácením karty jeho majiteli. Nejčastěji se s tímto jevem lze setkat na čerpacích stanicích, v restauracích, barech a hotelech.

FBI (2022) radí, jak se chovat při práci s bankomatem. Před jeho použitím je důležité bankomat a jeho terminál zkontrolovat. Žádné jeho části by neměly být uvolněný, nerovné, poškozené nebo poškrábané. Před zadáním kódu PIN je vhodné zatáhnout za okraje klávesnice a při zadávání PIN kódu zakrýt klávesnici, aby bylo zabráněno kamerovým systémům jej získat. Bankomaty by měly být používány v dobře osvětlených vnitřních prostorách, protože jsou méně zranitelnými cíli.

- **Podvody s kryptoměnami**

Ačkoli je pojem kryptoměna stále považován za poměrně nový, Marr (2017) z časopisu Forbes tvrdí, že existuje již od roku 2009. Technologie, na kterých je tato oblast obchodování postavena, byly však vyvinuty ještě mnohem dříve. Již krátce na to, kdy

zcela poprvé došlo ke zpřístupnění bitcoinového softwaru veřejnosti a Bitcoin se začal těžit, se objevily první kriminální činy v této oblasti.

Výstižně hovoří o bitcoinu Lipovská (2018), dle které „Vznikl původně jako módní hříčka, do které se zamilovali technologičtí nadšenci. Obestřel se přiměřeně lákavou příchutí zakázaného ovoce – je přece „anonymní“, takže se jím mohou hradit nelegální transakce.“

Vzhledem k povaze kryptoměny jakožto anonymního platebního nástroje, jež postrádá dostatečnou míru kontroly, se stala přitažlivým a lukrativním cílem podvodníků. V roce 2014 došlo k pádu Mt. Gox, tehdy největší burzy na světě. Burza zastavila svůj web a všichni její uživatelé ztratili veškerý přístup ke svým prostředkům. Stala se totiž obětí útoku, během kterého bylo odcizen majetek ve výši tehdejších $ 450 milionů. Dnes by se jednalo o částku v řádech miliard dolarů (Marr, 2017).

„Zachovat si utajení a anonymitu na internetu byl vždy problém, avšak dvě technologie první dekády 21. století při jeho řešení pomohly: anonymizační sítě a kryptoměny. Anonymizační sítě jako temná ulička a kryptoměny jako digitální hotovost“ (Chovanculiak, 2020).

Lipovská (2018) však oponuje, že kryptoměna ve skutečnosti anonymní není. Pro její účely je vedena zvláštní databáze nesoucí označení blockchain, který je dle Lipovské „[…] pouze pseudoanonymní systém, který při troše úsilí umožňuje vypátrat totožnost každého, kdo bitcoinem platí“.

Hokrová (2021) uvádí, že je to právě Bitcoin s rostoucí hodnotou, který je pro podvodníky stále více atraktivní. Zločinci spoléhají na to, že se uživatel v problematice kryptoměn příliš dobře neorientuje a obchoduje s ní s naivní vidinou rychlého a snadného zhodnocení svých prostředků. Policisté varují před falešnými reklamami s kryptoměnou. Tato taktika může fungovat například tak, že uživatel klikne na reklamu, čímž je vzápětí přesměrován na podvodný web, který představuje možnost investice do Bitcoinu. Informace sice mohou být zavádějící, to však nedostatečně informovaný investor snadno přehlédne. Aby podvodník získal důvěru návštěvníků webu, poskytuje jim upravené fotografie z médií nebo z rozhovorů veřejně známých osobností.

3.3 Prevence podvodů páchaných na klientech bank

Za účelem detekce bankovních podvodů byl v roce 2008 zahájen projekt, jehož výsledkem bylo vytvoření Jednotné platební euro zóny (Single Euro Payments Area, dále jen SEPA) (Kantnerová, 2016, s. 189).

SEPA vydává soubor nástrojů a standardů, které zjednodušují přeshraniční platby a snaží se o harmonizaci bezhotovostních plateb v eurech napříč Evropou. Umožňuje zákazníkům, podnikům a vládním institucím z různých evropských zemí provádět za stejných podmínek následující transakce:

- bezhotovostní úhrady;
- přímá inkasa;
- platby prostřednictvím platebních karet.

Jednou z několika výhod SEPA je, že zajišťuje levnější, bezpečnější a rychlejší mezinárodní platby, ale také transparentnější stanovování cen díky jednotnému souboru platebních schémat a standardů (Evropská unie, 2021c).

Jak uvádí Petříček (2021) ve svém článku, „Experti se shodují, že v drtivé většině případů bývá chyba na straně klientů“. Právě proto Česká bankovní asociace (ČBA) na svých webových stránkách uvádí tzv. Desatero bezpečnosti, které má lidem ukázat, jak lze chránit jejich finance a osobní údaje. Obsahuje těchto deset zásad bezpečného chování na internetu:

1) *Zabezpečte si počítač*

   Dle ČBA je žádoucí, aby uživatelé internetu měli na svém zařízení nainstalovány antiviry a firewally. Důležité je také průběžně je aktualizovat, aby byly programy schopné rozpoznat i nejnovější viry a hrozby.

2) *Zabezpečte si mobilní telefon*

   Nutnost zabezpečení není přítomna pouze u osobního počítače, ale také u chytrého telefonu. ČBA radí, aby si lidé nainstalovali aplikace nabízené v App Store (pro iOS) či Google Play (pro Android), které jsou buď zcela bezplatné nebo velmi cenově dostupné.

3) *Ověřujte si původ aplikací*

   ČBA lidem dále doporučuje, aby aplikace bezhlavě nestahovali ze všech možných zdrojů, ale naopak využívali výhradně oficiálních mobilních obchodů. Ještě před samotným pořízením aplikace je vhodné si projít recenze předchozích uživatelů.

4) *Chraňte své přihlašovací údaje*

   Přihlašovací údaje jsou citlivými informacemi, načež je nutné s nimi náležitě zacházet. ČBA považuje za nepřípustné je někomu sdělovat, ukládat je na otevřeně přístupných sítích či zadávat na neověřených serverech.

5) *PIN jako oko v hlavě*

   Nastavování co nejsnáze zapamatovatelného hesla, např. zvolením po sobě jdoucích čísel nebo čísel z datumu narození, se nevyplácí. Pro případ zapomenutí je vhodné heslo uložit na bezpečné místo, rozhodně ne blízko platební karty.

6) *Mějte bezpečné heslo*

   Aby bylo možné heslo považovat za bezpečné, musí dle ČBA splňovat čtyři kritéria. Heslo má být *neodhadnutelné*, *silné*, *nezjistitelné* a *unikátní*. Heslo nesmí obsahovat existující slova a slova nějakým způsobem související s osobou uživatele. Mělo by být určeno výhradně pro danou službu (např. není vhodné používat jedno heslo pro internetové bankovnictví a e-mail) a kombinovat velká písmena, malá písmena i zvláštní znaky.

7) *Pozor na neznámé přílohy*

   ČBA upozorňuje na podvodnou poštu, kterým se odesílatelé často snaží vzbudit v příjemci strach (varování před odcizením peněžních prostředků, upozornění na exekuci apod.) či naopak nadšení (oznámení o výhře apod.). E-maily tohoto typu je vhodné vůbec neotevírat, zejména pak jeho přílohy a vložené odkazy. Příjemce by měl věnovat pozornost užívanému jazyku zprávy (pravopis) a adrese odesílatele.

8) *Nakupujte jen u prověřených on-line prodejců*

   Přihlašování a nákup přes internet je nutné provádět pouze na důvěryhodných webových stránkách které lze poznat tak, že před URL adresou zobrazují ikonu zámečku. I zde ČBA vyzdvihuje důležitost recenzí.

9) *Čtěte upozornění banky*

   Mezi mnoha nežádoucími e-maily se mohou objevit i ty, které varují před novými triky hackerů. Přečtení předmětu zprávy nezabere mnoho času ani úsilí a může pomoci příjemce ochránit.

10) Informujte banku

I při sebemenším podezření na jakoukoli nekalou činnost týkající se platební karty či bankovního účtu by měl klient neprodleně kontaktovat zákaznickou podporu své banky (ČBA, 2021a).

Kvůli velkému nárůstů kybernetických trestných činů v bankovnictví se ČBA, Policie ČR a společnost ESET rozhodli v roce 2021 spojit a spustit tzv. Kyberkampaň. Jejím heslem je „Cílem útočníka můžete být i vy!“ a stojí zejména na webové aplikaci Kybertest.cz (ČBA, 2021b).

4 Povědomí klientů bank o rizicích platebního styku a zodpovědnost jejich chování na příkladu České republiky a Francie

Kromě metody dedukce v teoretické části práce je nyní použita také metoda dotazníkového šetření v českém a francouzském prostředí. Jeho cílem bylo zjistit, jak se respondenti orientují v problematice bankovních podvodů a jak jsou zodpovědní v bankovním styku, a zároveň porovnat výsledky mezi oběma zeměmi. Sběr dat probíhal metodou dotazování, která je dle Egera a Egerové (2014, str. 90) vhodná k získávání postojů, názorů, motivace, preferencí, citových stavů, znalostí apod., což zcela koresponduje s autorčinými účely.

Autorka se rozhodla zaměřit na respondenty narozenými v letech 1977-2000, kteří jsou podle Kotlera a Armstronga (2018) představiteli tzv. generaci Y, jež je známá také pod pojmem mileniálové. Lze je považovat za spotřebitele, kteří jsou nejméně stabilní z hlediska jejich financí. Podle Shafiqa a Jana (2017) se jedná o generaci s velkou kupní silou a rozmanitými společenskými a profesními hodnotami, ve které se objevují různé osobnostní profily, postoje a chování. Dle mínění Barské (2018) žijí mileniálové v online světě a ve značné míře využívají k získávání informací internet.

Podle Netzera (2021) patří mezi další charakteristiky této generace v souvislosti s bankovním sektorem jejich poptávka po úvěrech. Jsou jejími nejsilnějšími tahouny a stejný trend je předpokládán i do několika následujících let. Mileniálové si k řízení svých financí zakládají běžné a spořicí účty a návštěva kamenných poboček je pro ně stále méně častá. Pokud nejsou se službami své banky spokojení, neotálejí s přechodem ke konkurenci, a to častěji než jiné generace. Své bankovní aktivity se snaží co nejvíce ulehčit využíváním technologií, a to zejména aplikací mobilního bankovnictví (Lake, 2022). White (2021) sumarizovala výsledky průzkumu „Digital Banking Attitudes Study by Chase“, podle které mobilní bankovní aplikace používá pro své bankovní činnosti rutinního charakteru 98 % všech mileniálů.

Dotazník byl vytvořen pomocí Google Forms, neboť s tímto nástrojem již autorka měla předchozí zkušenosti. Bylo využito možnosti distribuování dotazníku do několika sekcí, což umožnilo jeho větvení v závislosti na odpovědích respondentů. Většina otázek byla uzavřená, pro hlubší analýzu však v dotazníku byly obsaženy i otázky otevřené.

Na úvod dotazníkového šetření byly zařazeny tři filtrační otázky. Cílem bylo, aby dotazník vyplňovali jen mileniálové, kteří jsou majiteli běžného účtu a mají k němu zřízenou platební kartu a používají internetové bankovnictví. Respondenti, kteří nevyhovovali těmto kritériím, byli ze šetření vyloučeny, aby se předešlo případnému pokřivení výsledků.

Za účelem větší přehlednosti jsou výsledky dotazníku rozděleny do těchto kategorií:

- orientace v problematice nelegálních činností v bankovnictví;
- využívání základních služeb k podpoře bezpečnosti bankovního klienta;
- zodpovědnost nakládání s přihlašovacími údaji a hesly;
- zodpovědnost chování na internetu;
- míra optimismu respondentů v otázce bankovních útoků;
- doplňující otázky.

4.1 Výsledky výzkumu

Výsledky zkoumání jsou rozděleny do dvou podkapitol, z nichž první se vztahuje k šetření mezi českými respondenty a druhá k šetření mezi francouzskými respondenty.

4.1.1 Dotazníkové šetření v českém prostředí

V České republice se dotazníkového šetření zúčastnilo celkem 220 lidí, přičemž prvními třemi filtračními otázkami prošlo **206 lidí** ve složení 80 mužů a 126 žen.

Nejvíce respondentů (44 %) má dokončené vysokoškolské vzdělání v bakalářském programu. Další dvě nejpočetnější skupiny představují respondenti se středním vzděláním s maturitou (31 %) a s vysokoškolským vzděláním v magisterském programu (20 %).

Respondenti byli vyzváni k uvedení všech bank, jejichž služby využívají. Většina respondentů je klienty ČSOB (56), Komerční banky (48), Raiffeisenbank (47), Air Bank (37) a České spořitelny (37). Většina respondentů uváděla více bankovních institucí, věrnost jedné bance ukázalo pouze 132 lidí.

- Faktory ovlivňující výběr banky

Pro uvedení do tématu a poskytnutí náhledu do problematiky bezpečnosti bankovních aktivit autorka zjišťovala, jaké faktory jsou pro respondenty nejdůležitější při výběru

banky. Jejím cílem bylo získat představu o tom, na jaké místo klienti řadí bezpečnost, byť v širokém kontextu. Respondenti měli na škále od 1 do 5 (kde 1 = nejvíce; 5 = nejméně) zhodnotit důležitost 13 faktorů, které autorka jmenovala. Z tabulky č. 1 je patrné, že faktor bezpečnosti je pro klienty při výběru banky nejdůležitější. Pro tento údaj je modus roven 1, medián taktéž a aritmetický průměr je 1,47. Dalšími dvěma významnými faktory jsou bankovní poplatky a uživatelské prostředí mobilní aplikace. Naopak za nejméně důležitý faktor lze považovat atraktivitu reklamních sdělení banky.

Tab. č. 1: Faktory výběru banky

Faktory ovlivňující výběr banky	**Hodnotící stupnice míry důležitosti**					**Modus**	**Medián**	**Aritmet. průměr**
	1	**2**	**3**	**4**	**5**			
	Absolutní četnost							
Bankovní poplatky	141	40	15	4	6	**1**	**1**	**1,51**
Šíře balíčku služeb	36	85	59	20	6	2	1	2,39
Hustota sítě poboček	24	68	58	44	12	2	1	2,77
Uživatelské prostředí IB	72	68	46	15	5	1	1	2,09
Uživatelské prostředí mobilní aplikace	96	64	18	8	20	1	1	**1,99**
Komunikace banky se zákazníkem	56	64	56	22	8	2	1	2,33
Prestiž banky	47	86	41	24	8	2	1	2,32
Recenze	59	83	39	15	10	2	1	2,19
Zkušenosti příbuzných a přátel	73	91	26	1	15	2	1	2,00
Bezpečnost	160	22	10	2	12	**1**	**1**	**1,47**
Možnost vedení spoř. účtu, míra zhodnocení	54	70	42	23	17	2	1	2,41
Nabídka úvěr. služeb, výše úrok. sazeb	20	58	58	31	39	2; 3	2	3,05
Atraktivita reklamy	0	21	72	38	75	5	4	3,81
Aritmetický průměr oblasti	-	-	-	-	-	-	-	**2,33**

Zdroj: vlastní výzkum, 2022

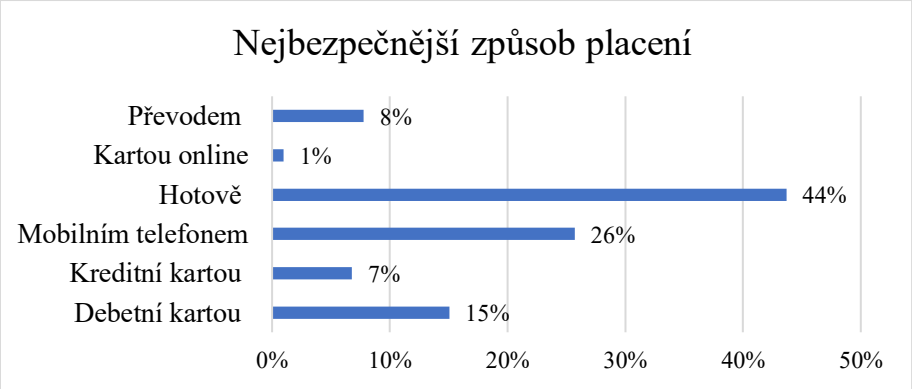
– **Orientace v problematice nelegálních činností v bankovnictví**

Za účelem posouzení orientace respondentů v hrozbách, které na ně jako bankovní klienty čekají, bylo nejprve zjišťováno, jaká forma placení je dle jejich uvážení nejvíce bezpečná.

Respondenti za nejbezpečnější považují hotovostní platby, na druhé místo pak řadí platby mobilním telefonem. Naopak jednoznačně nejméně bezpečné je dle respondentů platit

kartou online. Konkrétní procentuální zastoupení pro jednotlivé platební metody lze vidět na obr. č. 5.

Obr. č. 5: Nejbezpečnější způsob placení

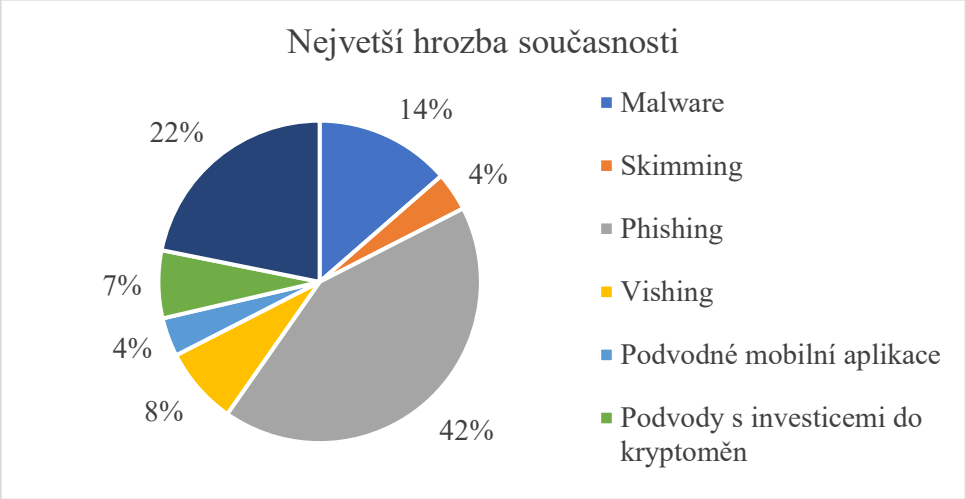


Zdroj: Vlastní zpracování, 2022

Autorka dále vybídla respondenty k uvedení všech nelegálních činností v bankovním sektoru, které je napadají. Respondenti měli prostor pro uvedení jejich vlastní odpovědi. Celkem 16 % dotazovaných z uvádí, že je žádná nelegální činnost nenapadá. Nejčastější jmenovanou praktikou je **zcizení přístupových údajů k internetovému bankovnictví** (15 %). Následují **praní špinavých peněz** (14 %), **phishing** (11 %), **krádeže bez bližší specifikace** (10 %) a krádeže nebo jiné formy zneužití platebních karet (7 %). O něco méně se pak objevují hackerské útoky bez bližší specifikace. Několik málo odpovědí se také týká zneužití bezkontaktních platebních karet. Další jmenované nelegální činnosti autorka kvůli jejich velmi nízkému zastoupení neuvádí.

Respondentům také bylo vypsáno několik různých bankovních útoků na klienty, a to i se stručným vysvětlením. Jejich úkolem bylo zvolit ten z nich, který dle jejich názoru v současnosti představuje největší hrozbu. Tato otázka byla zařazena až na konec dotazníku, kdy už si respondenti na problematiku udělali vlastní obrázek. Chyták byl však v tom, že správnou odpovědí (ve skutečnosti však lze jen těžko s jistotou říci, který z uvedených je aktuálně nejčastější/nejnebezpečnější – ať už z důvodu neustále se měnících praktik, tak i z důvodu nedostatečných či pokřivených statistik) byl phishing, o kterém v předchozí části dotazníku nebyla ani zmínka. Povědomí o existenci tohoto typu útoku mohli respondenti dokázat pouze jeho vyslovením v předchozí otevřené otázce (viz výše). Všechny typy útoků a jejich procentuální zastoupení ukazuje obr. č. 6.

Obr. č. 6: Největší hrozba současnosti



Zdroj: vlastní průzkum, 2022

– **Využívání základních služeb k podpoře bezpečnosti bankovního klienta**

Způsobů, kterými se klienti bank mohou chránit před útoky různého charakteru, je celá řada. Příkladem je používání antivirových systémů, což bylo předmětem jedné z otázek výzkumu. Respondenti měli uvést, zda používají antivirové systémy, přičemž na výběr měli ze čtyř odpovědí a mohli zvolit jednu či více z nich.

Celkem 48 % respondentů z má instalovaný antivirový program ve svém počítači, 16 % pak ve svém mobilním telefonu. 25 % respondentů uvádí, že antivirové systémy vlastní a zároveň aktualizují a pouze 11 % je zcela nepoužívá.

Pro informace o tom, jak zvýšit ochranu svých financí, klienti bank nemusejí chodit daleko. Množství rad a tipů jim předávají sami jejich bankovní poskytovatelé. Z tohoto důvodu bylo dále zkoumáno, jak často (na škále od 1 do 5, kde 1 = vždy, 5 = nikdy) klienti čtou zprávy a oznámení v došlé korespondenci od banky.

Mezi respondenty lze nalézt nejvíce odpovědí přesně ve středu stupnice, hodnoty 3 nabývá modus i medián. S ohledem na zjištěný aritmetický průměr lze vyvodit, že respondenti zprávám zasílaných bankami pozornost spíše nevěnují. Výsledky přehledně zobrazuje tab. č. 2.

Tab. č. 2: Čtení zpráv a oznámení od banky

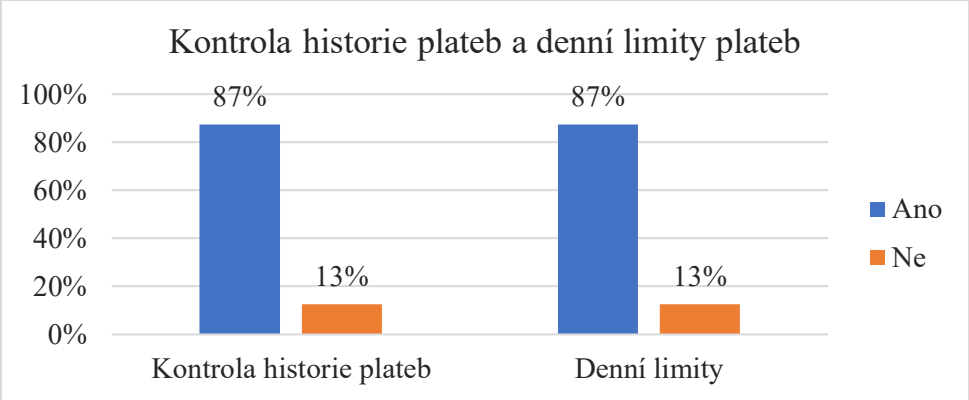
Faktor zkoumání	Hodnotící stupnice míry frekvence					Modus	Medián	Aritmet. průměr
	1	2	3	4	5			
	Absolutní četnost							
Čtení zpráv a oznámení od banky	7	33	85	67	14	3	3	3,23

Zdroj: Vlastní zpracování, 2022

Pro doplnění autorka zjišťovala, zda je uvedená oznámení obtěžují. 20 % dotazovaných přiznává, že ano. Pouze 24 % respondentů odpovídá zcela pozitivně a neutrální postoj pak zastává 55 % z nich.

Dalším způsobem, kterým klienti bank mohou posílit svou bezpečnost, je zachování přehledu o jejich transakcích. Respondentům tedy byla položena otázka, zda průběžně kontrolují historii svých plateb či nikoli. Z výsledků je dále patrné, že naprostá většina pravidelnou kontrolu historie svých plateb preferuje. Také nastavování denních limitů pro maximální výši transakci má mezi respondenty oblibu. Obě tyto oblasti zkoumání ukázali naprosto stejný výsledek, což graficky znázorňuje obr. č. 7.

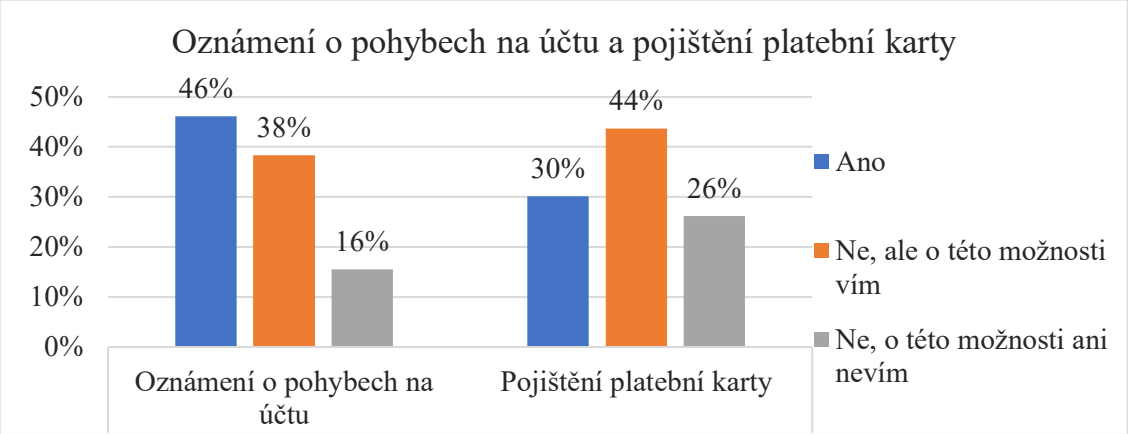
Obr. č. 7: Kontrola historie plateb a nastavování maximální výše limitů plateb



Zdroj: Vlastní zpracování, 2022

Posuzována také byl znalost dalších služeb banky, které pomáhají klientovi chránit jeho prostředky. Jedná se o oznámení o pohybech na účtu a pojištění platební karty. Výsledky ukazují, že téměř polovina respondentů má nastavenou službu, která jim oznamuje pohyby prostředků na jejich bankovním účtu. Pouze malá část dotazovaných o této možnosti neví. Služby pojištění své platební karty už využívá méně respondentů a stejně tak větší část z nich o existenci této ani nemá tušení. Konkrétní míru využívání obou zmíněných služeb zachycuje obr. č. 8.

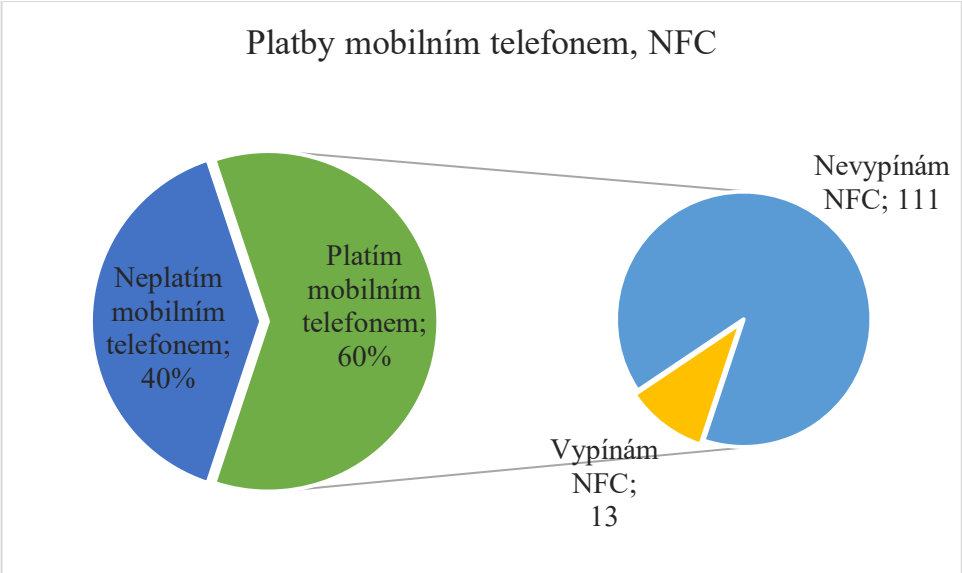
Obr. č. 8: Využívání služeb: zasílání oznámení o pohybech na účtu a pojištění karty



Zdroj: vlastní průzkum, 2022

Dalším předmětem zkoumání bylo placení v obchodech pomocí mobilního telefonu jakožto náhrady za fyzickou kartu. Více než polovina respondentů tímto způsobem platby provádí (124 osob). V případě pozitivní odpovědi byli respondenti přesměrováni na otázku týkající se technologie NFC. Pojem NFC byl respondentům vysvětlen, aby se předešlo jakýmkoli nedorozuměním. Otázkou tedy bylo, zda si respondenti NFC vypínají, pokud ji právě nepoužívají. Z výsledků jasně plyne, že převážná většina respondentů tak nečiní. Výsledky je pro lepší představu možné zhlédnout v obr. č. 9.

Obr. č. 9: Platby mobilním telefonem a vypínání technologie NFC



Zdroj: vlastní průzkum, 2022

S respondenty využívajícími k platbám mobilní telefon bylo pracováno i dále. Bylo zjišťováno, jaké ověření respondenti pro tento druh placení používají, přičemž měli na výběr ze čtyř možností či mohli udat vlastní odpověď. Nejčetnější zastoupení má sken

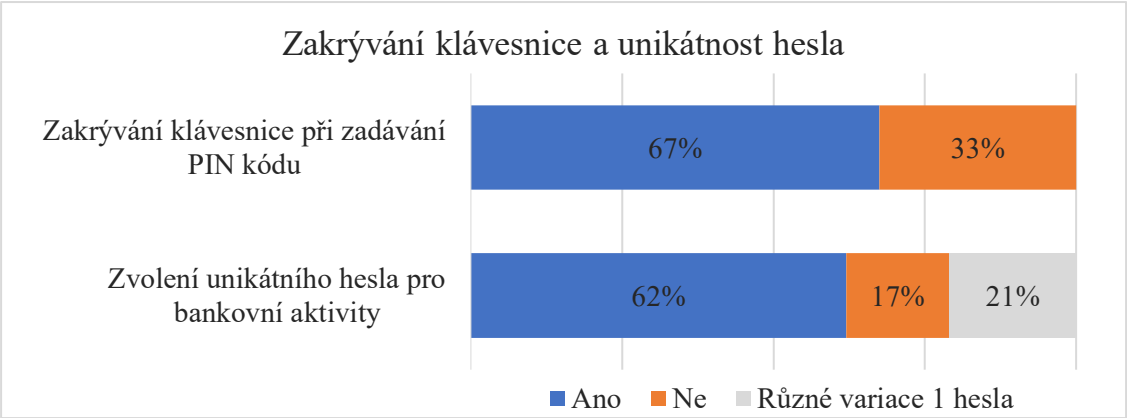
obličeje (66 %) a druhý v pořadí je otisk prstu (31 %). Poslední návaznou otázkou bylo, zda pro odemknutí telefonu dotazovaní používají stejnou kombinaci, jako je jejich PIN ke kartě. Podoba těchto dvou kódů je totožná u téměř každého čtvrtého respondenta (27 %).

– **Zodpovědnost nakládání s přihlašovacími údaji a hesly**

Dotazník dále obsahoval několik otázek, jejichž cílem bylo zhodnotit, jak zodpovědný přístup mají respondenti ke svým citlivým údajům a heslům. Snadno lze mezi sebou porovnávat následující dvě.

Tou první je, zda si respondenti při zadávání PIN kódu zakrývají klávesnici (platebního terminálu/bankomatu apod.). Větší část respondentů se v tomto smyslu chová zodpovědně. Bodem zájmu druhé otázky byla unikátnost hesel. Volbu jednoho unikátního hesla výsadně pro bankovní aktivity potvrzuje více než polovina dotazovaných. Tendenci k používání různých variací jednoho hesla pro více služeb/webů pak má přibližně jedna pětina respondentů. Grafické shrnutí výsledků těchto dvou otázek zobrazuje obr. č. 10.

Obr. č. 10: Zakrývání klávesnice při zadávání kódu a unikátnost zvolených hesel

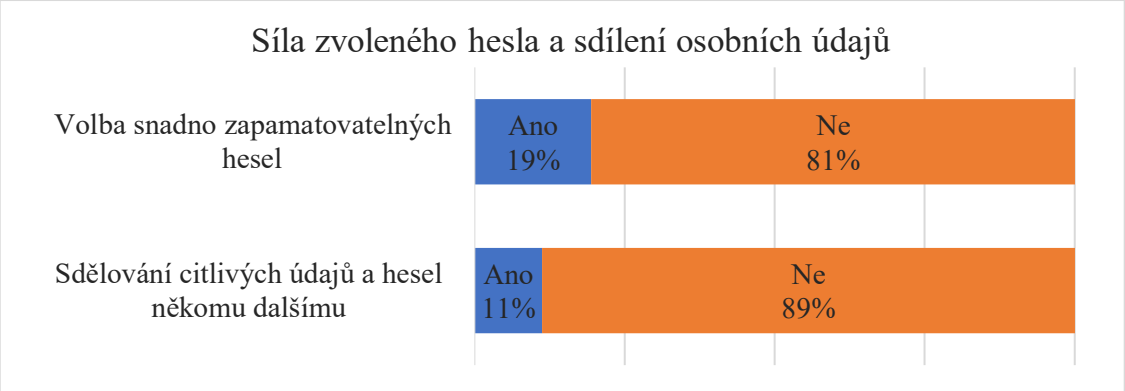


Zdroj: vlastní průzkum, 2022

Častou chybou klientů bank je nastavování snadno zapamatovatelných hesel, která jsou pak podstatně náchylnější ke zneužití. Tázaní proto měli uvést, zda si pro své bankovní činnosti volí snadno zapamatovatelná hesla, přičemž jim byly poskytnuty dva příklady takového jednání (hesla obsahující celá slova či data narození). Z výsledků je patrné, že se většina respondentů snaží volit spíše obtížněji zapamatovatelná hesla. Dalším nevhodným způsobem nakládání s hesly je jejich sdělování někomu dalšímu. V závislosti na tom byli respondenti dotazováni, zda někdo zná jejich přihlašovací údaje k internetovému bankovnictví nebo PIN ke kartě. Naprostá většina dotazovaných tvrdí,

že nikdo nezná jejich údaje pro přihlášení do internetového bankovnictví ani PIN k jejich platební kartě.

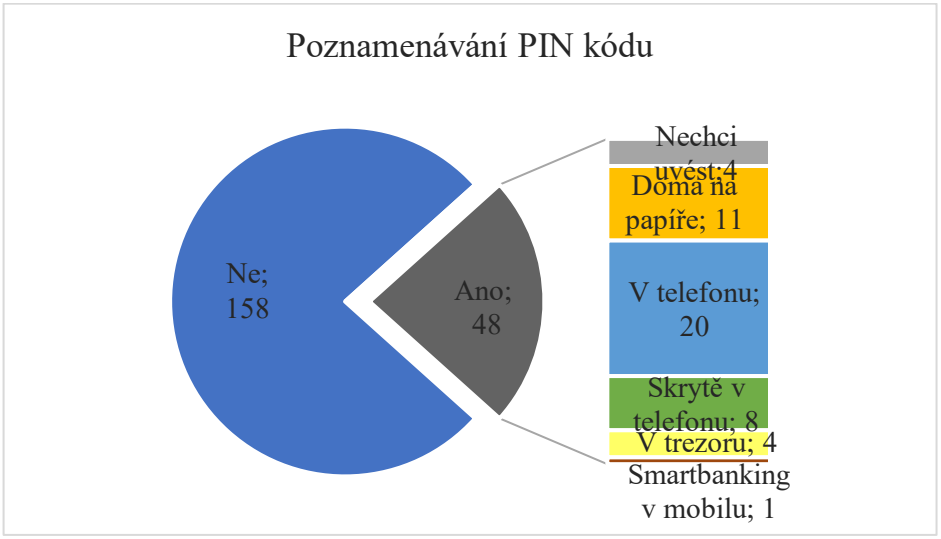
Obr. č. 11: Síla zvoleného hesla a sdílení osobních údajů



Zdroj: vlastní průzkum, 2022

Lidská paměť není všemocná a někdy zkrátka selže. Otázkou autorky tedy bylo, zda mají respondenti někde poznamenaný svůj kód ke kartě. Výsledky říkají, že naprostá většina z nich (77 %) má PIN kód pouze ve své paměti. Zbylá část respondentů byla dále pobídnuta k zodpovězení otevřené otázky, kde přesně mají PIN poznamenaný. Nejvíce respondenti uvádějí telefon, druhou nejfrekventovanější odpovědí je papírová forma u nich doma a třetí pak opět telefon, kdy však respondenti blíže specifikují, že nalezení tohoto údaje je pro cizí osobu zkomplikováno. Jak byly nejčastější odpovědi poměrově rozloženy, lze vidět na obr. č. 12.

Obr. č. 12: Poznamenávání PIN kódu



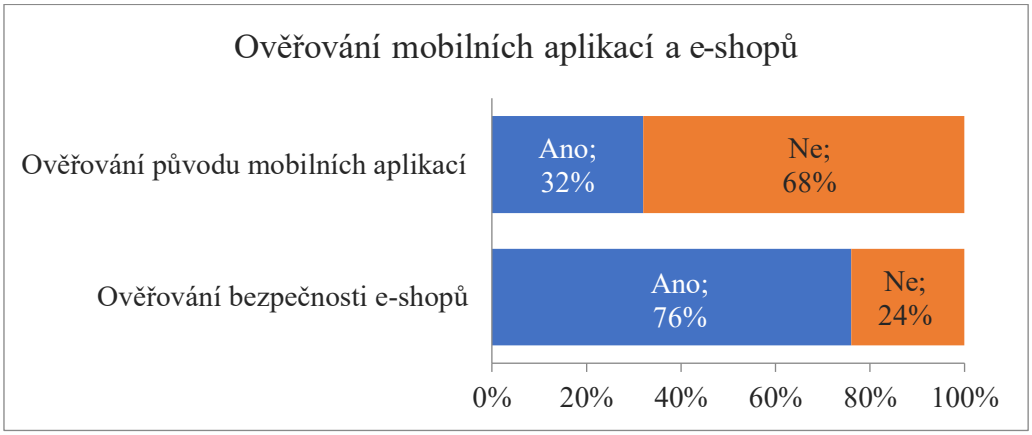
Zdroj: vlastní průzkum, 2022

– **Zodpovědnost chování na internetu**

Se stále rostoucí mírou užívání internetu současně přibývá kybernetické kriminality. I v tomto ohledu však klienti mohou být proaktivní a snížit tako riziko útoku na ně a své finance.

Vzhledem k tomu, že se nákup a prodej ve velké míře přesouvá z kamenných prodejen na internet, bylo autorkou zjišťováno, zda si respondenti ověřují bezpečnosti e-shopů, ze kterých nakupují. Z výsledků plyne, že absenci ověřování přiznávají přibližně dvě třetiny respondentů. U dalšího dotazu, jehož předmětem je tentokrát ověřování bezpečnosti e-shopů, bylo dosaženo mnohem pozitivnějšího výsledku. Více než tři čtvrtiny respondentů tak provádí. Procentuální zastoupení a lepší představu o rozdílnosti výsledků těchto dvou zkoumaných skutečností poskytuje obr. č. 13.

Obr. č. 13: Ověřování e-shopů a mobilních aplikací



Zdroj: vlastní průzkum, 2022

Za účelem bližšího porozumění výše zmiňované problematiky autorka dále pracovala s respondenty s pozitivní odpovědí. Dotazovala se, jakým způsobem tato ověření provádí, přičemž odpověď byla otevřená a tedy plně v gesci každého z respondentů.

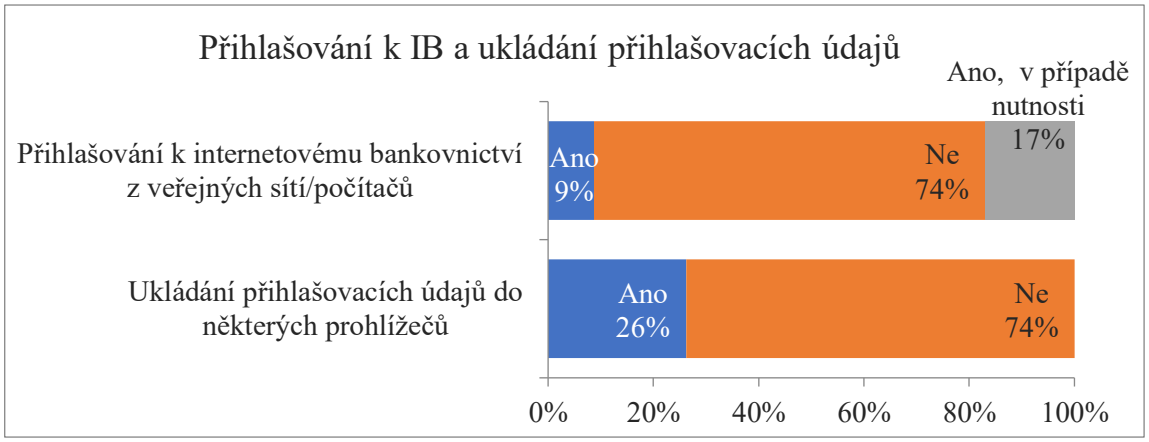
Synonymní odpovědi 66 respondentů, kteří si ověřují původ mobilních aplikací, byly sumarizovány do kategorií. Nejvíce krát se objevuje procházení recenzí na internetu (30 odpovědí), za nimiž následuje stahování aplikací pouze z oficiálních obchodů pro Andriod a iOS Google Play a App Store (24). Také ověření na základě vývojáře aplikace mělo relativně početné zastoupení (14).

V případě verifikace e-shopů jsou odpovědi mnohem rozmanitější, což je dáno také větším počtem respondentů (157), jak je výše znázorněno v obr. č. 3. I v tomto případě první místo bezesporu náleží recenzím na internetu (135 odpovědí). Další druhy ověření

jsou v početnosti poměrně vyrovnané, ale jejich zastoupení je mnohem slabší. Jedná se o známost e-shopu (12), předchozí osobní zkušenost a zkušenosti přátel (12), vzhled webu, jeho celkový dojem a důvěryhodnost (10), platnost webového certifikátu (10), informace na webu (kontakt, sídlo, obchodní podmínky apod.; 8) a dostupné platební metody (8).

V souvislosti s bezpečným chováním na internetu byly respondentům položeny další dvě otázky, jejichž odpovědi lze mezi sebou porovnávat. V prvním případě se jednalo o zjištění, zda se respondenti někdy ke svému internetovému bankovnictví přihlašují z veřejné sítě či veřejného počítače. V převážné většině případů se toto chování respondentů netýká a malá část z nich tak činí pouze v případě nutnosti. Výsledky byly podobné i u druhé otázky, jejímž předmětem bylo, zda si respondenti ukládají své přihlašovací údaje do některých prohlížečů. Pro přesnější vyjádření a ilustraci diskutovaných pojmů slouží obr. č. 14.

Obr. č. 14: Přihlašování k IB a ukládání přihlašovacích údajů

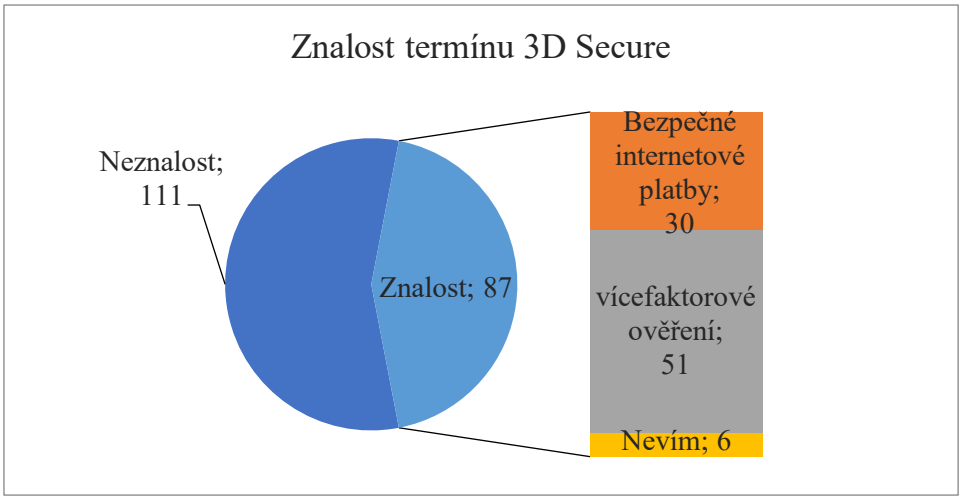


Zdroj: vlastní průzkum, 2022

Posledním zkoumaným pojmem v této kategorii šetření byl 3D Secure. Autorka se nejdříve ptala, zda respondenti platí kartou na internetu. Z celkového počtu 206 respondentů jich odpovědělo kladně 198. Právě těmto respondentům byla položena návazná otázka, zda vědí, co je systém 3D Secure. Neznalost vyjádřila více než polovina z nich. Ti, jež odpověděli, že je pro ně tento pojem familiární, byli vyzváni k vysvětlení pojmu prostřednictvím otevřené odpovědi. Nejvíce byla v odpovědích zaznamenána nějaká forma vícefaktorové verifikace. Značné množství respondentů tento pojem vysvětlovalo velmi zeširoka jako způsob zabezpečení internetových plateb, což autorka za znalost nepovažuje. Tato skutečnost totiž byla zřejmá z položené otázky, zda

respondenti platí kartou na internetu. Grafické vyhodnocení znalosti pojmu 3D Secure mezi respondenti ukazuje obr. č. 15.

Obr. č. 15: Znalost termínu 3D Secure



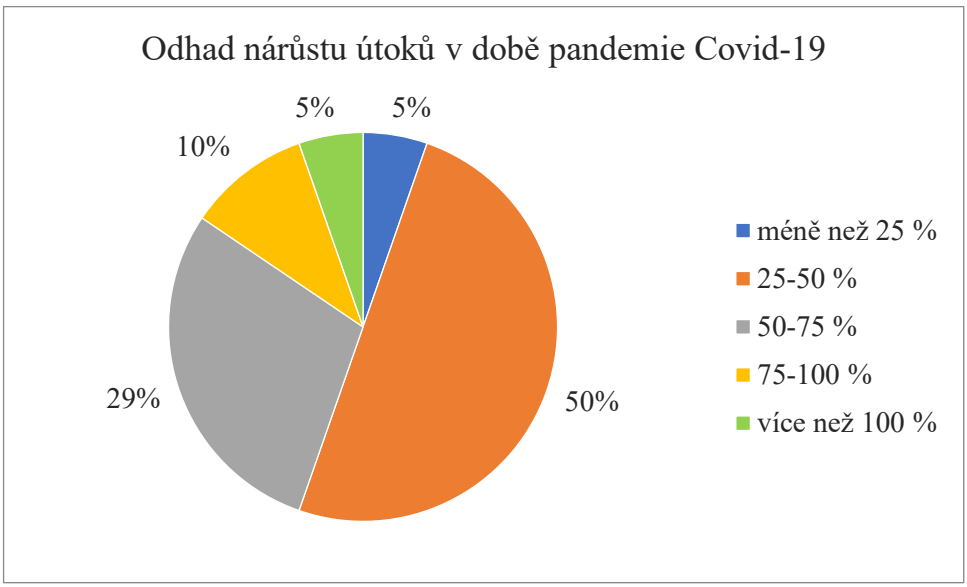
Zdroj: vlastní průzkum, 2022

– **Optimismus/pesimismus respondentů**

Dalším cílem autorky bylo získat představu o tom, zda na diskutovanou závažnost problematiky respondenti nahlížejí spíše optimisticky či pesimisticky.

Dotazovaným bylo sděleno, že v době pandemie Covid-19 došlo k nárůstu digitálních podvodů ve finančním sektoru. Respondenti pak měli odhadnout, jak velký byl tento nárůst, je-li jako srovnávací období uvažováno předpandemické období. Majoritní zastoupení získalo mezi respondenty rozmezí 25-50 %. Celkové výsledky je možné si prohlédnout v obr. č. 16.

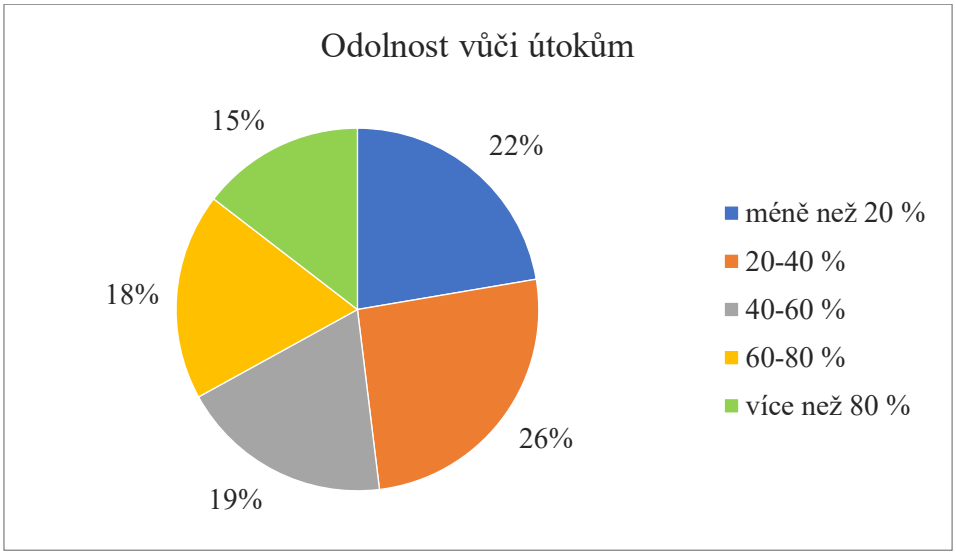
Obr. č. 16: Odhad nárůstu útoků v době pandemie Covid-19



Zdroj: vlastní průzkum, 2022

Následně měli respondenti odhadnout, jak velkou část útoků se v ČR daří zastavit. Dle údajů ČBA se jedná o 86 % útoků. Úspěšnost odhadu respondentů znázorňuje následující obrázek.

Obr. č. 17: Odhad míry zastavení útoků



Zdroj: vlastní průzkum, 2022

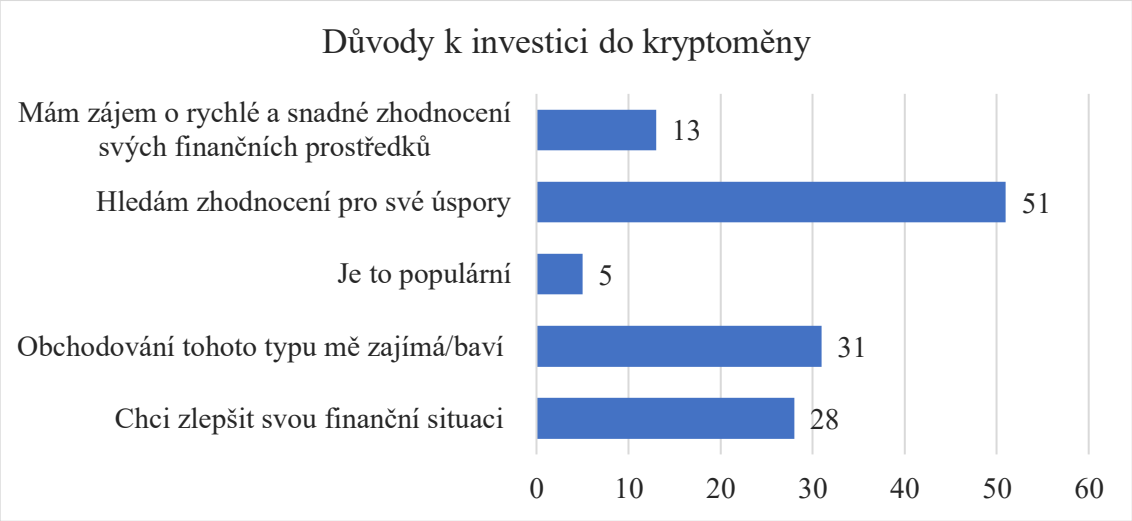
– **Doplňující otázky**

Ve snaze postihnout problematiku co nejkomplexněji bylo do dotazníku začleněno ještě několik málo otázek nad rámec výše popsaných tematických okruhů.

V poslední době je na vzestupu investování do kryptoměny, což je bohužel současně doprovázeno i jeho atraktivitou pro nejrůznější podvodníky. Vzhledem k této skutečnosti byli respondenti nejprve dotazováni, zda investují do kryptoměny nebo nad ní přinejmenším někdy uvažovali. Podle výsledků tato forma investování není v objektu zájmu více než poloviny respondentů, konkrétně se jedná o 128 (z 206) jedinců. Zbylí respondenti (78) byli dále dotazováni, z jakého důvodu je pro ně investice do kryptoměny přitažlivá. Autorku zajímalo zejména to, zda jsou respondenti v rozhodování o této investici racionální, či zda je jejich interes tažen převážně touhou po rychlém a snadném získání financí. Dotazovaní tedy měli vybrat motiv investice, přičemž měli na výběr z pěti možností, z nichž mohli zvolit jednu, či více. V případě potřeby také měli možnost vyjádřit se individuálně. Z výsledků lze vyvodit, že respondenti investují nebo chtějí investovat do kryptoměny převážně za účelem zhodnocení jejich úspor. Druhým nejčastějším důvodem je zanícenost pro tento druh obchodování. Na další pozici těsně

následuje zájem o zlepšení finanční situace respondenta. Všechny odpovědi a četnost jejich zastoupení znázorňuje obr. č. 18.

Obr. č. 18: Důvody k investici do kryptoměny

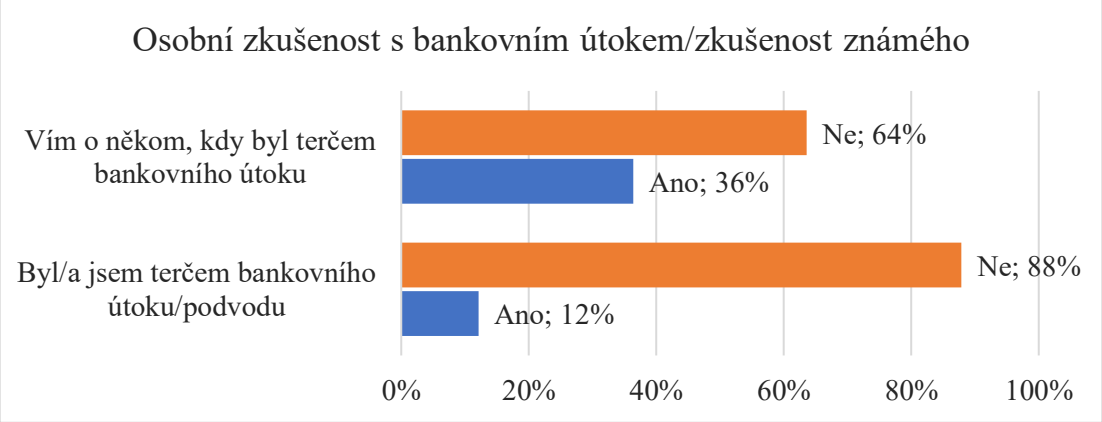


Zdroj: vlastní průzkum, 2022

Pro doplnění bylo zjišťováno, zda respondenti někdy klikli na reklamu s kryptoměnou. Přibližně 2/3 (69 %) tvrdí, že nikoli.

V závěru dotazníku byly formulovány dvě zásadní otázky. První z nich byla, zda se přímo dotazovaní někdy stali terčem bankovního útoku. Výsledky jednoznačně ukazují, že většina respondentů nikdy osobní zkušenost s bankovním útokem neměla. U druhé otázky už byl trend o něco lépe rozložen do kladného i negativního rozměru. Více než jedna třetina dotazovaných totiž uvádí, že se někdy s obětí bankovního podvodu setkala. Lépe výsledky zobrazuje obr. č. 19.

Obr. č. 19: Zkušenost s bankovním útokem



Zdroj: vlastní průzkum, 2022

O problémech sužujících společnost je nutné hovořit. Tím nejrozšířenějším prostředkem komunikace s veřejností je nějaká forma reklamy, která se na spotřebitele doslova řítí ze všech stran. Autorku tedy zajímalo, zda je i v této oblasti reklama aktivní. Otázkou na respondenty bylo, zda mají pocit, že jsou s praktikami útočníků zaměřených na bankovní klienty v dostatečné míře seznámeni prostřednictvím mediálních prostředků. Respondentům tedy bylo předloženo tvrzení „O problematice bankovních podvodů nás dostatečně informují média“, přičemž formou odpovědi byla škála, kde 1 odpovídá „silně souhlasím“ a 5 odpovídá „silně nesouhlasím“. Z níže uvedené tabulky (tab. č. 3) lze vypozorovat, že se respondenti přiklánějí spíše k názoru, že mediální angažovanost není v problematice bankovních útoků dostatečná. Nejčetnější zastoupení na škále má hodnota 4, medián nabývá hodnoty 3 a aritmetický průměr činí 3,34.

Tab. č. 3: Zhodnocení míry mediální informovanosti o bankovních podvodech

„O problematice bankovních podvodů nás dostatečně informují média.“

Hodnotící stupnice míry souhlasu					**Modus**	**Medián**	**Aritmet. průměr**
1	**2**	**3**	**4**	**5**			
Absolutní četnost							
8	26	75	81	16	4	3	3,34

Zdroj: vlastní průzkum, 2022

Posledním dotazem kladeným respondentům bylo, jaká banka je dle jejich mínění nejbezpečnější. Většina respondentů zmíněné nedokáže posoudit (42 %). Třemi nejčastěji jmenovanými bankami pak byla Česká spořitelna (20 %), Komerční banka (15 %) a ČSOB (11 %).

4.1.2 Dotazníkové šetření ve francouzském prostředí

S ohledem na ztížené podmínky provádění dotazníkového šetření mezi občany jiné než české národnosti bylo ve Francii získáno celkem 128 respondentů, z nichž filtrací prošlo **103 respondentů**, konkrétně 55 žen a 48 mužů.

Převládajícím dosaženým stupněm vzdělání bylo vysokoškolské magisterské (35 %), dále střední s maturitou (24 %) a vysokoškolské s licencí (23 %; odpovídá českému titulu „bakalář“).

Francouzští respondenti prokázali větší míru věrnosti jedné bance, neboť 97 respondentů vyplnilo pouze jednu banku, které jsou klienty. Nejčastěji se jednalo o banky Crédit Agricole (19), La Banque Postale (17), BNP Paribas (22) a Banque Populaire (10).

– Faktory ovlivňující výběr banky

Ještě před ponořením se hlouběji do problematiky útoků na klienty bank bylo autorkou zkoumáno, zda má bezpečnost banky v obecném měřítku své nezastupitelné místo v momentě, kdy se respondenti rozhodují o výběru banky. Respondentům bylo předloženo 13 faktorů, jež u nich mohou hrát roli v posuzování vhodnosti. U každého z těchto faktorů měli respondenti zhodnotit, jak důležitý je pro ně při výběru banky, a to na škále od 1 do 5, kde 1 = nejvíce důležité a 5 = zcela nedůležité. Z výsledků uvedených v tabulce níže plyne, že je to právě bezpečnost, která u respondentů v z hlediska důležitosti převažuje všechny ostatní faktory. Modus i medián nabývají hodnoty 2, aritmetický průměr pak 1,9. Druhým nejdůležitějším faktorem jsou bankovní poplatky a zkušenosti příbuzných a přátel. Na druhou stranu nejméně důležitá je dle respondentů atraktivita reklamy, modus zde dosahuje hodnoty 3, medián též a aritmetický průměr 2,73. Souhrn všech výsledných hodnot u jednotlivých faktorů poskytuje tab. č. 4.

Tab. č. 4: Faktory výběru banky

Druh služby	**Hodnotící stupnice míry důležitosti**					**Modus**	**Medián**	**Aritmet. průměr**
	1	**2**	**3**	**4**	**5**			
	Absolutní četnost							
Bankovní poplatky	41	33	22	7	0	**1**	**2**	**1,95**
Šíře balíčku služeb	22	45	26	10	0	2	2	2,23
Hustota sítě poboček	18	45	28	8	4	2	2	2,37
Uživatelské prostředí IB	25	45	31	2	0	2	2	2,10
Uživatelské prostředí mobilní aplikace	30	32	37	2	2	3	2	2,17
Komunikace banky se zákazníkem	22	42	28	11	0	2	2	2,27
Prestiž banky	19	45	33	3	3	2	2	2,28
Recenze	18	46	35	2	2	2	2	2,26
Zkušenosti příbuzných a přátel	33	43	23	4	0	**2**	**2**	**1,98**
Bezpečnost	38	41	20	4	0	**2**	**2**	**1,90**

Možnost vedení spoř. účtu, míra zhodnocení	24	42	33	4	0	2	2	2,17
Nabídka úvěr. služeb, výše úrok. sazeb	20	39	41	3	0	3	2	2,26
Atraktivita reklamy	17	25	36	19	6	3	3	2,73
Aritmetický průměr oblasti	-	-	-	-	-	-	-	**2,21**

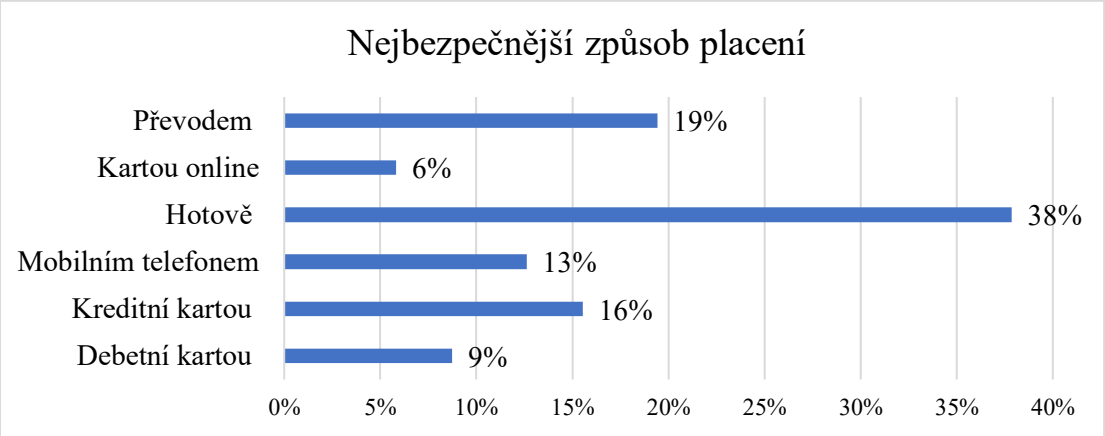
Zdroj: vlastní průzkum, 2022

– **Orientace v problematice bankovních podvodů**

Autorka nejprve zjišťovala, jak se respondenti orientují ve zkoumané problematice.

Její první otázkou bylo, jaký druh placení je dle mínění respondentů nejbezpečnější. Bezkonkurenčně nejvyššího výsledku dosahuje platba hotovostí. Následuje platba převodem a poté platba kreditní kartou. Nejnižší četnost zastoupení lze připsat platbě kartou na internetu, která je tedy podle respondentů nejrizikovějším způsobem transakce. Přehledné znázornění výsledků poskytuje obr. č. 20.

Obr. č. 20: Nejbezpečnější forma placení



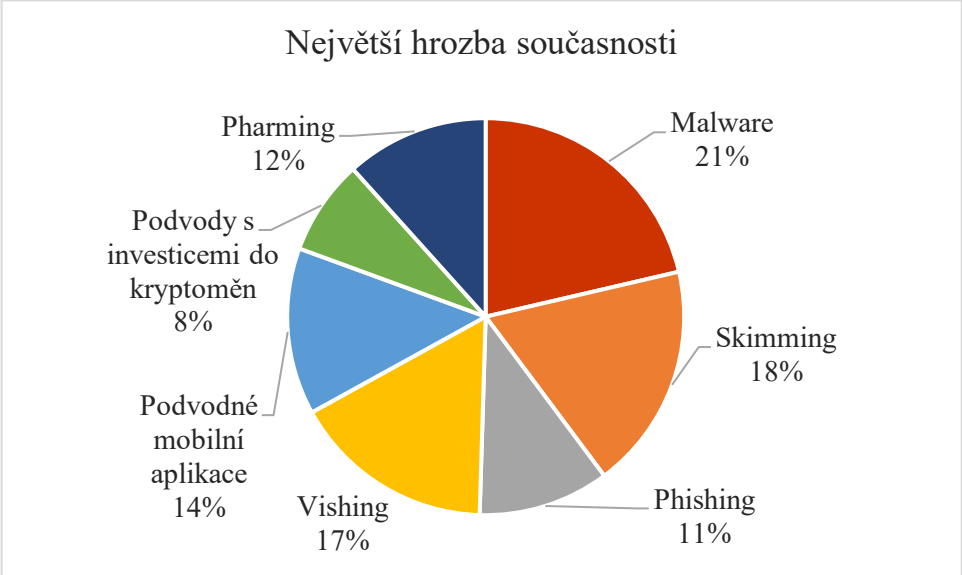
Zdroj: vlastní průzkum, 2022

Další otázka dala respondentům možnost se otevřeně vyjádřit a uvést, jaké všechny nelegální aktivity jim v souvislosti s bankovním stykem vyvstávají na mysli. Nejvíce respondenti zmiňují **falešné webové stránky** či **falešné aplikace**, které se v odpovědích vyskytují ve 22 % případů. Také zcizení karet či jiné formy **zneužití platebních karet** jsou v odpovědích významně zastoupeny (17 %). Relativně velké množství respondentů (16 %) prokazuje úplnou neznalost, neboť je žádná kriminální činnost v bankovnictví nenapadá. Další zmíněné aktivity zahrnují viry (15 %), skimming (11 %) a phishing (10

%). Několik málo dalších odpovědi autorka neuvádí, neboť jejich zastoupení není významné.

Na podvodné činnosti byla zaměřená i otázka, u které měli respondenti zvolit, jaká z vyjmenovaných praktik (vč. jejich vysvětlení) podvodníků aktuálně představuje pro klienty bank největší hrozbu. Možných odpovědí bylo sedm, přičemž z výsledků není jasně patrný převažující trend. S přihlédnutím na procentuální vyjádření četnosti odpovědí lze usoudit, že největší hrozbu respondenti spatřují v malwaru, za kterým následuje skimming. Nejmenší hrozbou se pak respondentům jeví podvody s investicemi do kryptoměny. Výsledek je graficky znázorněn v obr. č. 21.

Obr. č. 21: Největší hrozba současnosti



Zdroj: vlastní průzkum, 2022

– **Využívání základních služeb k podpoře bezpečnosti bankovního klienta**

Respondenti měli dále vyjádřit svou preferenci používání antivirových systémů. K dispozici měli čtyři odpovědi, přičemž povoleno bylo vybrat jednu či více z nich. Bylo zjištěno, že většina respondentů (44 %) má antivirem zabezpečený svůj počítač. Zato používání těchto systémů v mobilním telefonu potvrzuje pouze 11 % respondentů. Pouhá instalace antiviru však nemusí být dostačující. Aby byla podpořena jejich účinnost, je na místě také jejich pravidelná aktualizace. Celkem 24 % respondentů uvádí, že antivirové systémy používají a zároveň provádějí jejich aktualizace. Žádné antivirové systémy pak nepoužívá 21 % respondentů.

Autorka se dále dotazovala, jak často respondenti čtou zprávy a oznámení banky. Vzhledem k tomu, že se touto formou banky ve značné míře snaží varovat své klienty před nejrůznějšími hrozbami, považuje autorka tuto otázku za velmi důležitou. Respondenti měli odpovědět na základě hodnotící škály 1-5, kde 1 = vždy a 5 = nikdy.

Výsledky neprokazují znatelnější sklon respondentů k pozitivní nebo negativní odpovědi, modus i medián nabývají hodnoty 3 a aritmetický průměr hodnoty 3,13. V porovnání krajních pólů však lze zaznamenat znatelnou nerovnováhu. Zatímco zprávy od bank nikdy nečte 17 % respondentů, vždy jim pozornost věnují pouze 4 % respondentů. Výsledky jsou shrnuty v tab. č. 5.

Tab. č. 5: Čtení zpráv a oznámení od banky

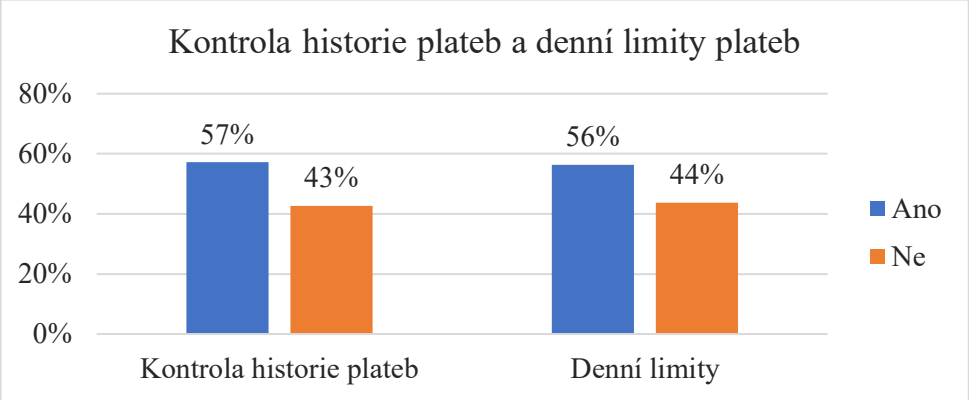
Faktor zkoumání	Hodnotící stupnice míry frekvence					Modus	Medián	Aritmet. průměr
	1	2	3	4	5			
	Absolutní četnost							
Čtení zpráv a oznámení od banky	4	29	37	16	17	3	3	3,13

Zdroj: vlastní průzkum, 2022

Aby byla předchozí otázka důkladněji posouzena, byli respondenti v její návaznosti dotazováni na to, zda je zprávy a oznámení od banky obtěžují. Pro většinu respondentů (47 %) není tento způsob komunikace banky obtěžující. Dalších 33 % dotazovaných v této otázce zastává neutrální postoj. Diskutovaná oznámení tedy obtěžují pouze 20 % respondentů.

Klienti bank mohou zvýšit bezpečnost svého finančního majetku také průběžnou kontrolou historie svých plateb. Z obr. č. 12 je zřejmé, že větší část respondentů tak činí, přesto lze výsledek považovat za poměrně vyrovnaný. Téměř totožně vypadají i odpovědi na dotaz, zda mají respondenti nastavené denní limity pro maximální výši transakcí. I v tomto případě kladně odpovídá pouze mírně přes polovinu respondentů. Výsledky obou těchto faktorů zkoumání znázorňuje obr. č. 22.

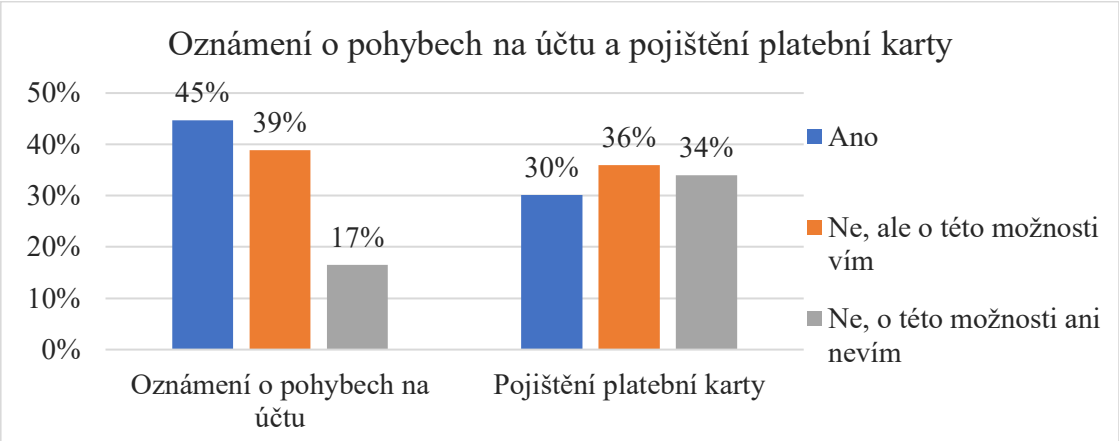
Obr. č. 22: Kontrola historie plateb a nastavování maximální výše limitů plateb



Zdroj: vlastní průzkum, 2022

Posuzována dále mezi respondenty byla preference oznámení o pohybech na účtu a pojištění platební karty. Oznámení o pohybech na účtu si dle výsledků nechá zasílat téměř polovina dotazovaných. Méně respondentů o existenci této služby vědí, ovšem nevyužívají ji. Horších výsledků z hlediska znalosti i míry používání bylo dosaženo v otázce pojištění platební karty. Sjednáno jej má méně než třetina respondentů a více než třetina si této možnosti není ani vědoma. K porovnání odpovědí v rámci každého ze dvou právě diskutovaných dotazů i porovnání výsledků mezi nimi slouží obr. č. 23.

Obr. č. 23: Využívání služeb: zasílání oznámení o pohybech na účtu a pojištění karty

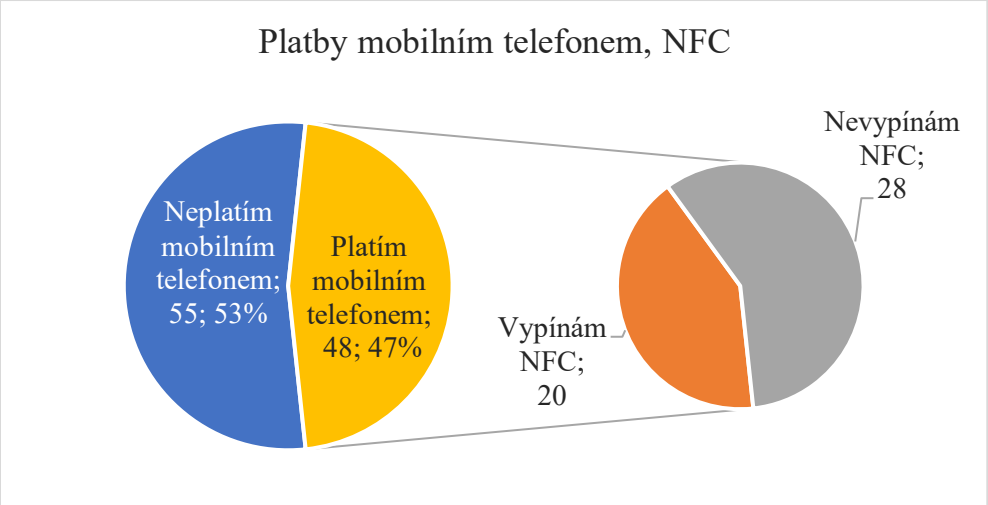


Zdroj: vlastní průzkum, 2022

Respondenti byli také dotazováni, zda k provádění transakcí někdy místo fyzické platební karty používají mobilní telefon. Bylo zjištěno, že mírně přes polovinu respondentů takto platí. Právě tito respondenti byli dále přesměrováni na otázku týkající se technologie NFC. Pro přesnost dotazu byl respondentům pojem vysvětlen, načež se autorka tázala, vypínají-li si NFC, pokud jej zrovna nepoužívají. Více než polovina respondentů

přiznává, že službu nechává stále aktivní. Grafický náhled na výsledky zkoumání je poskytnut v obr. č. 24.

Obr. č. 24: Platby mobilním telefonem a vypínání technologie NFC



Zdroj: vlastní průzkum, 2022

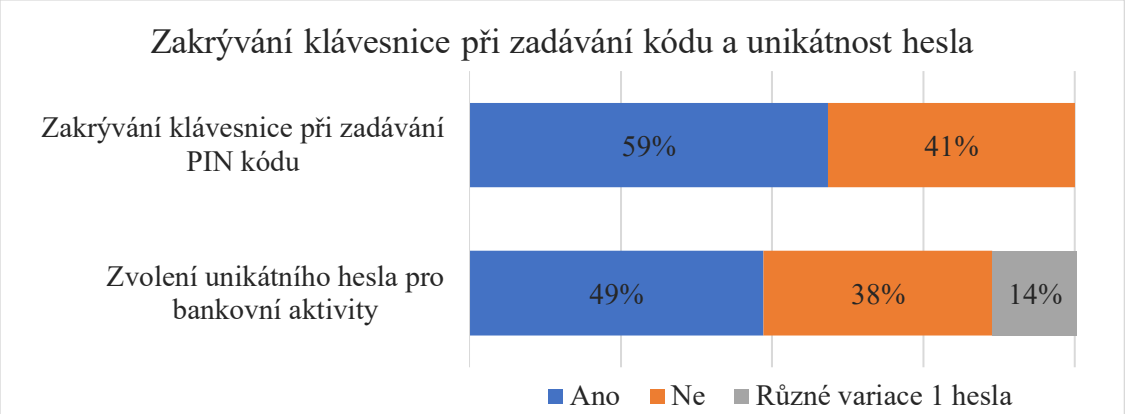
Pro úplnost problematiky placení pomocí mobilního telefonu bylo zjišťováno, jakým způsobem takto provedené platby respondenti ověřují. Mohli přitom vybrat jednu ze čtyř odpovědí či uvést odpověď vlastní. Největší četnost odpovědí je rovnoměrně rozložena mezi otisk prstu (38 %) a sken obličeje (38 %).

– **Zodpovědnost nakládání s přihlašovacími údaji a hesly**

Bezpečnost bankovního klienta je ve velké míře ovlivněna jeho přístupem a zodpovědnosti k nakládání s jeho citlivými osobními údaji a hesly.

Bylo zkoumáno, zda si respondenti při zadávání jejich PIN kódu zakrývají klávesnici platebního terminálu/bankomatu apod. Pro více než polovinu respondentů je tento způsob ochrany hesla běžný. Druhá poměrně znatelná část respondentů však takto nečiní. Další položenou otázkou bylo, zda si pro své bankovní účely respondenti nastavují pouze jedno unikátní heslo, tedy takové, které nepoužívají pro žádné jiné služby. Kladně odpovídá téměř polovina respondentů, ale velké zastoupení mají i respondenti, kteří na unikátnost hesla pro bankovní aktivity nedbají. Menší část respondentů uvádí, že používají různé variace jednoho hesla pro více služeb nebo webů. Nahlédnutím na obr. č. 25 lze zodpovědnost respondentů v diskutovaných oblastech porovnat.

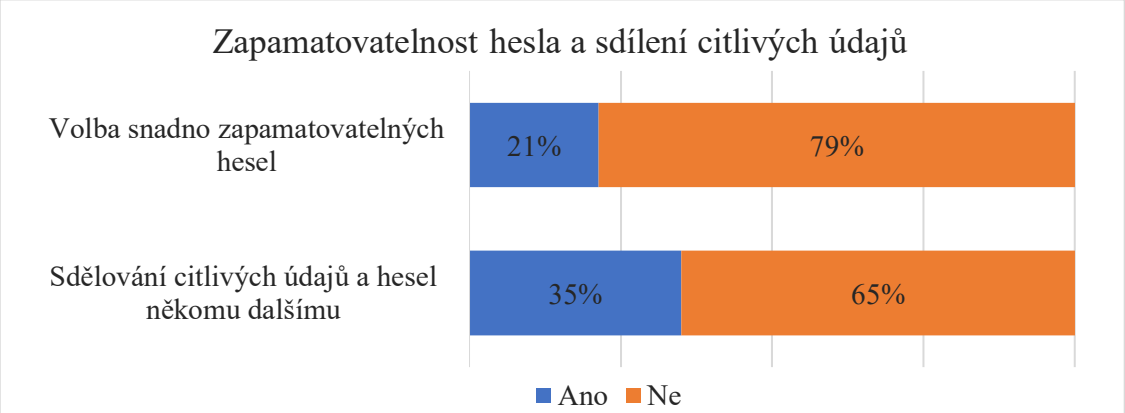
Obr. č. 25: Zakrývání klávesnice při zadávání kódu a unikátnost zvoleného hesla



Zdroj: vlastní průzkum, 2022

V tématice odpovědného nakládání s byli respondenti dále dotazováni, zda si pro své bankovní činnosti volí snadno zapamatovatelná hesla. Autorka poskytla respondentům pro lepší představu dva příklady (hesla obsahující celá slova či data narození). Převážná většina respondentů je v této otázce opatrná a volí taková hesla, která nejsou snadno zapamatovatelná. Dalším nevhodným způsobem nakládání s hesly je jejich sdělování někomu dalšímu. V závislosti na tom byli respondenti dotazováni, zda někdo zná jejich přihlašovací údaje k internetovému bankovnictví nebo PIN ke kartě. Většina respondentů tyto údaje nikdy nikomu nesděluje, ovšem více než třetina respondentů přiznává opak. Porovnání výsledků těchto dvou dotazů předkládá obr. č. 26.

Obr. č. 26: Volba snadno zapamatovatelných hesel a sdílení svých osobních údajů

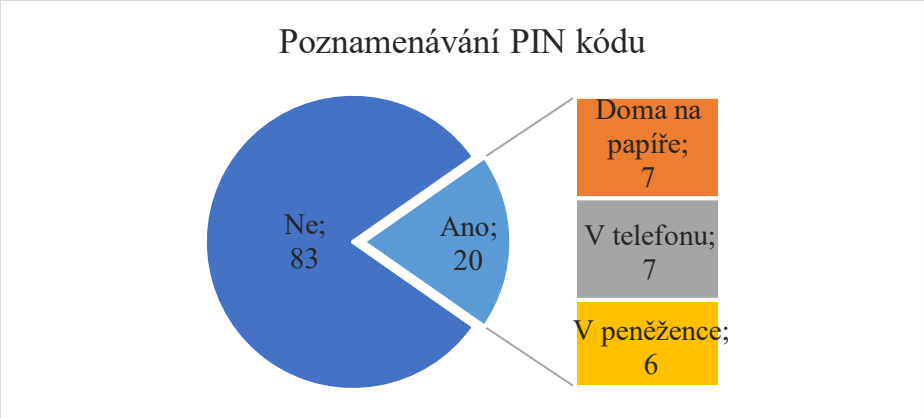


Zdroj: vlastní průzkum, 2022

V souvislosti s tématikou hesel a kódů bylo dále zjišťováno, zda si PIN kód ke kartě dotazovaní někam poznamenávají pro případ jeho zapomenutí. Naprostá většina spoléhá na to, že kód nezapomene a nikam si ho nepíše. Zbylí respondenti pak měli v rámci vlastní odpovědi uvést, kde přesně mají tento citlivý údaj poznamenaný. V odpovědích zazněly

tři druhy odpovědí ve vyrovnaném rozložení. PIN kód mají poznamenaný buď doma v papírové podobě, v telefonu nebo v peněžence (viz obr. č. 27).

Obr. č. 27: Poznamenávání PIN kódu

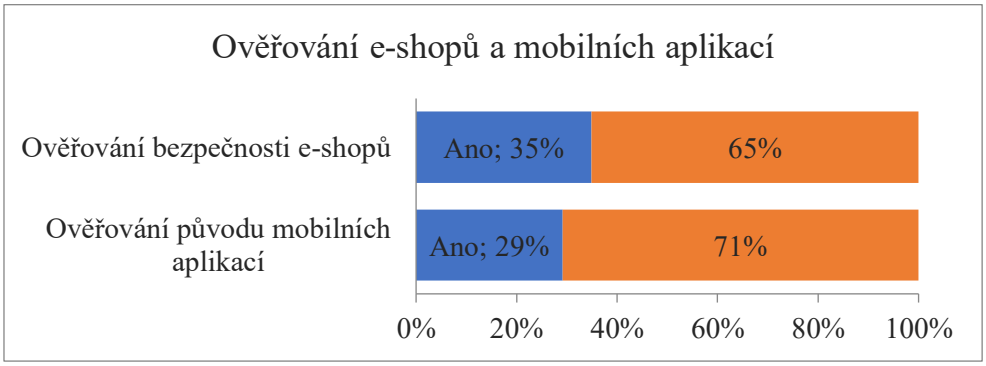


Zdroj: vlastní průzkum, 2022

– **Zodpovědnost chování na internetu**

Další sada otázek se týká zodpovědného chování na internetu ve vztahu s osobními financemi. Bylo dotazováno, zda si respondenti ověřují původ aplikací, které si stahují do svých mobilních zařízení. Výsledky ukazují, že této formě ochrany většina respondentů pozornost nevěnuje. Respondentům byl položen ještě jeden podobný dotaz, ve kterém však tentokrát měli uvést, zda ověřují původ aplikací, které si stahují do svého mobilního telefonu. Ani v tomto případě nejsou respondenti příliš obezřetní, byť o něco více než v případě e-shopů. Obr. č. 28 ukazuje výsledky obou diskutovaných dotazů.

Obr. č. 28: Ověřování e-shopů a mobilních aplikací



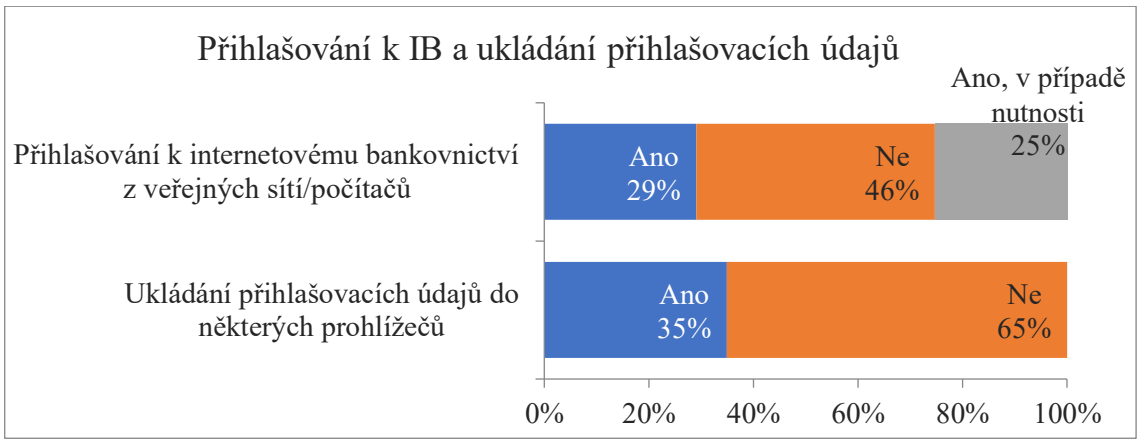
Zdroj: vlastní průzkum, 2022

Otázkou však zůstává, zda tato ověření provádějí efektivně. Proto byli respondenti následně vyzváni k zodpovězení otevřené otázky, jak si ověřují bezpečnost e-shopů. Byly zaznamenány pouze dva druhy odpovědí, častější z nich jsou recenze na internetu (24 ze

36) a předchozí osobní zkušenost či zkušenosti známých (13 ze 36). Také způsobů ověření mobilních aplikací nebylo jmenováno více než dva. Nejčastěji respondenti opět spoléhají na internetové recenze (25 ze 30). Méně zastoupené pak je nakupování pouze u verifikovaných prodejců Google Play a App Store (9 ze 30).

Dalším riskantním počínáním je přihlašování se k internetovému bankovnictví z veřejných sítí či veřejných počítačů, což byl další dotaz na respondenty. Z výsledků je možné konstatovat, že se většina respondentů takovému přihlašování vyhýbá. K veřejným sítím a PC se přihlašuje méně než třetina respondentů a jedna čtvrtina respondentů tak činí jen v případě naléhavosti. Řada lidí si pro úsporu času a ulehčení práce navíc ukládá své přihlašovací údaje do prohlížečů, čímž se také vystavují riziku. Výsledky říkají, že v tomto ohledu rizikově chová více než třetina respondentů. Konkrétní procentuální zastoupení spolu s grafickým znázorněním obou otázek představuje obr. č. 29.

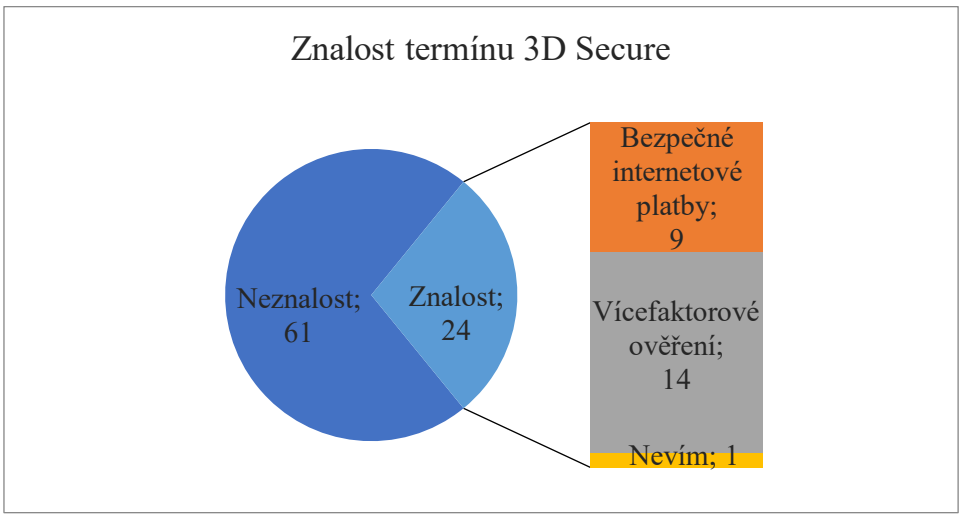
Obr. č. 29: Přihlašování k IB a ukládání přihlašovacích údajů



Zdroj: vlastní průzkum, 2022

Dalším předmětem dotazu na respondenty byl pojem 3D Secure. Prvotní a zásadní otázkou bylo, zda respondenti někdy provádí platby kartou online. Bylo zjištěno, že takto platí 83 % z nich, načež úkolem této části respondentů pak bylo sdělit, zda vědí, co je služba 3D Secure. Větší část respondentů (72 %) přiznala neznalost tohoto pojmu. Ti, co odpověděli kladně, pak měli vlastními slovy popsat, co 3D Secure znamená. Více než polovina odpovědí byla správná, neboť zmiňovala nějakou formu vícefaktorového ověření transakce. Část respondentů tento termín vysvětlila jako způsob zabezpečení plateb online, což je však vysvětlení velmi univerzální a jaksi vyplývající z předmětu předchozí otázky. Míru znalosti služby 3D Secure mezi respondenty ukazuje obr. č. 30.

Obr. č. 30: Znalost termínu 3D Secure



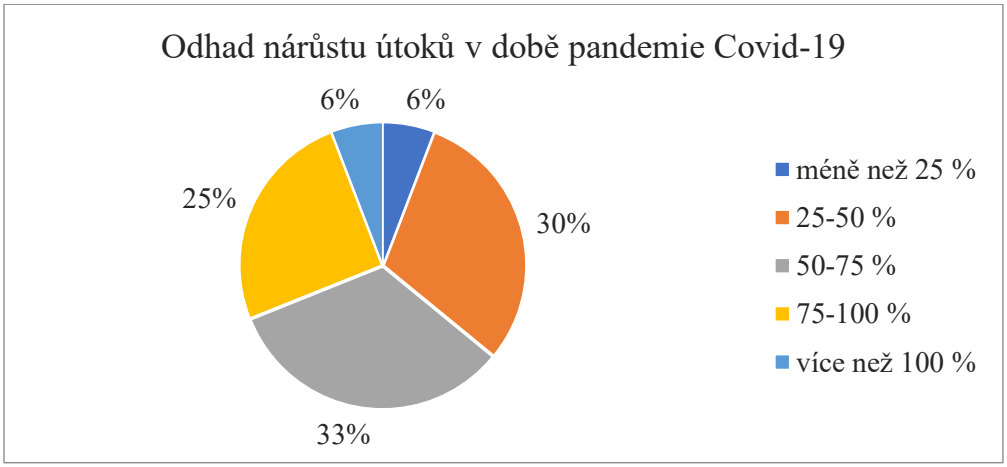
Zdroj: vlastní průzkum, 2022

– **Optimismus/pesimismus respondentů**

Autorku dále zajímalo, v jaké míře jsou respondenti v hledisku bankovních útoků optimističtí.

Autorka respondentům sdělila, že během pandemie Covid-19 došlo k celosvětovému nárůstu pokusů o digitální podvody ve finančních službách. Jejich úkolem bylo odhadnout, jak velký byl tento nárůst v porovnání s obdobím před pandemií. Dva krajní póly jsou zastoupeny nejméně, nejvíce se respondenti přiklánějí k rozmezím 50-75 % a 25-50 %. Lépe jsou výsledky znázorněny v obr. č. 31.

Obr. č. 31: Odhad nárůstu útoků v době pandemie Covid-19

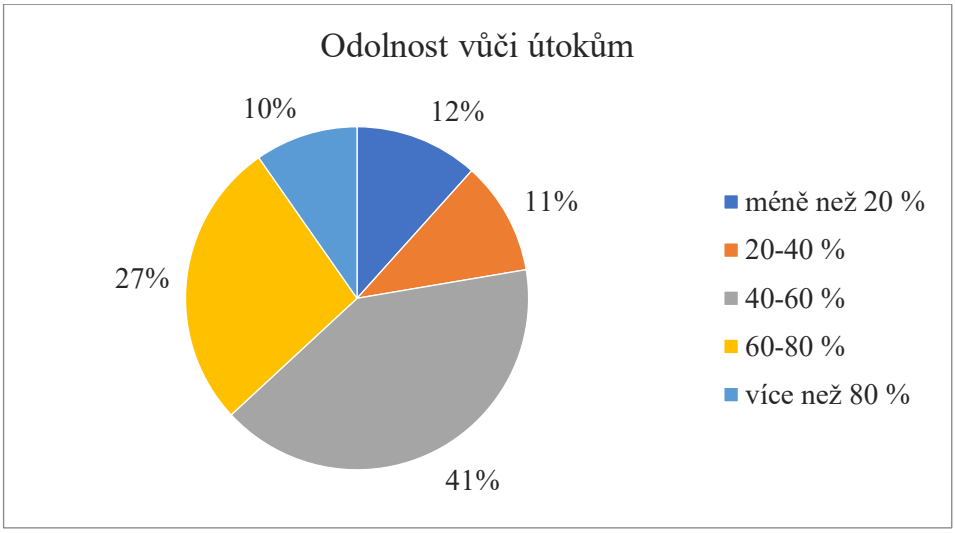


Zdroj: vlastní průzkum, 2022

Do této kategorie je zařazena i otázka, v jaké míře je dle názoru respondentů útokům na bankovní klienty úspěšně zabráněno. Většina respondentů odhaduje, že zastavit se daří

40-60 % útoků. Druhým nejvíce zastoupeným rozmezím je 60-80 %. Autorka tento výsledek ukazuje spíše na optimistický postoj respondentů. Všechna procentuální rozmezí a jim přidělená zastoupení respondentů lze vidět v obr. č. 32.

Obr. č. 32: Odolnost vůči útokům



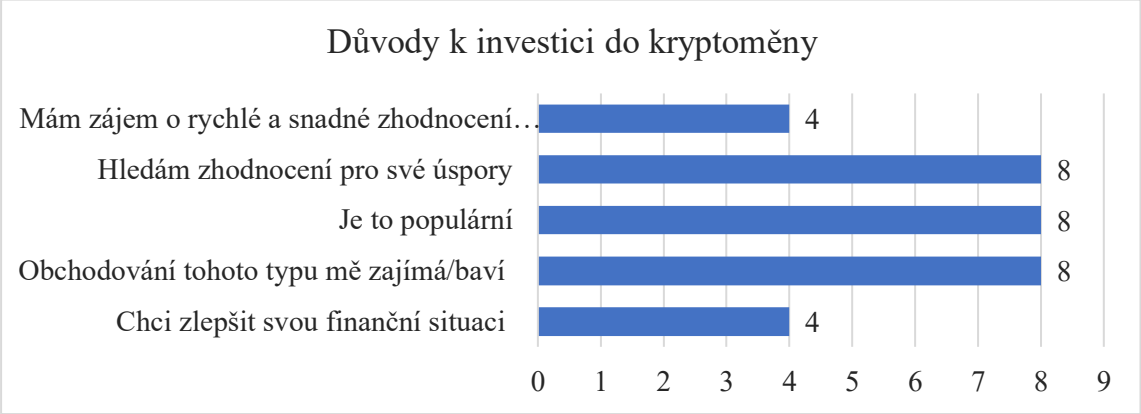
Zdroj: vlastní průzkum, 2022

– **Doplňující otázky**

V dotazníku se objevilo ještě několik dalších otázek, které lze jen těžko kategorizovat, nicméně jejich zodpovězení vhodně doplní celou problematiku podvodů v bankovním styku.

Respondenti byli dotazování, jestli investují nebo někdy přemýšleli o investici do digitální měny. Kladně odpovědělo pouze 21 % respondentů (tedy 22 respondentů), na které autorka mířila další dotaz. Tito respondenti měli uvést, z jakého důvodu je pro ně investice do kryptoměny přitažlivým tématem. Respondenti měli na výběr z pěti odpovědí a měli povoleno zvolit jednu nebo více z nich. Třemi nejčastějšími a zároveň v četnosti vyrovnanými odpověďmi jsou popularita investování do kryptoměny, touha po zhodnocení úspor a obliba tohoto druhu investování (viz obr. č. 33).

Obr. č. 33: Důvody k investici do kryptoměny

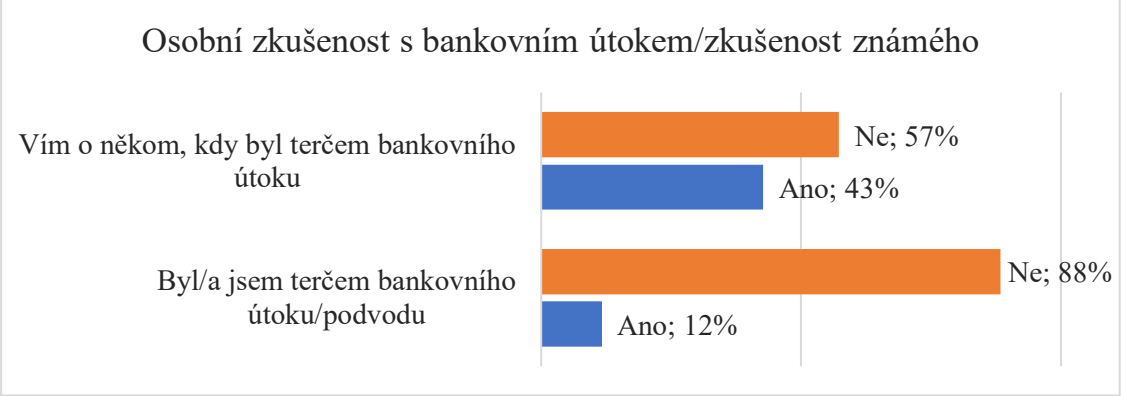


Zdroj: vlastní průzkum, 2022

Skutečnosti, že je kryptoměna v posledních letech velmi diskutována, je využíváno podvodníky, kteří právě v současných trendech obvykle vidí zajímavý potenciál. Takový podvod může vypadat třeba tak, že kyberkriminálníci umísťují na weby reklamy lákající k obchodování s kryptoměnou, přičemž po jejich rozkliknutí dochází k přesměrování oběti na podvodnou internetovou stránku. Proto se autorka dotazovala respondentů, jež investují nebo uvažují o investici do kryptoměny, někdy klikli na reklamu s kryptoměnou. Většina respondentů (73 %) odpovídá odmítavě.

Jednou z posledních zásadních otázek k zodpovědění bylo, zda se sami respondenti někdy stali obětí bankovního útoku či zda přinejmenším nějakou oběť znají. Na jednoznačnou většinu respondentů nikdy nebyl žádný typ bankovního útoku učiněn nebo si jej nejsou vědomi. U druhé zmiňované otázky však bylo dosaženo mnohem zajímavějšího výsledku. Téměř polovina respondentů totiž alespoň zná někoho, kdo má s bankovním útokem osobní zkušenost. Výsledky zpřehledňuje obr. č. 34.

Obr. č. 34: Zkušenost s bankovním útokem/podvodem – osobní či někoho známého



Zdroj: vlastní průzkum, 2022

V boji proti bankovním podvodům hraje velkou roli zvyšování povědomí o tomto tématu a jeho závažnosti, čehož lze dosahovat například prostřednictvím reklamy, která může mít širokou působnost. Bylo tedy zjišťováno, zda respondenty dle jejich názoru o této problematice dostatečně informují média. Bylo jim předloženo níže uvedené tvrzení (tab. č. 6) a jejich úkolem bylo vyjádřit, v jaké míře s ním souhlasí, a to pomocí hodnotící škály od 1 do 5, kde 1 = zcela souhlasím a 5 = zcela nesouhlasím. Z níže uvedené tabulky (tab. č. 6) lze vyvodit, že se většina respondentů nedokáže rozhodnout, zda jsou média v otázce upozorňování na nelegální činnosti v bankovním styku dostatečně proaktivní či nikoli. Modus i medián dosahují hodnoty 3, aritmetický průměr 3,07.

Tab. č. 6: Zhodnocení míry mediální informovanosti o bankovních podvodech

„O problematice bankovních podvodů nás dostatečně informují média.“

Hodnotící stupnice míry souhlasu					Modus	Medián	Aritmet. průměr
1	2	3	4	5			
Absolutní četnost							
3	17	56	24	3	3	3	3,07

Zdroj: vlastní průzkum, 2022

Poslední otázkou na respondenty bylo, jaká francouzská banka je dle jejich uvážení nejbezpečnější. Na výběr měli z osmi bank, jež jsou dle webu Statista (2021) i Corporate Finance Institute (2022) současně nejsilnějšími aktéry na bankovním trhu Francie. Nejčastěji jmenovanými bankami byla Banque Populaire (21 %), Société Générale (20 %), Caisse d’Epargne (17 %), Crédit Agricole (16 %) a BNP Paribas (13 %). 12 % respondentů pak uvádí, že tuto dotazovanou skutečnost nemohou posoudit.

4.2 Sumarizace dotazníkového šetření a komparace zjištěných poznatků

Metoda dotazníkového šetření pomohla komplexně zkoumat chování respondentů v bankovním styku. Důraz byl přitom kladen na jejich přístup k rizikům, které jim jako bankovním klientům vyvstávají. Šetření bylo prováděno na území České republiky a Francie, přičemž cílem autorky bylo porovnat výsledky dosažené v každé z těchto zemí.

České bankovní asociace (2021c) již od roku 2015 pravidelně sestavuje tzv. index kyberbezpečnosti, jehož předmětem je chování Čechů na internetu. Na základě průzkumu České bankovní asociace (2021c) bylo v roce 2021 dosaženo zatím nejlepšího výsledku indexu kyberbezpečnosti. Dosáhl totiž 68 %, což je nejvíce za dobu jeho existence. Tento výzkum nezaznamenal odlišnosti v souvislosti s věkem, pohlavím či bydlištěm respondentů, vliv na rozdílnost výsledků však mělo dosažené vzdělání respondentů. Podle průzkumu jsou obezřetnější osoby s vysokoškolským vzděláním. Mezi respondenty dotazníkového šetření sestaveného autorkou se v rámci České republiky nacházelo 64 % vysokoškolsky vzdělaných, v rámci Francie pak šlo o 58 %. Srovnání výsledků mezi nimi tedy autorka považuje za relevantní.

– **Preference respondentů**

Čeští respondenti prokázali znatelně nižší věrnost jedné bance než francouzští respondenti. Dotazovaní z Francie totiž v 94 % případů uváděli jen jednu banku, které jsou klienty, zatímco u dotazovaných z České republiky to bylo jen 64 %.

V případě obou zemí stojí při výběru banky na prvním místě její bezpečnost. Postavení bezpečnosti v žebříčku důležitosti ustálo i nátlak dalších 12 faktorů, jež byly respondenty posuzovány. Autorku překvapilo, že ani na bankovní poplatky respondenti neberou tak velký zřetel. Otázkou však zůstává, zda jsou si respondenti vědomi toho, že zodpovědnost za jejich finance nemůže banka převzít v plném rozsahu. Pro dosažení co nejvyšší odolnosti vůči hrozbám třetích stran se v celém bezpečnostním procesu musejí sami klienti aktivně angažovat. Průzkum ČBA (2021c) ukazuje, že téměř tři čtvrtiny Čechů spoléhají na to, že jejich data a finance ochrání banka. Velmi podobný trend dokazuje i nedávný průzkum ACI Worldwide (2021), podle kterého 80 % Francouzů věří, že je před podvody ochrání jejich banka.

V otázce, zda je problematika bankovních podvodů dostatečně diskutována v médiích, jsou respondenti nerozhodní. Přesto lze konstatovat, že byl zaznamenán mírný sklon k souhlasu s tvrzením, že proaktivita médií není dostatečná (v ČR je tato tendence patrnější).

- **Orientace v problematice nelegálních činností v bankovnictví**

Úkolem respondentů bylo jmenovat všechny nelegální činnosti v bankovním sektoru, které je napadají. Zatímco čeští respondenti zmiňovali zejména zcizení či jiné zneužití přístupových údajů k internetovému bankovnictví, praní špinavých peněz a phishing, u francouzských respondentů se jednalo o falešné weby a aplikace, krádeže a zneužití platebních karet, třetí nejčastější pak byla odpověď „nevím“, načež následovali viry, skimming a phishing. Kromě těchto se však u českých respondentů objevila celá řada dalších praktik podvodníků, byť v nižším zastoupení. U respondentů z Francie byla škála příkladů mnohem užší, navíc nebyla nalezena žádná zmínka o podvodech s šeky, které jsou dle Banque de France (2020) nejčastěji zneužívaným platebním prostředkem.

Podle českých respondentů je největší hrozbou současnosti jednoznačně phishing, uvádí jej 42 % z nich. Dotazovaní z Francie udávají na první místo malware, přičemž těsně za něho řadí skimming a phishing (17 %). Právě phishing podle Petříčka (2021) aktuálně představuje největší hrozbu pro klienty bank. V roce 2020 došlo oproti roku 2019 k dvojnásobnému počtu případů (ČBA, 2021b). Vishing, který je telefonickou obdobou phishingu, stál za zpronevěrou již více než 26 milionů korun (Česká televize, 2021). Podle údajů České bankovní asociace (2021b) bylo již v prvním pololetí roku 2021 zaznamenáno šestkrát více případů vishingu než za celý rok předcházející. Úspěšnost útoků se pak pohybuje okolo 25 %. Phishing a malware považuje od roku 2020 za jednu z největších hrozeb také Banque de France (2020). Skimming, který byl respondenty z Francie také často jmenovaný, v počtu útoků již několik let soustavně klesá (Banque de France, 2020).

Za nejbezpečnější způsob placení považují respondenti obou zemí hotovost (Češi 44 %, Francouzi 38 %), přičemž na dalších příčkách již lze zaznamenat rozdílné tendence. Česká část respondentů považuje za druhou nejbezpečnější formu placení transakce mobilním telefonem, a naopak francouzská část respondentů na druhé místo řadí platby převodem. V opačném úhlu pohledu, tedy který platební nástroj je naopak nejvíce nebezpečný, bylo napříč odpověďmi českých i francouzských respondentů opět dosaženo

harmonie. Shodli se totiž na tom, že nejrizikovější jsou platby kartou na internetu. Podobně průzkum ACI Worldwide (2021) došel k závěru, že Francouzi považují za nejbezpečnější způsob platby hotovost (71 %). Důvěra v nové digitální platební metody je u Francouzů stále nízká, pouze 30 % spotřebitelů důvěřuje platbám mobilním telefonem. Podle průzkumu ACI Worldwide (2021) mobilní peněženku aktivuje jen 8 % Francouzů. Zato Češi jsou inovacím otevřeni, k transakcím využívá mobilní telefon jedna pětina populace. I ti jsou však stále věrní hotovosti, kterou platí 55 % z nich. Nejrozšířenějším platební prostředkem je debetní karta (69 %) (ČBA, 2021d). Na základě Nelson Report (2019) tvořily v roce 2018 CNP transakce (platby bez přítomnosti karty) pouze 15 % všech transakcí světa, přitom byly spjaty s 54 % všech finančních ztrát z důvodu kriminální bankovní činnosti.

- **Využívání základních služeb k podpoře bezpečnosti bankovního klienta**

Francouzští respondenti ve větší míře přiznávají, že nepoužívají antivirové systémy, přesněji se jedná o jednu pětinu z nich. Absenci antiviru v počítači i mobilním telefonu pak čeští respondenti potvrzují v 11 % případů. Pro upřesnění lze uvést, že antivirové systémy ve svém počítači používá 48 % českých respondentů a 44 % francouzských. Daleko horších výsledků dosahuje používání antivirů v mobilním telefonu, které potvrzuje pouze 16 % českých respondentů a 11 % francouzských respondentů. Výsledky průzkum ČBA (2021c) staví absenci antivirových systémů do popředí nejčastějších pochybení českých klientů bank v souvislosti s chováním na internetu. V otázce vlastnění a pravidelné aktualizaci antivirů je u obou zemí zodpovědná přibližně čtvrtina respondentů. Jmenovaný průzkum přitom dosahuje pozitivnějších výsledků, neboť absenci antiviru v počítači potvrzuje 28 % Čechů, v mobilním telefonu poté 44 % Čechů.

Respondenti z obou zemí v podobném rozsahu čtou zprávy a oznámení bank, pozornost jim spíše nevěnují. Téměř polovinu respondentů z Francie tato oznámení neobtěžují, zatímco většina českých respondentů v této otázce zastává spíše neutrální nebo negativní postoj. Je zajímavé pozorovat, že ačkoli je vztah francouzských respondentů k bankovní korespondenci kladnější, ve zvýšeném zájmu a všímavosti se to neodráží.

Naprostá většina českých respondentů kontroluje historie svých plateb a nastavuje denní limity pro maximální výši transakcí (87 %). U francouzských respondentů tak činí pouze více než polovina z nich.

Respondenti z Francie sice podle výsledků o něco méně platí mobilním telefonem, ovšem v mnohem větší míře vypínají NFC, když jej zrovna nepoužívají. Čeští respondenti NFC téměř nikdy nevypínají.

V České republice i Francii si téměř polovina respondentů nechává zasílat notifikace o pohybech prostředků na jejich bankovním účtu. Taktéž možnosti pojištění platební karty je v obou zemích využíváno v podobném poměru, konkrétně se jedná o 30 % u českých respondentů a 36 % u francouzských respondentů.

- **Zodpovědnost nakládání s přihlašovacími údaji a hesly**

V otázce zodpovědného nakládání s hesly a dalšími citlivými údaji bylo u obou národností zjištěno, že přibližně 4/5 respondentů je obezřetných a volí si pro své bankovní aktivity taková hesla, která neobsahují celá slova, datumy narození či cokoli dalšího, co by usnadňovalo jejich zapamatovatelnost, a tedy zároveň zvyšovalo jejich náchylnost ke zneužití. Dle ČBA (2021c) si pro bankovní aktivity volí silná hesla 63 % Čechů, přitom nejméně zodpovědní jsou v tomto ohledu osoby ve věku 18-34 let.

O něco větší obezřetnost prokázali čeští respondenti oproti francouzským v otázce zakrývání klávesnice při zadávání PIN kódu ke kartě a volby unikátního hesla pro své bankovní aktivity (62 % oproti 49 %). Průzkum ČBA (2021c) přesto řadí volbu jednoho hesla pro více aplikací a webů na druhé místo v otázce nezodpovědnosti Čechů v kyber prostoru. Podle ČBA nedbá na unikátnost heslo výhradně pro bankovnictví 16 % Čechů, přičemž na základě výzkumu autorky se jedná o 38 % českých respondentů.

Čeští respondenti navíc téměř nikdy nesdělují své přihlašovací údaje do internetového bankovnictví a PIN kód ke kartě někomu dalšímu (89 %). To potvrzuje i výzkum ČBA (2021c). Na straně druhé 35 % respondentů z Francie přiznává, že jejich citlivé bankovní údaje někdo zná.

Větší odpovědnost při nakládání s citlivými údaji lze připsat českým respondentům i v otázce poznamenávání PIN kódu pro případ zapomenutí. Zatímco čeští respondenti jej mají poznamenaný zejména doma v papírové podobě, v telefonu nebo jinými bezpečnými způsoby, u francouzských respondentů se jako místo pro uložení tohoto údaje několikrát objevila peněženka. Ve většině případů se však respondenti obou zemí spoléhají na svou paměť a PIN nikde poznamenaný nemají.

- **Zodpovědnost chování na internetu**

Napříč oběma skupinami dotazovaných je zaznamenána vysoká absence ověřování původu mobilních aplikací (činí tak pouze 32 % z respondentů z ČR a 35 % z respondentů z Francie). Pokud respondenti ověření provádějí, většinou tak činí na základě recenzí. Druhým nejčastějším způsobem ověření je pak nákup výhradně v App Storu nebo Google Play.

Pozornost ověřování bezpečnosti e-shopů věnují mnohem více respondenti z České republiky (76 %) než z Francie (29 %). Podle výzkumu ACI Worldwide (2021) se francouzští spotřebitelé necítí při nákupech na internetu v bezpečí, neboť se obávají podvodu, tvrdí tak 8 z 10 Francouzů. Přesto však na internetu nakupuje téměř každý Francouz (98 %). Méně než tři z deseti zákazníků věří, že je ochrání bezpečnostní postupy online obchodníka (dvoufaktorová autentizace, logo „bezpečné platby“, webová stránka začínající „https“).

V závislosti na velké nedůvěřivosti francouzských respondentů autorku velmi zajímala znalost pojmu 3D Secure, který je aktuálně nejlepším řešením ochrany plateb přes internet. Vysvětlit správně tento pojem dokázalo jen 28 % respondentů v porovnání s 44 % českých respondentů. Opatrnější jsou čeští respondenti taktéž v otázce přihlašování do internetového bankovnictví z veřejných sítí a ukládání hesel do prohlížečů.

– **Míra optimismu respondentů v otázce bankovních útoků**

Francouzští respondenti jsou o něco optimističtější v otázce, jak velkému množství útoků se dle jejich odhadu daří zabránit. Podle ČBA (2021) se jedná o 86 % útoků, které jsou úspěšně zastaveny, přičemž čeští respondenti nejčastěji odhadují rozmezí 20-40 %. Nejčastější odhad francouzských respondentů na straně druhé činí 40-60 %.

Čeští respondenti jsou však optimističtější v odhadu nárůstu podvodů v digitálních službách v době pandemie Covid-19. Na základě studie společnosti TransUnion (2021) se jednalo o 149% nárůst v porovnání posledních čtyř měsíců roku 2020 a prvních čtyř měsíců roku 2021. Toto zvýšení v globálním měřítku však bylo mnohem mírnější v období mezi druhým čtvrtletím roku 2020 a druhým čtvrtletím roku 2021, konkrétně se jednalo o 19 %. Více než 50% nárůst tipovalo dle výzkumu autorky 44 % českých respondentů a 64 % francouzských respondentů.

V těchto otázkách neexistovala správná odpověď, autorka se dotazovala pouze za účelem zjištění, která část respondentů vnímá problematiku závažněji.

4.2.1 Odhad možného budoucího vývoje

Přesun aktivit z kamenných poboček bank do digitálního prostředí, zvyšující se preference nákupů na internetu a další podobné tendence, jež byly navíc posíleny pandemií Covid-19, ale také stále rostoucí globalizace a tlak na propojování trhů, to vše a mnohem více otevírá stále nové dveře útočníkům, kteří mohou získat přístup k majetku bankovních klientů. Přesto, že pandemie je již na ústupu, dle úsudku autorky nedojde k úplnému návratu do dříve zaběhnutých standardů. Spotřebitelé si na fungování v online prostředí zvykli a stejný trend pravděpodobně bude převládat i v následujících letech. Budoucímu poklesu útoků na bankovní klienty navíc nenasvědčuje ani skutečnost, že podvodníkům již po dobu několika let postačí mimo jiné tradiční způsoby páchání diskutovaných trestných činů. E-mail, telefon, sms zprávy, sociální sítě, to vše jsou kanály, ke kterým má společnost přístup již velice dlouhou dobu. Jejich prostřednictvím však stále v obrovském objemu dochází k únikům peněžních prostředků od obětí ke kriminálníkům. Ve velké míře totiž útočníci spoléhají ne na vyspělé technologie, ale na psychologický aspekt – na zranitelnost bankovního klienta. Vyvolávání strachu a úzkosti v oběti a další časté metody útočníků budou, bohužel, velmi křehkou a mnohdy účinnou záležitostí i nadále. Kromě zvýšené komunikace praktik útočníků veřejnosti a rozvoj zabezpečovacích systémů bude dle mínění autorky i nadále hrát zásadní roli proaktivita klientů bank a vznik iniciativ pro prevenci bankovních podvodů. V oblasti technologií se pak napříč literaturou ve stále větší míře objevuje umělá inteligence, ve které autorka vidí velký potenciál. Předmětem zájmu tak v boji proti bankovním podvodům nebudou nejrůznější a nejnovější typy podvodů, jakož spíše chování bankovního klienta. Stanovení vzorců jeho chování povede ke včasné detekci podvodné transakce.

Závěr

Bezpečnost je u respondentů jakožto bankovních klientů bezesporu na prvním místě. A není divu. Osobní finance jsou pro většinu společnosti tím nejcennějším majetkem, ať už jich jedinec má nadbytek, nebo naopak přesně tolik, kolik nutně potřebuje k bytí. Lze však zpozorovat, že ve velké míře spoléhají účastníci bankovního styku na to, že se o aspekt bezpečnosti postará jejich banka.

Hlavním cílem předložené práce bylo objasnit chování klientů bank ve vztahu k bezpečnosti v bankovním styku na příkladu České republiky a Francie.

Za jeden ze zásadních poznatků výzkumu lze považovat skutečnost, že ačkoli (nebo právě proto) jsou dle výsledků šetření v ochraně svých dat a financí mnohem méně obezřetní francouzští respondenti, předpokládají relativně větší míru odolnosti bankovního sektoru proti vnějším hrozbám.

Čeští respondenti znají podle výsledků průzkumu větší množství nejrůznějších podvodných praktik. Výběr nelegálních činností v bankovnictví byl mezi francouzskými respondenty nejen mnohem omezenější, zcela navíc opomenul podvody v souvislosti s šeky, které jsou ve Francii velkým problémem. Za velmi pozitivní lze považovat závěr, že čeští i francouzští respondenti jsou si vědomi toho, že v současnosti musejí být obezřetní zejména k phishingu a malwaru. Francouzští respondenti však mylně považují za jednu z největších hrozeb také skimming, který v počtech útoků zaznamenává v posledních letech kontinuální pokles.

K moderním způsobům placení, jako je například platba mobilním telefonem, jsou pak důvěřivější spíše Češi než Francouzi. Přestože Češi také mobilním telefonem platí více, v mnohem větší míře zapomínají na vypínání NFC technologie vždy, když zrovna není používána.

K ochraně svých dat používají respondenti dotazníkového šetření antivirové systémy zejména ve svém počítači. Uvádí tak méně než polovina respondentů, což autorka nepovažuje za příznivý výsledek. V mobilním telefonu je pak absence antiviru jednoznačně většinová. Navíc ti, co antivir vlastní, jen málokdy dbají také na jeho pravidelnou aktualizaci.

Zvýšenou pozornost by měly obě skupiny respondentů věnovat zprávám a oznámením bank. Právě ta totiž často upozorňují na aktuální nelegální činnosti, vůči kterým by klienti

bank měli být ostražití. Dle názoru autorky se jedná o pasivní, byť velmi snadný způsob, kterým mohou klienti zvyšovat své povědomí o problematice a snížit tak pravděpodobnost podlehnutí praktikám útočníků. Podobně jsou na tom respondenti obou zemí v souvislosti s nastavením služby, která jim zasílá notifikace o pohybech prostředků na jejich bankovním účtu (využívá ji přibližně polovina z nich) a také v otázce pojištění platební karty (sjednáno asi jednou třetinou respondentů). Čeští respondenti jsou velmi opatrní v ohledu nastavování denních limitů pro maximální výši transakcí, francouzští respondenti za nimi výrazně zaostávají.

Velmi příznivým výstupem autorčina výzkumu je fakt, že majoritní část respondentů si pro své bankovní činnosti volí silná hesla, která neobsahují nic, co by vedlo k jejich snazší zapamatovatelnosti a tedy vyšší náchylnosti ke zneužití. Naproti tomu na unikátnost hesla výhradně pro bankovní aktivity dbají hlavně čeští respondenti. Zodpovědnější jsou také jde-li o ochranu svého PIN kódu ke kartě. Majorita z nich uvádí, že tento citlivý nezná nikdo jiný než oni sami. Respondenti obou zemí si kód ke kartě pro případ zapomenutí jen zřídkakdy někam poznamenávají.

Obě skupiny respondentů by měli být obezřetnější v otázce ověřování původu mobilních aplikací. Nicméně bezpečnost e-shopů si ověřují mnohem více čeští respondenti. Výsledek je velmi překvapivý s ohledem na skutečnost, že se francouzští spotřebitelé nákupu na internetu z hlediska bezpečnosti mnohem více obávají. V souvislosti se zhodnocením zodpovědnosti chování respondentů na internetu jsou ti z České republiky úspěšnější také proto, že se méně často přihlašují k internetovému bankovnictví z veřejných sítí. Za poslední zásadní poznatek v této oblasti autorka považuje zjištění, že si jednoznačná většina respondentů z České republiky neukládá hesla do prohlížečů.

Ačkoli jsou spotřebitelé obecně velmi asertivní k reklamě, k angažovanosti médií v problematice bankovních podvodů měli respondenti velmi neutrální postoj. Je tedy možné konstatovat, že tato tématika potřebuje v médiích větší prostor.

Z výsledků dotazníkového šetření jasně plyne, že na ochranu svých dat a financí aktivně dbají zejména čeští respondenti. Autorka se domnívá, že důvodem je zejména silná tendence francouzských klientů bank k převádění veškeré odpovědnosti na bankovní instituci. Dle názoru autorky se však i v chování Čechů v bankovním styku objevují značné nedostatky. Mezi ty nejzásadnější autorka řadí absenci antivirových systémů v jejich chytrých zařízeních, ignoraci došlé bankovní korespondence, vysokou míru

používání jednoho univerzálního hesla pro více aplikací a webů a nedbání na původ mobilních aplikací. Právě na tyto oblasti by dle autorky měly banky a další iniciativy koncentrovat své snahy v boji za prevenci nelegálních bankovních praktik.

Seznam použité literatury

ACI Worldwide (2021). *80 Percent of French Consumers Fear eCommerce Payments Fraud, New Survey by ACI Worldwide and OpinionWay Reveals.* Dostupné 20. 4. 2022 z https://investor.aciworldwide.com/node/23231/pdf

American Bankers Association (2021). *How Americans Bank: Before and During COVID-19.* Dostupné 15. 3. 2022 z https://www.aba.com/news-research/research-analysis/preferred-banking-methods

Bakeš, M., Marková, H., Karfíková, M., & Kotáb P. (2012). *Finanční právo* (6. vyd.). Praha, Česko: C. H. Beck.

Bank of America (2022). *Protect yourself against identity theft.* Dostupné 15. 4. 2022 z https://www.bankofamerica.com/security-center/identity-theft-protection/

Banque de France (2020). *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2020.* Dostupné 18. 4. 2022 z https://www.banque-france.fr/sites/default/files/medias/documents/821162_osmp_2020_interieur_definitif_web.pdf

Barska, A. (2018). Millennial consumers in the convenience food market. *Management*, 22(1), 251–264. doi: https://doi.org/10.2478/manment-2018-0018

Beattie, A. (2020). *How Did Nick Leeson Contribute To The Fall of Barings Bank?* Dostupné 1. 12. 2021 z https://www.investopedia.com/ask/answers/08/nick-leeson-barings-bank.asp

Bidrmanová, M. (2022). *Jaké triky na nás zkoušejí bankéři a jak odolat. Radí expertka.* Dostupné 15. 4. 2022 z https://www.seznamzpravy.cz/clanek/audio-podcast-ve-vate-kdyz-reknou-ze-zisk-je-jisty-utikejte-jak-na-manipulace-bankeru-198267#utm_content=freshnews&utm_term=manipulace%20bank%C3%A9%C5%99%C5%AF&utm_medium=hint&utm_source=search.seznam.cz

Blahová, N. (2018). *Rizika bank a jejich regulace.* Jesenice, Česko: Ekopress.

Blažek, J., & Uklein, J. (1997). *Bankovnictví.* Brno, Česko: Doplněk.

Bradley (2021). *Card Not Present Fraud: How Companies Lose Nearly $10 Billion Per Year.* Dostupné 16. 4. 2022 z https://www.merchantfraudjournal.com/card-not-present-fraud/#how-to-detect-and-prevent-card-not-present-fraud

Cavaglieri, C. (2021). *Is your bank protecting you from number spoofing scams?* Dostupné 14. 4. 2022 z https://www.which.co.uk/news/2021/06/is-your-bank-protecting-you-from-number-spoofing-scams/

CFI (2022). *Top Banks in France.* Dostupné 15. 4. 2022 z https://corporatefinanceinstitute.com/resources/careers/companies/top-banks-in-france/

Citizens Advice (2022). *Banking – security and fraud.* Dostupné 7. 4. 2022 z https://www.citizensadvice.org.uk/debt-and-money/banking/banking-security-and-fraud/

Česká bankovní asociace (2021b). *Útoky na klienty bank rapidně narůstají a jsou sofistikovanější. ČBA, Policie ČR a ESET proto spouští „Kyberkampaň".* Dostupné 13. 11. 2021 z https://cbaonline.cz/utoky-na-klienty-bank-rapidne-narustaji-a-jsou-cim-dal-sofistikovanejsi-cba-policie-cr-a-eset-proto-spousti-kyberkampan-

Česká bankovní asociace (2021c). *Průzkum ČBA: Češi jsou oproti kybernetickým hrozbám obezřetnější.* Dostupné 19. 4. 2022 z https://cbaonline.cz/pruzkum-cba-cesi-jsou-oproti-kybernetickym-hrozbam-obezretnejsi

Česká bankovní asociace (2021d). *Češi se nebrání inovacím, pětina už platí mobilem. Hotovosti se přesto vzdát nechtějí.* Dostupné 21. 4. 2022 z https://cbaonline.cz/pruzkum-cba-cesi-a-platebni-styk-2021

Česká bankovní asociace (2021a). *Desatero bezpečnosti.* Dostupné 8. 9. 2021 z https://cbaonline.cz/desatero-bezpecnosti

Česká bankovní asociace (2022). *ČBA opět varuje před podvodníky.* Dostupné 5. 4. 2022 z https://cbaonline.cz/cba-opet-varuje-pred-podvodniky-tentokrat-v-internetovych-bazarech

Česká národní banka (2022). *K institutu bankovního tajemství.* Dostupné 19. 3 2022 z https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2021-06

Česká národní banka (2020). *Co to je praní peněz.* Dostupné 2. 3. 2022 z https://www.cnb.cz/cs/o_cnb/cnblog/Co-to-je-prani-penez/

Česká spořitelna (2020). *Počet kybernetických útoků na firmy roste, i jedno kliknutí může ohrozit vaše podnikání. Jak se bránit?* Dostupné 14. 11. 2021 z https://www.csas.cz/cs/firmy/articles/pocet-kybernetickych-utoku-na-firmy-roste-i-jedno-kliknuti-muze-ohrozit-vase-podnikani

Česká televize (2021). *Přibývá útoků na klienty bank. Podvodníci jim stále častěji volají.* Dostupné 20. 11. 2021 z https://ct24.ceskatelevize.cz/domaci/3340260-pribyva-utoku-na-klienty-bank-podvodnici-jim-stale-casteji-volaji

ČTK: České noviny (2006). *První phishing v Česku, terčem byla CitiBank.* Dostupné 23. 11. 2021 z https://www.ceskenoviny.cz/zpravy/prvni-phishing-v-cesku-tercem-byla-citibank/178228

Dowd, K. (1996). The Case for Financial Laissez-Faire. *The Economic Journal,* 106(436), 679–687. doi: https://doi.org/10.2307/2235576

Eger, L., & Egerová, D. (2014). *Základy metodologie výzkumu: pro studenty ekonomických oborů.* Plzeň, Česko: Západočeská univerzita.

ESET (2022). *Krádež identity.* Dostupné 3. 4. 2022 z https://www.eset.com/cz/kradez-identity/

ESET (2022). *Malware.* Dostupné 5. 4. 2022 z https://www.eset.com/cz/malware/

Europol (2018). *Phishing, vishing, sms.* Dostupné 17. 3. 2022 z https://www.europol.europa.eu/sites/default/files/documents/3_phishing_vishing_sms.pdf

Evropská unie (2021a). *Kapitálové požadavky na bankovní sektor.* Dostupné 9. 9. 2021 z https://www.consilium.europa.eu/cs/policies/banking-union/single-rulebook/capital-requirements/

Evropská unie (2021b). *Řešení problémů finančních institucí v potížích.* Dostupné 9. 9. 2021 z https://eur-lex.europa.eu/legal-content/CS/LSU/?uri=CELEX:32014L0059

Evropská unie (2021c). *Single euro payments area (SEPA).* Dostupné 8. 9. 2021 z https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/single-euro-payments-area-sepa_en

FBI (2022). *Scams and Safety. Skimming.* Dostupné 12. 4. 2022 z https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/skimming

Freeman, R. B. (2010). Financial crime, near crime, and chicanery in the wall street meltdown. *Journal of Policy Modeling*, 32(5), 690-701. doi: https://doi.org/10.1016/j.jpolmod.2010.07.009

Galante, M. (2017). *What Is a Card-Not-Present (CNP) Transaction and Why It Costs More.* Dostupné 27. 11. 2021 z https://squareup.com/us/en/townsquare/what-is-a-card-not-present-transaction

Garanční systém (2022). *O pojištění vkladů a jeho historii.* Dostupné 19. 4. 2022 z https://www.garancnisystem.cz/o-pojisteni-vkladu

Haentjens, M., & Gioia-Carabellese, P. D. (2015). *European banking and financial law.* London, United Kingdom: Routledge.

Havlíková, A. (2021). *Útoky na klienty bank rapidně narůstají a jsou čím dál sofistikovanější. ČBA, Policie ČR a ESET proto spouští „Kyberkampaň“.* Dostupné 27. 11. 2021 z https://www.komora.cz/news/utoky-na-klienty-bank-rapidne-narustaji-a-jsou-cim-dal-sofistikovanejsi-cba-policie-cr-a-eset-proto-spousti-kyberkampan/

Hodačová, V. (2021a). *Kyberkampaň - poznáte útok na váš bankovní účet?* Dostupné 20. 11. 2021 z https://www.policie.cz/clanek/kyberkampan.aspx

Hodačová, V. (2021b). *SMISHING.* Dostupné 29. 11. 2021 z https://www.policie.cz/clanek/smishing.aspx

Hokrová, V. (2021). *Podvod s investicemi do kryptoměny.* Dostupné 20. 11. 2021 z https://www.policie.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx

Chmelík, J., & Bruna, E. (2015). *Hospodářská a ekonomická trestná činnost.* Praha, Česko: Eupress.

Choudhry, M. (2012). *The Principles Of Banking.* Singapore: John Wiley & Sons Singapore.

Chovanculiak, R. (2020). *Pokrok bez povolení: Jak sdílená ekonomika, crowfunding a kryptoměny změnily svět.* Praha, Česko: Grada.

IDFC FIRST Bank (2021*). The banking revolution: How millennials and Gen Z are driving change.* Dostupné 15. 3. 2022 z https://www.idfcfirstbank.com/finfirst-blogs/beyond-banking/how-tech-has-changed-the-way-millennials-and-gen-z-banks

Institut pro kriminologii a sociální prevenci v Praze (2004). *Výzkum ekonomické kriminality.* Praha: IKSP.

Janáček, K. (2020). *Jsou centrální banky za zenitem své slávy?* Praha, Česko: Institut Václava Klause.

Janovec, M. (2018). *Dohled nad finančním trhem a jeho integrace.* Praha, Česko: Wolters Kluwer.

Jílek, J. (2013). *Finance v globální ekonomice I: Peníze a platební styk.* Praha, Česko: Grada.

Jurošková, L. (2012). *Bankovní regulace a dohled.* Praha, Česko: Auditorium.

Kantnerová, L. (2016). *Základy bankovnictví: Teorie a praxe.* Praha, Česko: C. H. Beck.

Kotler, P., & Armstrong, G. (2018). *Principles of Marketing* (17. vyd.). Harlow, United Kingdom: Pearson Education Limited.

Lake, R. (2022). *Surprising Millennial Banking Trends: Millennial banking habits set them apart from other banking customers.* Dostupné 15. 3. 2022 z https://www.thebalance.com/where-do-millennials-bank-and-why-4428054

Laure, B (2020). Financial crime spillovers. Does one gain to be avenged? *Journal of Economic Behavior & Organization*, 173, 196-215. doi: https://doi.org/10.1016/j.jebo.2020.03.008.

Lipovská, H. (2018). *Kdo chce naše peníze? Ekonomie bez politické korektnosti.* Praha, Česko: Grada.

Lochmanová, A. (2018). *Bankovnictví: Základy bankovnictví.* Prostějov, Česko: Computer Media.

Mandelbrot, B., Hudson, R. (2004). *The (Mis)behaviour of Markets: A Fractal View of Risk, Ruin and Reward.* Dostupné 1. 2. 2022 z https://archive.org/details/misbehaviorofmar00beno/page/255/mode/2up?q=spirits

Mann, R. J. (2016). *Payment Systems and Other Financial Transactions: Cases, Materials, and Problems* (6. vyd.). New York, United States: Wolters Kluwer.

Marr, B. (2017). *A Short History Of Bitcoin And Crypto Currency Everyone Should Read.* Dostupné 20. 11. 2021 z https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/?sh=7c7047503f27

Mejstřík, M., Pečená, M., & Teplý, P. (2008). *Základní principy bankovnictví* (1. vyd.). Praha, Česko: Karolinum.

Mejstřík, M., Pečená, M., & Teplý, P. (2014). *Bankovnictví v teorii a praxi.* Praha, Česko: Univerzita Karlova v Praze.

Mersch, Y. (2019). *The changing role of central banking.* Dostupné 3. 4. 2022 z https://www.bis.org/review/r190204c.pdf

Molnár, V. (2021). *Povinné minimální rezervy.* Dostupné 15. 3. 2022 z https://www.cnb.cz/cs/o_cnb/cnblog/Povinne-minimalni-rezervy/#:~:text=Povinn%C3%A9%20minim%C3%A1ln%C3%AD%20rezervy%20(PMR)%20p%C5%99edstavuj%C3%AD,z%C3%A1vazky%20bank%20v%C5%AF%C4%8Di%20nebankovn%C3%ADm%20subjekt%C5%AFm

Nelson Report (2020). *Card Fraud Losses Reach $28.65 Billion.* Dostupné 2. 3. 2022 z https://nilsonreport.com/mention/1313/1link/

Nelson Report (2019). *Card Fraud Losses Reach $27.85 Billion.* Dostupné 2. 3. 2022 z https://nilsonreport.com/mention/407/1link/

Netinbag (n. d.). *Co je PIN pad?* Dostupné 20. 2. 2022 z https://www.netinbag.com/cs/finance/what-is-a-pin-pad.html

Netzer, A. (2021). *How Millennials And Gen Z Could Reinvent The Banking Industry.* Dostupné 15. 3. 2022 z

https://www.forbes.com/sites/forbescommunicationscouncil/2021/02/03/how-millennials-and-gen-z-could-reinvent-the-banking-industry/?sh=1bf3a3d14e14

Petříček, M. (2021). *Bankovní účty pod palbou.* MLADÁ FRONTA DNES, str. 8.

Pihera, V., Smutný, A., & Sýkora, P. (2011). *Zákon o bankách - komentář.* Praha, Česko: C. H. Beck.

Policie ČR (2022). *Skimming.* Dostupné 8. 3. 2022 z https://www.policie.cz/clanek/ncoz-skimming.aspx

Polouček, S., Frait, J., Skaunic, I., Stavárek, D., & Vodová, P. (2013). *Bankovnictví* (2. vyd.). Praha, Česko: C. H. Beck.

Rejnuš, O. (2014). *Finanční trhy* (4. vyd.). Ostrava, Česko: Key Publishing.

Revenda, Z., Mandel, M., Kodera, J., Musílek, P., & Dvořák, P. (2012). *Penežní ekonomie a bankovnictví* (5. vyd.). Praha, Česko: Management Press.

SEC (2016). *About the SEC.* Dostupné 1. 3. 2022 z https://www.sec.gov/about.shtml

Shafiq, A., & Jan, A. (2017). Factors Influencing Gen-Y Undergraduates' Choice of Research. *Educational Process: International Journal*, 6(4), 20-34. doi: http://dx.doi.org/10.22521/edupij.2017.64.2

Square (2022). *What Are ACH Payments and How Do ACH Transactions Work?* Dostupné 1. 2. 2022 z https://squareup.com/us/en/townsquare/ach-payments#:~:text=ACH%20stands%20for%20Automated%20Clearing,%2C%20wire%20transfers%2C%20or%20cash.

Statista (2021). *Ranking of the main banks in France in 2021, according to the number of customers.* Dostupné 15. 4. 2022 z https://www.statista.com/statistics/766868/ranking-bank-according-to-number-customers-la-france/

TransUnion (2021). *Fraudsters Shift Focus at Mid-Point of 2021 from Financial Services to Travel and Leisure and other Industries.* Dostupné 20. 4. 2022 z https://www.globenewswire.com/news-release/2021/08/11/2278745/0/en/Fraudsters-Shift-Focus-at-Mid-Point-of-2021-from-Financial-Services-to-Travel-and-Leisure-and-other-Industries.html

UcadaVelez, T. (2004). *Phishing for Banks: A Timely Analysis on Identity Theft & Fraud in the Financial Sector.* Dostupné 20. 4. 2022 z https://www.giac.org/paper/gsec/4323/phishing-banks-timely-analysis-identity-theft-fraud-financial-sector/107044

Vaněk, F. (2021). *Bubliny na finančních trzích – Proč a jak vznikají? Jak z nich profitovat?* Dostupné 31. 3. 2022 z https://finex.cz/bubliny-na-financnich-trzich/

White, A. (2021). *Millennials and Gen Z are the most likely to use mobile banking apps—here's why, plus budgeting tips.* Dostupné 15. 3. 2022 z https://www.cnbc.com/select/why-millennials-gen-z-use-mobile-banking-apps/

Zorz, Z. (2021). *SniperPhish: An all-in-one open-source phishing toolkit.* Dostupné 15. 4. 2022 z https://www.helpnetsecurity.com/2021/04/26/sniperphish-phishing-toolkit/

Zrůst, L. (2019). *Selhání subjektů finančního trhu.* Praha, Česko: Wolters Kluwer.

Legislativa

Nařízení Evropského parlamentu a Rady (EU) č. 596/2014 ze dne 16. dubna 2014 o zneužívání trhu (nařízení o zneužívání trhu) a o zrušení směrnice Evropského parlamentu a Rady 2003/6/ES a směrnic Komise 2003/124/ES, 2003/125/ES a 2004/72/ES

Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012.

Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015, o platebních službách na vnitřním trhu.

Trestní zákoník č. 40/2009 Sb.

Vyhláška č. 253/2013 Sb., kterou se stanoví podmínky tvorby povinných minimálních rezerv.

Vyhláška č. 346/2013 Sb., o předkládání výkazů bankami a pobočkami zahraničních bank České národní bance.

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

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

Zákon č. 21/1992 Sb., o bankách.

Zákon č. 6/1993, o České národní bance.

Seznam tabulek

Seznam obrázků

Seznam použitých zkratek

apod. a podobně

CB Centrální banka

CNP Card not present

ČBA Česká bankovná asociace

ČNB Česká národní banka

ČR Česká republika

ČSOB Česko-slovenská obchodní banka

ČTK Česká tisková kancelář

EBA Evropská bankovní asociace

ECB Evropská centrální banka

et al. a kolektiv

EU Evropská unie

EUR euro

GBP Great British Pound – libra

IB internetové bankovnictví

MFČR Ministerstvo financí České republiky

mld. miliarda

např. například

obr. obrázek

odst. odstavec

sb. sbírky

tab. tabulka

USA Spojené státy americké

vč. včetně

Seznam příloh

Příloha A: Dva základní finanční systémy

Kolektiv autorů vysvětluje, že v závislosti na tom, kdo je nejangažovanější do diskutovaného zprostředkování úspor (zda banky nebo finanční trh), lze kategorizovat dva základní finanční systémy:

- B-systém

Jsou to právě banky, které mají v tomto systému výsadní postavení v transformaci úspor a v investování na trhu kapitálu. Banky jsou cílovým institutem pro většinu úspor domácností, přičemž tyto prostředky nabízejí firmám ve formě úvěrů. Finanční trh plní v tomto případě z hlediska forem financování domácností pouze komplementární úlohu. Cizí zdroje financování totiž domácnosti získávají především úvěrováním bank.

- M-systém

V M-systému hrají z hlediska zprostředkovatelských aktivit dominantní roli finanční trhy. Domácnosti už k obchodování na trhu cenných papírů banky nepotřebují, konají tak samy nebo za účasti investičních a penzijních fondů (Polouček et al., 2013, s. 7).

Příloha B: Definice banky a její funkce

Pro vysvětlení pojmu banka lze uvést definici Blažka a Ukleina (1997, str. 44), podle kterých se bankou rozumí „podnikatelský subjekt, jehož nejdůležitější náplní je přijímat vklady od právnických nebo fyzických osob a poskytovat úvěry na vlastní účet“.

Jak říká Zrůst (2019, s. 19), „[…] finanční instituce jsou dalším ze základních stavebních prvků finančního systému“. Jsou součástí kruhu subjektů finančního systému, zastávají funkci uživatelů a také finančních zprostředkovatelů. Třetí zmíněnou skupinu můžeme rozdělit na:

- finanční instituce provozované s udělením licence orgánu bankovního dohledu;
- finanční instituce provozované s udělením jiného typu povolení;
- ostatní (Zrůst, 2019, str. 19).

Definici je možné hledat i nahlédnutím do zákona č. 21/1992 Sb., o bankách, který na českém území udává postavení bank. Dle § 1 odst. 1 tohoto zákona banky jsou „akciové společnosti se sídlem v České republice, které a) přijímají vklady od veřejnosti, a b) poskytují úvěry, a které k výkonu činností podle písmen a) a b) mají bankovní licenci“.

Jak vysvětluje Lochmanová (2018), vklady se rozumí prostředky poskytnuté klientem, které banka musí vkladateli vrátit zvýšené o úrok, tudíž je považuje za své závazky. Na druhou stranu úvěr pro banku představuje pohledávku, neboť se jedná o poskytnuté peněžní prostředky klientovi. Nyní je to tedy klient, který je povinen prostředky vrátit a zaplatit úrok.

Mohlo by se zdát, že se definice pojmu banka nebude ve světě zásadně lišit. Zrůst (2019, s. 22) ovšem zmiňuje, že například v Anglii a jejím právním řádu žádná taková definice ani neexistuje. Konkrétní povaha bankovní instituce tedy není zřejmá a každý subjekt je hodnocen individuálně na základě soudního rozhodnutí. Dalším názorným případem může být Německo, v jehož legislativě sice definici banky najít lze, ta však opomíjí nutnost získání licence. Banka je zde vymezena jako úvěrová instituce zaměřující se na bankovní obchody, a to podnikatelským způsobem (Pihera, Smutný, & Sýkora, 2011, str. 5).

Jak čtenář může tušit, banky mají ve skutečnosti mnohem početnější funkce, než jaké jsou postiženy v základních zjednodušených definicích. Obvykle se dají rozdělit do čtyř

skupin, z nichž první dvě jsou již známé, ovšem pro lepší shrnutí jsou ve výčtu též obsaženy. Jedná se o tyto **základní funkce banky**:

1) nabídka přístupu k mechanismům placení a zúčtování;
2) transformace zdrojů a jejich alokace;
3) management rizika;
4) zpracování informací;

monitorování dlužníků (Polouček et al., 2013, s. 10).

Příloha C: Pravomoci centrální banky a kritický pohled na její makroprudenční politiku

Janáček (2020, stránky 11-15) jmenuje seznam pravomocí centrálních bank tak, jak jich postupně přibývalo:

- měnová suverenita – vydávání peněz, řízení peněžního oběhu;
- věřitel poslední instance (viz Kapitola …);
- zachovávání stability cen (regulace množství peněžní zásoby v ekonomice);
- vykonávání dohledu nad sektorem bankovnictví, jeho regulace
- péče o finanční stabilitu – prevence vzniku finančních krizí pomocí makroobezřetnostní (makroprudenční) politiky.

Janáček (2020, str. 15) k makroobezřetnostní politice doplňuje J. C. Tricheta, druhého prezidenta ECB: „Všichni o makroobezřetnostní politice mluví, ale málokdo ví, o co vlastně jde“. V makroprudenční politice je dle Mersche (2019) stále postrádána jistota, která by umožnila makroobezřetnostní postoj, který je na jednu stranu podobný, ale zároveň dostatečně odlišný od měnové politiky. „Nemáme jednotný názor na definici a měření cíle. Jak tedy můžeme identifikovat jasné a dobře definované cíle politiky spojené s metrikami a potenciálními cílovými úrovněmi?“ (Mersch, 2019, vlastní překlad)

Příloha D: Trilema centrálního bankovnictví

Janáček (2020, stránky 16-18) ve své publikaci hovoří o tzv. trilematu centrálního bankovnictví.

Nezávislost banky je posuzována z vícero hledisek, ale za ta nejdůležitější Janáček považuje cílová a operační. Cíl si může centrální banka buď stanovit sama, nebo tak učiní jiná instituce (ministerstvo financí). Operační nezávislost lze vysvětlit tak, že má CB naprostou autonomii při používání instrumentů její monetární politiky (není ovlivněna vnějšími zásahy).

Nezávislost poté jde ruku v ruce s **odpovědnost**í. Nikdo jiný, než CB sama nemůže být odpovědný za její výstupy. S ohledem na dříve zmíněnou skutečnost, kterou lze mimo jiné ukázat i na příkladu ČNB a ECB, že si některé centrální banky své cíle nastavují samy, je otázka odpovědnosti velmi diskutabilní.

Na autonomii centrální banky je nutné pohlížet jako nástroj pro plnění jí udělené legislativy a odpovědnost je nutné podepírat komunikací se širokou veřejností a transparentností. CB tedy zveřejňuje reporty o aktuální i v budoucnu očekávané inflaci a měnovém kurzu, zprávy o své monetární politice, reporty o jednáních orgánů řízení apod. A naposled přichází na řadu **důvěryhodnost**. Ta se formuje na základě minulých činnostech CB a důsledcích monetární politiky. I pro zajištění důvěryhodnosti pak platí pravidlo transparentnosti a propracované komunikaci.

Příloha E: Důležitost a efektivita centrálních bank v současnosti

Janáček (2020, stránky 75-79) se ve své publikaci zabývá otázkou, zda jsou centrální banky stále tak důležité a efektivní, jako tomu bývalo dříve. Uvádí několik problematických okolností, se kterými se v současnosti banky musejí potýkat. Jedná se o následující:

- **globalizace a sjednocování finančních systémů –** což výrazně omezuje schopnost účinné kontroly a řízení;
- **inovativní technologie –** ztráta kontroly CB nad množstvím peněz v ekonomice z důvodu úvěrování a vydávání peněz prostřednictvím nových technologií (v nesouladu s monetární politikou CB);
- **existence bublin finančních aktiv** – Vaněk (2021) tento jev vysvětluje jako *„významné odpoutání reálné vnitřní hodnoty aktiva od ceny, za kterou se aktivum obchoduje“* a dotýká se především kapitálového trhu, trhu s komoditami, obchodování s kryptoměnou či trhu nemovitostí;
- **rostoucí nabídka bankovních služeb nefinančními subjekty** – tyto subjekty se pouze tváří jako banky, ale nejsou jimi a nepodléhají tak příslušným regulacím;
- **obcházení regulačních a dohledových pravidel** – snaha o únik před dohledem či alespoň jeho minimalizace, vytváření vlastních institucí mimo oficiální rámec.
- **nedostatečné dynamické modely** – Janáček (2020, s. 79) zastává názor, že by monetární politika centrálních bank měla být postavena spíše na standardních metodách ekonomických analýz.

Příloha F: Argumenty proti regulaci

Mezi hlavní argumenty odpůrců regulace bankovnictví patří narušování přirozeného tržního prostředí a podpora oligopolní struktury. Právě to pak vede ke vzniku zmíněných odlišností sektoru, neboť banky tomuto přizpůsobují své chování. Tíhnou tak k fungování založeném na rizikovosti, složení jejich aktiv a pasiv je iracionální, finanční disciplína upadá a podobně. Zásah do tržního mechanismu podle odpůrců stojí za vznikem diskutované asymetrie informací. Fungoval-li by tento mechanismus bez vnějších regulatorních opatření, banky by to přimělo k poskytování většího množství informací svým vkladatelům. Zastánci deregulace dále tvrdí, že poskytování výhod bankám (pojištění depozit a možnost získání pomoci od CB) vede ke snížení jejich opatrnosti, a tedy zvýšené míře podstupování rizik. Dalším negativem regulace, o které se opírají její odpůrci, je vznik dodatečných nákladů na bankovní dohled. Pro úhradu těchto nákladů pak banky zvyšují cenu svých služeb nebo si zvolí cestu oželení části jejich zisku. Konkurenční nebankovní subjekty se pak dostávají do výhody. Mezi další nedostatky regulačního systému se řadí absence včasné identifikace potenciálních problémů banky v budoucnosti (Revenda a další, 2012, s. 263-267).

Zastáncem volného bankovnictví je například Dowd (1999). Diskutuje o tom, z jakého důvodu se naprostá většina společnosti shoduje na tvrzení, že liberální obchod je v pořádku, ba i velmi žádoucí, ale liberální bankovnictví nikoli. Podle jeho názoru by si vkladatelé v případě deregulovaného bankovnictví byli velmi dobře vědomi toho, že v případě krachu své banky přijdou o své peníze, protože by neexistoval žádný záchranný mechanismus. Chtěli by tedy mít jistotu, že jejich hotovost je v bezpečí, a pokud by se domnívali, že jejich bance hrozí vážné nebezpečí úpadku, okamžitě by své účty zrušili. Vedení bank by si uvědomilo, že jejich dlouhodobá životaschopnost závisí na schopnosti udržet si důvěru vkladatelů. V důsledku toho by přijali konzervativní úvěrovou politiku, podrobili by se externímu monitoringu a zveřejňovali auditované finanční výkazy. Zajistili by vám také klid tím, že by drželi dostatek hotovosti v pokladně. Konkurence bank by měla zajistit, že banky budou konvergovat k takové úrovni kapitalizace, jakou jejich zákazníci požadují. Totiž čím lépe je banka kapitálově vybavena, tím je bezpečnější a pro vkladatele atraktivnější.

Zajímavý je také přístup, který tvrdí, že regulace banky neusměrňuje, ale jen je navádí k hledání způsobů, jak se nastaveným pravidlům vyhnout. Pravidla navíc nejsou plně

respektována ani samotnými orgány dohledu, natož potom regulovanými institucemi (Revenda a další, 2012, s. 263-267).

Příloha G: Zákon o ČNB, jiné právní předpisy

Důležitý je §1 odst. 3, ve kterém stojí, že „České národní bance jsou svěřeny kompetence správního úřadu v rozsahu stanoveném tímto zákonem a jinými právními předpisy“ (Zákon o České národní bance, 1992).

Příklady zmíněných jiných právních předpisů uvádí Janovec (2018, str. 107) a jsou jimi následující:

- zákon č. 21/1992, o bankách;
- zákon č. 219/1995 Sb., devizový zákon;
- zákon č. 256/2004 Sb., o podnikání na kapitálovém trhu;
- zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech;
- zákon č. 240/2013 Sb., o investičních společnostech a investičních fondech;
- zákon č. 277/2009 Sb., o pojišťovnictví;
- zákon č. 426/2011 Sb., o důchodovém spoření;
- zákon č. 427/2011 Sb., o doplňkovém penzijním spoření.

Příloha H: Rizika v bankovní praxi

Mejstřík, Pečená a Teplá (2015, s. 170) uvádějí, že „Pod pojmem riziko zpravidla rozumíme nejistotu spojenou s budoucími čistými výnosy. Základním nástrojem pro měření rizika je volatilita (tedy standardní odchylka vývoje cen určitého podkladového aktiva)“

Blahová (2018, s. 64) provádí výčet rizik, která v bance vznikají a jejichž řízení ovlivňuje úspěch banky. Uvádí několik možných členění rizik, např. z hlediska makro a mikroekonomického či z hlediska velikosti dopadu na finanční situaci banky. Autorka této práce považuje za nejpodstatnější následující typologii bankovních rizik:

- kreditní (úvěrové) riziko;
- tržní riziko;
- provozní (operační) riziko;
- likviditní riziko;
- reputační riziko a
- strategické riziko (Blahová, 2018, s. 69).

Blahová (2018, s. 65) vyzdvihuje skutečnost, že neexistuje jednotná typologie rizik, rizika od sebe nelze oddělit, jsou tedy neohraničená a vzájemně se prolínají. S rostoucí globalizací a vznikem revolučních finančních nástrojů se navíc objevují stále nová a nová rizika.

Nesourodost typologie napříč dostupnou literaturou dokazuje například Mejstřík, Pečená a Teplý (2014), kteří rizika dělí na finanční (kreditní, tržní, likviditní) a nefinanční (operační, vypořádací, regulační, právní, daňové, politické, reputační, riziko modelu a další).

Blahová (2018, s. 179) identifikuje následujících sedm kategorií událostí, které lze považovat za provozní rizika banky:

2) **interní podvod** – ztráty, jež jsou důsledkem zpronevěry majetku nebo neplnění předpisů, interních zásad banky či legislativy, a to za účasti nejméně jedné osoby z vnitřního prostředí banky;
3) **externí podvod** – ztráty, jež jsou důsledkem zpronevěry majetku nebo neplnění legislativy, a to za účasti nejméně jedné osoby z vnějšího prostředí banky;

4) **klienti, produkty, obchodní postupy** – ztráty, jež jsou důsledkem nechtěného počínání či nepozornosti, kvůli kterým nebylo možné dostát závazkům vůči klientům; ztráty, jež jsou důsledkem samotné povahy bankovního produktu;
5) **škody na hmotném majetku** – ztráty, jež jsou důsledkem poškození majetku hmotné podstaty vnějšími faktory (např. přírodní katastrofa) nebo jinými událostmi, či pozbytím tohoto majetku;
6) **postupy při zaměstnávání, bezpečnost na pracovišti** – ztráty, jež jsou důsledkem protiprávního jednání a jednání, které není v souladu s dohodami platnými na úrovni zaměstnávání, ochrany zdraví a bezpečnosti; ztráty, jež jsou důsledkem finančních nákladů na vyplácení újem na zdraví či ztráty způsobené výdaji z důvodu diskriminace a sociální a kulturní odlišnosti;
7) **transakce, dodávky, procesní řízení** – ztráty, jež jsou důsledkem pochybení při provádění plateb či při řízení procesů; ztráty vyplývající z dodavatelských vztahů a vztahů s obchodními partnery;
8) **přerušení obchodní činnosti, selhání systému** (a ztráty z toho plynoucí).

Příloha I: Činnosti EBA

Činnosti EBA blíže specifikují Haentjens a Gioia-Carabellese (2015, s. 95) a Blahová (2018), podle kterých EBA usiluje o to, aby byla zajištěna efektivní a konzistentní regulace a dohled napříč evropským bankovním systémem. Jeho obecnými cíli jsou udržení finanční stability a zabezpečení integrity, účinnosti a řádného fungování bankovního sektoru. Hlavní úlohou EBA je přispívat k vytvoření jednotného evropského systému pravidel, jehož cílem je poskytnout jednotný soubor vzájemně sladěných obezřetnostních pravidel pro všechny finanční instituce v rámci celé EU. Blahová (2018, s. 20) doplňuje, že EBA zasahuje v případě, kdy orgán vykonávající dohled v dané zemi buď vůbec nejedná nebo jedná, avšak aniž by respektoval legislativu platnou v EU. Pokud národní orgán není schopen vyřešit jistou situaci i přes komunikaci a přijetí rad od orgánu nadnárodního, odpovědnost přebírá právě sama EBA a rozhoduje o tom, jaké kroky budou učiněny (Blahová, 2018, s. 21).

Příloha J: Praní špinavých peněz slovy Martyho Byrde

Autorka si v souvislosti s tématikou praní špinavých peněz vybavila pasáž ze seriálu Ozark, který od roku 2017 vysílá streamovací služba Netflix. Marty Byrde, hlavní postava seriálu, pracuje jako finanční poradce. Co je ale důležitější, Marty v americkém státě Missouri pere špinavé peníze pro drogový kartel. Podstatu této protiprávní činnosti Marty v jednom z prvních dílů vysvětluje, a to s jistou nadsázkou a způsobem, kterému dokáže porozumět i naprostý laik. Právě z důvodu odlehčené interpretace, snadnosti pochopení a výstižnosti textu se jej autorka rozhodla uvést:

„Oukej, dnešní lekce: praní špinavých peněz. Řekněme, že narazíš na kufr, ve kterym je pět milionů babek. Co si koupíš? Jachtu? Panský sídlo? Sporťák? O tom si můžeš nechat jen zdát. Finančák tě za to nenechá koupit nic hodnotnýho. Měl bys ty peníze teda radši dostat do bankovního systému. Tady ale nastává ten háček. Ty špinavý peníze jsou až moc čistý. Skoro to vypadá, jako by zrovna vylezly z tiskárny centrální banky. Musíš je trochu opotřebovat, zmuchlat je, vyválet je ve špíně, přejet autem… Prostě cokoli pro to, aby to vypadalo, že ty peníze už něco zažily. Potom potřebuješ nějakej business, kde frčí hotovost. Něco milýho, veselýho. Něco, kde se dá snadno zmanipulovat účetnictví. Žádný účtenky, nic takovýho. Těch 5 milionů teď smícháš s hotovostí, kterou ti hodil ten radostnej business. Tenhle mix poputuje z americký banky do banky kterýkoli země, která nemusí poslouchat americký úřady. Peníze pak jdou na standardní běžný účet, a voila, to jediný, co potřebuješ, je mít přístup k jednomu ze tří milionů bankomatů. Máš hotovo. Tvoje peníze jsou teď čistý. Stejně legitimní jako kterýkoli jiný.“

(Netflix, 2017, Season 1, Ep. 4, 0:00-1:40, vlastní překlad)

Příloha K: Chování klientů bank v bankovním styku

Vážená respondentko, vážený respondente,

prosím Vás o vyplnění dotazníku, který vznikl pro účely mé diplomové práce a zabývá se chováním klientů bank v bankovním styku. Dotazník je určen pouze pro osoby narozené mezi lety 1977 a 2000. Jeho vyplnění vám zabere méně než 10 minut.

Sektor bankovnictví je vzhledem ke své povaze velmi atraktivním cílem útočníků. V tržním hospodářství však zastává mimořádně významnou pozici, neboť jeho stabilita do značné míry určuje dynamiku hospodářského vývoje. O aktuálnosti a důležitosti tématu není pochyb.

Dotazník je zcela anonymní, žádám Vás tedy o naprostou upřímost a nezaujatost při jeho vyplňování.

Mockrát děkuji za Váš čas!

Daniela Platzová

Část první – filtrační otázky

1) Narodil/a jste se v letech 1977–2000? (vyberte jednu odpověď)
    a) Ano
    b) Ne
2) Jste majitelem běžného účtu a máte k němu zřízenou platební kartu? (vyberte jednu odpověď)
    a) Ano
    b) Ne
3) Používáte internetové bankovnictví? (vyberte jednu odpověď)
    a) Ano
    b) Ne

Část druhá - výzkum

1) Jak důležité jsou pro Vás následující faktory při výběru banky? (1= nejvíce, 5= nejméně)
    a) Bankovní poplatky

b) Šíře balíčku služeb
c) Hustota sítě poboček
d) Uživatelské prostředí internetového bankovnictví
e) Uživatelské prostředí mobilní aplikace
f) Komunikace banky se zákazníkem
g) Prestiž banky
h) Recenze
i) Zkušenosti příbuzných a přátel
j) Bezpečnost
k) Možnost vedení spořicího účtu a míra zhodnocení
l) Nabídka úvěrových služeb a velikost úrokových sazeb
m) Atraktivita reklamy

2) Se kterým z následujících tvrzení se nejvíce ztotožňujete? (vyberte jednu odpověď)

a) Své bance jsem oddaný/á, zásadně ji neměním
b) Přechod k jiné bance zvažuji jen v případě vzniku silné nespokojenosti
c) Ke změně banky jsem otevřený/á, ale učiním tak pouze po důkladném předchozím zhodnocení finančního trhu (porovnání bank, zhlédnutí recenzí apod.)
d) Svou banku klidně měním kdykoli mám pocit, že pro mě jiná banka může být lepší
e) Svou banku nemám problém kdykoli změnit, a to i bez konkrétního důvodu
f) Jiná (doplňte)

3) Jak často používáte následující způsoby placení? (velmi často – často – občas – málokdy - nikdy)

a) Debetní kartou
b) Kreditní kartou
c) Mobilním telefonem
d) Hotově
e) Kartou online
f) Převodem

4) Který způsob placení je dle Vás nejbezpečnější? (vyberte jednu odpověď)

a) Debetní kartou

b) Kreditní kartou
c) Mobilním telefonem
d) Hotově
e) Kartou online

5) Jaké Vás napadají nelegální činnosti v sektoru bankovnictví? (otevřená odpověď)

6) Používáte antivirové systémy? (vyberte jednu odpověď)

a) Ano, ve svém PC
b) Ano, ve svém mobilním telefonu
c) Ano, používám a pravidelně aktualizuji
d) Ne

7) „Své bance důvěřuji.“ Do jaké míry je pro Vás osobně tento výrok pravdivý? (škála 1-5)

1=zcela pravdivý, 5=zcela nepravdivý

8) Jak často čtete zprávy a oznámení od Vaší banky? (škála 1-5)

1=vždy, 5=nikdy

9) Obtěžují Vás tyto zprávy? (vyberte jednu odpověď)

a) Ano
b) Ne
c) Neutrální postoj

10) Kontrolujete průběžně historii svých plateb? (vyberte jednu odpověď)

a) Ano
b) Ne

11) Máte nastavené denní limity pro maximální výši transakcí? (vyberte jednu odpověď)

a) Ano
b) Ne

12) Máte nastavenou službu, která Vám oznamuje pohyby na Vašem účtu? (vyberte jednu odpověď)

a) Ano
b) Ne, ale o této možnosti vím
c) Ne, o této možnosti ani nevím

13) Přihlašujete se někdy ke svému internetovému bankovnictví z veřejné sítě či veřejného PC? (vyberte jednu odpověď)

a) Ano
b) Ano, ale jen v případě nutnosti
c) Ne

14) Víte o možnosti pojištění Vaší platební karty? (vyberte jednu odpověď)
a) Ano, této možnosti využívám
b) Ano, ale nevyužívám ji
c) Ne

15) Zná někdo Vaše přihlašovací údaje k internetovému bankovnictví nebo PIN ke kartě? (vyberte jednu odpověď)
a) Ano
b) Ne

16) Máte pro své bankovní aktivity zvolené unikátní heslo, které nepoužíváte pro žádné jiné služby? (vyberte jednu odpověď)
a) Ano
b) Ne
c) Používám různé variace jednoho hesla pro více služeb/webů (včetně internetového bankovnictví)

17) Ukládáte si své přihlašovací údaje do některých prohlížečů? (vyberte jednu odpověď)
a) Ano
b) Ne

18) Volíte pro své bankovní činnosti snadno zapamatovatelná hesla (např. obsahující celá slova, datum narození apod.)? (vyberte jednu odpověď)
a) Ano
b) Ne

19) Zakrýváte si při zadávání PIN kódu klávesnici (platebního terminálu/bankomatu apod.)? (vyberte jednu odpověď)
a) Ano
b) Ne

20) Máte někde poznamenaný PIN ke kartě pro případ zapomenutí? (vyberte jednu odpověď)
a) Ano*
b) Ne**

*pokračování otázkou č. 21

**pokračování otázkou č. 22

21) Kde máte poznamenaný PIN pro případ zapomenutí? (otevřená odpoveď)

22) Platíte kartou na internetu? (vyberte jednu odpověď)

a) Ano*
b) Ne**

*pokračování otázkou č. 23

**pokračování otázkou č. 25

23) Víte, co je to systém 3D Secure? (vyberte jednu odpověď)

a) Ano*
b) Ne**

*pokračování otázkou č. 24

**pokračování otázkou č. 25

24) Vysvětlete pojem 3D Secure: (otevřená odpověď)

25) Používáte někdy k placení v obchodech místo fyzické karty mobilní telefon? (vyberte jednu odpověď)

a) Ano*
b) Ne**

*pokračování otázkou č. 26

**pokračování otázkou č. 29

26) Jaké ověření pro tento druh placení používáte? (vyberte jednu odpověď)

a) kódový zámek
b) otisk prstu
c) sken obličeje
d) znak/gesto
e) jiná

27) Vypínáte si NFC službu ve vašem mobilu, když ji nepoužíváte? (vyberte jednu odpověď)

a) Ano
b) Ne

28) Používáte stejnou kombinaci pro odemknutí telefonu a PIN ke kartě? (vyberte jednu

odpověď)

a) Ano
b) Ne

29) Ověřujete si bezpečnost e-shopů? (vyberte jednu odpověď)

a) Ano*
b) Ne**

*pokračování otázkou č. 30

**pokračování otázkou č. 31

30) Jak si ověřujete bezpečnost e-shopů? (otevřená odpověď)

31) Ověřujete si původ aplikací, které si stahujete do svého mobilního telefonu? (vyberte jednu odpověď)

a) Ano*
b) Ne**

*pokračování otázkou č. 32

**pokračování otázkou č. 33

32) Jak si ověřujete původ aplikací? (otevřená odpověď)

33) Investujete nebo jste někdy přemýšlel/a o investici do kryptoměny? (vyberte jednu odpověď)

a) Ano*
b) Ne**

*pokračování otázkou č. 34

**pokračování otázkou č. 36

34) Pokud ano, z jakého důvodu? (více odpovědí)

a) Chci zlepšit svou finanční situaci
b) Obchodování tohoto typu mě zajímá/baví
c) Je to populární
d) Hledám zhodnocení pro své úspory
e) Mám zájem o rychlé a snadné zhodnocení svých finančních prostředků
f) Jiné

35) Klikl/a jste někdy na reklamu s kryptoměnou? (vyberte jednu odpověď)

a) Ano

b) Ne

36) Byl/a jste někdy terčem bankovního útoku/podvodu? (vyberte jednu odpověď)

a) Ano
b) Ne

37) Víte o někom, kdy byl terčem bankovního útoku? (vyberte jednu odpověď)

a) Ano
b) Ne

38) Zúčastnil/a jste se nebo víte o někom, kdo by se někdy zúčastnil tzv. insider tradingu v bance? (vyberte jednu odpověď)

a) Ano
b) Ne

39) Který z následujících bankovních podvodů podle Vašeho odhadu aktuálně představuje největší hrozbu pro klienty bank? (vyberte jednu odpověď)

a) Malware
b) Skimming
c) Phishing
d) Vishing
e) Podvodné mobilní aplikace
f) Podvody se zaměřením na investice do kryptoměn
g) Pharming

40) „O problematice bankovních podvodů nás dostatečně informují média.“ V jaké míře souhlasíte s tímto tvrzením? (škála 1-5)

1=silně souhlasím, 5=silně nesouhlasím

41) Která česká banka je dle Vašeho mínění nejbezpečnější? (vyberte jednu odpověď)

a) ČSOB
b) Česká spořitelna
c) Fio banka
d) Air Bank
e) Moneta Money Bank
f) Reiffeisenbank
g) Nedokážu posoudit

42) Během pandemie Covid-19 došlo k celosvětovému nárůstu pokusů o digitální podvody ve finančních službách. Odhadněte, jak velký byl tento nárůst v porovnání

s obdobím před pandemií. (vyberte jednu odpověď)

a) méně než 25 %

b) 25-50 %

c) 75-100 %

d) více než 100 %

43) Jak velkou část útoků na bankovní sektor se dle Vašeho odhadu daří v České republice zastavit? (vyberte jednu odpověď)

a) méně než 20 %
b) 20-40 %
c) 40-60 %
d) 60-80 %
e) více než 100 %

Část třetí - identifikační otázky

1) Jaké je Vaše pohlaví? (vyberte jednu odpověď)

a) Muž

b) Žena

2) Jaké je Vaše nejvyšší dosažené vzdělání? (vyberte jednu odpověď)

a) Základní
b) Střední s výučním listem
c) Střední s maturitou
d) Vyšší odborné (VOŠ)
e) Vysokoškolské – bakalářský studijní program
f) Vysokoškolské – magisterský studijní program
g) Vysokoškolské – doktorský studijní program

3) V jakém oboru je Vaše nejvyšší dosažené vzdělání? (otevřená odpověď)

4) Jsem klientem této banky: (otevřená odpověď. Prosím, uveďte všechny bankovní instituce, jejichž služby využíváte.)

Příloha L: Étude de comportement des clients bancaires

Chers réspondants,

Veuillez remplir ce questionnaire qui a été créé pour les besoins de ma thèse. L'objectif du questionnaire est de comprendre le comportement des clients dans le milieu bancaire. Le questionnaire s'adresse uniquement aux personnes nées entre 1977 et 2000. Il vous faudra moins de 10 minutes pour le remplir.

En raison de sa nature, le secteur bancaire est une cible très attrayante pour les attaquants. Cependant, il occupe une place extrêmement importante dans une économie de marché, car sa stabilité détermine largement la dynamique du développement économique. L'actualité et l'importance du sujet ne font aucun doute.

Le questionnaire est totalement anonyme, je vous demande donc une totale honnêteté et impartialité en le remplissant.

Je vous remercie d'avance pour le temps accordé!

Daniela Platzová

Première partie – les questions à filtrer

c) Êtes-vous né en 1977-2000? (choisir une réponse)
   a) Oui
   b) Non

d) Êtes-vous titulaire d'un compte bancaire et avez vous une carte de paiement? (choisir une réponse)
   1. Oui
   2. Non

e) Utilisez-vous les services bancaires par Internet? (choisir une réponse)
   1. Oui
   2. Non

Deuxième partie

g) Quelle est l'importance des facteurs suivants lors du choix d'une banque? (1 = très important - 5 = complètement sans importance)
    1. Les frais bancaires
    2. Largeur du pack de services
    3. Densité du réseau de succursales
    4. Interface utilisateur des services bancaires par Internet
    5. Interface utilisateur de l'application mobile
    6. Communication bancaire avec le client
    7. Le prestige de la banque
    8. La revue
    9. Expériences de parents et d'amis
    10. Sécurité
    11. La possibilité de maintenir un compte d'épargne et le taux d'appréciation
    12. Offrir des services de crédit et des taux d'intérêt
    13. L'attractivité de la publicité

h) À laquelle des affirmations suivantes vous identifiez-vous le plus? (choisir une réponse)
    1. Je me suis engagé envers ma banque, je ne la change pas du tout
    2. J'envisage de changer de banque uniquement en cas de forte insatisfaction
    3. Je suis ouvert à changer de banque, mais je ne le ferai qu'après une évaluation préalable approfondie du marché financier (comparaison des banques, examen des avis, etc.)
    4. Je peux changer de banque chaque fois que je sens qu'une autre banque pourrait être meilleure pour moi
    5. Je n'ai aucun problème à changer de banque à tout moment, même sans raison précise

i) À quelle fréquence utilisez-vous les modes de paiement suivants? (très souvent – souvent – parfois – rarement - jamais)
    1. Carte de débit
    2. Carte de crédit
    3. Téléphone mobile

4. En espèces
5. Carte en ligne
6. Par virement

j) Selon vous, quel mode de paiement est le plus sûr? (choisir une réponse)
    1. Carte de débit
    2. Carte de crédit
    3. Téléphone mobile (NFC)
    4. En espèces
    5. Carte en ligne
    6. Par virement

k) Quelles activités illégales dans le secteur bancaire vous viennent à l'esprit? (réponse ouverte)

l) Utilisez-vous des systèmes antivirus? (choisir une réponse)
    1. Oui, sur mon PC
    2. Oui, sur mon téléphone portable
    3. Oui, j'utilise et mets à jour régulièrement
    4. Non

m) "Je fais confiance à ma banque." Dans quelle mesure cette affirmation este vraie pour vous personnellement? (1= complétement vrai – 5= complétement faux)

n) À quelle fréquence lisez-vous les nouvelles et les annonces de votre banque? (1= toujors – 5= jamais)

o) Ces messages vous dérangent? (choisir une réponse)
    1. Oui
    2. Non
    3. Attitude neutre

p) Regardez-vous l'historique de vos paiements? (choisir une réponse)
    1. Oui
    2. Non

q) Avez-vous des limites quotidiennes pour le montant maximum de transactions? (choisir une réponse)
    1. Oui
    2. Non

r) Avez-vous mis en place un service qui vous informe des mouvements sur votre

compte? (choisir une réponse)

1. Oui
2. Non, mais je connais cette possibilité
3. Non, je ne connais même pas cette possibilité

s) Utilisez vous la banque en ligne à partir d'un réseau public ou d'un PC public? (choisir une réponse)

1. Oui
2. Oui, mais seulement si nécessaire
3. Non

t) Connaissez-vous la possibilité d'assurer votre carte de paiement? (choisir une réponse)

1. Oui, j'utilise cette option
2. Oui, mais je ne l'utilise pas
3. Non

u) Est-ce que quelqu'un connaît vos identifiants de connexion aux services bancaires par Internet ou le code PIN de votre carte? (choisir une réponse)

1. Oui
2. Non

v) Avez-vous un mot de passe unique pour vos activités bancaires que vous n'utilisez pas pour d'autres services? (choisir une réponse)

1. Oui
2. Non

w) Stockez-vous vos informations de connexion dans certains navigateurs? (choisir une réponse)

1. Oui
2. Non

x) Choisissez-vous des mots de passe faciles à retenir pour vos activités bancaires (par exemple contenant des mots complets, date de naissance, etc.)? (choisir une réponse)

1. Oui
2. Non

y) Couvrez-vous le clavier (terminal de paiement) lors de la saisie du code PIN? (choisir une réponse)

1. Oui
2. Non

z) Conservez vous le code PIN de votre carte bancaire (ex. dans le portefeuille) en cas d'oubli? (choisir une réponse)
    1. Oui*
    2. Non**

*continuer avec la question numéro 21

**continuer avec la question numéro 22

aa) Si oui, où? (réponse ouverte)

bb) Payez-vous par carte en ligne? (choisir une réponse)
    1. Oui*
    2. Non**

*continuer avec la question numéro 23

**continuer avec la question numéro 25

cc) Savez-vous ce qu'est 3D Secure? (choisir une réponse)
    1. Oui*
    2. Non**

*continuer avec la question numéro 24

**continuer avec la question numéro 25

dd) Expliquez le terme 3D Secure: (réponse ouverte)

ee) Utilisez vous un téléphone portable pour payer dans les magasins au lieu d'une carte physique? (choisir une réponse)
    1. Oui*
    2. Non**

*continuer avec la question numéro 26

**continuer avec la question numéro 29

ff) Quelle vérification utilisez-vous pour ce type de paiement? (choisir une réponse)
    1. Serrure à code
    2. Empreinte digitale
    3. Balayage facial
    4. Signe / geste

gg) Désactivez-vous le service NFC sur votre téléphone mobile lorsque vous ne l'utilisez pas? (NFC = technologie de paiement par téléphone mobile) (choisir une réponse)

1. Oui
2. Non

hh) Utilisez-vous la même combinaison pour déverrouiller votre téléphone et le code PIN de votre carte? (choisir une réponse)

1. Oui
2. Non

ii) Vérifiez-vous la sécurité des boutiques en ligne? (choisir une réponse)

1. Oui*
2. Non**

*continuer avec la question numéro 30

**continuer avec la question numéro 31

jj) Si c'est le cas, comment? (réponse ouverte)

kk) Vérifiez-vous l'origine des applications que vous téléchargez sur votre téléphone portable? (choisir une réponse)

1. Oui*
2. Non**

*continuer avec la question numéro 32

**continuer avec la question numéro 33

ll) Si c'est le cas, comment? (réponse ouverte)

mm) Investissez-vous ou avez-vous déjà envisagé d'investir dans une crypto-monnaie? (choisir une réponse)

1. Oui*
2. Non**

*continuer avec la question numéro 34

**continuer avec la question numéro 36

nn) Si oui, pour quelle raison? (choisir plusiers réponses)

1. Je veux améliorer ma situation financière
2. Je suis intéressé/apprécie le trading de ce type
3. C'est à la mode

4. Je cherche à valoriser mon épargne
5. Je suis intéressé par une évaluation rapide et facile de mes fonds

oo) Avez-vous déjà cliqué sur une annonce de crypto-monnaie? (choisir une réponse)
1. Oui
2. Non

pp) Avez-vous déjà été la cible d'une attaque/fraude bancaire? (choisir une réponse)
1. Oui
2. Non

qq) Connaissez-vous quelqu'un qui a été la cible d'une attaque bancaire? (choisir une réponse)
1. Oui
2. Non

rr) Avez-vous participé ou connaissez-vous quelqu'un qui participerait un jour à "insider trading" dans une banque? (Insider trading = Connaissance d'informations privilégiées en raison de l'emploi dans la banque et de leur utilisation à votre avantage) (choisir une réponse)
1. Oui
2. Non

ss) Selon vous, laquelle des fraudes bancaires suivantes représente actuellement la plus grande menace pour les clients des banques? (choisir une réponse)
1. Malware (attaquer les comptes clients par des virus malveillants)
2. Skimming (les données de la bande magnétique de la carte sont copiées électroniquement sur une autre carte)
3. Phishing (e-mails frauduleux, l'expéditeur se fait souvent passer pour une banque ou une boutique en ligne)
4. Vishing (semblable à phishing, mais il a lieu par téléphone)
5. Applications mobiles frauduleuses
6. Fraude ciblant les cryptomonnaies
7. Pharming (redirection du client vers de faux sites bancaires en ligne)

tt) « Nous sommes suffisamment informés par les médias sur la problématique de la fraude bancaire. » Dans quelle mesure êtes-vous d'accord avec cette affirmation? (1= Je suis entiérement dˇaccord – 5= Je suis fortement en désaccord)

uu) A votre avis, quelle banque française est la plus sûre? (choisir une réponse)

1. Crédit Agricole (CA)
2. BNP Paribas
3. Société Générale
4. Caisse d'Epargne (CE)
5. Banque Populaire (BP)
6. Crédit Mutuel
7. La Banque Postale
8. LCL

vv) Pendant la pandémie de Covid-19, il y a eu une augmentation mondiale des tentatives de fraude numérique dans les services financiers. Estimez l'ampleur de cette augmentation par rapport à la période précédant la pandémie. (choisir une réponse)

1. Mois que 25 %
2. 25–50 %
3. 50–75 %
4. 75–100 %
5. Plus que 100 %

ww) D'après votre estimation, combien d'attaques contre le secteur bancaire sont arrêtées en France? (choisir une réponse)

1. Mois que 20 %
2. 20–40 %
3. 40–60 %
4. 60–80 %
5. Plus que 80 %

Troisième partie - les questions à identification

c) Quel est votre sexe? (choisir une réponse)

1. Homme
2. Femme

d) Quel est ton plus haut niveau d'éducation? (choisir une réponse)

1. Enseignement primaire
2. Certificat professionnel

3. Baccalauréat
4. Lycée professionnel
5. Université - titulaire d´une licence
6. Université – master
7. Université – doctorat

e) Dans quel domaine se situe votre niveau d'études le plus élevé? (réponse ouverte)

Abstrakt

Platzová, D. (2022). *Bankovní podvody* (Diplomová práce), Západočeská univerzita v Plzni, Fakulta ekonomická, Česko.

Klíčová slova: bankovnictví, banka, podvod, kriminalita, bezpečnost, klient banky

Předložená práce pojednává o problematice bankovních podvodů. V teoretické části práce je nejdříve proveden úvod do bankovnictví, ve kterém jsou představena specifika sektoru a bankovní soustava. Další část práce se věnuje bankovní regulaci a bankovnímu dohledu. Pozornost je věnována především důvodům pro regulaci bank a systému regulace a dohledu v České republice. Práce se dále soustředí na podvodná jednání v bankovním sektoru, a to ve členění na podvody páchané bankou, podvody páchané vůči bance a podvody páchané na klientech banky. Praktická část práce je založena na dotazníkovém šetření, jehož cílem je objasnit chování klientů bank ve vztahu k bezpečnosti v bankovním styku na příkladu České republiky a Francie. Výstupem práce je komparace výsledků mezi oběma zeměmi a shrnutí nejzásadnějších poznatků výzkumu.

Abstract

Platzová, D. (2022). *Banking Frauds* (Diploma Thesis). University of West Bohemia, Faculty of Economics, Czech Republic.

Key words: banking, bank, fraud, crime, security, bank client

This thesis deals with the issue of bank fraud. In the theoretical part of the thesis, an introduction to banking is first made, in which the specifics of the sector and the banking system are introduced. The following part of the thesis deals with bank regulation and supervision. The reasons for bank regulation, as well as the Czech Republic's regulatory and supervisory structure, receive the most attention. Furthermore, the thesis focuses on fraudulent acts in the banking sector, broken down into fraud perpetrated by the bank, fraud perpetrated against the bank and fraud perpetrated against the bank's customers. The empirical part of the thesis is based on a questionnaire survey, the aim of which is to clarify the behaviour of bank customers in relation to security in banking relations using the examples of the Czech Republic and France. The thesis concludes with a comparison of the outcomes between the two countries and a summary of the research's most relevant findings.