Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Ochrana údajů a soukromí na internetu se zaměřením na problematiku bankovní identity

Jaroslava Havlovicová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Mgr. Bc. Jaroslava Havlovicová

Systémové inženýrství a informatika
Informatika

Název práce

Ochrana údajů a soukromí na internetu se zaměřením na problematiku bankovní identity

Název anglicky

Data protection and privacy on the Internet with a focus on banking identity issues

---

Cíle práce

Obsahem teoretické části práce bude popis informačně technologických aspektů ochrany údajů a soukromí osob na internetu z obecného hlediska včetně posouzení momentálních možností oveření totožnosti osoby prostřednictvím prvků dálkového přístupu, zejména prostřednictvím bankovní identity. Součástí teoretické části dále bude posouzení právního zakotvení ochrany osobních údajů a soukromí na internetu a vyhodnocení souladu právního rámce s aktuálně funkčními a používanými technologiemi online ověřování totožnosti. V praktické části budou obecné postupy ověření totožnosti z teoretické části práce aplikovány na konkrétní situace a prostředí.

Metodika

Diplomová práce vychází z předpokladu systematického zpracování teoretických východisek, kdy budou shromažďována, tříděna a analyzována sekundární data z oblasti ochrany údajů a soukromí osob v prostředí internetu s důrazem zejména na prvky ověřování totožnosti online v kontextu v České republice aktuálně účinných relevantních právních předpisů. Na základě získaných informací bude vyhodnocen soulad technologického pokroku v oblasti ověřování totožnosti online a právního rámce pro danou oblast, případně budou navrženy změny s účelem co největší využitelnosti moderních prvků ověření totožnosti prostřednictvím dálkového přístupu.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

ochrana osobních údajů, ověření totožnosti, bankovní identita

---

Doporučené zdroje informací

DONÁT, Josef a Jan TOMÍŠEK. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4.

JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4

LENTNER, Gabriel & PARYCEK, Peter. Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. Transforming Government: People, Process and Policy. 2016. 10. 8-25. 10.1108/TG-11-2013-0047.

POLČÁK, Radim. Právo informačních technologií. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8

REZGUI, Abdelmounaam, BOUGUETTAYA, Athman, ELTOWEISSY, Marwa. Privacy on the Web: Facts, Challenges, and Solutions. IEEE Security & Privacy Magazine. 2003. 1. 40-49. 10.1109/MSECP.2003.1253567.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Mgr. Vladimír Očenášek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 28. 03. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „*Ochrana údajů a soukromí na internetu se zaměřením na problematiku bankovní identity*“ jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30. března 2022 _____

Poděkování

Ráda bych touto cestou poděkovala panu Mgr. Ing. Vladimíru Očenáškovi, Ph.D., za jeho cenné rady a připomínky v průběhu zpracování předkládané diplomové práce. Dále bych ráda poděkovala svým nejbližším, kteří mi trpělivě stojí po boku při plnění studijních cílů.

Ochrana údajů a soukromí na internetu se zaměřením na problematiku bankovní identity

Abstrakt

Problematika ochrany osobních údajů a soukromí v prostředí internetu je velice komplexním tématem, které se zejména v posledních letech vyvíjí skutečně dynamicky a pojímá dílčí otázky právní, informačně technologické i jiné. V této souvislosti je třeba reagovat mimo jiné na rozmach nových způsobů ověření totožnosti na dálku, které mohou řadu každodenních procesů významně usnadnit a zrychlit, zároveň s sebou ale přináší nové dosud neznámé hrozby.

Předkládaná diplomová práce poskytuje odborné teoretické základy témat souvisejících s ochranou osobních údajů a soukromí v online prostředí, přičemž zvýšený důraz je kladen na způsoby ověřování totožnosti osob na dálku, jež nabízí současná technologická úroveň. Zejména je pozornost věnována v poslední době velmi diskutovanému ověřování totožnosti pomocí bankovní identity, na jejíž nezanedbatelný nárůst popularity reagovala již i česká právní regulace. Pod prizmatem rozšiřování možností využití bankovní identity je tento způsob ověřování totožnosti osob na dálku otestován při užití pro veřejné i soukromé účely, načež jsou jednotlivé případy vzájemně porovnány. Závěrem předkládaná diplomová práce nabízí analýzu zjištěných výsledků a závěry z nich vyvozené, včetně vyhodnocení přihlašování pomocí bankovní identity z pohledu praktických zkušeností nabytých samotnými uživateli této služby.

Klíčová slova: ochrana osobních údajů, ověření totožnosti, bankovní identita

Data protection and privacy on the Internet with a focus on banking identity issues

Abstract

The issue of personal data protection and privacy in the Internet environment is a very complex topic, which has been developing dynamically in recent years and includes legal, information technology and other issues. In this context, it is necessary to react, among other things, to the rise of new methods of remote identity verification, which can significantly facilitate and speed up many everyday processes, but at the same time bring with them new, hitherto unknown threats.

The submitted thesis provides a professional theoretical basis for topics related to the protection of personal data and privacy in the online environment, with an increased emphasis on the methods of remote identity verification offered by the current technological level. In particular, attention is paid to the recently much discussed identity verification using bank identity, to whose not insignificant increase in popularity the Czech legal regulation has already responded. Under the prism of expanding the possibilities of using bank identity, this method of remote identity verification is tested for both public and private use, after which individual cases are compared with each other. Finally, the thesis offers an analysis of the results and conclusions drawn from them, including an evaluation of the login using bank identity from the perspective of practical experience gained by the users of this service themselves.

Keywords: data protection, identity verification, banking identity

Obsah

Úvod

Ochrana údajů a soukromí osob na internetu je v dnešním stále se zrychlujícím světě stále častěji diskutovanou otázkou, když vývoj moderních technologií neustále posouvá dosud známé hranice a vytváří nové možnosti, ale i hrozby. Zejména platforma internetu je prostředím, v němž je třeba ochranu soukromí pojmout ve významně odlišném smyslu než tu v reálném světě, čemuž je třeba přizpůsobit mimo jiné i právní úpravu. S ochranou soukromí a osobních údajů pak blízce souvisí identifikace osob a ověřování jejich totožnosti na dálku, autentizační mechanismy a další související technologické náležitosti. Právě dálkové ověření totožnosti je významným nástrojem, který umožňuje právně jednat vůči protistraně bez nutnosti vzájemné fyzické přítomnosti, čímž přispívá k usnadnění řady procesů, s nimiž se nutně setkává úplně každý na denní bázi. Mechanismy umožňující s jistotou určit, že se jedná o tu či onu fyzickou osobu, ale musí být vykazovat dostatečnou míru bezpečnosti, jelikož neúplné a nedokonalé nástroje by mohly vést ke zneužívání lidských, občanských či jiných práv a zájmů ověřovaných i třetích osob. V tomto kontextu je třeba hledat kompromisní řešení, které umožní ověření totožnosti na dálku při zajištění náležité ochrany osobních údajů a veškerých dalších právních náležitostí, ale které bude zároveň odpovídat úrovni současného technologického vývoje a nebude bránit zužitkování učiněných pokroků.

Předkládaná diplomová práce se pokusí propojit všechny faktory, na které je nezbytné brát ohled při ochraně soukromí na internetu, ať již jde o aspekty právní, technologické, uživatelské či jiné. Primárním cílem je podání podrobného výkladu právní úpravy ochrany údajů a soukromí osob na internetu a vysvětlení souvisejících informačně technologických vazeb včetně posouzení momentálních možností ověření totožnosti osoby na dálku. Ze způsobů ověřování totožnosti na dálku zažívá v poslední době významného rozmachu především bankovní identita, na kterou bude upřena zvýšená pozornost. Sekundárním cílem předkládané práce bude provedení praktického testování ověřování totožnosti na základě dálkového přístupu, přičemž předmětem testování a následné analýzy bude právě bankovní identita. Praktická část práce bude zaměřena na různé oblasti využívající bankovní identity, ať již ze sektoru veřejného či komerčního.

Za účelem naplnění stanovených cílů budou systematicky zpracována teoretická východiska v potřebné podrobnosti. Metodami využitými v teoretické části práce budou zejména shromažďování, třídění a analýza dat. Z hlediska zpracovávaných dat se bude

zpravidla jednat o data sekundární. V praktické části práce bude ústřední metodou testování a analýza postupů při ověřování totožnosti na dálku pomocí bankovní identity, popřípadě potenciálně uvažované dotazníkové šetření.

Z obecného hlediska budou v teoretické části práce podrobně zpracovány právní základy ochrany osobních údajů na české i unijní úrovni, přičemž nebudou opomenuty ani definice a vysvětlení důležitých témat a pojmů souvisejících s ochranou osobních údajů na internetu, možnostmi dálkového ověřování totožnosti, u kterých bude zvýšená pozornost zaměřena především na bankovní identitu. Samostatné podkapitoly budou věnovány také například zvláštní kategorii osobních údajů (citlivým údajům) nebo souborům cookies, které si vysloužily již speciální právní úpravu na evropské úrovni. Dále bude představena oblast digitálního evropského trhu, přičemž bude shrnut také jeho vývoj uskutečněný v posledním desetiletí. Opomenuty nebudou v teoretické části předkládané diplomové práce ani základy kryptografie či obecné náležitosti zajištění bezpečnosti dat, což jsou témata nepochybně také blízce související s problematikou ochrany soukromí. Závěr teoretických východisek, o něž bude opřena navazující praktická část diplomové práce, bude věnován již samotné bankovní identitě jako modernímu představiteli způsobů dálkového ověření totožnosti osob.

Obsahem vlastní, tedy prakticky zaměřené části práce bude otestování využití bankovní identity pro různé účely. Jednotlivé možnosti přihlášení pomocí bankovní identity budou rozděleny do dvou hlavních skupin, a to na účely veřejné a soukromé (komerční). Postupy přihlašování v jednotlivých testovaných a analyzovaných případech budou následně vzájemně porovnány. Pokud se podaří prostřednictvím dotazníkového šetření shromáždit dostatečné množství podkladových dat, budou dále v praktické části vyhodnoceny zkušenosti respondentů s přihlašováním pomocí bankovní identity. V úplném závěru předkládané diplomové práce bude věnována samostatná kapitola přehlednému shrnutí výsledků a závěrům, které budou ze zjištěných skutečností vyvozeny.

1 Cíl práce a metodika

1.1 Cíl práce

Obsahem teoretické části práce bude popis informačně technologických aspektů ochrany údajů a soukromí osob na internetu z obecného hlediska včetně posouzení momentálních možností ověření totožnosti osoby prostřednictvím prvků dálkového přístupu, zejména prostřednictvím bankovní identity. Součástí teoretické části dále bude posouzení právního zakotvení ochrany osobních údajů a soukromí na internetu a vyhodnocení souladu právního rámce s aktuálně funkčními a používanými technologiemi online ověřování totožnosti. V praktické části budou obecné postupy ověření totožnosti z teoretické části práce aplikovány na konkrétní situace a prostředí.

1.2 Metodika

Diplomová práce vychází z předpokladu systematického zpracování teoretických východisek, kdy budou shromažďována, tříděna a analyzována sekundární data z oblasti ochrany údajů a soukromí osob v prostředí internetu s důrazem zejména na prvky ověřování totožnosti online v kontextu v České republice aktuálně účinných relevantních právních předpisů. Na základě získaných informací bude vyhodnocen soulad technologického pokroku v oblasti ověřování totožnosti online a právního rámce pro danou oblast, případně budou navrženy změny s účelem co největší využitelnosti moderních prvků ověření totožnosti prostřednictvím dálkového přístupu.

2 Teoretická východiska

2.1 Ochrana osobních údajů

Právo na ochranu osobních údajů a soukromí je jedním ze základních práv člověka a jedním z klíčových institutů, které by měly být v právním státu zajištěny. Přestože konkrétně ochrana osobních údajů je v rámci komplexu veškerých práv souvisejících se soukromím člověka považována za institut spíše mladší (Polčák, 2018), například ve Švédsku byl přístup k veřejným záznamům regulován již v roce 1776. Dalším historicky podloženým aktem chránícím osobní údaje a soukromí byl například francouzský zákon zakazující veřejně publikovat údaje o soukromí člověka, jenž vstoupil v účinnost roku 1858 (Klausová, 2017).

Neoddělitelnost rozvíjejícího se internetového prostoru a tomu adekvátně se vyvíjejících právních pravidel tohoto prostředí je nezpochybnitelná. Internetové právo či právo informačních a komunikačních technologií pojednává zejména o přizpůsobení legislativy a postojů právní vědy vzhledem k neustále postupujícímu vývoji v oblasti online prostoru (Matejka, 2013). Co se týče nakládání s osobními údaji osob v prostředí počítačových technologií a internetu, ačkoliv může být tato oblast považována za disciplínu poslední doby, již v roce 1972 Velká Británie zveřejnila ve zprávě Výboru pro soukromí doporučení Mladšího výboru zahrnující desatero základních principů při užívání počítačů zpracovávajících osobní údaje (Carey, 2004).

Významnou událostí v oblasti právní úpravy ochrany osobních údajů byl samozřejmě vstup České republiky do Evropské unie, přičemž právě unijní předpisy jsou v poslední době hlavním pramenem regulace dané oblasti. Přestože ochrana osobních údajů tedy již má svou historii a také v technologiích využívaných v internetovém prostředí byl zaznamenán znatelný vývoj, pro účely této diplomové práce bude brán v potaz zejména současný stav legislativy. Jak již bylo naznačeno, stále se vyvíjející střet potřeby ochrany soukromí osob s dokonalejšími technologiemi, jejichž užívání může soukromí narušit, implikuje čím dál větší výzvu v oblasti adekvátní právní regulace (Rezgui, Bouguettaya, 2003).

Za základní principy ochrany osobních údajů jsou dle Matesa, Janečkové a Bartíka (2012) považovány:

a) Časové omezení

Osobní údaje by měly být uchovávány pouze po dobu nezbytně nutnou ke stanovenému účelu. V případě, že jsou uchovávány déle, mělo by tomu tak být pouze za účelem sběru statistických dat (a to jen ve vymezených případech), za účelem vědeckým či za účelem archivace.

a) Potřebnost a přiměřenost

Nakládání s osobními údaji by mělo probíhat vždy pouze v rozsahu nezbytně potřebném, přiměřeně a v souladu se stanoveným účelem.

b) Průhlednost

Rozsah, účel i způsob nakládání s osobními údaji by měly být vždy transparentní, přičemž dostupná by měla být také informace o tom, kterým osobám jsou osobní údaje zpřístupněny.

c) Bezpečnost

V duchu ochrany osobních údajů by měla být aplikována dostatečně účinná bezpečnostní opatření, jejichž účelem je zamezit neoprávněnému či nahodilému přístupu k osobním údajům, neoprávněnému zničení, ztrátě či změně a dalším nežádoucím situacím, ať se jedná o zneužití úmyslné či nesprávné zacházení bez identifikovaného úmyslu. Bezpečnost osobních údajů by měla být zajišťována i po skončení jejich zpracovávání.

d) Právo přístupu k datům

Každý subjekt osobních údajů neboli osoba, k níž se dané údaje vážou a o níž podávají informace, má právo být informován o způsobu nakládání s osobními údaji k němu se vztahujícími.

e) Nezávislý dozor

Jako dozorující orgán v oblasti ochrany osobních údajů byl s účinností od 1. června 2000 zřízen Úřad pro ochranu osobních údajů, který sídlí v Praze.

f) Právo na opravu a výmaz

Dále má každý subjekt údajů právo v případě nepřesnosti požádat o vysvětlení či o nápravu takového stavu, a to zejména domnívá-li se subjekt údajů, že jeho osobní údaje jsou zpracovávány v rozporu se zákonem či v rozporu s ochranou jeho soukromého a osobního života.

g) Legitimita zpracování údajů

Nakládání s osobními údaji musí být vždy legitimní, tedy musí existovat zákonný důvod k jejich zpracování a samotné nakládání s nimi musí probíhat v mezích zákona.

h) Omezení účelem

Rozsah osobních údajů, s nimiž je nakládáno, musí být vždy omezen účelem daného nakládání, přičemž podle této zásady by měly být osobní údaje zpracovávány vždy pouze v rozsahu co nejmenším možném vzhledem k účelu zpracování.

Zachování soukromí na internetu má důležitý dopad na mnoho činností a aplikací provozovaných na webu, z nichž nejdůležitější jsou právě oblasti e-businessu a digitální veřejné správy (Rezgui, Bouguettaya, 2003). Obecně lze říci, že k problému ochrany soukromí v internetovém prostředí přispívají dva hlavní faktory:

- otevřená a nedeterministická povaha webu a
- složitý tok informací, který je náchylný k únikům, a to u mnoha webových transakcí, které zahrnují přenos citlivých osobních údajů (Rezgui, Bouguettaya, 2003).

Abychom pochopili první faktor, můžeme porovnat internetové prostředí s tradičními, uzavřenými, deterministickými víceuživatelskými systémy, jako jsou například podnikové sítě. Do těchto systémů mohou přistupovat pouze známí uživatelé se sadou předem definovaných oprávnění. Internetová stránka je naopak otevřeným prostředím, ve kterém je mnoho a priori neznámých uživatelů, kteří mohou přistupovat k informacím.

Příkladem druhého faktoru může být aplikace veřejné správy. V rámci některých z těchto aplikací mohou být zpracovávány osobní údaje, které uživatel webu poskytne s vědomím, že je dává k dispozici skutečně pouze veřejnému subjektu, u něhož se předpokládá zajištění bezpečnosti těchto informací. V důsledku vlastního pracovního postupu aplikace ale mohou být navzdory tomuto očekávání osobní údaje zpřístupněny jedné nebo více dalším stranám (Rezgui, Bouguettaya, 2003).

2.1.1 Právní úprava osobních údajů

2.1.1.1 Definice osobních údajů

Dle Matoušové (2004) jsou za osobní údaje považovány informace, které popisují určitou osobu a vypovídají o jejím soukromí, přičemž se může jednat o jakýkoliv údaj

popisující a konkretizující danou osobu. Osobní údaje lze na základě teoretického výkladu Matoušové (2003) dělit následovně:

- reálné – osobní údaje spojené s konkrétní fyzickou osobou,
- úplně anonymní – osobní údaje, u nichž není možné určit jejich původní subjekt,
- částečně anonymní – osobní údaje, u nichž při splnění stanovených podmínek lze určit jejich subjekt (např. oblast údajů o zdravotním stavu),
- identifikační – osobní údaje sloužící k určení (popřípadě ověření) totožnosti osoby (např. jméno, příjmení, datum narození, místo narození, rodné číslo apod.),
- adresní – osobní údaje informující o místním určení ve vztahu k osobě (např. adresa trvalého pobytu, adresa přechodného pobytu, adresa zaměstnání apod.),
- popisné – osobní údaje podávající další informace o určité osobě (např. její zaměstnání, vzdělání, jmění apod.),
- citlivé – osobní údaje, u nichž je třeba dbát zvýšené opatrnosti při zacházení s nimi, jelikož mohou být snadno zneužitelné, čímž může docházet k ohrožení základních lidských práv subjektu údajů (např. údaje o zdravotním stavu, sexuální orientaci apod.).

Na úrovni právních předpisů byl pojem „*osobní údaj*“ definován již v zákoně č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, který byl však zrušen ke dni 24. dubna 2019 (dále jen „***Zrušený ZOOÚ***“), následovně:

> „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.*“

Obsahově podobná, jako ve Zrušeném ZOOÚ, je pak i současně platná definice v čl. 4 odst. 1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „**Nařízení GDPR**“):

> „*…„osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická*

osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“

Ochranu osobních údajů v souladu s Nařízením GDPR zdůrazňuje mimo jiné také Agentura Evropské unie pro kybernetickou bezpečnost (dále jen „***ENISA***“) na svých webových stránkách právě v souvislosti s rozrůstajícím se sektorem online prostoru a prostředí mobilních aplikací (ENISA, 2021).

2.1.1.2 Česká legislativa

Právo každého člověka na ochranu osobních údajů je nedílnou součástí práva na ochranu osobnosti a soukromí, které je zakotveno již na ústavní úrovni v Ústavním zákoně č. 2/1993 Sb., Listině základních práv a svobod, ve znění pozdějších předpisů (dále jen „***Listina***“). Relevantními články jsou zejména čl. 10 odst. Listiny, konkrétně jeho odst. 3:

„Článek 10

(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) ***Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě****.“*

Problematiky ochrany soukromí člověka a určitých údajů se však dotýkají i následující články Listiny:

„Článek 7

(1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“

„Článek 13

Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“

Obecně lze říci, že ochrana osobních údajů zahrnuje celý soubor práv a povinností souvisejících s nakládáním s informacemi a údaji o konkrétních osobách, přičemž tuto oblast je nepochybně třeba náležitě regulovat a zajistit dodržování stanovených pravidel, aby nebylo dotčeno žádné ze základních lidských práv a svobod. Paralelně k Listině je právo na soukromí zakotveno i v čl. 8 Úmluvy o ochraně lidských práv a základních svobod.

Jako tomu u základních lidských práv bývá zvykem, dostávají se poměrně často do konfliktu s jinými hodnotami a chráněnými zájmy. Důsledkem toho je, že je vždy třeba snažit se najít určitý kompromis a přiměřenou rovnováhu mezi konkrétním lidským právem a zájmy, které mohou takové právo ohrozit. V prostředí informační společnosti k takovým konfliktům dochází stále častěji (Matejka, 2013).

Na ústavní úroveň navazuje úprava ochrany soukromí v zákoně č. 89/2012 Sb., občanském zákoníku, ve znění pozdějších předpisů (dále jen „***Občanský zákoník***“), který právo na ochranu osobnosti zakotvuje již ve svém úvodu věnovaném základním zásadám, na nichž je občanské právo postaveno, konkrétně v § 3 odst. 2 písm. a):

> „*každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí*“.

Úvodní obecné ustanovení je následováno oddílem 6 (Osobnost člověka) v rámci druhé hlavy (Osoby) první části (Obecná část) – § 81 až § 117 Občanského zákoníku, oddílem 5 (Jméno a bydliště člověka) v rámci druhé hlavy (Osoby) první části (Obecná část) – § 77 až § 80 Občanského zákoníku a oddílem 3 (Způsob a rozsah náhrady) v rámci třetí hlavy (Závazky z deliktů) čtvrté části (Relativní majetková práva) – § 2951 až § 2971 Občanského zákoníku.

Existuje také řada zákonů upravujících konkrétní oblasti, ve kterých musí být ochrana osobních údajů řešena, například zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů a mnoho dalších předpisů, které na danou problematiku naráží. Pro účely této práce jsou však relevantní zejména následující právní předpisy speciální (mající přednost) vůči Občanskému zákoníku:

- zákon č. 110/2019 Sb., o zpracování osobních údajů,
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

2.1.1.3 Unijní legislativa

Dnem 25. května 2018 nabylo účinnosti již výše zmíněné Nařízení GDPR, které bylo poměrně průlomovým právním předpisem v oblasti ochrany osobních údajů, a to zejména proto, že díky své formě (obecně platné nařízení) se stalo ode dne své účinnosti závazným pro všechny osoby (fyzické i právnické) příslušné ke všem členským státům EU. Smyslem Nařízení GDPR je ochránit evropské občany před neoprávněným zacházením s jejich daty a osobními údaji. V současné době poslední změny doznalo znění Nařízení GDPR prostřednictvím třetí tiskové opravy ze dne 4. března 2021, která přinesla celkem 28 textových změn.

V principech a základních zásadách Nařízení GDPR navazuje na předchozí unijní úpravu a potvrzuje, že osobní údaje mají být chráněny i na přeshraničním principu. Práva subjektů osobních údajů jsou ale Nařízením GDPR významně rozvíjena a zpřísněny jsou požadavky na bezpečnost některých zvláštních kategorií údajů (viz následující kapitola). Zdůrazňována je také povinnost aktivnějšího přístupu ze strany správců a zpracovatelů osobních údajů, zejména potřeba posouzení vlivů jednotlivých zpracování na ochranu osobních údajů a zvolení a aplikace vhodných nástrojů ochrany údajů při každém novém zpracování. Dále si správci a zpracovatelé musí například za určitých podmínek vyžádat předběžnou konzultaci u dozorového úřadu. Ohledně rozsahu povinností správců a zpracovatelů osobních údajů je směrodatným faktorem zejména hrozící riziko, které je dovozováno z rozsahu zpracování, zpracovávaných osobních údajů a používaných technologií (ÚOOÚ, 2021). Novou povinností, kterou Nařízení GDPR přineslo, je pak například povinnost ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu a občanům, jichž se porušení zabezpečení týká.

Hlavní zásady ochrany osobních údajů sledované Nařízením GDPR přibližně odpovídají zásadám již výše uvedeným, dle Ministerstva vnitra (2021) jimi jsou:

- zákonnost, korektnost, transparentnost,
- omezení účelu,
- minimalizace údajů,
- přesnost,
- omezení uložení,
- integrita a důvěrnost.

2.1.2 Zvláštní kategorie osobních údajů

Zvláštní kategorie osobních údajů neboli citlivé údaje jsou z obecné úpravy nakládání s osobními údaji vyčleněny z důvodu potřeby jejich zvýšené ochrany, kterou je nezbytné zajistit s ohledem na charakter těchto údajů. Jedná se o informace, které mají potenciál samy o sobě způsobit subjektu údajů újmu na jeho základních lidských právech, jelikož subjekt může na základě nesprávného nakládání s těmito údaji být například diskriminován či může být poškozen jiným způsobem ve vztahu k jeho společenskému postavení, zaměstnání atd. Zvýšená ochrana této skupiny údajů je zajištěna zejména skrze omezení možných důvodů, na základě kterých může být s citlivými údaji nakládáno, pouze na stanovené zvláštní právní důvody. Dalšími opatřeními jsou pak například posouzení vlivu zpracování údajů, ustavení pověřence, důraz na vyšší úroveň zabezpečení apod.

Údaje spadající do zvláštní kategorie jsou určeny taxativním (úplným) výčtem v čl. 9 odst. 1 Nařízení GDPR, jsou jimi osobní údaje, které „*vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.*“ Uvedený výčet je obsahově v podstatě stejný, jaký byl zakotven Zrušeným ZOOÚ, vyjma informace o předchozím odsouzení za trestný čin, která podle Nařízení GDPR za citlivou považována není.

Jak bylo zmíněno výše, zvláštní kategorie osobních údajů mohou být zpracovávány pouze na základě zvláštních právních důvodů stanovených v čl. 9 odst. 2 Nařízení GDPR, jež jsou formulovány v podobě následujících podmínek, z nich alespoň nějaká musí být naplněna:

- subjekt údajů udělil výslovný souhlas se zpracováním,
- zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a to za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy takového seskupení nebo na osoby, které s tímto subjektem

udržují pravidelné styky v souvislosti s naplňováním cílů subjektu, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány třetím osobám vně tohoto subjektu,

- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů,
- zpracování je nezbytné z důvodu významného veřejného zájmu,
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.,
- zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků,
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.

2.1.2.1 Cookies

Pod pojmem „*cookies*“ se skrývají textové soubory menší velikosti, které jsou ukládány do různých zařízení uživatelů na základě navštívení webových stránek, načež tyto malé soubory odesílají zpět na server informace o chování tohoto zařízení v průběhu návštěvy daného webu. Soubory cookies jsou ukládány na disk do prostoru vyhrazeného pro internetový prohlížeč, v rámci něhož je za účelem uložení cookies vyčleněn speciální prostor.

Soubory cookies jsou předávány oboustranně, typicky server odešle soubor cookie klientovi, který jej uloží lokálně. Klient pak soubor odešle zpět na server, když si jej server vyžádá. Tento proces umožňuje sledování online aktivity uživatelů serverem. V mnoha situacích sledování tohoto typu představuje porušení soukromí uživatelů (Rezgui, Bouguettaya, 2003), jelikož jejich aktivita je monitorována popsaným způsobem, ačkoliv si to často vůbec neuvědomují.

Identické označení těchto souborů s označením sušenek (angl. cookies) není náhodné. Princip fungování cookies a právě i jejich název navrhl programátor Lou Montulli v roce 1994, přičemž vycházel z americké a britské zvyklosti nabídnout sušenku příchozím

návštěvám. Sušenka i soubory cookies mají totiž stejný účel, a to rychlé navození příjemné atmosféry na úvod setkání (Topranker.cz, 2021).

Jansa a kol. (2016) identifikuje následující druhy souborů cookies:

- sledovací a konverzní - umožňují analyzovat výkon různých prodejních kanálů,
- marketingové - napomáhají personalizovat obsah reklamy a díky tomu efektivněji zacílit na potřeby konkrétního zákazníka,
- analytické a esenciální cookies – vytváří efektivnější uživatelské prostředí internetové stránky a zlepšují funkčnost webu.

Marketingové cookies jsou pak nezbytným nástrojem pro marketingovou metodu nazvanou „*remarketing*“, která umožňuje marketující osobě zobrazit uživatelům internetu reklamy na stránky, které dříve navštívili. Uživateli se tedy následně zobrazují i při surfování již na jiných webových stránkách reklamy na produkty či služby, které hledali či kupovali dříve, tudíž je u nich větší předpoklad, že o tyto produkty budou mít zájem opakovaně. Výsledkem techniky remarketingu tedy je podprahové podsouvání uživatelům možnosti nakoupit produkt, o který již dříve určitý zájem projevili, a to i pokud si jej jen prohlíželi (nákup neuskutečnili). Zde je možné vznést odlehčující úvahu, a to že tento jev může být kromě ohrožení ochrany osobních údajů problematický například při vybírání dárků blízkým, když právě tyto reklamy na stránky dříve navštívené mohou utajovaný záměr uživatele prozradit.

Co se týče právní úpravy cookies, je pro účely této práce relevantní hlavně oblast předpisů věnujících se souborům cookies jako formě osobních údajů, které by měly být adekvátním způsobem chráněny. Za osobní údaje jsou některé soubory cookies považovány i Nařízením GDPR, které v čl. 30 preambule zmiňuje „*identifikátory cookies*“ které mohou být přiřazeny konkrétní fyzické osobě, čímž může být tato osoba identifikována. Právě identifikace konkrétní osoby je jedním ze znaků osobních údajů, proto za osobní údaje lze považovat pouze ty cookies, které obsahují informace, jež jsou schopny identifikovat konkrétní fyzickou osobu, či jsou informace z nich spojovány s informacemi o již identifikované fyzické osobě, například pokud je sledováno chování uživatele na internetu a vysledované informace následně propojeny s jeho uživatelským účtem (Slížek, 2018). Zásadním problémem přitom je, že většina uživatelů netuší, že jim je přiřazen takový identifikátor, natož že je tímto způsobem předáván na server (Matejka, 2013).

Soubory cookies jsou právně upraveny primárně Směrnicí Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „***směrnice e-Privacy***“). Na základě směrnice e-Privacy byla poskytovatelům elektronickým služeb uložena povinnost jasně a úplně informovat uživatele (např. zákazníky nakupující online), a to mimo jiné právě o účelech použití cookies a o rozsahu informací ukládaných do jeho zařízení.

Poměrně zásadní novely doznala směrnice e-Privacy prostřednictvím Směrnice Evropského parlamentu a Rady 2009/136/EC ze dne 25. listopadu 2009 (dále jen „***novela směrnice e-Privacy***“), kterou byl původní opt-out režim cookies, tedy že uživatel musí mít možnost odmítnout ukládání cookies, změněn na režim opt-in, ve kterém poskytovatel elektronických služeb musí získat uživatelův výslovný souhlas s ukládáním cookies ještě před samotným uložením cookies do zařízení. Výjimku z této povinnosti představují technické cookies, které i nadále fungují v režimu opt-out (Tichý, 2020). V praxi se tato nová povinnost projevila většině osob známým „*odklikáváním*“ lišty vyjadřující souhlas s uložením cookies na většině webových stránek. Novela směrnice výslovně zakotvuje v čl. 3 následující:

> „*Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí 95/46/ES, mimo jiné o účelu zpracování.*“

Jednoznačné odlišení režimů opt-out a opt-in ve spojitosti s cookies je výkladově poměrně složitou otázkou, což dosvědčuje i předběžná otázka, která byla položena Soudnímu dvoru EU německým Spolkovým soudním dvorem. Soudní dvůr EU v této věci rozhodl dne 1. října 2019 tak, že za splnění opt-in režimu lze považovat aktivní jednání uživatele v podobě zaškrtnutí souhlasného políčka. Naopak nesplněním povinnosti ze strany poskytovatele je předem připravené již předvyplněné zaškrtnuté políčko, které by uživatel musel naopak odškrtnout.

Ačkoliv Soudní dvůr EU postavil výklad na jisto, Česká republika novelu směrnice e-Privacy dosud náležitě neimplementovala do českého právního řádu. Vzhledem k tomu, že aby evropské směrnice zavazovaly české osoby, musí být náležitě transponovány do národního komplexu právních předpisů, v současné době je pro české poskytovatele elektronických služeb závazný pouze opt-out režim.

Za splnění povinnosti získání souhlasu uživatele lze dále považovat i obecné nastavení internetového prohlížeče uživatelem určitým způsobem, a to v souladu s čl. 66 preambule novely směrnice e-Privacy, který sděluje následující: „*Je-li to technicky možné a efektivní, může být v souladu s příslušnými ustanoveními směrnice 95/46/ES souhlas uživatele se zpracováním údajů vyjádřen vhodným nastavením prohlížeče nebo jiné aplikace.*“ Tento názor potvrdil i Úřad pro ochranu osobních údajů ve svém Doporučení ke zpracování cookies a obdobných prostředků sledování od 25. května 2018.

Nedostatek v podobě nesprávně transponované novely směrnice e-Privacy by mohl být napraven připravovaným Nařízením Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (dále jen „***Nařízení PECR***“). Nařízení mají totiž na rozdíl od směrnic tu výhodu, že jsou přímo aplikovatelná, tudíž by nebylo již třeba další transpozice na národní úrovni. Nařízení PECR by tedy nahradilo směrnici e-Privacy i českou právní úpravu této oblasti, čímž by mohl být nesoulad vyřešen. Nařízení PECR bude detailněji rozebráno níže.

2.2 Soukromí na internetu

Obecně přijímanou definici pojmu soukromí nenalezneme v českém právním řádu ani v judikatuře českých či zahraničních soudů a přesného vymezení se bohužel nedočkáme ani v jiných mezinárodních dokumentech či výkladových stanoviscích (Matejka, 2013). Úvahou ospravedlňující tuto skutečnost může být, že přesná definice pojmu soukromí pravděpodobně ani není žádoucí, aby jeho ochrana mohla být posuzována vždy individuálně, případně extenzivně (rozšiřujícím výkladem) v zájmu osob, jejichž soukromí je ohroženo či dotčeno.

Dle pravidel stanovených Evropskou unií osobním údajům na internetu náleží ochrana kdykoli jsou osobní údaje shromažďovány. Jedná se tedy o všechny případy nakupování prostřednictvím internetu, sdílení osobních údajů v souvislosti se zaměstnáním osoby a samozřejmě veškerá komunikace v bankovním prostředí a prostředí internetových platebních služeb (Your Europe, 2021), přičemž formát zpracovávaných údajů je naprosto nerelevantní.

Důležité je zdůraznit, že unijní pravidla jsou závazná kromě veškerých subjektů se sídlem na území EU (fyzické i právnické osoby, soukromé i veřejné osoby) také pro všechny subjekty usazené mimo Unii, pokud nabízejí v EU své zboží či služby, a to ve chvíli, kdy požádají o poskytnutí osobních údajů fyzických osob, jež jsou občany EU, nebo je

opakovaně používají. Evropskou legislativu tedy musejí dodržovat i velcí světoví hráči, jako například Facebook, Amazon apod.

Nařízení GDPR se na internetové prostředí bude aplikovat, jelikož fyzickým osobám mohou být přiřazeny konkrétní síťové identifikátory. Tyto síťové identifikátory využívají při své činnosti zařízení, aplikace, nástroje a protokoly (např. adresy internetového protokolu), cookies, nebo identifikátory fungující na jiné bázi, jako jsou štítky pro identifikaci na základě rádiové frekvence. Tímto způsobem bývají zanechávány stopy v online prostředí, které mohou být zejména v kombinaci s jedinečnými identifikátory (např. jméno, adresa, číslo mobilního telefonu, heslo, elektronický podpis apod.) a dalšími informacemi, které servery získávají o konkrétních fyzických osobách, použity k profilování těchto fyzických osob a k jejich identifikaci (Lentner, Parycek, 2016).

2.2.1 Jednotný digitální trh

Vytvoření jednotného trhu v Evropě je myšlenkou, která od počátku provází snahy o evropskou integraci. Jednotný nebo také vnitřní či společný trh je základní ideou, z níž vychází další a konkrétnější cíle současné Evropské unie. Vnitřní trh EU je tvořen územím všech členských států, přičemž vůdčím záměrem je vytvoření prostoru, ve kterém budou uplatňovány a dodržovány čtyři základní svobody, a to volný pohyb zboží, osob, služeb a kapitálu (Muller, Ministerstvo průmyslu a obchodu, 2016).

Jedním ze sektorů jednotného trhu EU je stále se rozšiřující digitální trh. Dle dokumentu „*Digitální agenda pro Evropu: klíčové iniciativy*“ ze dne 19. května 2010 bylo vytvoření jednotného digitálního trhu jednou ze sedmi prioritních oblastí činnosti. Dokument deklaroval například existující potřebu odstranění regulačních překážek, usnadnění elektronických plateb a elektronické fakturace, usnadnění řešení sporů a zvýšení důvěry spotřebitelů. Zajímavou zmínkou v uvedeném strategickém dokumentu je požadavek, aby Evropská komise vydala digitální zákoník, který bude shrnovat práva občanů v online světě jasným a přístupným způsobem. Skutečnost, že tento požadavek byl vysloven již v roce 2010 a do současnosti nebyl naplněn, je na pováženou. Nutno však přiznat, že určitých úspěchů na poli regulace digitálního prostředí dosaženo bylo, například v období let 2016 – 2017 došlo ke zrušení poplatků za roaming, zdokonalení ochrany údajů na internetu, přeshraniční přenositelnosti online obsahu nebo uzavření dohody o uvolnění elektronického obchodování na základě ukončení neopodstatněného zeměpisného blokování (CZ.NIC, 2017).

2.2.1.1 Milníky jednotného digitálního trhu

Níže popsaná časová osa událostí podstatných v souvislosti s utvářením jednotného digitálního trhu EU byla čerpána z oficiálních zdrojů Rady EU a Evropské rady, přičemž časová linka je dostupná na oficiálních stránkách Evropské rady a Rady EU (Consilium, 2021). S ohledem na relevantnost historických údajů pro současný stav digitálního trhu a v zájmu zjednodušení a přehlednosti bude zpětná časová linka zkrácena na období od roku 2015.

2015

Na úrovni ministrů kultury členských států EU byly projednány zejména audiovizuální aspekty strategie pro jednotný digitální trh. Výsledkem jednání bylo vyjádření podpory v oblastech přeshraniční přenositelnosti obsahu a boje proti nelegálnímu obsahu a zároveň byla nalezena shoda na potřebě řešit otázku autorských práv. Dále byla na ministerské úrovni deklarována potřeba aktualizace pravidel elektronického obchodování a v neposlední řadě byla otevřena otázka ochrany spotřebitele, zejména byla řešena potřeba posílení jeho důvěry a informovanosti (Consilium, 2021).

Na svém jednání ve dnech 28. – 29. května 2015 vymezila Rada pro konkurenceschopnost následující prioritní opatření (Evropská rada, Rada Evropské unie, 2020):

- vytvoření vhodných podmínek pro malé a střední podniky (zejména ty začínající),
- podpora digitalizace evropského průmyslu,
- používání a rozšiřování elektronické veřejné správy (e-government),
- zvyšování investic do digitální infrastruktury a sítí,
- posouzení dopadu fiskálních pravidel na digitální nástroje,
- posouzení možnosti uplatňovat zásadu „*automatické digitalizace*“ pro všechny nové právní předpisy EU.

Rada pro dopravu, telekomunikace a energetiku na svém zasedání ve dnech 11. - 12. června 2015 zdůraznila význam digitalizované ekonomiky pro podporu zaměstnanosti a růstu konkurenceschopnosti EU. Mimo jiné byla diskutována nutnost kybernetického zabezpečení a posilování důvěry v elektronické služby. V této oblasti je významnou institucí právě již výše zmiňovaná agentura ENISA, která byla zřízena v roce 2004 a jejíž činnost

byla následně posílena aktem EU o kybernetické bezpečnosti. ENISA se podílí na kybernetické politice EU, prostřednictvím systémů certifikace kybernetické bezpečnosti zvyšuje důvěryhodnost produktů, služeb a procesů informačních a komunikačních technologií, spolupracuje s členskými státy a subjekty EU a pomáhá Evropě připravit se na budoucí kybernetické výzvy (ENISA, 2021).

Vedoucí představitelé EU mezi závěry Evropské rady z jednání ve dnech 25. - 26. června 2015 důrazně vyzvali ke snaze zabránit tříštění digitálního trhu a k podpoře budování digitální infrastruktury (Consilium, 2021).

2016

V květnu roku 2016 vstoupilo v platnost přelomové Nařízení GDPR, jehož účinnost byla stanovena ode dne 25. května 2018. Nařízení GDPR znamenalo skutečně reformní změnu, v rámci které byl reflektován vývoj v mnoha oblastech, zejména ale rychlý technologický pokrok v oblasti toku a sdílení údajů mimo jiné právě na internetu (Consilium, 2021).

Evropská rada na svém zasedání ve dnech 28. - 29. června 2016 vyzvala ministry, aby od června následujícího roku (2017) podávali každoročně zprávu o pokroku při prohlubování jednotného trhu.

2017

Rada EU přijala nová pravidla upravující přenositelnost digitálních služeb. Platnost pravidel byla určena od 1. dubna 2018 a jejich hlavním cílem bylo umožnit spotřebitelům přístup k online službám, jež si zaplatili v domovském státě i v jiných členských státech, a to bez dodatečných poplatků. Jednalo se o předplacené filmy, hudbu, sportovní přenosy apod. (Consilium, 2021).

Za skutečný úspěch však bylo považováno zejména ukončení zpoplatněných roamingových služeb, a to napříč všemi členskými státy EU, ke kterému došlo od 15. června 2017. Ve společném prohlášení Rady EU, Evropského parlamentu a Evropské komise vydaném maltským předsednictvím byl tento krok společně s přenositelností digitálních služeb dle předchozího odstavce označen za důležitý pokrok při vytváření jednotného digitálního trhu.

Tallinský summit vedoucích představitelů EU k digitální problematice konaný dne 29. září 2017 byl z pohledu jednotného digitálního trhu zásadním, když se jeho účastníci

vyslovili pro ambiciózní digitální vizi pro Evropu, její společnost a ekonomiku, neboli pro úplné provedení strategie pro jednotný digitální trh. V návaznosti na závěry Tallinského summitu se Evropská rada dohodla na souboru priorit, mezi kterými mimo jiné bylo završení strategie pro jednotný digitální trh do konce roku 2018, a dále například také na potřebě společného postupu v oblasti kybernetické bezpečnosti (Consilium, 2021).

Optikou tématu předkládané diplomové práce byl jedním z nejdůležitějších milníků datum 25. října 2017, kdy byl poprvé podepsán legislativní akt EU elektronickým podpisem. Došlo k němu na zasedání Evropského parlamentu ve Štrasburku, na kterém předseda Antonio Tajani a zástupce estonského předsednictví Rady Matti Maasikas elektronicky podepsali nařízení o bezpečnosti dodávek zemního plynu po revizi. Podpis byl uskutečněn jako slavnostní akt, jenž měl dosvědčit, že EU pracuje na digitální transformaci. Matti Maasikas k aktu uvedl následující:

> *„Jsem přesvědčen, že brzy budeme tímto způsobem podepisovat všechny naše právní akty prostě proto, že to dává smysl. Elektronický podpis šetří papír, čas i peníze.“*

Dne 29. listopadu 2017 byla uzavřena Dohoda o odstranění překážek bránících elektronickému obchodování, neboli o zákazu tzv. neopodstatněného zeměpisného blokování, které je projevem diskriminace na internetu, když zákazníci nemohou nakoupit na internetu zboží prostřednictvím webové stránky na území jiného členského státu (Consilium, 2021).

Evropská rada přijala dne 30. listopadu 2017 postoj ke zřízení jednotné digitální brány, prostřednictvím které má docházet k poskytování informací a dalších služeb občanům a podnikům. Záměrem tohoto kroku je usnadnit přeshraniční činnosti díky lepší dostupnosti informací napříč členskými státy.

Dalším zásadním milníkem byl postoj přijatý Radou EU dne 20. prosince 2017, na jehož základě byl udělen mandát k zahájení jednání s Evropským parlamentem o návrhu, který má odstranit překážky bránící volnému toku údajů. Cílem návrhu je odstranění nedůvodných bariér pro ukládání a zpracování údajů. Navrhovaná právní úprava má zajistit snazší a přehlednější uchovávání a zpracování údajů, jakým je například cloud computing (Consilium, 2021).

2018

Nařízení zakazující neoprávněné zeměpisné blokování zmíněné výše přijala Rada EU dne 27. února 2018.

Ve věci jednotné digitální brány zmíněné výše přijali velvyslanci při EU dohodu dne 20. června 2018 a Rada EU přijala v návaznosti na tento krok nařízení o zřízení digitální brány, konkrétně dne 27. září 2018. Margarete Schramböcková, rakouská spolková ministryně pro digitální a hospodářské záležitosti, se k přijetí nařízení vyjádřila následovně:

> *„Jednotná digitální brána je dalším účinným nástrojem, jejž budou mít k dispozici občané i podniky využívající svobody volného pohybu a svobody usazení v jiném členském státě. On-line přístup k informacím a postupům bude za rovných podmínek snadno dostupný každému“* (Consilium, 2021).

Zásadním milníkem souvisejícím s ochranou osobních údajů bylo přijetí nových pravidel pro přenos údajů, jejichž cílem bylo odstranit překážky bránící volnému pohybu údajů (vyjma těch osobních). Deklarovanou ideou přijetí tohoto dokumentu byl rozvoj moderních technologií a podpora ekonomických aktivit spjatých s přenosem dat napříč EU.

Dne 29. listopadu 2018 Rada EU zveřejnila svůj nový postoj vůči podnikání v online prostředí, který vyjádřila přijetím pravidel, jež mají zajistit podnikům využívajícím online platformy rovnější podmínky ve vztahu s provozovateli těchto platforem a větší transparentnost a předvídatelnost vzájemných vztahů.

Rada EU přijala dne 5. prosince 2018 postoj, dle kterého se má právo obchodních společností více přizpůsobit modernizaci a pokroku v digitální sféře. Jedním z aspektů nových pravidel je snaha o snazší komunikaci mezi obchodními společnostmi a orgány veřejné moci, a to zejména pomocí digitálních nástrojů (Consilium, 2021).

2019

Dne 4. února 2019 uzavřelo předsednictví Rady EU předběžnou dohodu s Evropským parlamentem ohledně návrhu směrnice, která bude usnadňovat využívání online řešení v komunikaci obchodních společností s orgány veřejné moci po celou dobu jejich existence.

V rámci snahy o přizpůsobení pravidel v oblasti autorských práv digitálnímu pokroku uzavřela Rada EU předběžnou dohodu s Evropským parlamentem o právech tvůrců obsahu, vyjasnění právního rámce pro platformy určené ke sdílení obsahu a usnadnění elektronického vzdělávání. V návaznosti byla dne 17. dubna 2019 přijata Směrnice evropského parlamentu a Rady (EU) 2019/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES, která má za cíl zajistit náležitou ochranu pro autory a umělce a současně otevřít nové možnosti

pro přístup k online obsahu chráněnému autorským právem v celé Evropské unii a pro jeho sdílení (Consilium, 2021).

Další předběžnou dohodou evropských velvyslanců s Evropským parlamentem ze dne 13. února 2019 byla potvrzena snaha zaručit transparentní podmínky pro podnikové uživatele online platforem.

S cílem podporovat rozsáhlé zavádění a využívání klíčových digitálních technologií (například aplikace umělé inteligence a nástroje kybernetické bezpečnosti) byl zřízen nový program financování určený k podpoře digitalizace hospodářství a společnosti v členských státech v období 2021 - 2027 s názvem Digitální Evropa (Consilium, 2021).

Od 14. června 2019 byla zavedena nová pravidla zajišťující transparentnější, spravedlivější a předvídatelnější online prostředí, jakož i účinný systém pro uplatňování nároků na náhradu škody nebo pro zjednání nápravy, a to v podobě nařízení zaměřeného právě na vztahy mezi online platformami a podniky. Platformami, kterých se má nařízení dotknout, jsou například online tržiště, online obchody se softwarovými aplikacemi nebo internetová sociální média. Nařízení se bude dále aplikovat také na internetové vyhledávače bez ohledu na zemi jejich sídla, pokud slouží podnikovým uživatelům usazeným v EU a nabízejí zboží, nebo služby spotřebitelům, kteří se rovněž nacházejí na území EU.

2020

Dne 9. června 2020 oficiální prameny informovaly o tom, že Rada EU přijala závěry zabývající se prováděním digitální strategie EU, která se zaměřuje například na konektivitu, digitální hodnotové řetězce, elektronické zdravotnictví, ekonomiku založenou na datech, umělou inteligenci nebo digitální platformy. Přijaté závěry braly v úvahu již i dopad digitální transformace na boj proti pandemii a zásadní úlohu digitální transformace při oživení po krizi způsobené onemocněním covid-19 (Consilium, 2021).

2.2.1.2 Směřování EU v oblasti ochrany osobních údajů na digitálním trhu EU

Zásadním krokem v oblasti ochrany osobních údajů, jenž je prozatím ve fázi příprav, by mělo být přijetí již výše zmiňovaného Nařízení PECR, jehož cílem je obecně zvýšit důvěru a bezpečnost na jednotném digitálním trhu EU. Jedním z aspektů, kterými by se Nařízení PECR mělo zabývat, je unifikace pravidel pro poskytování osobních údajů uživatelů poskytovatelům elektronických služeb, tedy mimo jiné i sjednocení a vyjasnění pravidel používání marketingových cookies. Dle původního plánu mělo Nařízení PECR

nabýt účinnosti společně s Nařízením GDPR, v současné době je však účinnost Nařízení PECR odložena na neurčito, jelikož na znění návrhu nepanuje napříč EU shoda (Tichý, 2020). Je tedy možné, že návrh Nařízení PECR dozná ještě významných změn, či bude dokonce vytvořen návrh úplně nový.

Dle návrhu Nařízení PECR jsou cookies osobními údaji (s výjimkou technických cookies) a pro jejich užití v oblasti marketingu je třeba získat jednoznačný informovaný souhlas uživatele, což je podrobněji rozepsáno v čl. 24 preambule Nařízení PECR:

> *„Aby mohly internetové prohlížeče získat souhlas koncových uživatelů, jak jej definuje nařízení (EU) 2016/679, například s ukládáním sledovacích cookies třetích stran, měly by mimo jiné vyžadovat od koncového uživatele koncového zařízení* ***jasnou potvrzující akci, která by stvrzovala jeho svobodně poskytnutý, konkrétně informovaný a jednoznačný souhlas s uchovávání těchto cookies v jeho koncovém zařízení a s přístupem k nim****. Taková akce může být považována za potvrzující, pokud je například vyžadováno, aby koncoví uživatelé pro potvrzení svého souhlasu aktivně zvolili možnost „přijímat cookies třetích stran“, a jsou jim poskytnuty informace nezbytné k učinění volby.* ***Za tímto účelem je nezbytné vyžadovat, aby poskytovatelé softwaru umožňujícího přístup k internetu zajistili, že koncoví uživatelé jsou při instalaci informováni, že si mohou vybrat z různých možností nastavení ochrany soukromí, a aby je požádali o učinění volby****. Poskytnuté informace by neměly koncové uživatele odrazovat od výběru nastavení vyšší ochrany soukromí a měly by zahrnovat* ***relevantní informace o rizicích souvisejících s povolením toho, aby byly v počítači uchovávány cookies*** *třetích stran, včetně sestavování dlouhodobých záznamů o historii prohlížení internetu danou osobou a využívání těchto záznamů k zasílání cílené reklamy. Internetové prohlížeče se vyzývají k tomu, aby koncovým uživatelů poskytly snadné způsoby, jak kdykoli během používání změnit nastavení ochrany soukromí, a aby uživateli umožnily dělat výjimky pro určité internetové stránky, přidávat takové stránky na seznam povolených stránek nebo upřesnit, pro které internetové stránky jsou cookies (třetích) stran povoleny vždy, nebo nikdy.“*

Nařízení PECR tedy ve znění současně dostupného návrhu ponechává možnost přijmout cookies nastavením internetového prohlížeče, je ovšem nutné dát uživatelům k dispozici výběr z více úrovní ochrany. Z toho vyplývá závěr, že nenabízí-li internetové prohlížeče takové možnosti, pravděpodobně budou muset být nejpozději s účinností Nařízení PECR učiněny softwarové změny v internetových prohlížečích. Důležitou

možností, kterou Nařízení PECR pro poskytovatele elektronických služeb zachovává, je, že i pokud má uživatel obecně nastaven zákaz ukládání cookies, na základě individuálního souhlasu bude ukládání v konkrétním případě umožněno.

2.2.2 Odpovědnost provozovatele webu

Odpovědnost provozovatele webových stránek je upravena zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů (zákon o některých službách informační společnosti, dále jen „***ZSIS***“). Ačkoliv ZSIS nabyl účinnosti již 7. září 2004, následující novely do něj zapracovaly i potřebné požadavky unijního práva. Současné znění tak dle § 1 ZSIS upravuje odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení, tedy poskytovatele mnohých služeb poskytovaných online. ZSIS doléhá především na provozovatele služeb spočívajících v ukládání obsahu informací – „*hosting provider*“, zároveň ale stanovuje pravidla pro poskytovatele připojení nebo přístupu, kteří pouze zprostředkovávají přenos informací – „*conduit*“, nebo pro poskytovatele služby typu dočasného mezistupně ukládaní informací „*caching*“ (Čech, 2020).

A. <u>poskytovatelé hostingu</u>

Odpovědnost poskytovatele služby za ukládání obsahu informací vkládaných uživatelem (hostingu) je upravena v § 5 ZSIS. V případě vlastního obsahu zveřejňovaného na webu provozovatelem není pochyb o jeho odpovědnosti za takový obsah. Problematickou otázkou však je, kdo je odpovědný za cizí obsah vložený uživatelem, který je základním znakem hostingu. Právě možnost zveřejňování uživatelského obsahu je totiž odlišovacím znakem hostingových webových stránek. Mezi poskytovatele hostingových služeb patří například provozovatelé sociálních sítí, online nákupních zón (eBay, Booking), e-shopů umožňujících vkládat vlastní recenze, osobních blogů, diskuzních fór a dalších. U cizího obsahu provozovatelé nesou omezenou odpovědnost za obsah na stránkách, přičemž primárně za takový obsah provozovatel neodpovídá, pokud jeho web je tzv. „*bezpečným přístavem*“ nebo anglicky „*safe harbor*“, tedy že splňuje stanovené podmínky (viz níže 1. – 4.), a to kumulativně, neboli všechny najednou.

1. absence konkrétní vědomosti

Absence konkrétní vědomosti znamená, že provozovatel si nebyl vědom charakteru cizího obsahu, přičemž vědom si nesmí být jak protiprávnosti obsahu, tak protiprávnosti jednání daných uživatelů webu. Vědomost je založena již jen případným „*nahlášením*“ protiprávnosti třetí osobou. Nahlášení však musí jasně identifikovat nahlašovanou informaci a zároveň musí být z nahlášení jasné, že informace je protiprávní. Nahlásit může daný obsah kdokoliv, navíc nahlašovatel nemusí uvést svou identitu, tudíž jsou relevantní i anonymní nahlášení. Není stanovena ani konkrétní forma či podoba potřebného úkonu, přípustné tak jsou veškeré formy nahlášení. Obecně se však doporučuje za účelem co nejrychlejšího procesu nahlašování a jeho zpracování implementovat „*notice*“ tlačítko umožňující uživatelům protiprávní obsah nahlásit snadným a rychlým způsobem.

Obdrží-li provozovatel webu nahlášení protiprávního obsahu, vzniká mu povinnost zakročit na ochranu ohrožených či zasažených práv třetí osoby, tento krok je také nazýván „*takedown*“. Takedown může být vykonán buď odstraněním nahlášené informace, nebo jejím znepřístupněním, přičemž volba mezi těmito možnostmi je na provozovateli webu (Čech, 2020). Takto zakročit je provozovatel povinen neprodleně po zjištění škodlivosti obsahu.

2. absence konstruktivní vědomosti

Absence konstruktivní vědomosti znamená, že provozovatel neměl a nemohl vědět o protiprávním charakteru cizího obsahu. Tato podmínka míří hlavně na jiné cesty, jakými se provozovatel může o protiprávnosti dozvědět, než je výše uvedené nahlášení uživatelem.

3. absence kontroly

Absence kontroly znamená, že provozovatel nemá kontrolu nad jednáním uživatele, tedy že nemá na činnost uživatele žádný přímo nebo nepřímo rozhodující vliv. Vliv může existovat na základě pracovněprávního vztahu, rodinného vztahu, ale i na základě jakýchkoli dalších vazeb mezi původcem protiprávního obsahu a provozovatelem webu.

4. pasivní přístup

Aby provozovatel webu nebyl za cizí obsah odpovědný, nesmí obsah kontrolovat, měl by tedy k poskytování služby přistupovat pasivně. Provozovatel by tudíž neměl obsah předem filtrovat, podněcovat uživatele k vložení daného obsahu či být uživatelům při vkládání obsahu jinak nápomocný (Čech, 2020).

Vodítkem při určení, zda je zajištěn pasivní přístup provozovatele webu, může být Rozhodnutí Soudního dvora Evropské unie ve věci C-610/15, ze dne 14. června 2017, přičemž daná věc je známá spíše pod názvem „*The Pirate Bay*“. Soudní dvůr rozhodl, že provozovatel webu nedodržel výše uvedené podmínky a nemohl tak být zbaven odpovědnosti za cizí obsah, a to zejména z těchto důvodů:

- provozovatel indexoval uživateli nahrané soubory, aby je bylo možné snadno nacházet,
- provozovatel poskytoval nejen vyhledávač, ale i rejstřík souborů,
- provozovatel sám odstraňoval zastaralé uživatelské soubory a aktivně obsah filtroval,
- provozovatel své služby a uživatelský obsah sám propagoval, když na fórech výslovně uváděl, že jeho cílem je zpřístupnit chráněná díla uživatelů a
- provozovatel aktivně věděl o protiprávnosti uživatelského obsahu, respektive nemohl nevědět, že platforma slouží k umožnění přístupu k dílům zveřejněným bez svolení nositelů práv (Čech, 2020).

B. poskytovatelé conduit

Odpovědnost poskytovatele služby za obsah přenášených informací (conduit) je upravena v § 3 ZSIS, a na rozdíl od předchozího případu je vymezena pozitivně, tedy že odpovědnost provozovatele vzniká jen ve stanovených případech, což je pro provozovatele mnohem mírnější nastavení vzniku jeho odpovědnosti. Jak bylo již zmíněno výše, conduit znamená zprostředkování přenosu informací prostřednictvím sítí elektronických informací nebo zprostředkování přístupu k těmto sítím. Jedná se tedy o poskytování připojení či přístupu. Odpovědnost provozovateli webu za obsah přenášených informací v tomto případe vzniká, pokud:

- provozovatel přenos sám iniciuje, včetně automatického krátkodobého a dočasného ukládání přenášených informací,
- provozovatel zvolí uživatele přenášené informace, nebo
- provozovatel zvolí nebo změní obsah přenášené informace.

C. poskytovatelé cachingu

Caching znamená poskytování služby typu dočasného meziukládaní informací a stejně jako u conduit vzniká provozovateli webu odpovědnost jen v případech pozitivně stanovených v § 4 ZSIS, tedy když:

- provozovatel změní obsah informace,
- provozovatel nevyhoví podmínkám přístupu k informaci,
- provozovatel nedodržuje pravidla o aktualizaci informace, která jsou obecně uznávána a používána v příslušném odvětví,
- provozovatel překročí povolené používání technologie obecně uznávané a používané v příslušném odvětví s cílem získat údaje o užívání informace, nebo
- provozovatel ihned nepřijme opatření vedoucí k odstranění jím uložené informace nebo ke znemožnění přístupu k ní, jakmile zjistí, že informace byla na výchozím místě přenosu ze sítě odstraněna nebo k ní byl znemožněn přístup nebo soud nařídil stažení či znemožnění přístupu k této informaci.

2.2.3 Zabezpečení dat

Mezinárodní důležitost ochrany dat, jež jsou ukládána, zpracovávána a distribuována v informačních systémech, byla deklarována již v roce 2009 na Koncilu národní americké rady pro výzkum, přičemž data je třeba chránit před neidentifikovanými závažnými hrozbami (Knopová, 2011). Pod pojmem zabezpečení dat je třeba si představit soubor pravidel zajišťujících důvěrnost, integritu a dostupnost dat (U. S. Department of Defense, 2022). Trojúhelník těchto cílů uvádí mimo jiné na svých stránkách také ENISA:

Obrázek 1 - Zabezpečení dat

Zdroj: ENISA, 2021.

Data lze zabezpečit na třech úrovních (Castano, Fugini, 1995; Knopová, 2011):

- fyzická (úroveň hardwaru, zálohování dat),
- logická (softwarové řešení autentifikace či autorizace) a
- organizační (doplňková snaha o ochranu systému).

Logická úroveň kontroly je založena na zpřístupnění určitých dat pouze oprávněné osobě. Aby mohlo být toto omezení přístupu uvedeno do praxe, je třeba zapracovat dostatečné mechanismy ověřující identitu osoby (Knopová, 2011). Následující podkapitoly budou věnovány zejména výkladu s touto problematikou souvisejících pojmů, jako je identifikace, autentizace a autorizace.

2.2.3.1 Identifikace, autentizace a autorizace

Identifikace, autentizace a autorizace jsou součástí tzv. identity managementu neboli řízení přístupových oprávnění k datům, souborům, adresářům, operacím apod. (ManagementMania.com, 2022).

A. Identifikace

Podstatou identifikace je jednoznačné zjištění totožnosti osoby. K identifikaci osoby tedy například při přihlašování dojde zadáním jedinečného uživatelského jména. Mimo prostředí informačních technologií si lze představit, že osoba se identifikuje tím, že se představí.

Identifikace je možná celou řadou způsobů, od již zmíněného představení, dále pak například zadáním uživatelského jména, pomocí biometrických údajů, ale třeba i jen rozpoznáním osoby jinou osobou pomocí zrakových vjemů podle jedinečného vzhledu. Zajímavým zjištěním je, že samotná identifikace pomocí biometrických údajů nemusí bezpečnost dat zvyšovat, ale naopak snižovat, a to jelikož osoba dává k dispozici citlivá data v případě, kdy ani není potřeba ověřit její totožnost (OPTAGLIO, 2022).

B. Autentizace

Jak již bylo výše zmíněno, autentizace (angl. authentication) slouží k ověření, zda je daná osoba skutečně tou, za kterou se vydává (ManagementMania.com, 2022). V návaznosti na identifikaci je tedy identifikovaná totožnost osoby pomocí autentizace ověřena. Pokud je autentizace úspěšná, zpravidla na ni bezprostředně naváže proces autorizace (viz níže).

Metody autentizace mohou být založeny na různých principech, přičemž třemi základními jsou následující:

- **vlastnictví** – osoba vlastní (má v držení) určitou věc, na základě které je možné provést autentizaci (karta, klíč, token apod.),
- **znalost** – osoba zná určitou informaci (heslo, PIN apod.),
- **vlastnost** – osoba je ověřena na základě určitého jedinečného prvku, zpravidla fyziologického (biometrické údaje).

V praxi často dochází k tomu, že jednotlivé metody jsou kombinovány, čímž se důvěryhodnost provedené autentizace posiluje. Na základě této skutečnosti je možné rozdělovat autentizace dle počtu jednotlivých faktorů, které jsou ověřovány.

Jednofaktorová autentizace proběhne pouze na základě jedné z výše uvedených metod pomocí jediného faktoru, tedy typicky na základě znalosti nastaveného hesla. Pokud odhlédneme od světa informačních technologií, tak dalším naprosto typickým příkladem autentizace metodou vlastnictví je odemčení dveří nebo trezoru klíčem. V návaznosti na výše uvedený způsob identifikace osoby jejím představením může autentizace proběhnout předložením občanského průkazu, čímž bude totožnost ověřena.

Za účelem posílení zabezpečení ale lze zařadit autentizačních faktorů více. Hovoříme pak o vícefaktorovém ověření (angl. multi-factor authentication), přičemž celkový počet faktorů může být různý a podle toho je také způsob ověření nazýván. K úspěšnému provedení autentizace dvoufaktorové je třeba totožnost osoby ověřit využitím dalšího prvku navíc, tedy zpravidla aplikací dvou metod. V případě kombinace metod znalosti a vlastnictví se může jednat například o kombinaci hesla a tokenu. Dalším příkladem kombinace hesla a vlastnictví pak bude využití nějakého dalšího zařízení, přičemž v případě mobilního telefonu bývá jako prostředek potvrzení vlastnictví užíváno zadání jednorázového SMS kódu nebo potvrzení v aplikaci instalované do daného mobilního telefonu. K tomu, aby bylo možné používat aplikaci jako potvrzení vlastnictví telefonu je ale nejprve třeba se do aplikace přihlásit, což opět vyžaduje buďto znalost hesla či přihlášení pomocí biometrického údaje. Poslední uvedený příklad tedy fakticky lze považovat za autentizaci dokonce třífaktorovou.

Pro úplnost je na místě zmínit, že vícefaktorová autentizace teoreticky nemusí nutně probíhat kombinací více metod, osoba může být vícefaktorově ověřena i pomocí jediné metody při použití více jednotlivých prvků.

C. Autorizace

Autorizace (angl. authorization) sama o sobě je určité oprávnění, zpravidla přístupu k určitým datům nebo do konkrétní oblasti. V tomto smyslu lze tedy autorizaci vykládat jako již získaný souhlas. Proces autorizace je pak ověření, zda má daná osoba mít přístup do této hlídané oblasti či ke konkrétním datům (IT Slovník.cz, 2022). Typickým příkladem je, když autorizace proběhne vyhledáním zadaného jména či jiných údajů v seznamu oprávněných subjektů, ale autorizační algoritmus může být založen na jakémkoliv jiném principu.

Autorizační procesy jsou užívány zejména v oblastech, ve kterých je třeba zacházet s citlivými údaji, může se tedy jednat o zdravotnictví, finanční sektor, státní správu apod. (ManagementMania.com, 2022).

2.2.3.2 Biometrické údaje

Biometrickými údaji jsou identifikační a unikátní znaky určité fyzické osoby, které vychází z jedinečnosti jejích fyzických či fyziologických parametrů (GDPR.cz, 2022). Dle čl. 4 odst. 14 Nařízení GDPR jsou biometrickými údaji „*osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje*“. Jedná se tedy o veškeré údaje, které jsou založeny na biologické podstatě člověka a zároveň umožňují jeho identifikaci (Karlovka Online, 2022). Kategorie biometrických údajů spadá mezi zvláštní kategorii osobních údajů, z čehož plyne, že i biometrickým identifikátorům osob je přiznána zvýšená ochrana.

V současné době nejčastěji používanými biometrickými údaji jsou otisk prstu a rozpoznávání obličeje (faceID), teoreticky se ale může jednat o řadu dalších znaků, jako například snímek oční duhovky, snímek sítnice, hlas apod. (GDPR Solutions, 2022). Do budoucna tak může být spektrum užívaných biometrických údajů pro ověření totožnosti (autentizaci) či identifikaci ještě nepochybně dále rozšiřováno.

Příkladem identifikace prostřednictvím biometrických údajů může být automatizované rozpoznávání obličejů na kamerových záznamech nebo přístupové systémy, jež umožní vstup na základě biometrických údajů (turnikety). V případě turniketů si lze představit identifikaci prostřednictvím tradičního otisku prstu, ale například i pomocí přístroje snímajícího krevní řečiště (Karlovka Online, 2022).

Užití biometrických údajů k autentizaci slouží k ověření, že daná osoba je tou, za níž se vydává. Autentizace je na rozdíl od identifikace zpravidla prováděna za vědomé součinnosti autentizované osoby (Karlovka Online, 2022). Příkladem může být přihlašování do mobilního bankovnictví otiskem prstu či odemykání telefonu prostřednictvím obličeje.

Není výjimkou, že autentizace a identifikace biometrickými údaji je kombinována, například po výše uvedeném rozpoznání obličeje osoby na kamerovém záznamu (identifikace) může následovat ověření identity osoby na základě jejího otisku prstu.

2.2.4 Ohrožení zabezpečení

Nařízení GDPR definuje „*porušení zabezpečení osobních údajů*“ v čl. 4 odst. 12 jako „*porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.*“ Zejména s ohledem na to, že informace, mezi které nepochybně patří právě osobní údaje, jsou považovány za „*měnu internetu*“, je nezbytné právě v online prostoru dbát zvýšené bezpečnosti při jejich transferech.

Rozvíjející se možnosti internetových technologií s sebou samozřejmě přinášejí také rozšiřování způsobů, jak je možné nové technologie zneužít, nejinak je tomu i v oblasti ochrany soukromí osob. Informační stopa konkrétních fyzických osob po jejich činnostech vykonávaných online je nepochybná, přičemž nejčastěji hrozí neoprávněné získání citlivých informací jako je IP adresa uživatele zařízení, e-mailová adresa osoby, místo, kde se osoba momentálně fyzicky nachází (určení polohy), či adresa bydliště nebo pracoviště.

V této souvislosti budou dále rozebrány některé nejčastější postupy, kterými mohou být osobní údaje osob zneužity (Tomášek, 2016).

A. Spam

Pod pojmem spam se skrývá rozesílání nevyžádané pošty (e-mail, messenger atd.), přičemž jejím obsahem nejčastěji bývá reklamní nebo jiné komerční sdělení, jehož cílem je přesvědčit adresáta k nákupu zboží či služby. Postupem času se však spamy dostaly i na diskuzní fóra a jiné komunikační kanály (Internetem bezpečně, 2021). E-mailové schránky často automaticky filtrují příchozí poštu a velkou část těchto obchodních sdělení dokáží samy rozpoznat a zařadit rovnou do kategorie Spam. Prostřednictvím spamu lze rozšiřovat trojské koně, viry a jiné nežádoucí návštěvníky zařízení, které následně mohou získat právě velký objem osobních údajů v zařízení dostupných (Rezgui, Bouguettaya, 2003).

B. Hoax

Hoax je poplašná zpráva, jejímž obsahem může být například varování před fiktivním nebezpečím, žádost o pomoc s nepravdivým podkladem apod. Rysem tohoto druhu napadení zařízení je zejména vyzývání k přeposlání dalším uživatelům. Stejně jako u spamu může být prostřednictvím hoaxu rozšiřován vir, který ohrožuje mimo jiné osobní údaje uživatelů. Užitečným nástrojem při obraně proti hoaxům může být server hoax.cz (Hoax.cz, 2021), který vede databázi hoaxů, díky níž se mohou uživatelé relevantně informovat (Internetem bezpečně, 2021).

C. Phishing

Obzvláště nebezpečným je phishing, jehož podstatou je získání citlivých údajů s pomocí technik sociálního inženýrství, kdy se útočník vydává za důvěryhodnou autoritu (Eset.com, 2021). Jde o neoprávněné získání citlivých údajů od uživatele, například přihlašovacích údajů k internetovému bankovnictví, hesel k platebním kartám, PINu k potvrzování plateb apod. To vše pod klamnou záštitou osoby nebo instituce, která k těmto údajům zpravidla má oprávnění, aby v uživateli nebylo vzbuzeno pro podvodníky nežádoucí podezření, tedy například banky, zaměstnavatele atd. K rozpoznání těchto útoků jsou zpracovány různé metodiky, které doporučují například všímat si jazyka, kterým je zpráva psána, nebo kontrolovat domény, ze kterých jsou zprávy odeslány, čímž může být zneužití těchto extrémně citlivých údajů zamezeno.

D. Pharming

Za speciální případ phishingu je považován pharming, který k získání citlivých údajů uživatelů využívá napadení DNS a přepsání IP adresy instituce oprávněné od uživatele vyžadovat citlivé údaje, tedy zpravidla banky, pojišťovny, platební instituce apod. Z důvodu přepisu IP adresy této oprávněné osoby po vyhledání její internetové stránky dojde k přesměrování uživatele na falešnou stránku internetového bankovnictví (Wikipedie, 2021). Obranou proti pharmingu může být sekundární způsob ověření osoby, tedy například dvoufaktorová autentizace uskutečňovaná prostřednictvím jednorázové SMS.

E. Sniffing

Sniffing je specifická technika, jež umožňuje sledování počítačů v rámci lokální sítě (ukládání a následné čtení TCP paketů), která se používá např. při diagnostice sítě. Takovým

sledováním lze získat přístupová hesla a další důležité informace, které uživatel během používání zařízení zadává do zařízení, či jen zařízením „*protékají*“. Sniffing tak funguje podobně jako spyware (špionáž dat) či keylogger, přičemž sniffující software je nazýván sniffer. Stejně tak může ke sniffingu dojít kvůli trojskému koni, který bude mít v sobě skrytou techniku sniffingu.

F. Carding

Carding funguje na principu zneužití platebních karet při placení online jejich prostřednictvím. Cardingem může být ale nazýváno zneužití karty i mimo online prostor, například odsledování údajů z karty pomocí kamery přidělané na bankomatu (Tomášek, 2016).

G. Sociální sítě

Nezpochybnitelnou hrozbou v oblasti zabezpečení a ochrany osobních údajů jsou různé sociální sítě, které ačkoli jsou zdarma, cenou účtovanou uživatelům je právě úplný přístup provozovatelů sociálních sítí k osobním údajům, fotkám, videím, GPS poloze apod. Často diskutovanou oblastí je využívání těchto dat uživatelů sociálních sítí třetími osobami, které mohou získané informace využívat nejčastěji k reklamním účelům, konkrétně k přesnému zacílení reklamy, výše zmiňovanému remarketingu, ale teoreticky i k dalším nekalým činnostem. Alespoň částečnou ochranou proti takovému užití osobních údajů může uživatel svou činností sdíleným osobním údajům zajistit minimalizací vkládaného objemu informací na sociální sítě. Samotné sociální sítě jako platforma pro sdílení osobních údajů však nejsou předmětem této práce, proto budou dále spíše zanedbány.

2.3 Kryptografie

Kryptografie neboli šifrování s tématem ochrany přenášených dat úzce souvisí. Dle České terminologické databáze knihovnictví a informační vědy (Databáze Národní knihovny ČR, 2022) je kryptografie „*nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí*.“ Cílem šifrování dat je zabezpečení komunikačních kanálů, kterými data protékají. Způsobů a prostředků ochrany dat mají uživatelé vedle šifrování samozřejmě větší množství, přičemž samotná ochrana dat bývá uzpůsobena různým druhům hrozeb. Vedle šifrování může být formou ochrany dat například jejich zálohování, archivace apod. (Durčák, 20018). Vzhledem k tématu práce a zaměření

následujících částí práce zejména na ověřování totožnosti a na bankovní identitu budou ale tyto další způsoby a prostředky ochrany dat zanedbány.

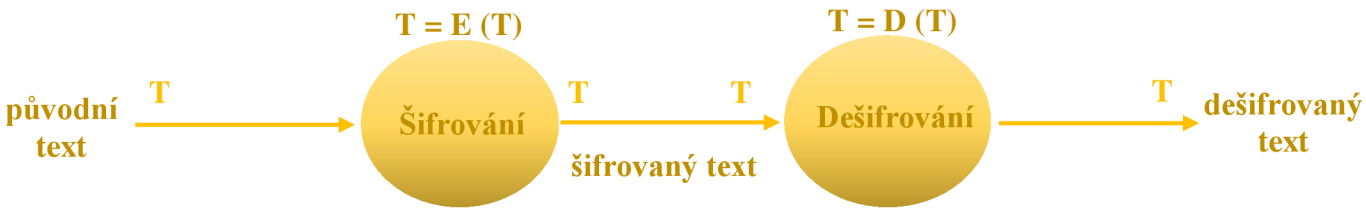
Pro úplnost je třeba zmínit, že šifrování se nepoužívá pouze za účelem přenosu dat, ale také například pro ochranu dat ve vlastním zařízení (bez potřeby jejich přenosu) před případnými útočníky (Durčák, 20018).

2.3.1 Základní pojmy

A. Transformace

Kryptografická transformace je základním principem šifrování. Právě přeměna (transformace) dat podle stanovených pravidel totiž zajistí jejich nečitelnost pro neoprávněné osoby během přenosu těchto dat. Jakmile se data dostanou do sféry dispozice adresáta, ten provede jejich zpětné dešifrování, tedy transformuje je zpět do původní podoby (Olbrich, 2002). Nutno pro úplnost uvést, že Amirová (2007) rozlišuje termíny rozšifrování a dešifrování. Za rozšifrování považuje proces zpětné transformace s použitím klíče, kdežto dešifrování je pokusem přečíst zašifrovaný text bez znalosti klíče, tedy „*prolomení*" šifry. Například Durčák (2018) ale používá termín dešifrování i pro zpětnou transformaci při znalosti klíče. Za účelem zjednodušení tedy bude dále používán pouze termín dešifrování.

Obrázek 2 – Schéma transformace



Zdroj: Almirová, 2007, vlastní zpracování.

B. Šifra

Šifra je dvojice algoritmů, které realizují dvě výše uvedené transformace, tedy šifrování a dešifrování (Amirová, 2007). Šifrovací i dešifrovací algoritmus spolu musí korespondovat, aby bylo možné data transformovat na obou stranách procesu.

C. Šifrovací klíč

Souvisejícím termínem s pojmem šifra je termín šifrovací klíč (či jen klíč), kterým může být slovo, věta, číslo, či jiná sekvence znaků konstantní délky. Šifrovací klíč se používá

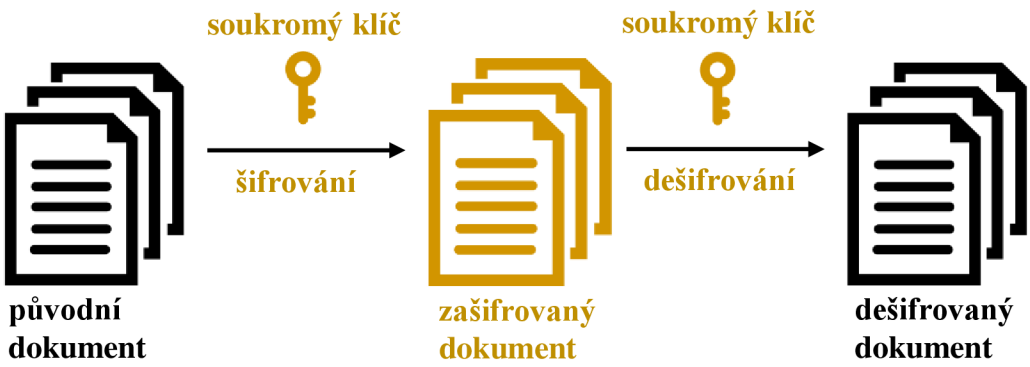
jako druhý vstup do šifrovacího algoritmu, přičemž při šifrování do algoritmu vstupuje vedle původního textu a při dešifrování vedle zašifrovaného textu. Důležitým poznatkem je, že dle pravidel kryptografie právě tajnost šifrovacího klíče zajišťuje bezpečnost, nikoliv tajnost šifrovacího algoritmu (Olbrich, 2002).

2.3.2 Symetrické algoritmy

Různé typy šifrování jsou postaveny na odlišných matematických základech, převážná většina z nich ale vychází z principu transformace dat určitým klíčem (Durčák, 2018). Symetrické (také konvenční) šifrování využívající symetrické algoritmy je postaveno na transformaci dat pomocí jediného klíče, který je tajný a soukromý (privátní) (Amirová, 2007). Samotný algoritmus tajný být přitom nemusí, podstatná je tajnost klíče, jak již bylo zmíněno výše (Olbrich, 2002).

Jak v šifrovacím algoritmu, tak při dešifrovacím algoritmu se používá stejný soukromý klíč. Výhodou tohoto typu šifrování je poměrně nízká výpočetní náročnost, lze jej tedy použít i při přenosu větších objemů dat a proces transformace je rychlejší (Durčák, 2018). Zásadní nevýhodou symetrického šifrování ovšem je, že obě (případně všechny) zúčastněné strany, které provádějí transformaci dat, musí disponovat daným konkrétním privátním klíčem, který tedy musí být před transformací nezbytně určitým důvěryhodným způsobem předán (OZP, 2021). V případě, že je tedy šifrovaný dokument určen většímu množství osob, je využití této metody značně nepraktické a s rostoucím počtem adresátů téměř neproveditelné.

Obrázek 3 – Schéma symetrického šifrování



Zdroj: Durčák, 2018, vlastní zpracování.

2.3.3 Asymetrické algoritmy

Na rozdíl od symetrických algoritmů, ty asymetrické jsou od svého počátku určeny k ochraně dat při jejich přenosu mezi subjekty (Amirová, 2007). Se zásadní nevýhodou symetrického šifrování pro přenos dat v podobě nutnosti sdílení šifrovacího klíče se vypořádává metoda využívající asymetrické algoritmy tak, že využívá dva šifrovací klíče (Durčák, 2018). Jeden klíč je využíván při šifrování dat a druhý při jejich zpětném dešifrování. Důležitou vlastností asymetrického šifrování je, že proces šifrování dat je nevratný i v případě, že známe šifrovací klíč, dešifrovat je možné jen a pouze s klíčem dešifrovacím. Na základě tohoto principu může být šifrovací klíč bez rizika veřejný, protože k dešifrování textu nepostačuje, šifrovací klíč je proto nazýván klíčem veřejným. Naproti tomu dešifrovací klíč musí zůstat tajným, tedy soukromým (Durčák, 2018).

Dohromady tvoří soukromý i veřejný klíč tzv. klíčový pár, přičemž ze soukromého lze odvodit ten veřejný, ale nikoliv naopak. V praxi pak komunikace mezi dvěma subjekty pomocí asymetrického šifrování probíhá tak, že si navzájem pošlou veřejné klíče, aby odesílatel mohl zašifrovat dokument určený pro adresáta, který si jej pak sám dešifruje pomocí svého soukromého klíče, který uchovává v tajnosti (Durčák, 2018). Důležitým bezpečnostním prvkem tudíž je, že soukromý klíč nemusí být při komunikaci předáván a riziko jeho vyzrazení je tak významně sníženo.

Navzdory velkému množství bezpečnostních výhod má proces asymetrického šifrování zásadní nevýhodu v podobě velké výpočetní náročnosti. Často tedy za účelem získání výhod symetrického i asymetrického šifrování a zároveň eliminace jejich nevýhod dochází ke kombinaci obou metod: klíč k symetrickému šifrování je mezi stranami vyměněn pomocí asymetricky zašifrované zprávy a následně může komunikace probíhat již za nižšího výpočetního výkonu (Durčák, 2018).

Obrázek 4 - Schéma asymetrického šifrování

Zdroj: Durčák, 2018, vlastní zpracování.

Ačkoli z výše uvedeného vyplývá, že veřejný klíč nemusí být tajný, může vznikat odlišný bezpečnostní problém. Je třeba totiž zajistit ověření, že daný veřejný klíč skutečně patří osobě, která jej za své vlastnictví vydává. Demonstrativním příkladem může dle Olbricha (2002) být následující situace:

- určitá osoba (podvodník) uveřejní falešný veřejný klíč a proklamuje, že ten patří někomu jinému (Janu Novákovi);
- Jan Novák používá vlastní veřejný klíč a netuší, že se za něj někdo vydává a zveřejnil falešný veřejný klíč;
- odesílatelé tajných zpráv adresovaných Janu Novákovi nevědomky využijí podvodný veřejný klíč k zašifrování zprávy a odešlou ji;
- podvodník vlastní soukromý klíč, zprávu zachytí a dešifruje;
- podvodník pomocí skutečného veřejného klíče Jana Nováka zprávu opět zašifruje a odešle Janu Novákovi;
- Jan Novák obdržel zprávu, dešifroval svým soukromým klíčem a nemá tušení, že danou komunikaci někdo sledoval, stejně tak odesílatel nemá tušení, že zpráva měla „*zastávku*“ u podvodníka, který nepozorovaně zjistil její obsah.

Za účelem zamezení této hrozbě existují důvěryhodné certifikační autority, které ověřují, že daný veřejný klíč skutečně patří proklamované osobě. Této problematice budou věnovány následující kapitoly.

2.4 Dálkové ověření totožnosti

Prvním skutečně významným krokem (nebereme-li v úvahu datové schránky, které v některých případech přeneseně umožňovaly identifikaci na dálku) vstříc elektronické identifikaci a ověřování totožnosti bylo vydání zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů (zákon o elektronickém podpisu, dále jen „***ZoEP***“), který platil 16 let, ke dni 16. září 2016 byl však zrušen. Ke zrušení ZoEP došlo v souladu s celoevropskou harmonizací dané problematiky nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, známém spíše pod zkratkou eIDAS. Účinností nařízení eIDAS došlo ke sjednocení legislativy elektronického podpisu pro celou Evropskou unii.

V návaznosti na přímo použitelné nařízení byl v České republice vydán zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů (dále jen „***ZoEI***“). Ačkoliv je nařízení eIDAS přímo použitelným předpisem a není třeba jej tedy do českého právního řádu transponovat, bylo třeba české právní prostředí uzpůsobit změnám, které s sebou eIDAS přineslo. Jednou z těchto zásadních změn bylo, že eIDAS uložilo povinnost uznávat prostředky elektronické identifikace pro přístup k online službám poskytovaných subjekty veřejného sektoru (Ministerstvo vnitra, 2020). Původní ZoEP upravoval problematiku elektronických podpisů odlišně než nařízení eIDAS a měl být tedy zrušen současně s účinností daného nařízení. Čeští legislativci ale měli mírné zpoždění s vydáním ZoEI, a tak po dobu několika měsíců byly v České republice účinné dvě vzájemně si odporující právní úpravy. Ke zhojení tohoto stavu ale došlo právě vydáním ZoEI.

ZoEI stanovuje mnoho podmínek, které musely být při ověřování totožnosti splněny. Dle ustanovení § 2 ZoEI je možné na dálku identitu ověřit pouze prostřednictvím kvalifikovaného systému elektronické identifikace, přičemž za takový kvalifikovaný systém lze v souladu s ustanovením § 3 ZoEI považovat pouze ten, který splňuje následující podmínky:

- je spravován kvalifikovaným správcem systému elektronické identifikace,
- splňuje technické specifikace, normy a postupy alespoň pro jednu z úrovní záruky stanovených příslušným evropským předpisem,

- umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci (dále jen „***NIA***“),
- v jehož rámci jsou osobní identifikační údaje jedinečně identifikující osobu v okamžiku vydání prostředku pro elektronickou identifikaci spojeny s danou osobou,
- v jehož rámci je vydáván a používán pouze prostředek pro elektronickou identifikaci, který je spojen s osobou, jíž identifikuje.

ZoEI dále také upravuje osoby oprávněné službu elektronické identifikace poskytovat, jimiž jsou buďto státní orgány nebo osoby, kterým byla udělena akreditace pro správu kvalifikovaného systému a které jsou zároveň napojeny na NIA. Oprávněné osoby musí respektovat meze určené ZoEI i dalšími předpisy, jež užívání elektronického ověřování totožnosti upravují.

Seznam aktuálně dostupných identifikačních prostředků pro vzdálené prokazování totožnosti při využívání online služeb je dostupný na oficiální webové stránce Identity občana (Identita občana, 2022). Ke dni 26. ledna 2022 bylo možné využít následujících prostředků ověřujících totožnost:

a) státní poskytovatelé:
    - Občanský průkaz s aktivovaným kontaktním elektronickým čipem vydaný po 1. červenci 2018 (aktivace čipu je dobrovolná a k využití prostředku je třeba mít nainstalovánu aplikaci eObčanka),
    - NIA ID, které je nezpoplatněným prostředkem založeným na kombinaci jména, hesla a jednorázového SMS kódu (dříve označovaný jako uživatelský účet, OTP či UPS),
    - Mobilní klíč e-governmentu, který je nezpoplatněným prostředkem nabízejícím přihlašování bez potřeby zadávání dalších ověřovacích kódů,

b) soukromoprávní poskytovatelé:
    - čipová karta Starcos společnosti První certifikační autorita a.s.,
    - MojeID od sdružení CZ.NIC, zájmového sdružení právnických osob,
    - ČSOB Identita poskytovaná Československou obchodní bankou, a. s.,
    - Bankovní IDentita poskytovaná Českou spořitelnou, a. s.,
    - Bankovní identita KB poskytovaná Komerční bankou, a. s.,

- Bankovní Identita poskytovaná Air Bank, a. s.,
- Bankovní Identita poskytovaná MONETA Money Bank, a. s.,
- Bankovní Identita poskytovaná Raiffeisenbank, a.s.

Důležitou vlastností jednotlivých prostředků je také úroveň záruky, což je v podstatě míra jistoty, s jakou lze danému prostředku důvěřovat. Úrovně záruky (důvěry) jsou v souladu s eIDAS odlišovány tři (Ministerstvo vnitra, 2022):

1. nízká – k ověření totožnosti nedošlo, identita byla pouze deklarována (nastavením jména a hesla),
2. značná – dvoufaktorová autentizace pomocí přihlašovacích údajů (jméno a heslo) a jednorázového SMS kódu, přičemž totožnost byla ověřena předem na kontaktním místě veřejné správy prostředkem stejné nebo vyšší úrovně důvěry nebo pomocí datové schránky,
3. vysoká – identifikační prostředek je uložen na bezpečném zařízení, při jeho vydání byla totožnost zaručeně ověřena a oprávněná osoba zná přihlašovací údaje.

2.4.1 Elektronický podpis

Elektronický podpis je jedním z prostředků ověřujících totožnost osob na dálku, který má ale více funkcí. Jednou z nich je logicky již zmíněné ověření totožnosti osoby. Důležitou funkcí je nepochybně také zajištění integrity dokumentu, který po jeho podepsání již není možné měnit. Dalším významným parametrem elektronického podpisu je jeho unikátnost, a tedy že nikdo jiný stejným podpisem nedisponuje (CZ.NIC, 2022).

Elektronický podpis funguje na principu veřejného a soukromého klíče, tedy asymetrického šifrování, které bylo blíže vysvětleno výše. Elektronický podpis, jenž je připojován k dokumentu, je představován binárními daty, která odpovídají podepisující osobě a obsahu dokumentu. K opatření dokumentu elektronickým podpisem je třeba podpisového klíče, který se jako celek skládá z klíče soukromého a veřejného. Pomocí soukromého klíče, jenž je tajný, a daného dokumentu lze tato binární data zjistit. Na základě veřejného klíče lze naopak ověřit, že se jedná o stejný dokument, který byl podepsán a že binární data byla k dokumentu připojena pomocí odpovídajícího soukromého klíče (CZ.NIC, 2022).

2.4.1.1 Certifikační autority

Aby mohly konkrétní osoby být považovány za ověřené, na základě čehož jim je teprve poskytnuta možnost užívat elektronický podpis, existují certifikační autority. Tyto vydávají osobám digitální certifikáty, na jejichž základě je možné dokumenty opatřovat elektronickým (digitálním) podpisem (CZ.NIC, 2022).

Podstata certifikačních autorit spočívá v tom, že musí jít o entity dostatečně důvěryhodné, jejichž veřejný klíč je veřejně znám. Digitální certifikáty, které certifikační autority vydávají, jsou dokumenty obsahující veřejný klíč přidělený dané osobě a zároveň identifikační údaje této osoby. Certifikační autorita vydaný certifikát sama podepíše a vydá majiteli (CZ.NIC, 2022).

Pro snazší pochopitelnost uvedeme praktický příklad: Jana Levá má zájem nechat si vytvořit svůj elektronický podpis. Obrátí se tedy na certifikační autoritu. Ta Janě nové vytvoří její vlastní soukromý a veřejný klíč. Následně Janě vydá digitální certifikát, který obsahuje Jany veřejný klíč a její identifikační údaje (jméno). Zároveň Janě předá její soukromý klíč (není součástí certifikátu), který bude Jana používat při podepisování dokumentů. V případě, že pak Jana pošle podepsaný dokument kamarádovi, ten bude-li mít Jany certifikát (obsahující veřejný klíč), může ověřit, že jej podepsala skutečně Jana, přičemž certifikační autorita ručí za to, že podepsaný subjekt je tím, kým tvrdí být.

Certifikační autority mohou být různé úrovně důvěryhodnosti a ne každý potřebuje certifikát obecně přijímaný, proto například v rámci vnitropodnikové komunikace může být postačující podpis ověřený daným podnikem. Nejvyšší úroveň důvěryhodnosti ale poskytují pouze kvalifikovaní poskytovatelé certifikačních služeb, kterými jsou dle Ministerstva vnitra ke dni 26. ledna 2022 následující subjekty:

Obrázek 5 – Přehled kvalifikovaných poskytovatelů certifikačních služeb

Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb

Ministerstvo vnitra zveřejňuje v souladu s § 9 odst. 2, písm. e) zákona č. 227/2000 Sb.

Poř. číslo	Poskytovatelé certifikačních služeb	Kvalifikované služby	Zahájení vydávání
1.	První certifikační autorita, a. s., IČO 26439395, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek. Vydávání prostředků pro bezpečné vytváření elektronických podpisů.	03/2002 02/2006 02/2006 01/2016
2.	Česká pošta, s. p., IČO 47114983, Olšanská 38/9, PSČ 225 99 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek. Vydávání prostředků pro bezpečné vytváření elektronických podpisů.	09/2005 04/2005 07/2009 06/2016
3.	eIdentity a. s., IČO 27112489, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	08/2005 08/2005 08/2010

Zdroj: Ministerstvo vnitra ČR, 2022.

2.4.2 Bankovní identita

Bankovní identita znamená velký posun v oblasti ověření totožnosti na dálku prostřednictvím elektronických prostředků, a to nejen v oblasti bankovnictví, ale i v širších kruzích veřejné sféry a do budoucna nepochybně i v dalších sektorech. Mezi důvody k zavedení bankovní identity patří zejména úspora nákladů, zjednodušení použití různých online nástrojů a u komerčních subjektů v neposlední řadě získání nových klientů či lepší uspokojení potřeb těch stávajících. Prozatím jsou poskytovateli bankovní identity pouze banky, svůj zájem o bankovní identitu ale avizují například i telekomunikační operátoři a mnoho dalších komerčních subjektů.

Bankovní identita je někdy také označována pojmem „*BankID*“, v současnosti se ale má za to, že termín „*bankovní identita*” je název samotné identifikační metody, naproti tomu pojem „*BankID*” je označením konkrétní služby uskupení bank s názvem Bankovní identita a.s., které poskytuje technické řešení bankovní identity jednotlivým soukromým subjektům.

V obecném smyslu se tedy jeví vhodnějším používat pojem „*bankovní identita*“. Uvedené terminologické rozlišení bude respektováno i v této práci.

Od 1. ledna 2021 nabyl účinnosti zákon č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dále jen „***ZoBI***“), často nazývaný spíše jako zákon o bankovní identitě. ZoBI umožnil bankám elektronicky ověřovat totožnost osob, podepisovat dokumenty a činit další právní úkony elektronicky, což znamená velký krok v usnadnění komunikace mezi bankami a jejich klienty. Tento posun lze považovat za revoluci při ověřování totožnosti na dálku v českém prostředí, což je nepochybně krokem pozitivním, jelikož bankovní identita je jednou z nejbezpečnějších a nejvíce využívaných digitálních autentizačních metod současnosti. Inspirací v tomto ohledu byly zejména severské evropské státy, které jsou v oblasti dálkového ověřování velmi progresivní, např. v Norsku používá elektronickou identifikaci a podepisování pomocí bankovní identity 90 % aktivních obyvatel (Advokátní deník, 2021). V České republice má internetové bankovnictví 97 % Čechů s internetem (Česká bankovní asociace, 2021), tudíž i zde je potenciál velký. V současné době (říjen 2021) má bankovní identitu přibližně 5,5 milionu lidí (Česká bankovní asociace, 2021). Důležitým poznatkem také je, že bankovní identitu může každá osoba kdykoliv deaktivovat.

Celý projekt implementace bankovní identity v České republice je zastřešován Českou bankovní asociací (dále jen „***ČBA***“), která vykonává činnost od roku 1990 jako dobrovolné sdružení bank a stavebních spořitelen působících na českém trhu a reprezentujících více než 99 % českého bankovního sektoru. ČBA je důležitým zástupcem jednotlivých bank, jejichž společné zájmy prosazuje, ale podílí se také například na legislativním procesu harmonizace českého a evropského finančního práva. ČBA se významně podílela právě i na prosazování projektu bankovní identity, na němž se pracuje od roku 2019. Na začátku roku 2020 byla přijata zásadní legislativa s odloženou účinností od roku 2021 (viz výše) umožňující všem bankám v České republice poskytujícím elektronické bankovnictví být poskytovatelem bankovní identity. Jedním z nejdůležitějších důvodů, z jakých se ČBA podařilo prosadit novou legislativu, byla právě i využitelnost bankovní identity i pro potřeby státu.

Provozovatelem oficiálních webových stránek projektu bankovní identity (Česká bankovní asociace, 2021) je právě ČBA, přičemž na tomto webu je mimo jiné dostupné schéma života projektu bankovní identity, podle kterého je druhé pololetí 2021 určeno pro

implementaci bankovní identity soukromými firmami, a také oficiální logo projektu zobrazené níže.

Obrázek 6 – Schéma projektu bankovní identity

Zdroj: Česká bankovní asocicace, 2021.

Obrázek 7 – Logo bankovní identity

BANKOVNÍ IDENTITA

Zdroj: Česká bankovní asocicace, 2021.

2.4.2.1 Funkcionalita bankovní identity

Principem bankovní identity je ověření totožnosti fyzické osoby pomocí údajů primárně vytvořených pro přihlášení do internetového bankovnictví. Významným posunem při takovém ověřování je zejména v posledních letech navíc možnost přihlášení pomocí biometrických údajů, jako je otisk prstu, rozpoznání obličeje (faceID) apod., kterým byla věnována samostatná podkapitola výše. Biometrické údaje mohou nahradit PIN či heslo, což celé přihlášení usnadňuje a zrychluje.

2.4.2.2 Využití pro komerční účely

Vzhledem k tomu, že ČBA prosazuje zájmy jednotlivých bank na trhu, pochopitelně bude mít z fungující bankovní identity prospěch soukromý sektor, konkrétně banky, které se budou projektu účastnit. Ke zprovoznění bankovní identity musí každá banka akreditovat

své technické řešení bankovní identity u Ministerstva vnitra ČR, přičemž celý akreditační proces je poměrně náročný, jelikož předložená technická řešení musí projít testováním a dalšími kontrolami. Až následně na základě udělení akreditace může být bankovní identita nabízena klientům banky. Jako první začaly svým klientům bankovní identitu nabízet v prvním čtvrtletí 2021 následující banky (seřazeny abecedně): Air Bank, Česká spořitelna, ČSOB, Komerční banka a MONETA Money Bank. Ve třetím čtvrtletí byla akreditace udělena Raiffeisenbank, u které momentálně probíhá testovací provoz (říjen 2021)[1]. Ve čtvrtém čtvrtletí se očekává udělení akreditace Equa bank, Fio bance, mBank a UniCredit Bank (ČBA, 2021). V současné době tyto banky pracují na dalších technických řešeních využití bankovní identity v souvislosti s řadou dalších služeb nabízených jejich klientům v online prostoru.

Podmínkou k využívání bankovní identity fyzickými osobami je tedy platná smlouva s jednou z bank zapojených v projektu. Aktuální zapojené banky či do budoucna jiné soukromé subjekty lze snadno zjistit na oficiální webové adrese bankovní identity (Bankovní identita, 2021). Další nezbytnou podmínkou k využití bankovní identity i ve vztahu k třetím osobám (kromě dané banky) je souhlas klienta.

Důležitým aspektem napomáhajícím rozšíření využívání bankovní identity je, že bankovní identita je i komerčními subjekty poskytována klientům zdarma. Nejde tedy o další zpoplatněnou službu bank a platebních institucí, o kterou by přirozeně fyzické osoby nejevily takový zájem jako v případě bezplatného užívání. Stát bankám za ověření totožnosti fyzických osob také neplatí, zadarmo ale samozřejmě banky bankovní identitu neposkytují, především z toho důvodu, že i ony musely na bezpečnost přihlašování a ověřování totožnosti na dálku vynaložit nemalé prostředky.

Na čí účet tedy využívání bankovní identity jde? Poplatky za využívání bankovní identity bankám platí soukromé subjekty, které ověření totožnosti osoby vyžadují za účelem umožnění přístupu do svých aplikací, právě tyto subjekty jsou tedy platícími uživateli služby. Bankovní identita je bezpečným elektronickým nástrojem ověřujícím totožnost klientů na dálku, aniž by tyto soukromé osoby musely vynakládat velké prostředky na vlastní nástroje a jejich aktualizaci, které by oproti poplatkům, jež musí hradit bankám za využívání bankovní identity, byly jistě násobně vyšší. Úspora nákladů a zjednodušení procesů jsou

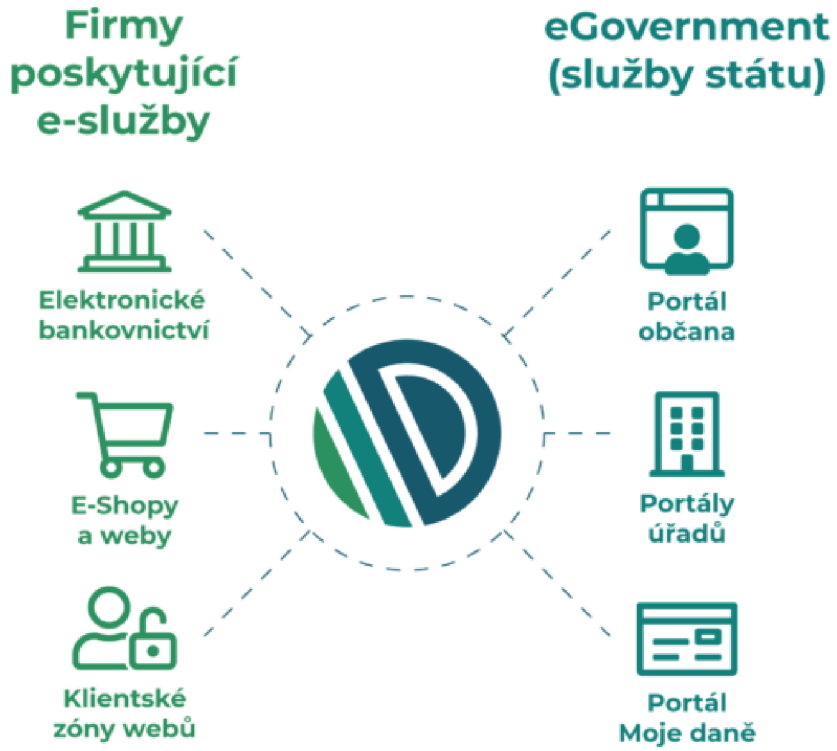
[1] V době odevzdání diplomové práce (březen 2022) již je bankovní identita Raiffeisenbank funkční.

tedy hlavními důvody, proč soukromé osoby mají zájem o ověřování totožnosti svých klientů pomocí bankovní identity.

2.4.2.3 Využití pro veřejně prospěšné účely

Jednou z významných výhod bankovní identity je možnost jejího širokého využití také pro účely veřejně prospěšné. Bankovní identita nyní již zdaleka není komerčním nástrojem pouze velkých institucí bankovního sektoru. Za veřejně prospěšný účel lze nepochybně označit využití bankovní identity při komunikaci se státními institucemi, které navíc bývá čím dál častěji skloňováno i na evropské legislativní úrovni. Po několika spíše neúspěšných pokusech (např. elektronické občanské průkazy) tak lze konečně mluvit o funkčním nástroji e-governmentu, neboli o nástroji pro komunikaci mezi příslušnými orgány veřejné moci a občany státu (Lentner, Parycek, 2016, Polčák, 2018). Tento způsob vykonávání státní správy je zásadně odlišným postupem od standardního „*analogového*“ postupu a je jednoznačně odpovědností vlády funkčnost a bezpečnost e-governmentu zajistit (Lentner, Parycek, 2016). Shrnutí zásadních oblastí využití bankovní identity je zachyceno následujícím schématem, které ale neobsahuje vyčerpávající výčet veškerých možností užití:

Obrázek 8 – Využití bankovní identity



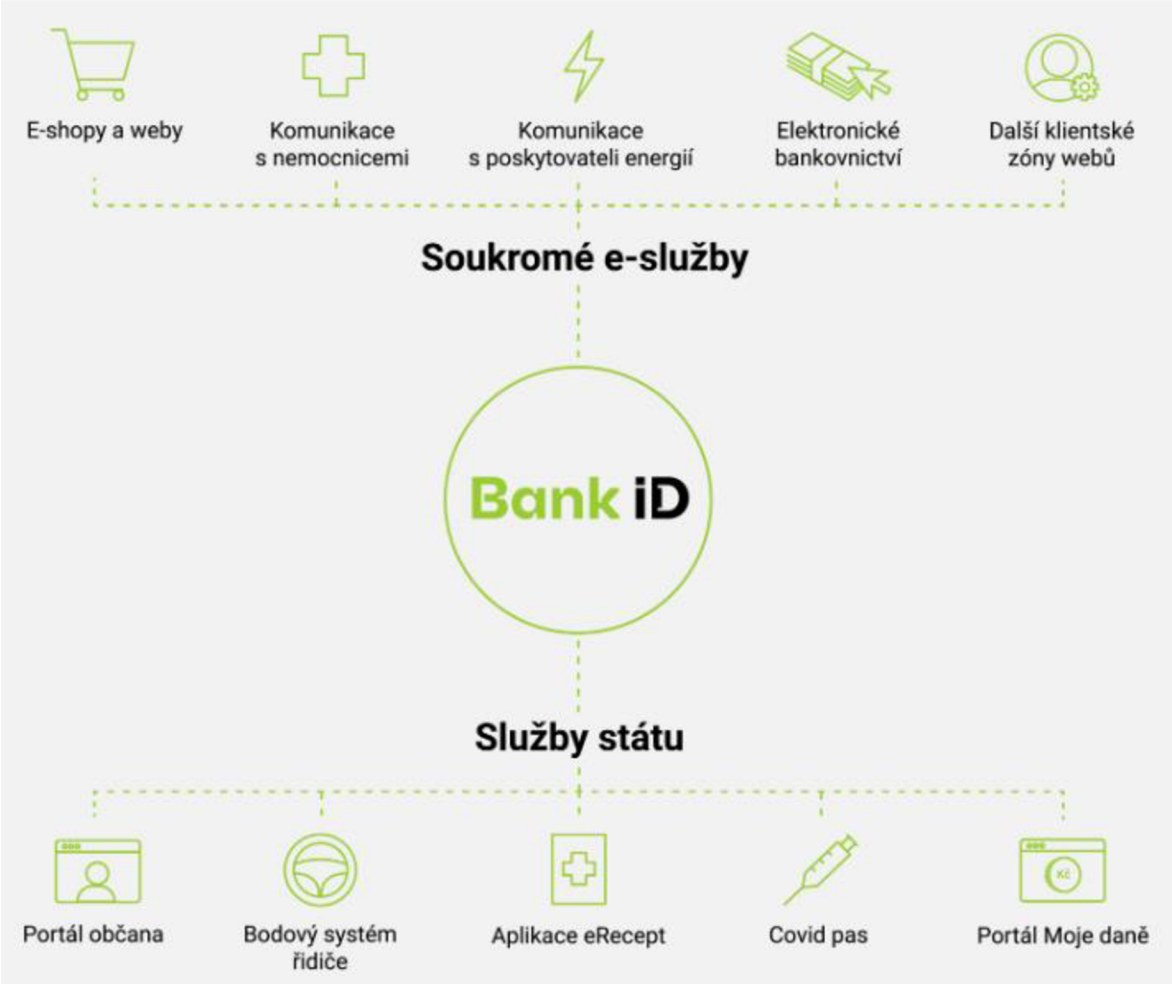
Zdroj: Česká bankovní asociace, 2021.

3 Vlastní práce

3.1 Testování využitelnosti bankovní identity pro různé účely

Možnosti využití bankovní identity jsou již v současné době různorodé a lze předpokládat, že se budou i nadále rozšiřovat. Jedná se totiž o velice snadný způsob, jak prokazatelně ověřit, že osoba sedící za počítačem či jiným zařízením je skutečně tou, za kterou se vydává, a to bez nutnosti osobního kontaktu. Stačí za tímto účelem učinit pouze ty kroky, které jsou třeba pro přihlášení do internetového bankovnictví. Příklady využití bankovní identity pro soukromé i veřejnoprávní (státní) účely jsou uvedeny na následujícím grafickém schématu:

Obrázek 9 – Využití bankovní identity



Zdroj: Air bank, 2021.

Následující kapitoly budou reprodukovat praktické zkušenosti s využíváním bankovní identity pro účely soukromé i pro účely veřejné (zpravidla komunikace se státní správou).

3.1.1 Soukromý sektor

Používání bankovní identity ke komunikaci s bankami a dalšími subjekty finančního trhu (pojišťovny, spořitelní a úvěrní družstva apod.) bylo primárním záměrem při vytvoření daného způsobu ověřování totožnosti člověka. Postupem času však k využití bankovní identity přistoupily soukromé subjekty i z jiných sektorů, v současné době tak tento způsob přihlašování využívají vedle subjektů finančního trhu například následující společnosti (Air Bank, 2022):

- Skupina ČEZ,
- MallPay s.r.o.,
- Pražská plynárenská, a. s.,
- SAZKA a.s.,
- Oborová zdravotní pojišťovna OZP a další.

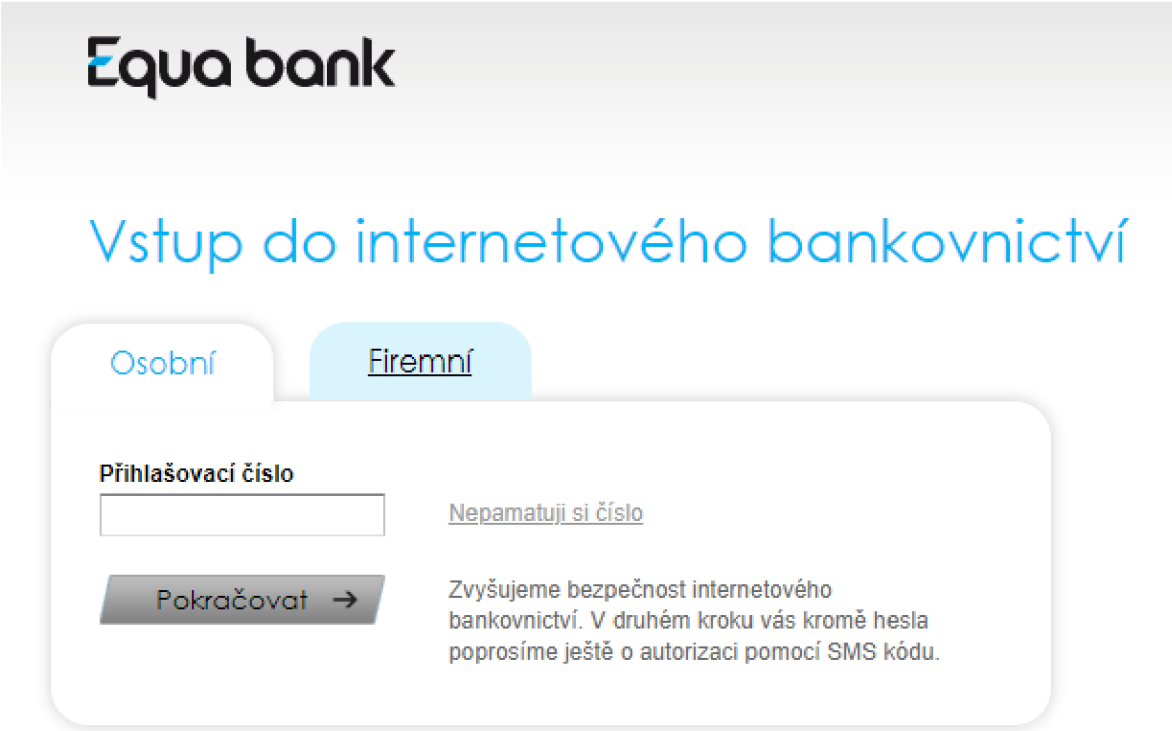
Vzhledem k tomu, že vývoj jednotlivých přihlašovacích prostředí soukromých subjektů je opravdu dynamický, je třeba vzít v úvahu, že následující testování funkčnosti bylo prováděno v průběhu ledna 2022.

3.1.1.1 Internetové bankovnictví

Při testování využití bankovní identity pro přihlášení do internetového bankovnictví bylo využito virtuální prostředí společnosti Equa bank, přičemž přihlašovací okno zobrazené na obrázku níže je dostupné na webových stránkách banky (Equa bank, 2022).

Prvním krokem přihlášení je zadání klientského čísla, jež je doručováno svému majiteli výhradně prostřednictvím služeb České pošty do vlastních rukou. Při takovém doručování je ověřována identita přejímajícího na základě ztotožnění osoby podle občanského průkazu. Klientské číslo se tedy může ke svému majiteli dostat pouze na základě osobního ověření totožnosti.

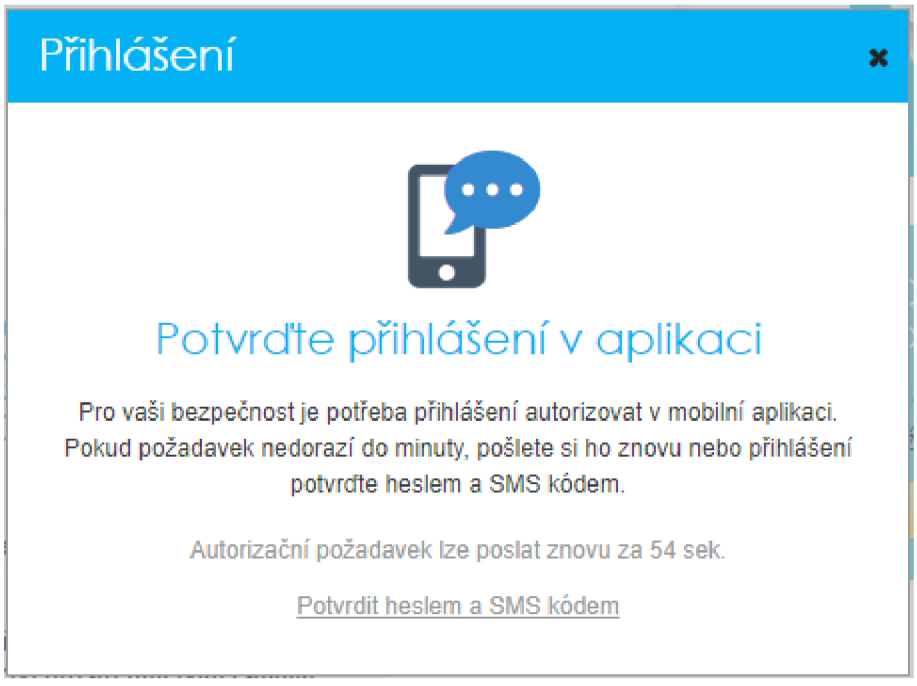
Obrázek 10 – Equa bank - zadání klientského čísla



Zdroj: Equa bank, 2022.

Na základě zadání správného klientského čísla se uživateli objeví následující vyskakující okno:

Obrázek 11 – Equa bank – potvrzení v mobilní aplikaci



Zdroj: Equa bank, 2022.

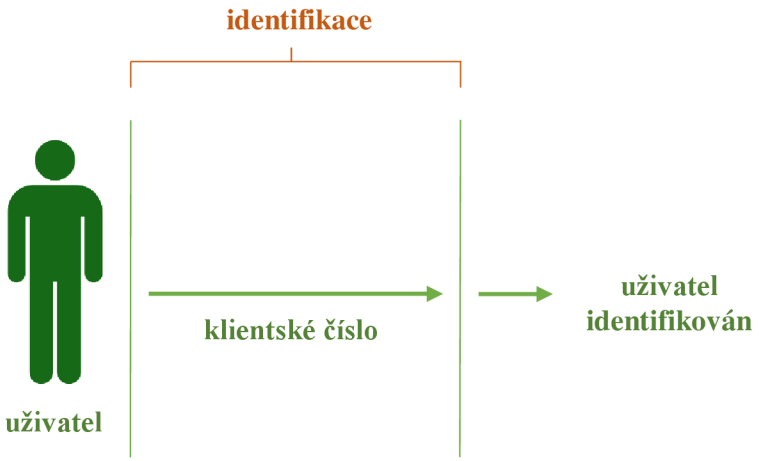
Možnost potvrzení v mobilní aplikaci pro přihlášení do internetového bankovnictví byla dobrovolně vybrána uživatelem a představuje autentizační prvek vlastnictví (mobilní telefon). Jak vyplývá z informací ve vyskakovacím okně, náhradní možností je potvrdit přihlášení nastaveným heslem, což symbolizuje autentizační prvek znalosti, načež je uživateli zaslán jednorázový ověřovací SMS kód, kterým je osoba ověřena pomocí prvku vlastnictví při autentizaci pomocí mobilního telefonu. Uživatel tak musí v případě obou možností ve chvíli přihlašování do internetového bankovnictví mít u sebe i svůj mobilní telefon (vlastnictví).

Při potvrzení v aplikaci na mobilním telefonu je vyžadováno potvrzení biometrickým údajem (otisk prstu nebo faceID) či heslem, a to dle volby uživatele. Využívání biometrických údajů pro přihlášení je pohodlné a v současné době čím dál více nahrazuje přihlašování heslem, přičemž při přihlašování pomocí bankovní identity je zadání biometrického údaje ověřením pomocí prvku vlastnost při autentizaci uživatele. Lze tedy konstatovat, že při přihlašování do prostředí internetového bankovnictví Equa bank je vždy nutné se při autentizaci prokázat prvkem vlastnictví (mobilní telefon) a druhý prvek je na volbě uživatele, a to buďto znalost (heslo), nebo vlastnost (biometrický údaj).

Obrázky potvrzování na mobilním telefonu nebylo možné vytvořit, a to na základě automatické kontroly, v důsledku které nelze udělat snímek (screenshot) obsahu mobilního bankovnictví. Ve chvíli, kdy se uživatel autentizuje, je mu zpřístupněno prostředí internetového bankovnictví, v němž může činit potřebné operace.

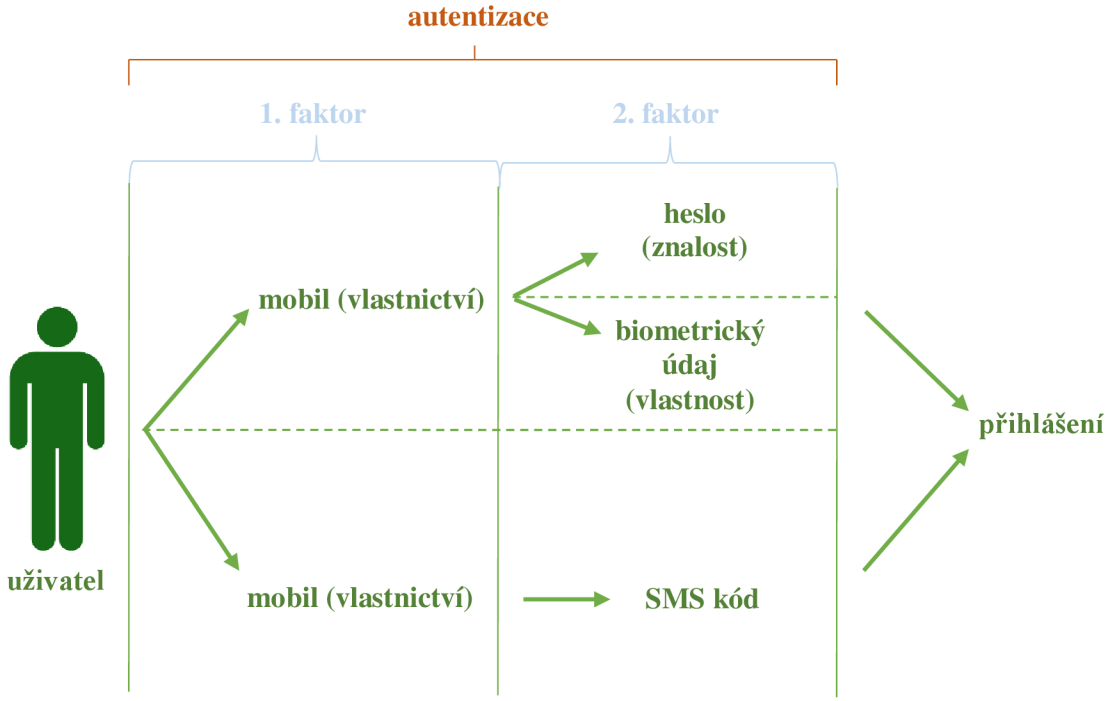
Postup při přihlášení do internetového bankovnictví (identifikace a autentizace) je znázorněn na následujících dvou schématech:

Obrázek 12 – Schéma přihlášení do internetového bankovnictví - identifikace



Zdroj: Vlastní zpracování, 2022

Obrázek 13 – Schéma přihlášení do internetového bankovnictví - autentizace



Zdroj: Vlastní zpracování, 2022.

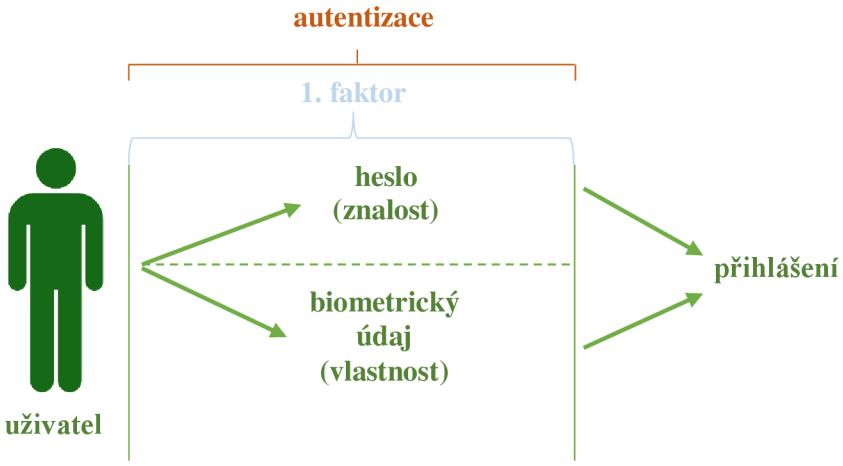
Jak vyplývá ze schématu výše, při volbě jakékoliv z nabízených možností bylo nezbytné, aby se uživatel autentizoval dvoufaktorově.

3.1.1.2 Mobilní bankovnictví

Za účelem otestování přihlášení do mobilního bankovnictví pomocí bankovní identity byla využita aplikace Equa bank instalovaná na zařízení Huawei P20 Pro model CLT-L29 s operačním systémem Android ve verzi 10, který disponuje čtečkou otisku prstu.

Pro přihlášení do mobilní aplikace je možné zvolit buďto předem nastavené heslo nebo biometrický údaj (otisk prstu nebo FaceID). K přihlášení tento krok postačuje, po potvrzení otiskem prstu je uživateli aplikace zpřístupněna, z čehož vyplývá, že ověření osoby při přihlašování do mobilního bankovnictví je možné uskutečnit jednofaktorově, viz následující schéma:

Obrázek 14 – Schéma přihlášení do mobilního bankovnictví



Zdroj: Vlastní zpracování, 2022.

Na rozdíl od internetového bankovnictví je tedy přihlášení do mobilního bankovnictví jednodušší. Z původních dvou faktorů, které jsou potřeba ověřit při přihlášení do internetového prostředí, v případě mobilního zařízení zůstává pouze ten druhý. Navíc při přihlášení do mobilního bankovnictví je možné využít možnosti ověření osoby pomocí biometrických údajů. V důsledku těchto skutečností lze konstatovat, že do mobilního bankovnictví je možné se dostat pouze na základě využití biometrických údajů, bez využití hesel či jednorázových SMS kódů, což z přihlášení do mobilního bankovnictví jednoznačně činí nejsnazší dosud testovaný postup ověření totožnosti osoby.

Nelze však přehlédnout skutečnost, že při instalaci samotné aplikace Equa bank je třeba ověřit totožnost (autentizovat) vícefaktorově. To však nic nemění na tom, že takové jedno ověření na počátku používání aplikace je dlouhodobé a není třeba jej opakovat při každém otevření aplikace. V důsledku toho je možné pak provádět jednotlivé bankovní operace již na základě jednofaktorového ověření. Zjednodušení přihlašování tímto způsobem tedy může být na úkor celkové bezpečnosti mobilního bankovnictví. Ačkoliv totiž při provádění jednotlivých operací aplikace vyžaduje opět zadání hesla (znalost) či biometrického údaje (vlastnost), stále se jedná o ten stejný prvek, který je využíván při jednofaktorové autentizaci při přihlašování do mobilní aplikace. Ve výsledku je ten stejný prvek tedy pouze opakovaně zadán, což za vícefaktorovou autentizaci považovat nelze.

3.1.1.3 Mallpay s.r.o.

Další možností využití bankovní identity v soukromém sektoru je ověření totožnosti osoby při uskutečňování platby pomocí služby mallpay, jejímž provozovatelem je společnost MallPay s.r.o. Mallpay je platební metodou, přičemž na svých webových stránkách (Mallpay, 2022) je služba označována jako „*fintech start-up*“. Zpočátku byla hlavní odlišností od ostatních platebních metod možnost odložené platby, v současné době však nabízejí samostatnou platební kartu a další dílčí služby (Mallpay, 2022).

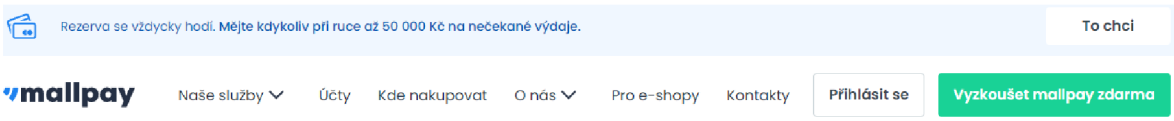
Za účelem otestování průběhu ověření totožnosti pomocí mallpay bylo zamýšleno zřízení uživatelského účtu. Fungování služby bylo na webových stránkách služby (MallPay, 2022) znázorněno následujícím schématem:

Obrázek 15 – Fungování MallPay

Zdroj: Mallpay, 2022.

Vzhledem k tomu, že na internetových stránkách služby (MallPay, 2022) je deklarována možnost vyzkoušet službu mallpay zdarma (viz zelené tlačítko vpravo na následujícím obrázku), byla tato v úvodní fázi zpracování předkládané diplomové práce zařazena do testovaných způsobů využití bankovní identity pro soukromé účely.

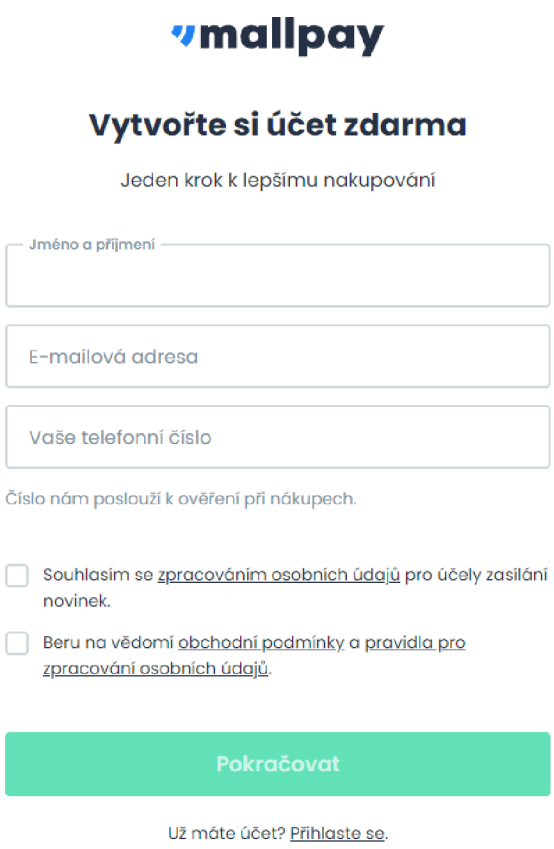
Obrázek 16 – Mallpay



Zdroj: Mallpay, 2022.

Také v dalším kroku je uživateli opakovaně sdělováno, že vytvoření účtu je bezplatné (viz následující obrázek), tudíž byl takový testovací účet uživatelem vytvořen.

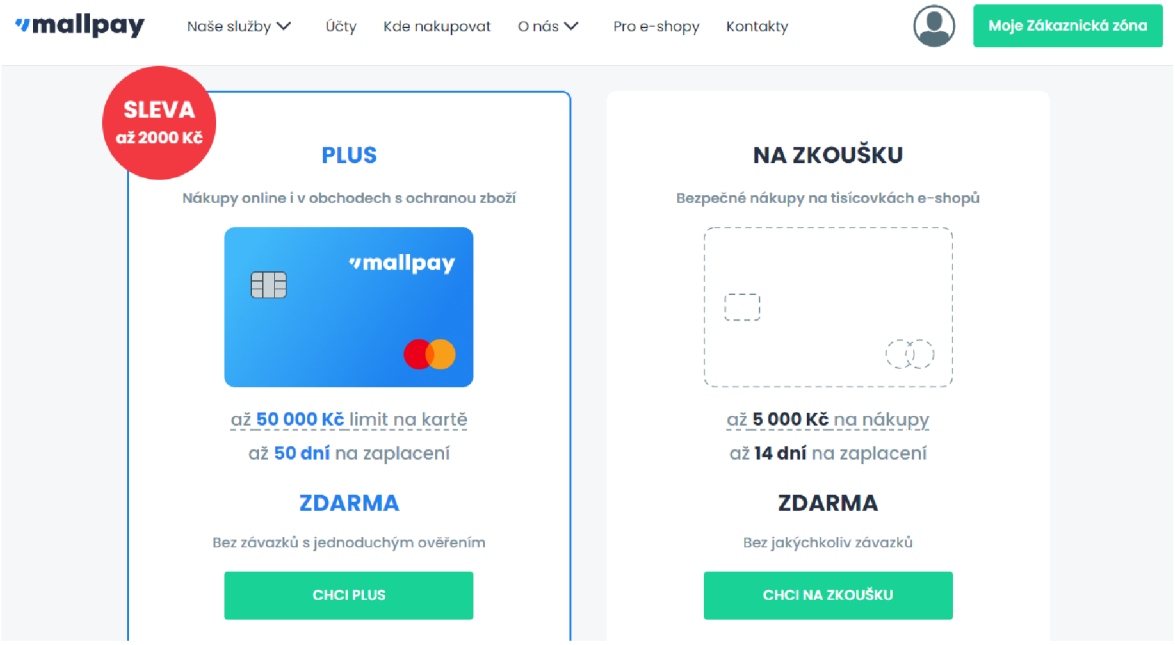
Obrázek 17 – Mallpay 2



Zdroj: Mallpay, 2022.

Bohužel po přihlášení do nově vytvořeného účtu bylo zjištěno, že bezplatné užívání služby možné není a je třeba si předplatit určitý „*tarif*“ mallpay (viz následující obrázek). Ačkoliv tedy bylo v předchozích krocích opakovaně zdůrazňováno, že je možné využít bezplatného tarifu, pro jeho spuštění bylo nutné zadat platební kartu. Dále už by tedy nebylo možné mít naprostou jistotu o tom, zda by finanční prostředky byly z karty strženy či nikoliv. Na základě této komplikace bylo od otestování využití bankovní identity při uskutečňování plateb pomocí mallpay upuštěno.

Obrázek 18 – Mallpay 3



Zdroj: Mallpay, 2022, vlastní zpracování – prostředí po přihlášení do nově vytvořeného účtu mallpay.

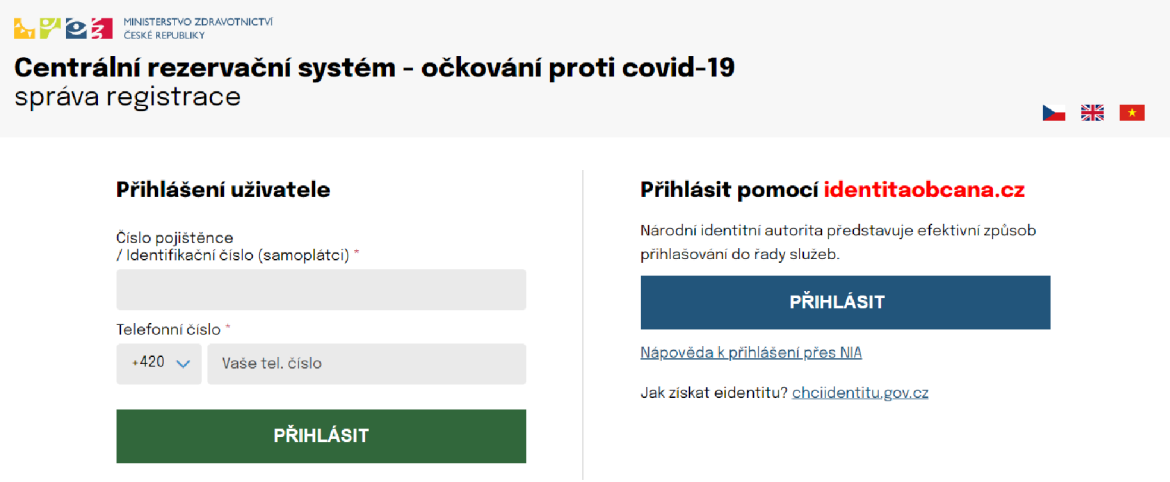
3.1.2 Veřejný sektor

Jak již bylo zmíněno dříve, bankovní identita také ve veřejném sektoru nachází stále širší uplatnění. Je využívána například Ministerstvem průmyslu a obchodu ČR, Ministerstvem vnitra ČR, Ministerstvem zdravotnictví ČR, Generálním ředitelstvím cel, Generálním finančním ředitelství a dalšími orgány veřejné moci. Aktuální seznam veřejných subjektů využívajících bankovní identitu je dostupný na webu Identity občana spravovaném Ministerstvem vnitra ČR (Identita občana, 2022).

3.1.2.1 Ministerstvo zdravotnictví ČR

Testování využitelnosti bankovní identity bude provedeno na několika příkladech, přičemž prvním z nich bude přihlášení do Centrálního rezervačního systému - očkování proti covid-19, jehož přihlašovací prostředí je dostupné na webu spravovaném Ministerstvem zdravotnictví ČR (Centrální rezervační systém, 2022). Vstupní brána do systému vypadá následovně:

Obrázek 19 – Přihlášení do Centrálního rezervačního systému 1



Zdroj: Centrální rezervační systém, 2022.

Uživatel má k přihlášení do systému dvě možnosti, a to přihlášení prostřednictvím zadání čísla pojištěnce a telefonního čísla nebo přihlášení pomocí serveru identitaobcana.cz, jehož součástí je právě i bankovní identita. Pro účely testování bude využita druhá jmenovaná možnost.

Přihlášení pomocí bankovní identity v současné době umožňují následující banky: Air Bank, Česká spořitelna, ČSOB, Komerční banka, MONETA Money Bank nebo Raiffeisenbank, jak zobrazuje následující obrázek:

Obrázek 20 – Přihlášení do Centrálního rezervačního systému 2

Zdroj: Centrální rezervační systém, 2022.

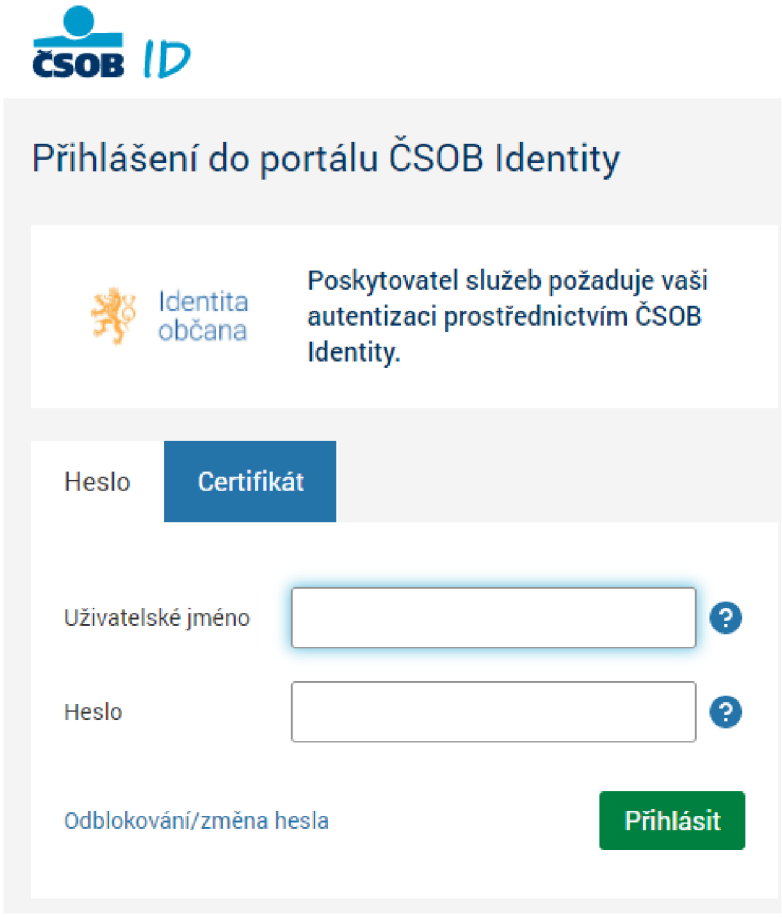
Z nabízených možností byla využita ČSOB, jež byla z uvedených subjektů vybrána namátkově a u níž byl za účelem provedení analýzy vytvořen běžný účet. Následně bylo zjištěno, že ČSOB navíc nabízí dokonce dva způsoby přihlášení o různých úrovních ověření, které jsou blíže popsány na následujícím obrázku:

Obrázek 21 – Přihlášení do Centrálního rezervačního systému 3

Zdroj: Centrální rezervační systém, 2022.

Plně ověřený přístup je možný pouze na základě dvoufaktorového ověření, načež je možné v portálu dělat všechny potřebné operace. Naproti tomu rychlý přístup do aplikace probíhá skrze zjednodušené přihlášení s jednofaktorovým ověřením totožnosti, přičemž následně je ale umožněn přístup pouze k základním informacím a službám. Z nabízených možností byl využit plně ověřený přístup, za účelem vykonávání všech dostupných akcí v aplikaci rezervačního systému. Pro získání přístupu v plném rozsahu následuje krok zadání přihlašovacího jména a hesla, která jsou nastavena pro přihlášení do internetového bankovnictví ČSOB:

Obrázek 22 – Přihlášení do Centrálního rezervačního systému 4

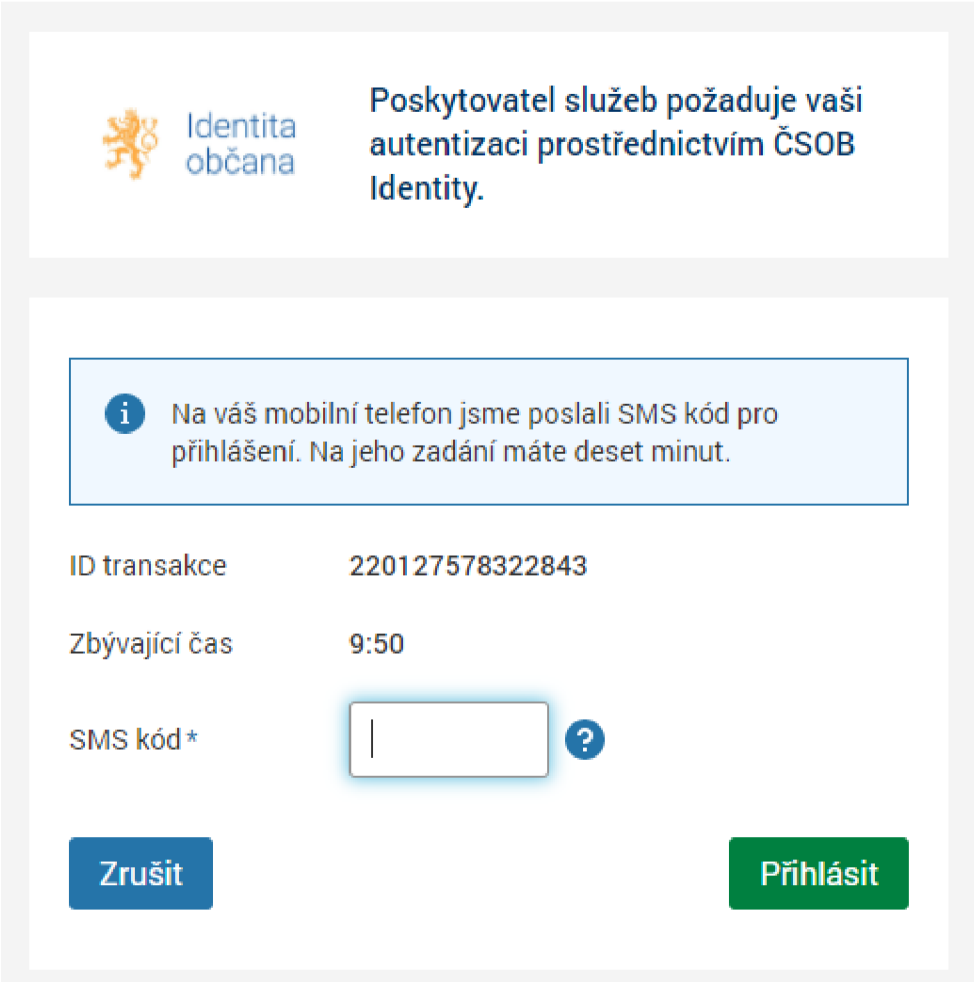


Zdroj: Centrální rezervační systém, 2022.

Vzhledem k tomu, že v případě zvolené možnosti přihlášení do internetového bankovnictví je ověření osoby dvoufaktorové, po zadání uživatelského jména (identifikace) a hesla (prvek znalosti při autentizaci) následuje požadavek ověření pomocí druhého faktoru, a to jednorázového kódu zaslaného prostřednictvím SMS (prvek vlastnictví při autentizaci), přičemž kód je možné zadat pouze v následujících 10 minutách. V případě, že by uživatel kód zadat nestihl, což se může snadno stát například v případě, že musí dojít pro telefon, pokud ho v tu chvíli nemá u sebe, bude nezbytné postup přihlašování opakovat.

Na základě praktického zaznamenání postupu při přihlášení bylo zjištěno, že ověření osoby pomocí druhého faktoru v případě Centrálního rezervačního systému není možné uskutečnit prostřednictvím biometrických údajů (prvek vlastnost při autentizaci), vždy je třeba zadat jednorázový SMS kód (prvek vlastnictví při autentizaci).

Obrázek 23 – Přihlášení do Centrálního rezervačního systému 5



Zdroj: Centrální rezervační systém, 2022.

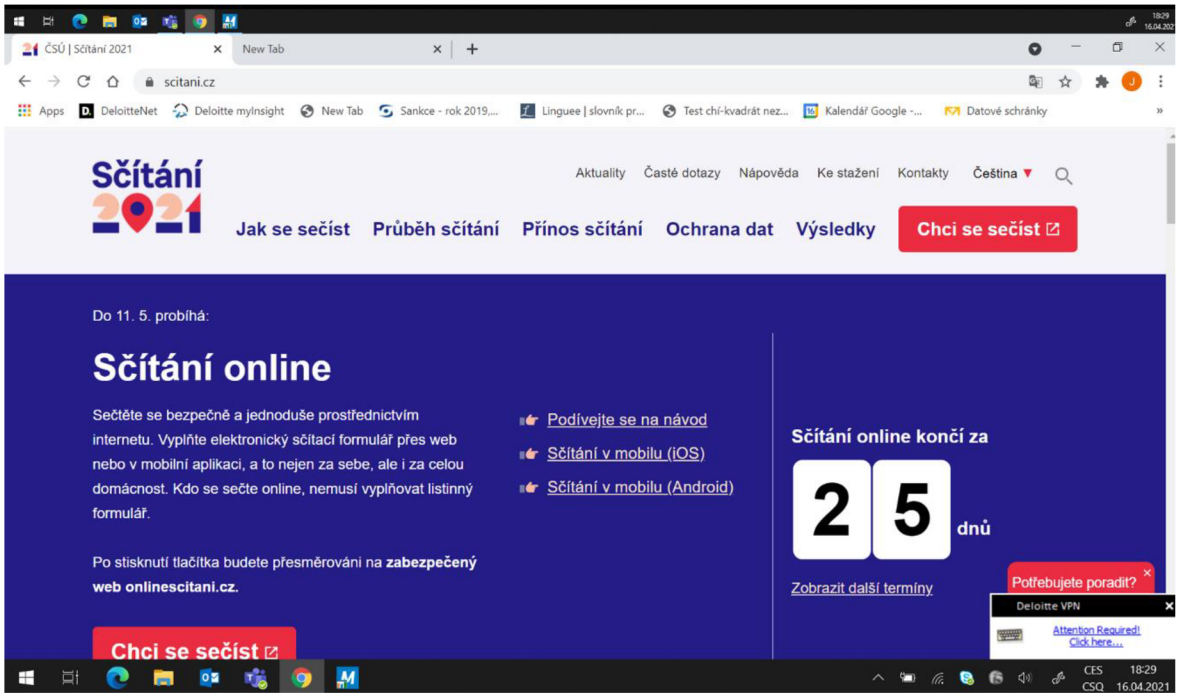
Na základě vložení správného SMS kódu je již uživateli zpřístupněno prostředí Centrálního rezervačního systému.

3.1.2.2 Sčítání lidu

Přihlášení pomocí bankovní identity bylo dále testováno pro ověření totožnosti osoby při sčítání lidu v květnu 2021. Historicky se jednalo o úplně první sčítání, které probíhalo v České republice hybridní formou, a tedy bylo se možné jej účastnit i na dálku. Vzhledem k tomu, že při sčítání nepochybně bylo nezbytně nutné mít jistotu, že informace poskytuje skutečně ta která osoba, přihlášení do portálu bylo třeba dostatečně zabezpečit. Vedle možnosti přihlášení prostřednictvím údajů k datové schránce osoby tak bylo umožněno ověřit totožnost také pomocí bankovní identity, která byla pro účely předkládané diplomové práce zvolena a otestována.

Přístupová stránka pro vyplnění požadovaných údajů při sčítání byla dostupná na oficiální webové stránce Českého statistického úřadu (Český statistický úřad, 2021), přičemž dané prostředí v květnu 2021 vypadalo následovně:

Obrázek 24 – Sčítání lidu 2021



Zdroj: Český statistický úřad, 2021.

Za účelem sečtení osoby bylo dostupné tlačítko „*Chci se sečíst*“, načež vyskočilo stejné okno jako v případě přihlašování do Centrálního rezervačního systému - Obrázek 20 – Přihlášení do Centrálního rezervačního systému 2. Také následující postup byl totožný, tudíž nebude zde duplicitně popsán.

Při sčítání lidu nebyl nabídnut rychlý přístup dostupný při přihlašování do Centrálního rezervačního systému, pokud uživateli postačoval omezený přístup do prostředí. V tomto případě tedy vždy bylo vyžadováno zadání uživatelského jména (identifikace), načež navázalo dvoufaktorové ověření. To spočívalo v zadání hesla (prvek znalost při autentizaci) a jednorázového SMS kódu, který byl jediným dostupným druhým autentizačním faktorem (prvek vlastnictví při autentizaci). Možnost využít biometrické údaje (prvek vlastnost při autentizaci) tedy do procesu ověření při sčítání lidu nebyla zapojena.

3.1.2.3 Portál občana

Bankovní identitu lze dále využít k přihlášení do Portálu občana, což je webová stránka, jejímž zřizovatelem je Ministerstvo vnitra ČR. Jedná se o platformu, díky které lze komunikovat s celou řadou orgánů veřejné moci prostřednictvím dálkového přístupu. Jak je uvedeno na webových stránkách Portálu občana, jedná se o „*bránu k elektronickým službám státu*“ (Portál občana, 2022).

Primárně lze Portál občana využít k získání dokladů či různých výpisů z centrálních státních registrů, evidencí a databází a seznam úřadů a institucí, se kterými lze díky platformě komunikovat, se stále rozšiřuje. V současnosti tak lze skrze Portál občana vyřizovat záležitosti týkající se např. finanční správy, eReceptů, očkovacího portálu, ČSSZ, Úřadu práce ČR a dalších subjektů nadaných veřejnou mocí. Výjimkou není ani možnost komunikace s obcí trvalého pobytu občana, pokud je tato obec součástí Portálu občana. Nepochybnou výhodou je také možnost stažení Portálu občana i jako mobilní aplikace, do níž je rovněž možné přihlásit se pomocí bankovní identity.

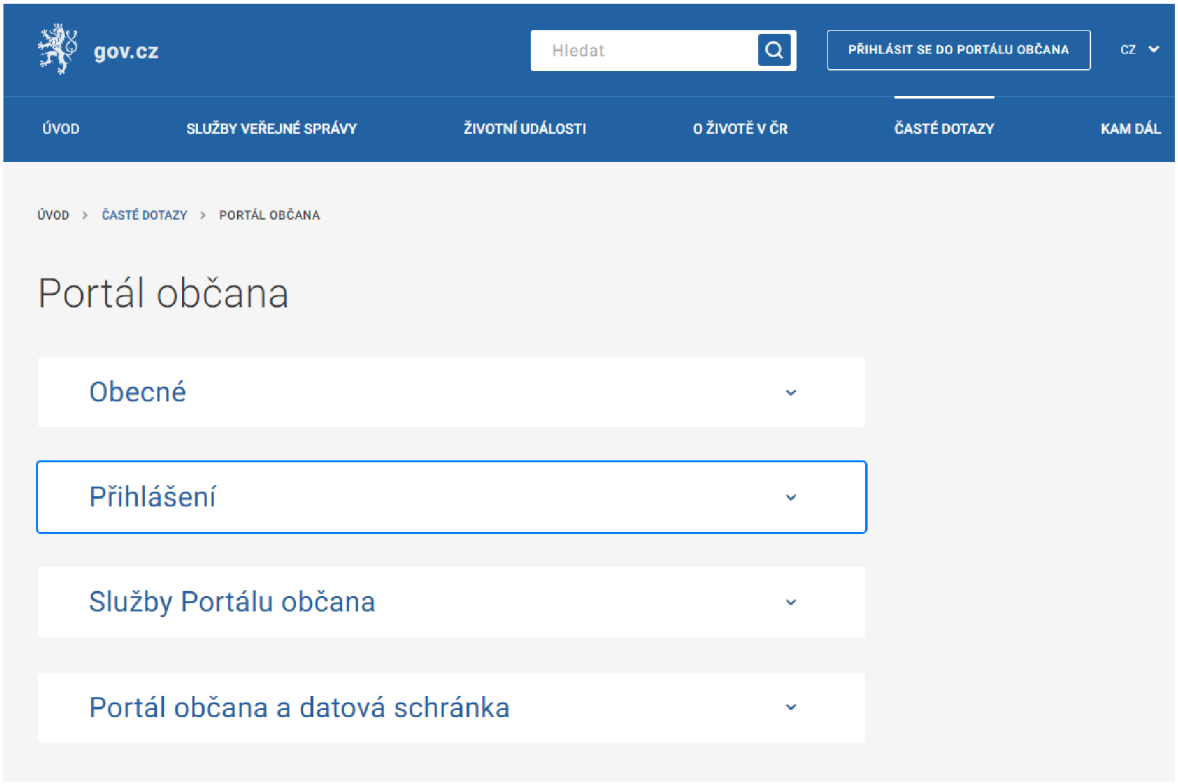
Pro názornost uvedeme níže příklady konkrétních operací, jež lze pomocí Portálu občana vyřídit na dálku (Portál občana, 2022):

- operace související s datovou schránkou (založení, přidání nové schránky, archivace zpráv apod.),
- žádost o nový řidičský průkaz z důvodu konce platnosti,
- potvrzení o studiu,
- výpis bodového hodnocení řidiče,
- výpis z rejstříku trestů,
- výpis z živnostenského rejstříku,
- výpis z registru obyvatel,
- výpis z katastru nemovitostí,
- výpis z registru silničních vozidel či registru řidičů,
- výpis z živnostenského rejstříku,
- kontrola tachometru vozidla,
- podání daňového přiznání,
- přístup do očkovacího portálu,
- přístup k eReceptu,

- přístup do ePortálu ČSSZ (informace o pracovní neschopnosti, o důchodovém pojištění),
- přístup do portálu Úřadu práce,
- vyřízení živnostenského oprávnění,
- registrace provozovatele dronu a online testu pilota dronu,
- přístup k Dluhopisu Republiky,
- přístup k portálům krajů, měst a obcí.

Přihlášení do Portálu občana bylo provedeno prostřednictvím prostředí dostupného na webové adrese českého e-governmentu spravované Ministerstvem vnitra ČR (Gov.cz, 2021).

Obrázek 25 – Přihlášení do Portálu občana 1



Zdroj: Gov.cz, 2021.

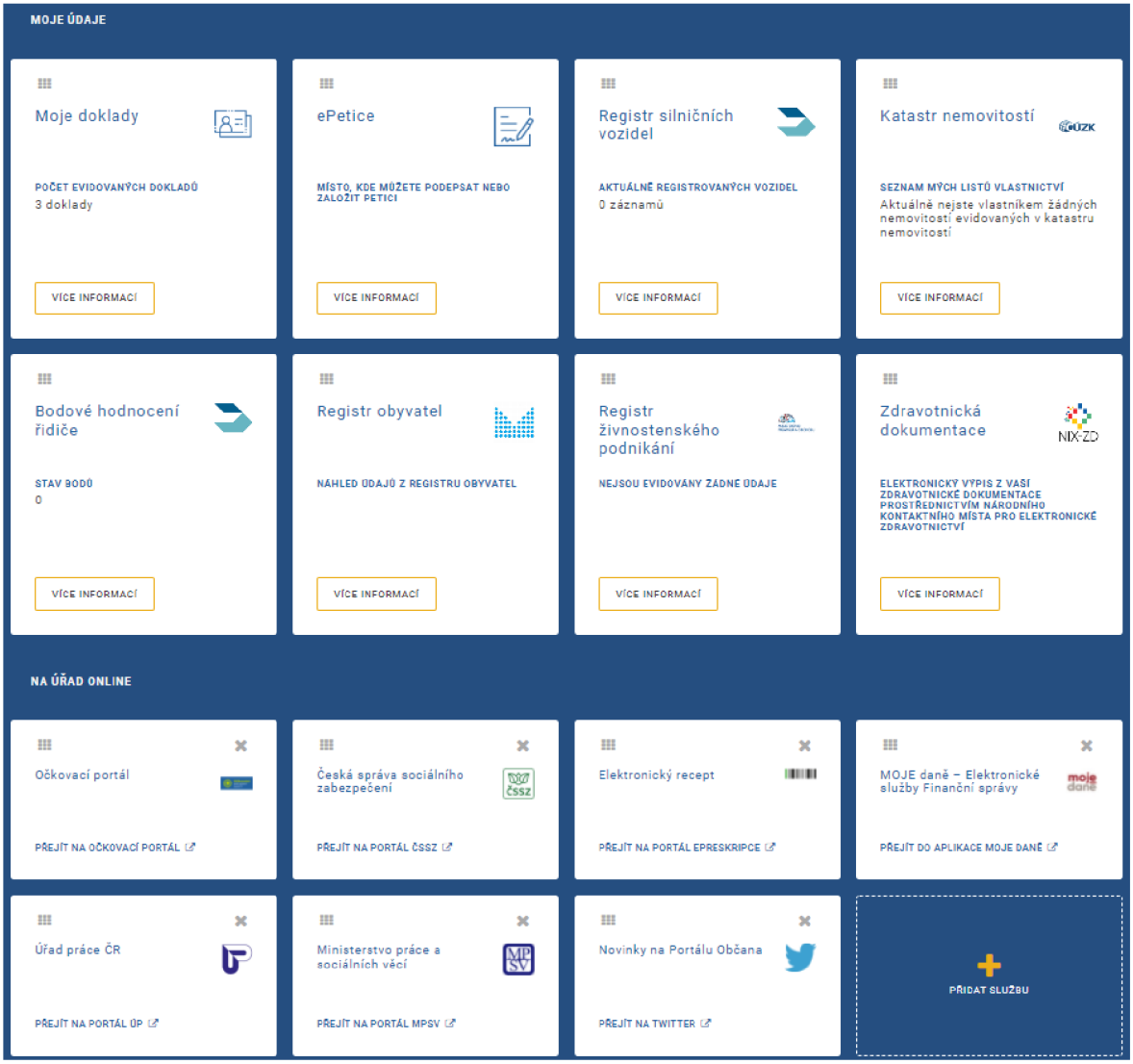
Po kliknutí na „*Přihlásit se do portálu občana*“ vpravo nahoře na Obrázek 25 výše bylo z nabízených možností vybráno přihlášení pomocí Identity občana. Následující postup byl obdobný jako při přihlášení do Centrálního rezervačního systému na Obrázek 20 a Obrázek 21, přičemž zvoleno bylo opět přihlášení pomocí bankovní identity ČSOB.

V případě přihlašování do Portálu občana není vůbec k dispozici rychlý přístup, tudíž jedinou možností přihlášení je plně ověřený přístup.

Následně jsou zadány přihlašovací údaje do internetového bankovnictví ČSOB, načež je uživateli zaslán jednorázový SMS kód na jeho mobilní zařízení. I v tomto případě tedy v návaznosti na identifikaci (zadání uživatelského jména) probíhá dvoufaktorová autentizace, při které je totožnost osoby ověřena pomocí prvků znalost (heslo) a vlastnictví (jednorázový SMS kód na mobilní telefon).

Ověření totožnosti na základě druhého autentizačního faktoru je v Portálu občana možné pouze prostřednictvím jednorázového SMS kódu, usnadnění přihlášení díky biometrickým údajům prozatím dostupné není. Při přihlašování do Portálu občana tedy dosud není zakomponován prvek vlastnosti při autentizaci ověřované osoby. Na základě úspěšné autentizace pomocí SMS kódu je uživateli zpřístupněno prostředí Portálu občana, ve kterém je možné plnoprávně vykonat jakoukoliv akci. Na úvodní stránce jsou uživateli nabídnuty například následující možnosti:

Obrázek 26 – Portál občana



Zdroj: Gov.cz, 2021.

3.2 Vyhodnocení zkušeností veřejnosti

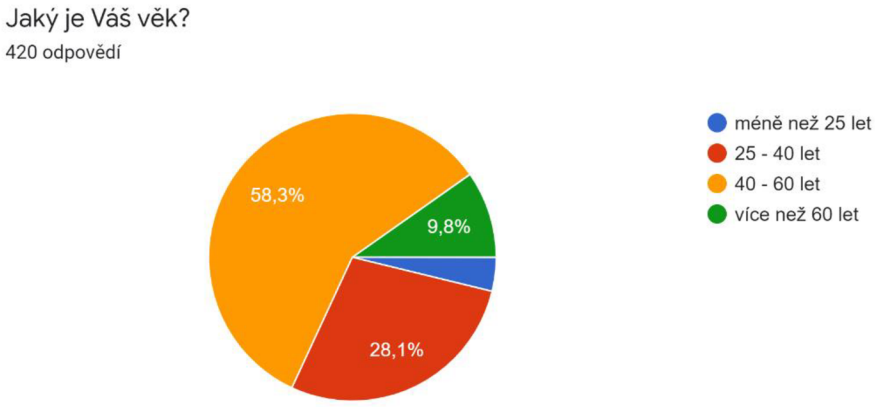
Za účelem zmapování využívání bankovní identity v praxi bylo provedeno dotazníkové šetření. Prostředkem k získání dostatečného vzorku relevantních odpovědí byl stručný dotazník, jenž se skládal celkem z pěti otázek, které byly respondenty zodpovídány skrze službu Formuláře Google, v níž byl dotazník vytvořen. Dotazník byl sestaven neutrálně a odpovědi respondentů byly vkládány při zajištění naprosté anonymity. K šíření dotazníku tedy bylo využito internetu, když osoby byly neadresně oslovovány prostřednictvím e-mailových zpráv, v nichž jim byl rozesílán odkaz na dotazník. Povoleno bylo také přeposílání dotazníku oslovenými respondenty dalším osobám. Sběr dat

k dotazníkovému šetření probíhal v termínu od 21. února 2022 do 14. března 2022 a nebylo cíleno na žádnou konkrétní skupinu respondentů. Výsledkem sběru dat bylo získání odpovědí od 420 účastníků šetření.

1. otázka – *„Jaký je váš věk?“*

Cílem první otázky bylo zjistit stáří respondentů, a to za účelem získání představy o zastoupené věkové skupině, jež převažovala. Záměrem zde bylo rozčlenit respondenty do čtyř věkových skupin, tudíž bylo možné vybrat pouze jedinou odpověď. Nejvíce respondentů spadalo do skupiny 40 – 60 let, a to konkrétně 58,3 % (245 osob). Tato skutečnost byla důležitým zjištěním, jelikož je třeba brát v úvahu, že výsledky dotazníku většinově reprezentují chování osob starších než 40 let. Na druhém místě se s 28,1 % (118 osob), což je více než čtvrtina všech odpovědí, umístila skupina respondentů ve věku 25 – 40 let. Dále pak téměř 10 % (41 osob) účastníků byly osoby starší než 60 let, což bylo poměrně překvapivým výsledkem, a to zejména s ohledem na skutečnost, že jich bylo více než osob mladších 25 let. Těch se dotazníkového šetření účastnilo jen 3,8 % ze všech respondentů (16 osob).

Obrázek 27 – Otázka 1



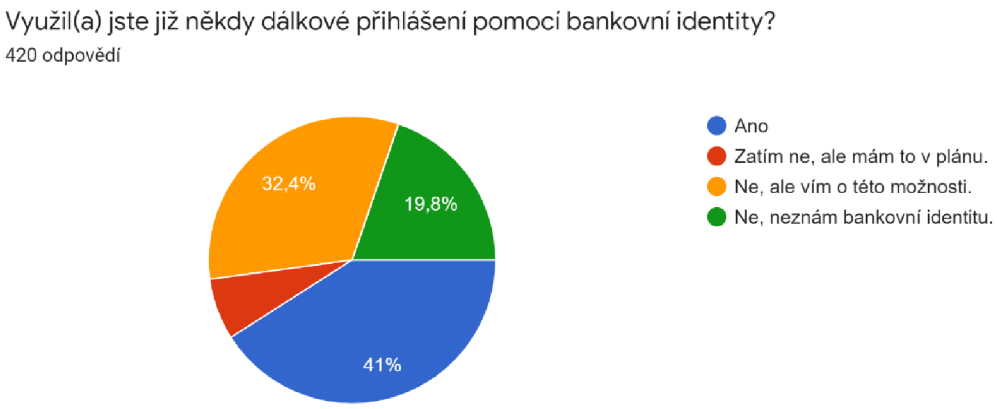
Zdroj: Vlastní zpracování, 2022.

2. otázka – *„Využil(a) jste již někdy dálkové přihlášení pomocí bankovní identity?“*

Další otázka byla položena za účelem zjistit dosavadní zkušenosti respondentů s využíváním bankovní identity, přičemž byly dány k dispozici 4 odpovědi znázorněné na grafu níže, z nichž bylo možné vybrat opět pouze jedinou. Na základě odpovědí lze

konstatovat, že ověření své totožnosti pomocí bankovní identity již někdy využilo celkem 41 % respondentů (172 osob). Odpověď „*Zatím ne, ale mám to v plánu*“ zvolilo 6,9 % respondentů (29 osob), což nasvědčuje ještě potenciálnímu zvýšení počtu osob využívajících bankovní identitu v blízké budoucnosti. Dále pak 32,4 % oslovených (136 osob) potvrdilo, že o bankovní identitě mají již nějaké povědomí, což lze také považovat za pozitivní výsledek vypovídající o tom, že úroveň informovanosti společnosti o bankovní identitě je poměrně vysoká. Stále je zde ale prostor pro zlepšování, a to jelikož téměř 20 % odpovídajících (83 osob), tedy 1/5 bankovní identitu vůbec nezná, v čemž lze shledávat indikaci potřeby zvýšení propagace ze strany orgánů státu nebo z pozice soukromých subjektů využívajících danou službu.

Obrázek 28 – Otázka 2



Zdroj: Vlastní zpracování, 2022.

3. otázka – „*K jakým účelům jste přihlášení pomocí bankovní identity využil(a)?*“

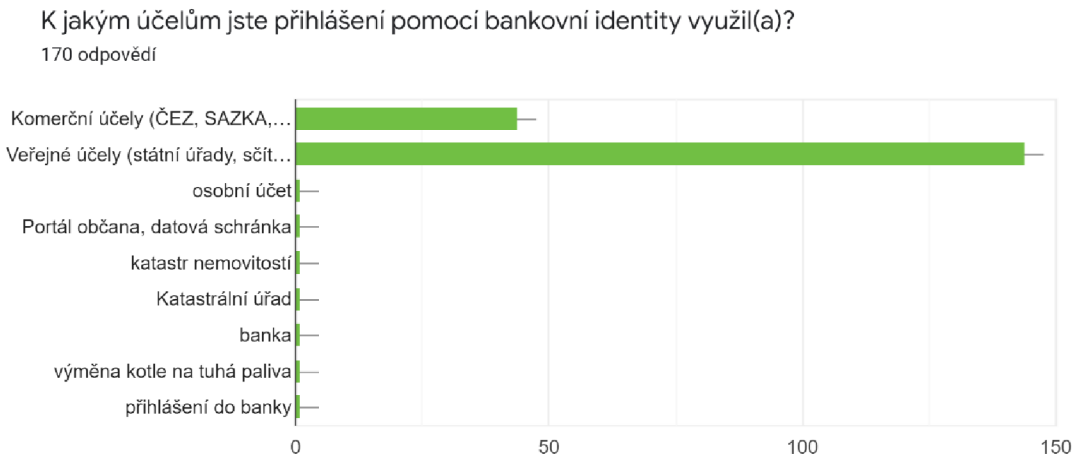
K třetí otázce se respondent přesunul pouze v případě, že na předchozí otázku odpověděl kladně, tedy že bankovní identitu již využil. Celkový počet respondentů se tak snížil na méně než polovinu a v následujících částech dotazníku odpovídalo 171 osob. Třetí otázka byla již formulována konkrétněji a cílila na zjištění specifické služby či oblasti služeb, při kterých respondent bankovní identitu využil. Předdefinovány byly dvě odpovědi: „*Veřejné účely (státní úřady, sčítání lidu, očkovací certifikát, Portál občana apod.)*“ a „*Komerční účely (ČEZ, SAZKA, mallpay, Pražská plynárenská, OZP, apod.)*“. Navíc mohli respondenti vložit jinou, vlastní odpověď, jež by odhalovala, k jakým nenabízeným účelům bankovní identitu využili. Zároveň bylo možné zaškrtnout všechny odpovědi

zároveň, tudíž v tomto případě nečinil procentuální součet výsledků 100 %. Větší vypovídací hodnotu tak mohou mít celkové počty respondentů, jež zvolili tu kterou možnost, a to s vědomím, že celkem bylo u této otázky zaznamenáno 170 odpovědí. Nejvíce respondentů zaškrtlo předdefinované možnosti, když k veřejným účelům údajně bankovní identitu již užilo 84,7 % odpovídajících (144 osob) a ke komerčním účelům pak čtvrtina respondentů, konkrétně 25,9 % (44 osob). Další odpovědi byly zadány vždy jedním respondentem, kteří dle svých odpovědí využili bankovní identitu v rámci následujících činností či aplikačních prostředí:

- „*osobní účet,*
- *Portál občana, datová schránka,*
- *katastr nemovitostí,*
- *Katastrální úřad,*
- *banka,*
- *výměna kotle na tuhá paliva,*
- *přihlášení do banky.*“

Na základě vložených vlastních odpovědí tedy lze konstatovat, že i výše citované individuálně vložené odpovědi by bylo možné zařadit do dvou předdefinovaných kategorií, tedy mezi veřejné a komerční účely.

Obrázek 29 – Otázka 3

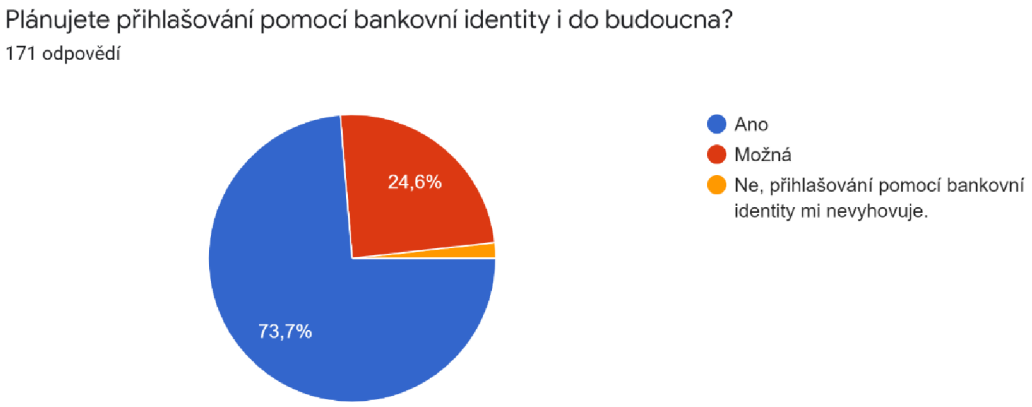


Zdroj: Vlastní zpracování, 2022.

4. otázka – *„Plánujete přihlašování pomocí bankovní identity i do budoucna?“*

Následující čtvrtá otázka byla opět uzavřená a bylo pro respondenty povinné vybrat jedinou možnost. Cílem bylo zjistit, zda respondent má v plánu bankovní identitu využívat i do budoucna, či nikoliv. Vzhledem k tomu, že otázka byla zobrazena pouze těm respondentům, kteří již bankovní identitu využili, je možné následující odpovědi považovat za vyplývající z předchozích zkušeností uživatelů s bankovní identitou. Zopakovat využití bankovní identity plánují téměř 3/4 respondentů, tedy 73,7 % (126 osob). Dále pak téměř čtvrtina odpovídajících zvolila možnost *„Možná“*, konkrétně 24,6 % (42 osob). Pouze marginální část respondentů, 1,8 % (3 osoby), uvedla, že jim přihlašování pomocí bankovní identity nevyhovuje a nemají v plánu jej znovu využívat. Tento výsledek svědčí o velice dobré uživatelské zkušenosti s přihlašování bankovní identitou a lze očekávat, že do budoucna se bude využívání této služby i s ohledem na získaná data významně rozšiřovat.

Obrázek 30 – Otázka 4



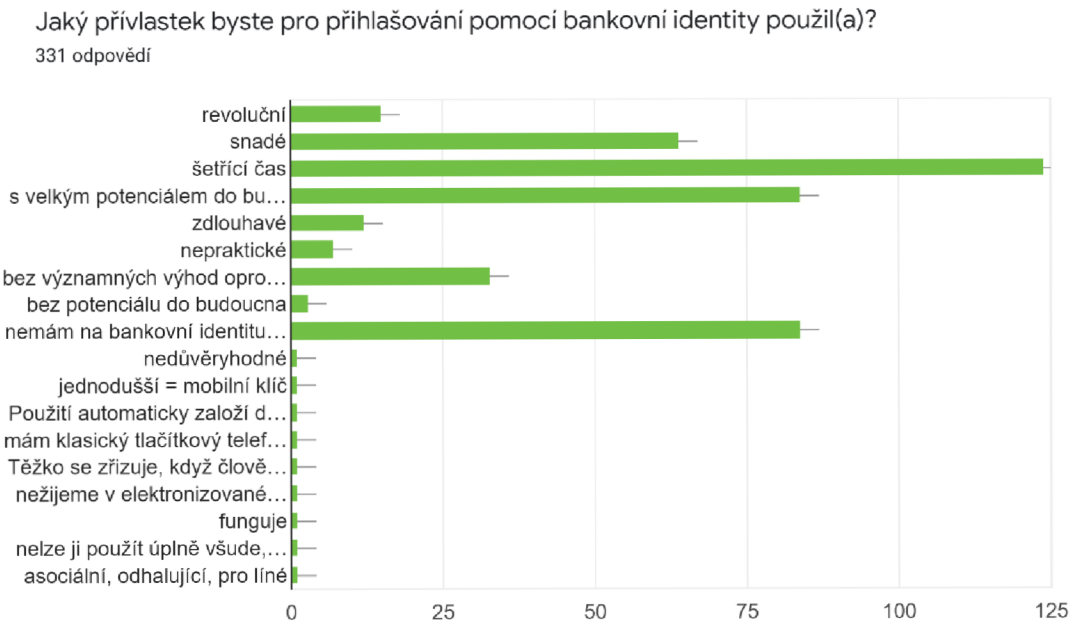
Zdroj: Vlastní zpracování, 2022.

5. otázka – *„Jaký přívlastek byste pro přihlašování pomocí bankovní identity použil(a)?“*

Poslední pátá otázka byla formulována s cílem zjistit osobní dojmy jednotlivých respondentů. Na výběr byly dány některé předdefinované přívlastky, kterými mohli respondenti přihlašování pomocí bankovní identity popsat (prvních 9 možností na grafu níže). Předdefinované odpovědi byly navrženy rovnoměrně tak, aby polovina byla spíše pozitivního charakteru (*„revoluční, snadné, šetřící čas, s velkým potenciálem do budoucna“*), polovina negativního vyznění (*„zdlouhavé, nepraktické, bez významných výhod*

oproti jiným metodám, bez potenciálu do budoucna“) a jedna odpověď neutrální („*nemám na bankovní identitu názor*“). Zároveň bylo ale možné zadat i jakýkoliv svůj vlastní přívlastek (zbývající možnosti na grafu níže). Odpovědí bylo možné zaškrtnout více, přičemž celkově bylo respondenty označeno 331 možností. Nejčastěji vybranou odpovědí bylo, že bankovní identita šetří čas, která byla zvolena v 37,5 % odpovědí (124 odpovědí). Celkově lze ale na základě sběru dat výsledek zobecnit a konstatovat, že významně převažovalo pozitivní hodnocení bankovní identity, když kromě úspory času byly kladně hodnoceny její velký potenciál do budoucna a snadné užívání. Velká část respondentů zvolila neutrální odpověď, že na bankovní identitu názor nemá, která byla označena v 25,4 % odpovědí (84 odpovědí). V ne úplně nevýznamném počtu se ale vyskytovaly i negativní odpovědi, kterých bylo z celkového počtu 16,6 % (55 odpovědí), a to zejména názor, že bankovní identita nemá výhod oproti jiným metodám, ke kterému se respondenti přihlásili v 10 % odpovědí (33 odpovědí). Tato skutečnost dosvědčuje, že existuje stále podstatný prostor pro rozvoj samotné služby a především její uživatelské přívětivosti. Jednou nabytá špatná zkušenost uživatele se podstatně složitěji přebíjí, tudíž ideálním stavem je, pokud uživatel získá již první zkušenost s bankovní identitou dobrou, z čehož plyne, že čím rychleji bude ke zlepšování docházet, tím lépe. Detailní rozložení odpovědí respondentů lze nahlédnout na grafu níže.

Obrázek 31 – Otázka 5



Zdroj: Vlastní zpracování, 2022.

4 Zhodnocení výsledků

Prakticky orientovaná kapitola 3 byla zaměřena na splnění dvou cílů, přičemž druhý z nich byl zařazen až v samotném průběhu zpracování předkládané diplomové práce, lze jej tedy považovat za cíl doplňkový. Primárním cílem bylo otestovat využitelnost bankovní identity a popsat jednotlivé kroky při jejím užívání, a to jak při použití pro účely veřejné, tak pro účely komerční. Druhým doplňkovým cílem bylo získat dostatečná data k vyhodnocení zkušeností uživatelů s přihlašováním pomocí bankovní identity, k čemuž bylo navrženo dotazníkové šetření. Výsledky obou oddílů zkoumání praktické části předkládané diplomové práce budou shrnuty v následujících podkapitolách.

4.1 Výsledky testování využitelnosti bankovní identity

Za účelem analýzy postupu při přihlašování pomocí bankovní identity byli vybráni jednotliví zástupci subjektů, kteří při využívání svých služeb umožňují přihlašování pomocí bankovní identity, a to jak ze sektoru veřejného, tak soukromého. Při výběru zástupců byla preferována co nejvyšší četnost využívání služby toho kterého subjektu, ale zároveň také další aspekty, například cena služby, přičemž upřednostněny byly služby bezplatné, při jejichž testování by nevznikaly zbytné vedlejší náklady.

4.1.1 Bankovní identita v soukromém sektoru

Nejvíce používanou je bankovní identita zatím v sektoru finančních služeb, ze kterého pochází. Za účelem analýzy přihlašování pomocí bankovní identity byla vybrána Equa bank, jež nabízí tuto možnost přihlášení do svého internetového i mobilního bankovnictví.

Postupem detailněji popsaným v příslušné části předkládané diplomové práce bylo zjištěno, že do internetového bankovnictví Equa bank se lze přihlásit pouze na základě dvoufaktorového ověření totožnosti osoby. Uživatel měl při přihlašování navíc možnost volby, buďto se mohl přihlásit pomocí klientského čísla (identifikace, nikoliv ověření), hesla (prvek znalosti při autentizaci) a následně zaslaného jednorázového SMS kódu (prvek vlastnictví při autentizaci), nebo pomocí klientského čísla a následného potvrzení přihlášení v mobilní aplikaci (mobilní telefon – prvek vlastnictví při autentizaci) heslem či biometrickým údajem (prvek vlastnosti při autentizaci). Uživatel měl tedy možnost autentizovat svou osobu buďto na základě kombinace prvků znalost a vlastnictví nebo vlastnictví a vlastnost.

Naproti tomu v případě přihlašování do mobilního bankovnictví Equa bank bylo zjištěno, že je dostačující jednofaktorové ověření totožnosti osoby. Pro zobrazení prostředí mobilního bankovnictví stačilo zadat buďto heslo (znalost) či biometrický údaj (vlastnost), z čehož jednoznačně vyplynulo, že do mobilního bankovnictví je přihlašování pomocí bankovní identity nejsnazší.

Zjednodušení postupu přihlášení však bylo na úkor bezpečnosti účtu, když jednofaktorové ověření je nepochybně zranitelnější než přihlašování na základě vícefaktorové autentizace. Ačkoliv lze namítat, že ověření (opět jednofaktorové) je opakovaně vyžadováno při operacích v mobilním bankovnictví, například při provedení platby, vždy se jedná o ověření stejným faktorem jako v případě přihlašování, ke zvýšení bezpečnosti tedy touto cestou nedochází.

Dalším argumentem proti výše uvedenému tvrzení může být, že vícefaktorová autentizace je provedena při prvním přihlášení po instalaci dané aplikace. Ani tuto skutečnost ale nelze považovat za rovnocennou vícefaktorovému ověření, když po prvním přihlášení již aplikace vyžaduje vždy jen jednofaktorovou autentizaci, a to bez ohledu na čas, který od prvního přihlášení uplynul. Fakticky tak k vícefaktorové autentizaci může dojít až při příští přeinstalaci aplikace, o dvoufaktorovém ověření tak v jednotlivých případech přihlašování do aplikace mluvit nelze.

Dále bylo zamýšleno otestovat postup při přihlašování pomocí bankovní identity při využívání služby mallpay, od čehož bylo ale upuštěno, a to z důvodu zpoplatnění dané služby.

4.1.2 Bankovní identita ve veřejném sektoru

Využití bankovní identity i pro veřejně prospěšné účely je zejména v poslední době významně diskutováno. Díky stále se rozšiřujícímu portfoliu možností využití bankovní identity i při komunikaci s orgány veřejné moci bylo možné otestovat její využitelnost i vůči státu a vzájemně testované situace porovnat.

Prvním analyzovaným případem bylo přihlašování do Centrálního rezervačního systému k očkování proti covid-19, jehož provozovatelem je Ministerstvo zdravotnictví ČR. Pro přihlášení bylo možné využít bankovní identitu těchto subjektů: Air Bank, Česká spořitelna, ČSOB, Komerční banka, MONETA Money Bank nebo Raiffeisenbank. Vzhledem k tomu, že uživatel neměl k dispozici žádnou z těchto bankovních identit, založil si běžný účet u namátkově vybrané banky, kterou byla ČSOB.

Uživatel měl v případě ČSOB navíc více možností přihlášení s odlišnými úrovněmi ověření osoby, respektive s rozdílnými úrovněmi zabezpečení přístupu. Jednalo se buďto o plně ověřený přístup nebo rychlý přístup. Rychlý přístup byl umožněn uživateli na základě zadání uživatelského jména (identifikace) a následného jednofaktorového ověření totožnosti, a to pomocí zadání hesla, které figurovalo při autentizaci jako faktor znalost. Na základě rychlého přístupu ale bylo možné zobrazit pouze základní informace a služby a nebylo možné provádět jakékoliv operace, např. vytvořit rezervaci k očkování. Nahlédnout ale mohl uživatel do systému i na základě jednofaktorového ověření, což se jeví výhodným, jelikož pokud uživatel potřebuje jen zjistit určitý údaj, může si celý proces tímto způsobem zjednodušit a zkrátit.

Plně ověřený přístup byl uživateli umožněn pouze na základě doufaktorové autentizace, při které bylo vedle hesla možné ověřit totožnost pouze prostřednictvím zadání jednorázového SMS kódu (prvek vlastnost při autentizaci), který musel být zadán během 10 minut od jeho vygenerování. Na rozdíl od přihlašování do internetového či mobilního bankovnictví tedy vůbec nebylo možné využít biometrických údajů.

Další možností využití bankovní identity ve veřejném sektoru bylo sčítání lidu, které probíhalo v květnu roku 2021. Sčítání lidu je velice významnou událostí z pohledu statistických dat, která jsou jím generována, tudíž je nepochybné, že bylo potřeba náležitě zajistit, aby údaje byly zadávány ztotožněnými osobami, a tudíž výsledky sčítání byly relevantní a správné. Vzhledem k tomu, že šlo o první sčítání, kterého bylo možné se účastnit na dálku, bylo velice důležité zvolit dostatečně bezpečný mechanismus ověření totožnosti, bankovní identita se tedy jevila být vhodnou cestou.

V případě sčítání lidu nebylo uživateli nabídnuto více úrovní ověření pro přístup do aplikačního prostředí. Vstup byl umožněn jen a pouze na základě dvoufaktorového ověření, kterému předcházela identifikace pomocí uživatelského jména. Prvním autentizačním faktorem bylo vždy zadání hesla (prvek znalost při autentizaci) a druhým jednorázový SMS kód (prvek vlastnictví při autentizaci). V tomto případě tedy vůbec nebyl zakomponován autentizační prvek vlastnost, kterým by mohla být osoba ověřena pomocí biometrických údajů.

Další oblastí, ve které bylo testováno přihlašování pomocí bankovní identity ve veřejném sektoru, byla platforma Portálu občana, která sjednocuje řadu jednotlivých státních institucí, se kterými lze touto cestou komunikovat. Portál občana lze považovat za jakýsi rozcestník, ze kterého může být uskutečňována řada operací vůči orgánům veřejné moci na

základě jediného ověření totožnosti. Přihlašování do Portálu občana probíhalo obdobně jako v případě Centrálního rezervačního systému nebo při sčítání lidu 2021. Jedinou možností přihlášení tedy bylo ověření dvoufaktorové. Prvním krokem opět byla identifikace pomocí uživatelského jména osoby, načež proběhla autentizace zadáním hesla (prvek znalost při autentizaci) a následně zaslaného jednorázového SMS kódu (prvek vlastnictví při autentizaci). Opět tedy nebylo možné uplatnit prvek vlastnost a zjednodušit uživateli celý postup možným ověřením pomocí biometrických údajů.

Ačkoliv je možnost vyřizovat záležitosti ve vztahu k orgánům veřejné moci na dálku jistě žádoucím pokrokem, nelze přehlédnout, že e-government má stále velké mezery a prostor ke zlepšování. Jednou z inovací, která by byla na místě, lze shledávat právě zapojení biometrických údajů do procesu autentizace osob. Jak bylo prokázáno při testování využití bankovní identity v soukromém sektoru, autentizace pomocí otisku prstu či jiných biometrických údajů ověření podstatně zjednodušuje a zrychluje. Zároveň je však třeba mít na mysli skutečnost také zjištěnou při testování v soukromém sektoru, a to že zjednodušení může někdy jít na úkor bezpečnosti. Aby bylo dosaženo snadnějšího ověření a zároveň nebyla snížena bezpečnost, lze uvažovat například o zařazení více autentizačních prvků vlastnost současně. Například se může jednat o identifikaci pomocí jména a navazující autentizaci pomocí otisku prstu a současně pomocí faceID, přičemž tento postup by bylo možné považovat za autentizaci dokonce třífaktorovou, která by ke snížení bezpečnosti nepřispěla.

4.2 Vyhodnocení zkušeností veřejnosti

Za účelem zjištění zkušeností široké veřejnosti s přihlašováním pomocí bankovní identity bylo navrženo dotazníkové šetření. Dotazník byl vytvořen pomocí služby Formuláře Google, která umožňovala jeho snadné rozšíření rozesláním URL odkazů. Celkem se dotazníkového šetření zúčastnilo 420 osob, které zodpověděly 5 stručných otázek. Vyplnění dotazníku zabralo respondentům přibližně 3 minuty, přičemž tato časová nenáročnost pravděpodobně významně napomohla velké účasti v průzkumu, a tím sběru statistických dat v dostatečném rozsahu, neboť 420 účastníků lze nepochybně považovat za statisticky relevantní vzorek.

První otázkou bylo zjištěno věkové složení respondentů, přičemž největší skupinu tvořily osoby mezi 40 a 60 lety, konkrétně 58,3 % (245 osob). Skupinou s druhou největší četností byli respondenti mezi 25 a 40 lety, kteří tvořili 28,1 % všech účastníků (118 osob).

Z uvedeného vyplývá, že osobami v rozmezí 25 až 60 let bylo generováno přibližně 85 % všech odpovědí. Zejména vysokou účast spíše starších osob ve výši téměř 60 % je třeba brát v úvahu při interpretaci výsledků, jelikož výsledky šetření v souvislosti s technologicky pokročilými nástroji, jako je bankovní identita, bývají u starších osob výrazně odlišné od mladší generace. Předpoklad spíše konzervativního náhledu starších respondentů na předmět průzkumu ale na základě výsledků dalších odpovědí spíše nebyl potvrzen.

Zkušenost s přihlášením pomocí bankovní identity mělo 41 % respondentů (172 osob). Do budoucna pak má v plánu tento způsob přihlašování využít, ačkoliv tak dosud neučinily, 6,9 % osob (29 osob). Dále bez vyjádření jakýchkoliv plánů či očekávání 32,4 % respondentů (136 osob) potvrdilo, že o této možnosti již slyšeli. Z uvedených počtů vyplývá, že potenciál nárůstu využívání bankovní identity do budoucna je značný. Necelých 20 % respondentů (19,8 %, 83 osob) pak v dotazníkovém šetření uvedlo, že bankovní identitu vůbec neznají. Z tohoto zjištění tedy lze vyvodit závěr, že propagace bankovní identity dosud neměla plošný dosah, když téměř k 1/5 respondentů se informace o novém způsobu přihlašování na dálku vůbec nedostala. Bohužel navržený dotazník v zájmu zachování co největší anonymity neumožňoval provázat odpovědi jednotlivých respondentů a není tak možné zjistit, ze které věkové skupiny byly osoby, jež bankovní identitu neznaly, na základě kteréžto informace by bylo možné komunikaci a propagaci služby daleko lépe zacílit.

Druhá otázka byla směrodatná pro další otázky zobrazované respondentům. Následující části dotazníku totiž vyplňovaly již pouze osoby, které potvrdily, že s přihlašováním pomocí bankovní identity mají zkušenost, jichž bylo 171 (z původního počtu 420 osob). Cílem třetí otázky bylo zjistit, k jakým účelům tyto osoby bankovní identitu využily. Předdefinovanými odpověďmi byly „*Veřejné účely (státní úřady, sčítání lidu, očkovací certifikát, Portál občana apod.)*“ a „*Komerční účely (ČEZ, SAZKA, mallpay, Pražská plynárenská, OZP, apod.)*“, přičemž respondenti mohli navíc v otevřené odpovědi vložit jakýkoliv jiný účel. Zároveň bylo umožněno zaškrtnout více odpovědí současně, vzhledem k tomu, že ale celkově u této otázky bylo zaznamenáno 170 odpovědí, respondenti evidentně této možnosti nevyužívali a více odpovědí najednou nekombinovali. Nejčastěji je dle výsledků bankovní identita užívána k veřejným účelům při komunikaci s orgány veřejné moci, což potvrdilo 84,7 % odpovídajících (144 osob). K soukromým účelům naopak bankovní identitu prý užila asi čtvrtina odpovídajících, tedy 25,9 % (44 osob), což je poměrně překvapivým závěrem, jelikož byl očekáván výsledek spíše opačný, a tedy že využití pro komerční účely bude převažovat. Vlastních doplněných odpovědí respondentů

bylo pouze 7 a šlo obvykle o případy, které byly zařaditelné i do dvou předdefinovaných kategorií. Otevřené otázky tedy nepřinesly žádných nových zjištění.

U čtvrté otázky už museli respondenti opět vybírat pouze z nabízených možností, přičemž mohli zvolit jedinou, jelikož se odpovědi vzájemně vylučovaly. Záměrem položené otázky bylo zjistit, zda mají respondenti v plánu použít bankovní identitu i do budoucna. Na rozdíl od otázky druhé ale byla tato zobrazena pouze respondentům, kteří se již pomocí bankovní identity dříve přihlašovali, tudíž bylo předpokládáno, že odpověď se bude odvíjet právě od již nabyté zkušenosti, respektive od spokojenosti nebo nespokojenosti s užitím tohoto způsobu ověření totožnosti. Pod tímto úhlem pohledu má do budoucna v plánu zopakovat přihlašování pomocí bankovní identity 73,7 % respondentů (126 osob), což jsou téměř tři čtvrtiny odpovídajících. S určitou nejistotou, ale stále relativně kladně, odpovědělo 24,6 % účastníků šetření (42 osob), a tedy že příští užití plánují „*možná*“. Pouze minimum respondentů tvořících 1,8 % (3 osoby) nemá v plánu se již přihlašovat pomocí bankovní identity, jelikož jim nevyhovovala. Tento výsledek vypovídá o většinově převládající pozitivní zkušenosti s užíváním bankovní identity. Sekundárním efektem této skutečnosti může být, že pokud budou spokojení uživatelé svou zkušenost šířit dál, může být takto předávaná pozitivní praxe tou nejlepší možnou reklamou bankovní identity, jelikož osobní zkušenost je zpravidla důvěryhodnější než oficiální propagace služby.

V páté otázce byli respondenti vyzváni k označení bankovní identity určitým přívlastkem, přičemž jim bylo dáno na výběr několik předdefinovaných, jež byly rovnoměrně navrženy tak, aby počet kladně vyznívajících odpovídal počtu negativně vyznívajících. Tento krok byl učiněn zejména v zájmu nepodsouvání respondentům jednostranných dojmů. Odpovědí bylo opět možné zaškrtnout více a celkem jich bylo sběrem dat získáno 331. Celkově u respondentů převažovaly pozitivní dojmy, přičemž úplně nejčastějším názorem bylo, že bankovní identita šetří čas (37,5 %, 124 odpovědí). Vedle toho bylo opakovaně uváděno, že v bankovní identitě se skrývá velký potenciál do budoucna a její užívání je snadné. Část respondentů ale zastávala také negativní názor vůči bankovní identitě, celkem 16,6 % odpovědí (55 odpovědí) bylo spíše záporného vyznění. Neutrálních odpovědí, a tedy že respondenti na bankovní identitu „*nemají názor*“, pak byla asi čtvrtina (25,4 %, 84 odpovědí).

V kontextu výsledků poslední otázky je třeba zdůraznit, že první zkušenost uživatelů je důležitá, jelikož první špatná zkušenost lze napravit poměrně obtížně, tudíž v zájmu zvyšování oblíbenosti přihlašování pomocí bankovní identity je na místě udržovat kvalitu na

dostatečné výši. Naopak ale dobrou zkušenost lze poměrně snadno přebít tou negativní, tudíž je vhodné uspokojivou uživatelskou přívětivost služby nejen udržovat, ale soustavně zvyšovat, jelikož názor uživatelů se celkem rychle může změnit k horšímu.

Závěr

Záměrem sledovaným při vytyčování cílů, jež měly být předkládanou diplomovou prací naplněny, bylo zpracovat problematiku ochrany soukromí na internetu zároveň z různých úhlů pohledu. Tento cíl byl stanoven s ohledem na skutečnost, že zvolené téma je skutečně průsečíkem řady odborných zaměření, přičemž obzvláště otázka informačně technologická a otázka právní úpravy jsou jedněmi z těch nejdůležitějších.

Stanovenými cíli bylo zejména podat a uspořádat podrobně zpracovaná teoretická východiska ochrany soukromí na internetu a současně dostupných možností ověřování totožnosti osob na internetu se speciálním zaměřením na bankovní identitu, načež bylo zamýšleno uskutečnit praktické testování a analyzovat dříve vymezené a popsané způsoby ověřování totožnosti. Lze konstatovat, že jmenované cíle byly na předcházejících stránkách naplněny.

V teoretické části předkládané diplomové práce byl podán výklad aktuálně účinných i již překonaných právních předpisů, jež se věnují ochraně soukromí osob a jejich osobních údajů, a to jak na národní, tak na unijní úrovni. Právě legislativa Evropské unie se prokázala jako pramen práva s podstatně rostoucím významem v této oblasti, když postupně vstupuje v platnost stále více zejména přímo aplikovatelných legislativních aktů, u kterých již není nezbytně třeba zapracování předpisů do jednotlivých právních řádů členských států národními legislativci. Z vyložené teorie také vyplynulo, že tento trend bude pravděpodobně pokračovat také v nejbližší budoucnosti, když jsou na unijní úrovni připravovány další právní předpisy zásadního charakteru pro oblast ochrany osobních údajů obzvláště v online prostředí (nařízení PECR). Opomenut však nebyl ani historický vývoj regulace, jelikož ten sám o sobě vypovídá mnohé o současném stavu. Pozornost byla věnována zejména pokroku v právní úpravě od roku 2015 do současnosti.

Teoretické základy byly položeny i v souvislosti s řadou dalších relevantních problematik, jako jsou způsoby kryptografického šifrování dat, obecné náležitosti zabezpečení dat či soubory cookies. Závěr teoretického úvodu byl již věnován elektronickému podpisu, který plynule navazoval na kryptografické základy, smyslu a působení certifikačních autorit či vysvětlení pojmů identifikace, autorizace a autentizace. Právě poslední jmenovaný termín autentizace byl směrodatným pro ústřední téma ověřování totožnosti na dálku, přičemž fungování současně dostupných technologických prostředků online autentizace bylo také v teoretické rovině nastíněno. Následně byl věnován adekvátní

prostor teoretickému seznámení se již se samotnou bankovní identitou jako prostředkem ověřování totožnosti moderní doby.

Zpracování teoretických východisek v dostatečném rozsahu bylo nezbytným podkladem pro praktickou část práce, jež byla věnována testování ověřování totožnosti pomocí bankovní identity pro různé účely. Vzhledem k tomu, že k využívání bankovní identity přistoupily v řadě případů i veřejnoprávní instituce, byly testované příklady přihlašování pomocí bankovní identity rozděleny na využití pro účely veřejné a soukromé.

Ze soukromého sektoru bylo testováno přihlašování pomocí bankovní identity do internetového bankovnictví a mobilního bankovnictví Equa bank. Výsledkem bylo zjištění, že pro přihlášení do internetového bankovnictví probíhá identifikace pomocí klientského čísla a následuje vždy dvoufaktorová autentizace. U té má uživatel na výběr, zda se ověří pomocí hesla a jednorázového SMS kódu, které představují autentizační prvky znalost a vlastnictví, nebo zda zvolí možnost autentizovat se potvrzením v mobilní aplikaci. V aplikaci může uživatel přihlášení potvrdit heslem, což znamená kombinaci prvků vlastnictví (mobilní telefon) a znalost (heslo), nebo potvrdit přihlášení pomocí biometrického údaje, což je kombinací prvku vlastnictví (mobilní telefon) a vlastnost (biometrický údaj). Naproti tomu v případě přihlašování do mobilní aplikace postačovalo jednofaktorové ověření totožnosti, když přihlášení proběhlo pouze na základě ověření heslem (znalost) či biometrickým údajem (vlastnost). Argumentace vícefaktorovým ověřením totožnosti při instalaci samotné aplikace neobstojí, a to s ohledem na skutečnost, že po této silnější autentizaci na počátku již její opakování vyžadováno není bez ohledu na čas uplynulý od prvního přihlášení. Aplikace tak uživatele k jednotlivým operacím v mobilním bankovnictví pustí na základě ověření jedním faktorem, kterým může být heslo (znalost) či biometrický údaj (vlastnost). Přihlašování pomocí bankovní identity do mobilního bankovnictví tak bylo ze všech testovaných případů nejsnazší, ale bylo tomu tak na úkor bezpečnosti.

Přihlašování pomocí bankovní identity v sektoru veřejném bylo testováno při přihlašování do Centrálního rezervačního systému k očkování proti covid-19, při sčítání lidu 2021 a při přihlašování do Portálu občana. Všechny uvedené platformy vyžadovaly obdobné postupy při přihlášení, a to vždy dvoufaktorové ověření prostřednictvím hesla (znalost) a jednorázového SMS kódu (vlastnictví). Ve veřejné sféře tedy nebylo zaznamenáno využívání biometrických údajů v žádném z testovaných případů, ačkoliv by jejich zavedení mohlo znamenat další významné zjednodušení procesu. Je třeba ale mít na mysli, že cílené

zjednodušování může mít negativní dopad na zabezpečení přihlašování, čemuž by bylo možné předejít například současným zařazením více autentizačních faktorů využívajících různé biometrické údaje osoby (otisk prstu, faceID, snímek sítnice apod.).

Vyhodnocení praktických zkušeností veřejnosti s využíváním bankovní identity bylo provedeno na základě výsledků dotazníkového šetření, kterého se účastnilo 420 respondentů, kteří byli osloveni bez preference jakékoliv konkrétní skupiny. Nadpoloviční většina všech respondentů (58,3 %) byla starší 40 let. V návaznosti na toto zjištění bylo očekáváno, že budou výsledky dotazníku inklinovat spíše ke konzervativnějšímu pojetí využití moderní služby, kterou bankovní identita je, tento předpoklad však nebyl výsledky dotazníkového šetření potvrzen. Zkušenost s přihlašováním pomocí bankovní identity byla potvrzena u 41 % respondentů, což je považováno za poměrně pozitivní výsledek, přesto nejde o nijak závratné číslo, když nezkušení respondenti měli stále převahu. Zmínku si také zaslouží informace, že 20 % všech zúčastněných vůbec bankovní identitu neznala. Další části dotazníku byly zodpovídány již pouze osobami s předchozí zkušeností s tímto způsobem přihlašování. Zkušenost drtivé většiny těchto osob (84,7 %) vycházela z přihlašování do platforem orgánů veřejné moci, což bylo poměrně překvapivým zjištěním, jelikož očekáván byl opačný výsledek, a to že veřejné účely využití bankovní identity budou v menšině. Co se týče charakteru respondenty nabyté zkušenosti, lze mluvit o převažující pozitivní praxi, přičemž celých 37,5 % respondentů bylo toho názoru, že bankovní identita šetří čas.

Závěrem tedy lze konstatovat, že o formalizovanou komunikaci na dálku, a to zejména vůči orgánům veřejné moci, má zájem poměrně velká část společnosti. Spektrum možností, jež by bylo možné zařizovat online, by tedy měly být adekvátně tomuto trendu rozšiřovány, jelikož bankovní identita se ukázala být uživatelsky přívětivým a vhodným autentizačním nástrojem.

5 Seznam použitých zdrojů

1. ADVOKÁTNÍ DENÍK. *Bankovní identita umožnila nový rozměr elektronického ověřování totožnosti*. Advokacie - Advokátní deník - Novinky ze světa advokacie. [online] [cit. 21. 10. 2021]. Dostupné na adrese: https://advokatnidenik.cz/2021/02/09/zakon-o-bankovni-identite-umoznil-novy-rozmer-elektronickeho-overovani-totoznosti/.
2. AIR BANK. *Dejte zelenou jednoduššímu přístupu k online službám*. [online] [cit. 21. 10. 2021]. Dostupné na adrese: https://www.airbank.cz/produkty/bankovni-identita/?airbid1=ppc_a_494929234059_12&gclid=Cj0KCQiAosmPBhCPARIsAHOen-P2OAxgJecl7Fb76XMK1B2fkREVtbAy7g3scno9VKBxO6IYhz1nrdUaAgCREALw_wcB.
3. AMIROVÁ, Kamilla. *Úvod do kryptografie*. [online] Copyright © Kamilla Amirová (xamirova[at]fd.cvut.cz), 2007 [cit. 29. 12. 2021]. Dostupné na adrese: https://sifrovani.fd.cvut.cz/index.html.
4. BANK ID. *Úvod*. BankID. [online] Copyright © BankID 2021. Všechna práva vyhrazena [cit. 27. 01. 2022]. Dostupné na adrese: https://www.bankid.cz/pro-firmy#vyuzivaji-bankid.
5. BANKOVNÍ IDENTITA. *Bankovní identita*. [online] Copyright © BankID 2021. Všechna práva vyhrazena [cit. 27. 11. 2021]. Dostupné na adrese: https://bankovni-identita.cz/banky-a-reseni/.
6. CAREY, P. *Data protection. A practical guide to UK and EU Law*. Second edition. Great Britain: Oxford University Press, 2004, s. 1-8.
7. CASTANO, Silvana, FUGINI, Maria Garzia. Database Security. Indianopolis: Addison Wesley, 1995. 456 s. ISBN 9780201593754.
8. CENTRÁLNÍ REZERVAČNÍ SYSTÉM. *Centrální rezervační systém - očkování proti covid-19, správa registrace - Ministerstvo zdravotnictví České republiky*. [online] Copyright © 2021 Ministerstvo zdravotnictví ČR [cit. 26. 01. 2022]. Dostupné na adrese: https://registrace.mzcr.cz/detail.
9. CONSILIUM. *Oficiální internetové stránky Rady EU a Evropské rady*. Home – Consilium. [online] [cit. 29. 10. 2021]. Dostupné na adrese: https://www.consilium.europa.eu/cs/.
10. CONSILIUM. *Oficiální internetové stránky Rady EU a Evropské rady. Jednotný digitální trh v Evropě*. [online] [cit. 29. 10. 2021]. Dostupné na adrese: https://www.consilium.europa.eu/cs/policies/digital-single-market/.
11. CVRČEK, Dan. *Kryptologie a informační bezpečnost*. 2005. Vysoké učení technické v Brně, Fakulta informačních technologií. Studijní materiál. [online] Copyright © Dan Cvrček, 2005 [cit. 25. 10. 2021]. Dostupné na adrese: https://adoc.pub/draft-not-proofread-kryptologie-fakulta-informanich-technolo.html.
12. CZ.NIC, správce národní domény CZ. *Jak na Internet - Elektronický podpis*. [online] Copyright © 2022 CZ.NIC, z. s. p. o. [cit. 26. 01. 2022]. Dostupné na adrese: https://www.jaknainternet.cz/page/1249/elektronicky-podpis/.
13. CZ.NIC, správce národní domény CZ. *Jak na Internet - Jednotný digitální trh*. Jak na Internet - Jak na Internet. [online] Copyright © 2021 CZ.NIC, z. s. p. o. [cit. 25. 06. 2021]. Dostupné na adrese: https://www.jaknainternet.cz/page/3052/jednotny-digitalni-trh/.

14. ČECH, Pavel. *Kdo nese odpovědnost za obsah aplikací, webů a cloudových služeb? 2020*. Domů - SEDLAKOVA LEGAL. [online] Copyright © 2021 SEDLAKOVA LEGAL s.r.o. Všechna práva vyhrazena. [cit. 25. 10. 2021]. Dostupné na adrese: https://www.sedlakovalegal.cz/aplikace-weby-a-cloudove-sluzby-kdo-nese-odpovednost-za-obsah-uzivatelu/.
15. ČESKÁ BANKOVNÍ ASOCIACE. O *projektu*. Bankovní identita – Otevřete si svět online služeb. [online] Copyright © 2021, Česká bankovní asociace, všechna práva vyhrazena [cit. 22. 10. 2021]. Dostupné na adrese: https://bankovni-identita.cz/o-projektu/.
16. ČESKÁ BANKOVNÍ ASOCIACE. *Bankovní identita*. Bankovní identita – Otevřete si svět online služeb. [online] Copyright © 2021, Česká bankovní asociace, všechna práva vyhrazena. [cit. 22. 10. 2021]. Dostupné na adrese: https://bankovni-identita.cz/banky-a-reseni/.
17. ČESKÝ STATISTICKÝ ÚŘAD. *Sčítání lidu 2021*. ČSÚ – Český statistický úřad. [online] [cit. 10. 05. 2021]. Dostupné na adrese: https://www.czso.cz/csu/scitani2021.
18. DATABÁZE NÁRODNÍ KNIHOVNY ČR. *Kryptografie*. Dostálek, 2001, Říha, 2002. Založení záznamu 2003/02/10. Systémové číslo 000000624 2022. [online] [cit. 29. 12. 2021]. Dostupné na adrese: https://aleph.nkp.cz/F/?func=direct&doc_number=000000624&local_base=KTD.
19. DONÁT, Josef a Jan TOMÍŠEK. *Právo v síti: průvodce právem na internetu*. V Praze: C. H. Beck, 2016. ISBN 978-80-7400-610-4.
20. DURČÁK, Pavel. *Symetrické a asymetrické šifrování*. Článek ve Verlag Dashöferze dne 18. 9. 2018. [online] [cit. 29. 12. 2021]. Dostupné na adrese: https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/.
21. EQUA BANK. *Vstup do internetového bankovnictví*. Equa bank. [online] Copyright © Equa bank a.s. 2011 – 2016. Všechna práva vyhrazena. [cit. 11. 03. 2022]. Dostupné na adrese: https://www.equabanking.cz/IBS/.
22. ENISA. *Data protection. Security of personal data*. The European Union Agency for Cybersecurity. ENISA. [online] [cit. 29. 08. 2021]. Dostupné na adrese: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data.
23. ESET.COM. *Co je phishing?* Malware Protection & Internet Security. ESET. [online] Copyright © 1992 [cit. 25. 10. 2021]. Dostupné na adrese: https://www.eset.com/cz/phishing/.
24. EUROPA.EU. *Jednotný digitální trh v Evropě - Consilium*. Home – Consilium. [online] [cit. 14. 10. 2021]. Dostupné na adrese: https://www.consilium.europa.eu/cs/policies/digital-single-market/.
25. GDPR.CZ. *Biometrické údaje*. GDPR. Obecné nařízení o ochraně osobních údajů — prakticky. Provozovatel: Mgr. Eva Škorničková. [online] [cit. 09. 03. 2022]. Dostupné na adrese: https://www.gdpr.cz/gdpr/heslo/biometricke-udaje/.
26. GDPR SOLUTIONS. *Co jsou to biometrické údaje?* GDPR Solutions a.s. Ochrana osobních dat nové dimenze. [online] Copyright © 2022 Ochrana osobních dat nové dimenze [cit. 09. 03. 2022]. Dostupné na adrese: https://www.gdprsolutions.cz/slovnik/biometricke-udaje/.
27. GOLDREICH, O. *Foundations of Cryptography: Basic Applications*. Vol 2. Cambridge University Press, 2004.

28. GOV.CZ. *Portál občana*. Ministerstvo vnitra ČR. [online] Copyright © Ministerstvo vnitra [cit. 11. 11. 2021]. Dostupné na adrese: https://portal.gov.cz/caste-dotazy/portal-obcana.
29. HOAX.CZ. *Podvodné a řetězové e-maily, poplašné zprávy, phishing, scam*. [online] Copyright © 2000-2022 Josef Džubák & HOAX.cz Code & design DIGITAL ACTION s.r.o. [cit. 11. 11. 2021]. Dostupné z: https://hoax.cz/cze/.
30. IDENTITA OBČANA. *Čím je možné se přihlásit v prostředí národního bodu*. Informační web elektronické identity. Elektronická identita - informační web. [online] Copyright © 2021 Správa základních registrů, Ministerstvo vnitra ČR [cit. 26. 01. 2022]. Dostupné z: https://info.identitaobcana.cz/idp/.
31. ILICHMAN, Dominik. *Akt o digitálních trzích aneb nová unijní regulace online prostředí*. Právní rozhledy: časopis pro všechna právní odvětví. Praha: C. H. Beck/SEVT, 1993-. ISSN 1210-6410, 9/2021, 29. ročník / 14. května, s. 324-330.
32. INTERNETEM BEZPEČNĚ. *Hoax*. Internetem bezpečně - Užívejme internet bezpečnějším způsobem. [online] Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 25. 10. 2021]. Dostupné na adrese: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/hoax/.
33. IT SLOVNÍK.CZ. *Co je to Autorizace?* IT SLOVNÍK.CZ. [online] Copyright © 2008 - 2022 IT-Slovnik.cz team [cit. 10. 03. 2022] Dostupné na adrese: https://it-slovnik.cz/pojem/autorizace.
34. IURIUM WIKI. *Ochrana osobních údajů*. [online] Copyright © 2017 [cit. 14. 10. 2021]. Dostupné na adrese: https://wiki.iurium.cz/w/Ochrana_osobn%C3%ADch_%C3%BAdaj%C5%AF.
35. JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal a MATEJKA, Ján. *Internetové právo*. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.
36. KARLOVKA ONLINE. *Biometrické údaje na UK: 1.) Pojmy a příklady*. Karlovka Online. Distanční vzdělávání. [online] Copyright © Univerzita Karlova [cit. 10. 03. 2022]. Dostupné na adrese: https://karlovkaonline.cz/chci-ucit/zpracovani-biometrickych-udaju-na-uk-1-pojmy-a-priklady/.
37. KLAUSOVÁ, Tereza. *Ochrana osobních údajů na internetu a sociálních sítích Facebook, Google*. Diplomová práce, Západočeská univerzita v Plzni, Fakulta právnická, Katedra občanského práva, 2017.
38. KNOPOVÁ, Martina. *Úvod do bezpečnosti informačních technologií*. Ikaros, Elektronický časopis o informační společnosti. ISSN 1212-5075. Roč. 15. č. 6 (2011). [online] [cit. 10. 03. 2022]. Dostupné na adrese: http://ikaros.cz/bezpecnost-dat-v-informacnich-systemech.
39. LENTNER, Gabriel & PARYCEK, Peter. *Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study*. Transforming Government: People, Process and Policy. 2016. 10. 8-25. 10.1108/TG-11-2013-0047.
40. MALLPAY. *Mallpay*. Vybírejte srdcem, platťe hlavou. mallpay.cz. [online] [cit. 14. 03. 2022]. Dostupné na adrese: https://mallpay.cz/.
41. MALLPAY. O *Mallpay*. Vybírejte srdcem, platťe hlavou. mallpay.cz. [online] [cit. 14. 03. 2022]. Dostupné na adrese: https://mallpay.cz/o-mallpay.
42. MALLPAY. *Registrace*. Vybírejte srdcem, platťe hlavou. mallpay.cz . [online] [cit. 14. 03. 2022]. Dostupné na adrese: https://mallpay.cz/registrace.

43. MANAGEMENTMANIA.COM. *Autentizace, ověření, identifikace (Authentication)*. ManagementMania.com. [online] Copyright © 2011 [cit. 10. 03. 2022]. Dostupné na adrese: https://managementmania.com/cs/autorizace.
44. MANAGEMENTMANIA.COM. *Autorizace, oprávnění (Authorization)*. ManagementMania.com. [online] Copyright © 2011 [cit. 10. 03. 2022]. Dostupné na adrese: https://managementmania.com/cs/autorizace.
45. MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha: CZ.NIC, 2013. 256 s. ISBN 978-80-904248-7-6.
46. MATES, Pavel, JANEČKOVÁ, Eva a BARTÍK, Václav. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 9 - 22, Praktik (Leges). ISBN: 978-80-87576-12-0.
47. MATOUŠOVÁ, M. – Hejlík, L. *Osobní údaje a jejich ochrana*. 1. vyd. Praha: ASPI, 2003. 415 s. ISBN 80-86395-50-2.
48. MATOUŠOVÁ, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. PRAHA: Aspi Publishing, s. r. o., 2004. 160 s. ISBN 80-7357-037-8.
49. MINISTERSTVO VNITRA ČR. *Biometrika.* Ministerstvo vnitra České republiky. [online] Copyright © 2021 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 09. 03. 2022]. Dostupné na adrese: https://www.mvcr.cz/clanek/biometrika.aspx.
50. MINISTERSTVO VNITRA ČR. *eIDAS, služby vytvářející důvěru a elektronická identifikace - Ministerstvo vnitra České republiky*. Úvodní strana - Ministerstvo vnitra České republiky. [online] Copyright © 2021 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 26. 01. 2022]. Dostupné na adrese: https://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx.
51. MINISTERSTVO VNITRA ČR. *Informační web elektronické identity. Elektronická identita - informační web*. [online] Copyright © [cit. 26. 01. 2022]. Dostupné na adrese: https://info.identitaobcana.cz/idp/.
52. MINISTERSTVO VNITRA ČR. *Seznam poskytovatelů služeb*. Ministerstvo vnitra České republiky. [online] Copyright © 2021 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 11. 03. 2022]. Dostupné na adrese:https://info.identitaobcana.cz/sep/.
53. MINISTERSTVO VNITRA ČR. *Zásady zpracování osobních údajů*. Ministerstvo vnitra České republiky. [online] Copyright © 2021 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 25. 11. 2021]. Dostupné na adrese: https://www.mvcr.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx.
54. MULLER, Thomas. *Vnitřní trh EU - základní principy*. MPO, Ministerstvo průmyslu a obchodu. [online] Copyright © Copyright 2005 [cit. 25. 06. 2021]. Dostupné na adrese: https://www.mpo.cz/cz/zahranicni-obchod/podnikani-v-eu/vnitrni-trh-eu/vnitrni-trh-eu---zakladni-principy--3363/.
55. OLBRICH, Libor. *Základy kryptografie a kryptoanalýzy*. Mgr. Libor Olbrich. [online] Copyright © 2002 [cit. 29. 12. 2021]. Dostupné na adrese: https://adoc.pub/zaklady-kryptografie-a-kryptoanalyzy.html.
56. OPTAGLIO. *Proč identifikace není autentizace*. BLOG společnosti OPTAGLIO. O bezpečnostních hologramech, nanotechnologiích, ochraně dokumentů a především o lidech. [online] [cit. 11. 03. 2022]. Dostupné na adrese: https://optaglioblog.wordpress.com/2017/07/11/proc-identifikace-neni-autentizace/.
57. OZP. *Odborná zdravotní pojišťovna - KRYPTOGRAFIE - informace o elektronické komunikaci*. [online] Copyright © [cit. 29. 12. 2021]. Dostupné na adrese: https://www.ozp.cz/o-nas.

58. POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.
59. PORTÁL OBČANA. *Co je Portál občana*. Časté dotazy. [online] Copyright © Ministerstvo vnitra [cit. 14. 02. 2022]. Dostupné na adrese: https://portal.gov.cz/caste-dotazy/portal-obcana.
60. REZGUI, Abdelmounaam, BOUGUETTAYA, Athman, ELTOWEISSY, Marwa. *Privacy on the Web: Facts, Challenges, and Solutions*. IEEE Security & Privacy Magazine. 2003. 1. 40-49. 10.1109/MSECP.2003.1253567.
61. SLÍŽEK, David. *GDPR last minute: A co cookies? Musí mít weby povinně lištu se souhlasem?* Lupa.cz, 22. května 2018. [online] Copyright © 1998 – 2021 Internet Info, s.r.o. [cit. 21. 10. 2021]. Dostupné na adrese: https://www.lupa.cz/clanky/gdpr-last-minute-a-co-cookies-musi-mit-weby-povinne-listu-se-souhlasem/.
62. SPRAVASITE.EU. *Co je sniffing?* Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT. [online] Copyright © [cit. 25. 10. 2021]. Dostupné na adrese: https://www.sprava-site.eu/sniffing/.
63. TICHÝ, Miloslav. *Právní regulace cookies pro marketingové účely*. EPRAVO.CZ. epravo.cz – Váš průvodce právem - Sbírka zákonů, judikatura, právo. [online] Copyright © EPRAVO.CZ [cit. 21. 10. 2021]. Dostupné na adrese: https://www.epravo.cz/top/clanky/pravni-regulace-cookies-pro-marketingove-ucely-111752.html.
64. TOMÁŠEK, Zdeněk. *Zneužívání osobních dat a možnosti jejich ochrany*. Bakalářská práce, Univerzita Hradec Králové, Přírodovědecká fakulta, Katedra informatiky, 2016. [online] [cit. 14. 10. 2021]. Dostupné na adrese: https://theses.cz/id/jklu5t/19375193.
65. TOPRANKER.CZ. *Co Je To Cookies?* Co Je SEO - Optimalizace Pro Vyhledávače 2021. Praha. [online] [cit. 21. 10. 2021]. Dostupné na adrese: https://topranker.cz/slovnik/cookies/.
66. U. S. Department of Defense. *„Information Assurance (IA) Policy for Space Systems Used by the Department of Defense" Instruction.* [online] [cit. 10. 03. 2022]. Dostupné na adrese: http://www.dtic.mil/whs/directives/corres/pdf/858101p.pdf.
67. ÚOOÚ. *Úřad pro ochranu osobních údajů: Titulní stránka*. [online] Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 14. 10. 2021]. Dostupné na adrese: https://www.uoou.cz/.
68. WIKIPEDIE. *Wikipedie, otevřená encyklopedie*. [online] [cit. 17. 10. 2021]. Dostupné na adrese: https://cs.wikipedia.org/wiki/Hlavn%C3%AD_strana.
69. YOUR EUROPE. *Ochrana údajů a soukromí na internetu*. YOUR Europe - Oficiální internetová stránka Evropské unie. [online] [cit. 17. 10. 2021]. Dostupné na adrese: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_cs.htm.

6 Další seznamy

Seznam obrázků

Seznam použitých zkratek

ČBA	Česká bankovní asociace
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost
Listina	Ústavní zákon č. 2/1993 Sb., Listině základních práv a svobod, ve znění pozdějších předpisů

Nařízení GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
Nařízení PECR	Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES
NIA	Národní bod pro identifikaci a autentizaci
novela směrnice e-Privacy	Směrnice Evropského parlamentu a Rady 2009/136/EC
Občanský zákoník	Zákon č. 89/2012 Sb., občanském zákoníku, ve znění pozdějších předpisů
směrnice e-Privacy	Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací
ZoBI	Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů
ZoEI	Zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů
ZoEP	Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů
Zrušený ZOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
ZSIS	Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů