Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Sociální sítě a jejich rizika v prostředí institucí veřejné správy v Královehradeckém kraji

Bc. Kristýna Benešová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Kristýna Benešová

Veřejná správa a regionální rozvoj – c.v. Hradec Králové

Název práce

Sociální sítě a jejich rizika v prostředí institucí veřejné správy v Královehradeckém kraji

Název anglicky

Social networks and their risks in the environment of public administration institutions in the Hradec Králové region

---

Cíle práce

Hlavním cílem práce je stanovení rizik, se kterými se v rámci využívání sociálních sítí instituce veřejné správy potýkají a navrhnout řešení pro jejich minimalizaci.

Dílčí cíle práce jsou:
1. charakterizování specifik veřejné správy z pohledu sociálních sítí
2. stanovení rizik využití
3. studie nasazení a využívání sociálních sítí
4. analýza šetření zaměřená na správce sociálních sítí
5. komparace využití sociálních sítí a rizik mezi státní správou a samosprávou
6. návrh ochrany/obrany proti rizikům, se kterými se instituce potýkají
7. formulace závěru a doporučení

Metodika

Metodika řešené práce je založena na analyticko-syntetickém přístupu. V první fázi bude provedeno studium a analýza odborných informačních zdrojů. Na základě syntézy zjištěných poznatků budou charakterizována specifika veřejné správy z pohledu sociálních sítí. Dále budou charakterizována různá rizika sociálních sítí, se kterými se veřejná správa potýká. Dojde k výzkumu a hodnocení nasazení a využívání sociálních sítí. V praktické části budou probíhat rozhovory se správci sociálních sítí, na základě kterých dojde ke komparaci v oblasti využití sociálních sítí a rizik mezi institucemi státní správy a samosprávy. Závěrem budou návrhy ochrany/obrany proti negativním vlivům využívání sociálních sítí ve veřejné správě.

Doporučený rozsah práce

50-60 stran

Klíčová slova

veřejná správa, sociální sítě, rizika, instituce veřejné správy, ochrana osobních údajů

Doporučené zdroje informací

HEGER, V. *Komunikace ve veřejné správě*. Praha: Grada, 2012. ISBN 978-80-247-3779-9.
JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
LIDINSKÝ, V. *eGovernment bezpečně*. Praha: Grada, 2008. ISBN 978-80-247-2462-1.
SVOBODA, V. *Public relations moderně a účinně*. Praha: Grada, 2009. ISBN 978-80-247-2866-7.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

doc. Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 5. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 27. 03. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Sociální sítě a jejich rizika v prostředí institucí veřejné správy v Královehradeckém kraji" 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 28. 3. 2023 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucímu své diplomové práce doc. Ing. Jiřímu Vaňkovi, Ph. D. za vstřícný přístup, odborné vedení, rady a pomoc, kterou mi po celou dobu zpracování této diplomové práce poskytoval. Dále bych chtěla poděkovat všem správcům sociálních sítí institucí veřejné správy, kteří se mnou ochotně komunikovali. V neposlední řadě děkuji své rodině, příteli a přátelům za obrovskou podporu, kterou mi po dobu studia věnovali.

Sociální sítě a jejich rizika v prostředí institucí veřejné správy v Královehradeckém kraji

Abstrakt

Diplomová práce „Sociální sítě a jejich rizika v prostředí institucí veřejné správy v Královehradeckém kraji“ se zabývá využíváním sociálních sítí a jejich riziky ve veřejné správě. Po úvodu následuje vymezení základních pojmů týkajících se sociálních sítí, rizik, komunikace a veřejné správy. Následuje vymezení specifik veřejné správy, specifik komunikace ve veřejné správě a shrnutí nejčastějších rizik. Praktická část zahrnuje provedené dotazníkové šetření zaměřené na správce sociálních sítí institucí veřejné správy. Na základě získaných dat dochází k zhodnocení využití sociálních sítí ve veřejné správě, jejich rizik a následně ke komparaci mezi státní správou a samosprávou, formulaci doporučení a návrhu na minimalizaci rizik.

Klíčová slova: veřejná správa, sociální sítě, rizika, instituce veřejné správy, ochrana osobních údajů, státní správa, samospráva

Social networks and their risks in the environment of public administration institutions in the Hradec Králové region

Abstract

The diploma thesis "Social networks and their risks in the environment of public administration institutions in the Hradec Králové region" deals with the use of social networks and their risks in public administration. The introduction is followed by a definition of basic concepts related to social networks, risks, communication and public administration. This is followed by a definition of the specifics of public administration, the specifics of communication in public administration and a summary of the most common risks. The practical part includes a questionnaire survey carried out on administrators of social networks of public administration institutions. On the basis of the obtained data, the use of social networks in public administration is evaluated, their risks are assessed and then a comparison between public administration and local government is made, recommendations and proposals for minimizing risks are formulated.

Keywords: public administration, social networks, risks, public administration institutions, personal data protection, state administration, local government

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Diplomová práce na téma „Sociální sítě a jejich rizika v prostředí institucí veřejné správy v Královehradeckém kraji“ navazuje na bakalářskou práci „Sociální sítě a rizika“, která byla v teoretické části zaměřena na běžného uživatele sociálních sítí a v praktické části na zaměstnance institucí veřejné správy. Tato práce se nyní v teoretické rovině zaměřuje výhradně na využívání sociálních sítí ve veřejné správě a následně v praktické části na správce sociálních sítí dané instituce.

Sociální sítě jsou součástí každodenního života mnoha lidí, využíváme je ke komunikaci, vyhledávání informací, sdílení obsahu, či odpočinku. Setkáváme se s nimi v případě propagace, zpravodajství, informování o kulturních akcích atp. S rozvojem informačních technologií a v posledních letech především kvůli onemocnění COVID-19 začaly sociální sítě více využívat také instituce veřejné správy. Je ale otázkou, do jaké míry mohou instituce veřejné správy sociální sítě využívat, jaký obsah mohou sdílet a jaká rizika s tím souvisí. Zda je vhodné prostřednictvím sociálních sítí občany nejen informovat, ale také s nimi komunikovat.

Cílem diplomové práce je stanovení rizik, se kterými se v rámci využívání sociálních sítí instituce veřejné správy v Královehradeckém kraji potýkají a navrhnout řešení pro jejich minimalizaci tak, aby využívání sociálních sítí ve veřejné správě bylo bezpečné, efektivní a mohlo tak dojít k nárůstu služeb poskytovaných prostřednictvím nich. K tomuto účelu jsou absolvovány rozhovory se správci sociálních sítí jednotlivých institucí. Na základě analýzy šetření jsou stanoveny návrhy na minimalizaci rizik, se kterými se instituce setkávají.

Diplomová práce je určená jako podklad pro správce sociálních sítí ve veřejné správě při rozhodování, jak sociální sítě využít tak, aby nedocházelo k výskytu rizik. V případě výskytu jsou navrženy doporučení, jak tuto situaci řešit a do budoucna minimalizovat.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je stanovení rizik, se kterými se v rámci využívání sociálních sítí instituce veřejné správy potýkají a navrhnout řešení pro jejich minimalizaci.

Dílčími cíli je v teoretické části práce charakterizovat specifika veřejné správy z pohledu sociálních sítí a stanovit rizika jejich využívání. Dále je v této části práce uvedena studie nasazení a využívání sociálních sítí ve veřejné správě. V praktické částí práce dochází k analýze šetření, které je zaměřené na správce sociálních sítí institucí veřejné správy v Královehradeckém kraji. Na základě analýzy šetření je provedena komparace využití sociálních sítí a rizik mezi státní správou a samosprávou a stanoveny návrhy na ochranu/obranu proti zjištěným rizikům.

2.2 Metodika

Metodika řešené práce je založena na analyticko-syntetickém přístupu. V první fázi je provedeno studium a analýza odborných informačních zdrojů. Na základě syntézy zjištěných poznatků jsou charakterizována specifika veřejné správy z pohledu sociálních sítí. Dále jsou charakterizována různá rizika sociálních sítí, se kterými se veřejná správa potýká. Dochází k výzkumu a hodnocení nasazení a využívání sociálních sítí.

V praktické částí probíhají rozhovory se správci sociálních sítí, na základě kterých dochází ke komparaci v oblasti využití sociálních sítí a rizik mezi institucemi státní správy a samosprávy. Závěrem jsou návrhy ochrany/obrany proti negativním vlivům využívání sociálních sítí ve veřejné správě.

3 Teoretická východiska

V teoretické části jsou vymezeny základní pojmy, které se v práci často objevují a dále se tato část práce zabývá specifiky veřejné správy, studií nasazení sociálních sítí ve veřejné správě a riziky související s jejich využíváním.

3.1 Vymezení základních pojmů

Sociální sítě

Jedná se o prostor, ve kterém uživatele vytvářejí obsah, stejně jako například na Wikipedii. Jejich podstatou je navíc vytváření virtuálních vztahů mezi uživateli a sebeprezentace. Forma sdíleného obsahu se liší dle zaměření konkrétní sociální sítě. Některé sítě jsou zaměřené primárně na sdílení kontaktů, textů, fotografií apod. Podstatné je, že jsou uživatelé informování o činnosti svých virtuálních přátel. Mnoho sociálních sítí pak umožňuje zasílat zpráv, které se podobají e-mailu. (1)

Mezi sociální sítě, které využívají úřady, patří Facebook, Instagram, Twitter, TikTok, LinkedIn atd.

Obrázek 1: Logo - Facebook, Instagram, Twitter

Zdroj: (2)

Facebook

Facebook byl spuštěn 4. února 2004 a umožňovala lidem mezi sebou sdílet nejrůznější obsah. Zakladateli Facebooku jsou: Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, Andrew McCollum a Chris Hughes. Facebook byl původně pouze pro studenty Harvardské univerzity, nicméně v březnu 2004 byl Facebook zpřístupněn studentům na univerzitách Stanford, Columbia a Yale. Do roku 2005 se Facebook rozrostl na stovky vysokých a středních škol. Facebook je stal tak populární, že byl 26. září 2006 otevřen všem starším třinácti let. Puštění Facebooku do světa udělalo obrovskou změnu v online komunikaci. Lidé

si dříve mohli posílat obrázky e-mailem a komunikovat spolu prostřednictvím internetových chatovacích místností, Facebook byl ale jiný. V roce 2006 Facebook spustil funkci živého zpravodajství, to znamená, když někdo aktualizoval stav nebo aktivitu, příspěvek nebo aktualizace byla sdílena v reálném čase, tedy okamžitě, s malým nebo žádným zpožděním. Lidé už nemuseli čekat, až jim někdo pošle e-mail o tom, co dělají. Uživatelé se mohou jednoduše přihlásit a sdílet své aktivity. Facebook se stal možností okamžitého připojení k ostatním a zároveň zdrojem zábavy pro mnoho lidí. (3)

Instagram

Instagram je mobilní aplikace, kterou vyvinuli v roce 2010 Kevin Syndrom a Mike Krieger. Stejně jako Facebook umožňuje Instagram vytvářet uživatelů, profily a sdílet fotografie. Na rozdíl od Facebook byl Instagram vytvořen výhradně pro sdílení fotografií a videí. (3)

Twitter

Twitter v průběhu let vyrostl ze svých skromných začátků jako platforma pro sdílení krátkých zpráv o 140 znacích, což je původní maximální počet znaků. Dnes je Twitter místem, kde se vedou velké zprávy a vážné diskuze mezi miliony lidmi. Na Twitteru se lidé mohou spojit s přáteli, rodinou, spolužáky a spolupracovníky. Mohou se ale také spojit s celebritami, politiky, sportovci a dokonce i se značkami. (4)

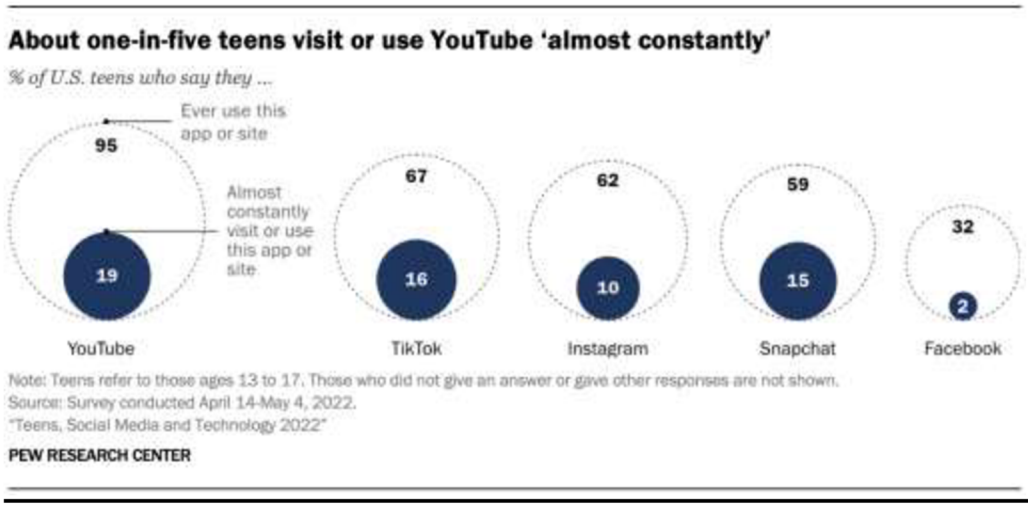
LinkedIn

Jedná se o profesionální síť, která byla založena v roce 2002, zakladatelem je Reid Hoffman a jejím cílem je spojit profesionály, aby byli produktivnější a úspěšnější. Díky této síti pro sebe mohou lidé najít ideální pozici či stáž. (5)

YouTube

YouTube je největší server na internetu, který slouží k vyhledávání a sdílení videosouborů. Dle průzkumu Centra ho používá 95% dospívajících. (6)

Obrázek 2: About one-in-five teens visit or use YouTube "almost constantly"



Zdroj: (6)

Snapchat

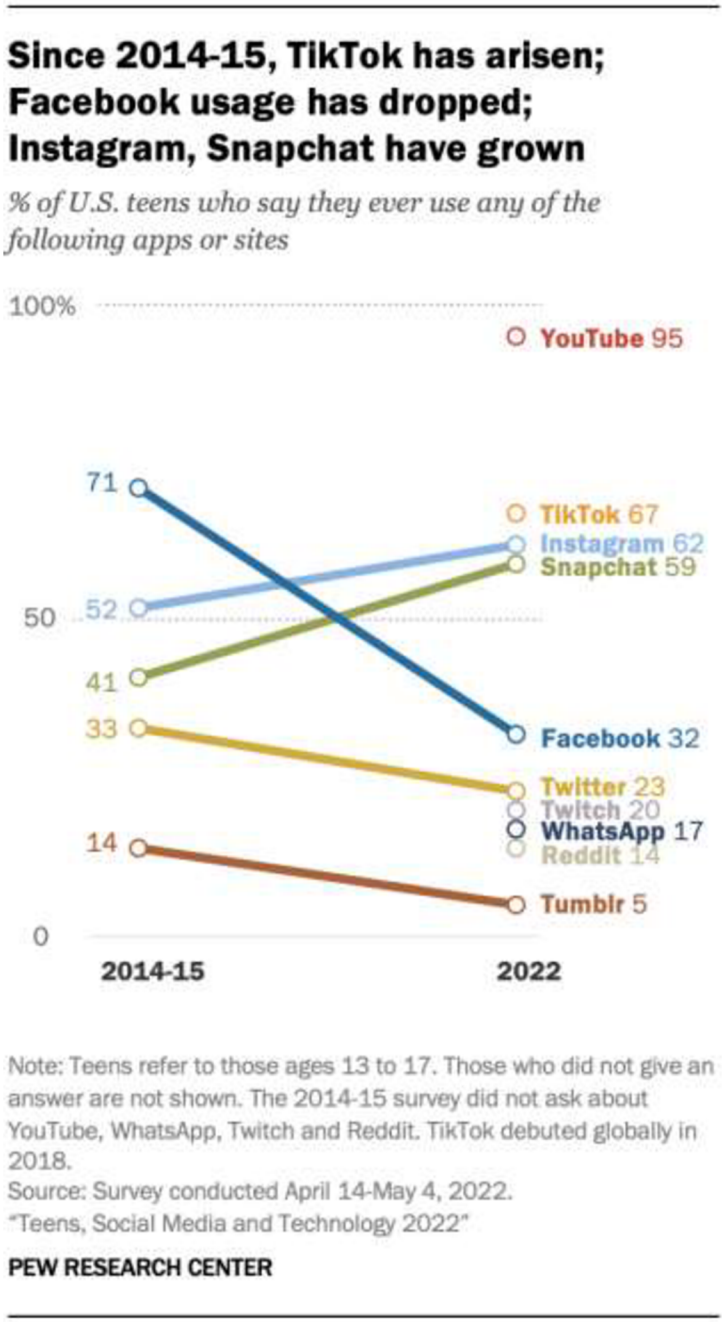
Snapchat slouží k chatování a videohovorům s přáteli odkudkoli. Aplikace byla vyvinuta společností Snap Inc., což je společnost zabývající se fotoaparáty. (7)

Tiktok

Tiktok je aplikace navržena pro mobilní videa s krátkou formou. Cílem aplikace je inspirovat ke kreativitě a přinášet lidem radost. (8)

Dle průzkumu Pew Research Center bylo zjištěno, že TikTok od svého severoamerického debutu před několika lety získal na popularitě a nyní je špičkovou platformou sociálních médií, a to především pro teenagery ve věku 13-17 let. Cca 67% dospívajících odpovědělo, že TitTok používá někdy, přičemž 16% všech dospívajících odpovědělo, že ho využívá téměř neustále. Počet dospívajících, kteří využívají Facebook, dominantní platformu sociálních sítí mezi dospívajícími v průzkumu Centra 2014-15, klesl z 71% na dnešních 32%. (6)

Obrázek 3: Since 2014-15, TikTok has arisen; Facebook usage has dropped; Instagram, Snapchat have grown



Zdroj: (6)

V březnu 2023 zveřejnil Národní úřad pro kybernetickou a informační bezpečnost varování před bezpečnostní hrozbou aplikace TikTok. Hrozba v oblasti kybernetické bezpečnosti souvisí s instalací a používání aplikace na zařízeních přistupujících ke komunikačním a informačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům. K vydání varování vedly NÚKIB vlastní poznatky, ale i poznatky partnerů. Hrozba vyplývá z množství

shromažďovaných dat o uživatelích a způsobu, jakým jsou sbírána, nakládání s nimi a také z právního a politického prostředí Čínské lidové republiky, jejímuž systému je podřízena společnost, která vyvinula aplikaci TikTok. Hrozba je vyhodnocena jako „Vysoká“, pravděpodobná až velmi pravděpodobná. Varování se týká povinných osob dle zákona o kybernetické bezpečnosti. Subjekty musí na varování reagovat přijetím přiměřených bezpečnostních opatření. Úřad doporučuje zakázat instalaci a používání aplikace TikTok na zařízeních, které mají přístup do regulovaného systému, jelikož jde o nejjednodušší způsob, jak zabránit uvedené hrozbě. (9)

Na základě výše uvedeného varování ruší státní úřady účty na TikToku a zakazují svým zaměstnancům aplikaci využívat na zařízeních k pracovním účelům. Jedná se například o ministerstvo životního prostředí, ministerstvo spravedlnosti, Akademie věd ČR atd. (10)

Česká obec

Účelem mobilní aplikace je především komunikace mezi úřady měst, městských částí a samostatných obcí s občany. Komunikace by měla být díky této aplikaci jednodušší, moderní a efektivní. Do aplikace se není potřeba registrovat v rámci GDPR. Aplikace umožňuje sdílet informace, ale i rozesílat cílené SMS zprávy v rámci určitých skupin. (9)

Veřejná správa

Cílem veřejné správy je, aby správní subjekt (instituce, orgán, organizace, úřad) vyvíjel cílevědomou činnost vedoucí k zajištění funkčního, životaschopného a rozvíjejícího se spravovaného subjektu (společnost, území, záležitosti občanů, záležitosti obyvatel státu, kraje, obce atd. Pojem veřejná správa má kořeny v římském právu, jedná se o správu lidské společnosti uspořádané ve stát se státním zřízením. (10)

Veřejnou správou se rozumí:

- Správa území
- Správa věci
- Správa záležitostí
- Správa financí
- Správa objektů

Její funkce:

- Mocenská
- Ochranná
- Organizační
- Regulační
- Služby veřejnosti

Veřejnou správu dělíme na státní správu a samosprávu. (10)

Státní správa

Státní správu lze definovat jako základ veřejné správy, kterou vykonává stát. Stát má ve své kompetenci vládnout, soudit a vytvářet zákony společnosti. Stát se vymezuje státní mocí, která je výkonná, zákonodárná a soudní, stálým obyvatelstvem a územím. (10)

Samospráva

Samospráva má své volené představitele, hospodaří se svým majetkem a má právní subjektivitu. Samosprávu dělíme na územní (kraje a obce) a zájmovou. (10)

Komunikace

Pojem komunikace má velmi široké použití. Význam slova je něco spojovat a je latinského původu. Může se jednat o označení pro dopravní síť, přemisťování lidí nebo materiálu, ale také informací, myšlenek, pocitů, postojů, a to od jednoho člověka k druhému. Mezi komunikační prostředky patří pošta, jazyk, telefon, počítač, televize, rozhlas, ale také vlaky, letadla, autobusy. (11)

Tradiční definice komunikace říká, že je komunikace „médium pozorovatelných manifestací lidských vztahů“. Komunikace není vždy viditelná, ale většinou ji můžeme zaregistrovat. (12)

Funkce komunikace:

- Informovat
- Instruovat – naučit, navést
- Přesvědčit
- Vyjednat, domluvit
- Pobavit

Typy komunikace:

- Přímá a zprostředkovaná – komunikace se dělí na tyto typy v závislosti na tom, zda můžou účastníci reagovat ihned, tedy tváří v tvář.
- Vnitřní a vnější – vnitřní v rámci organizace, vnější směřuje z organizace ven
- Interpersonální, skupinová a masová – závisí na poštu účastníků
- Formální a neformální

Mezi formy komunikace řadíme verbální a neverbální komunikaci. Neverbální komunikace upřesňuje nebo doplňuje informace předávané slovy, kdežto verbální komunikace prostřednictvím jazyka a řeči. (13)

Smyslem komunikace tváří v tvář je propojovat verbální a neverbální komunikaci tak, aby naše sdělení vyjadřovalo co nejpřesněji naše myšlenky. Při řeči využíváme mimiku, např. se usmíváme nebo mračíme. Neverbální komunikací můžeme zdůraznit verbální části sdělení, například zvýšit hlas, uhodit pěstí do stolu nebo dlouze zírat druhému do očí, když říkáte „Miluji tě“, dále můžeme neverbální komunikací doplňovat, popírat, regulovat, řídit, opakovat či nahrazovat verbální komunikaci. (14)

Riziko

Pravděpodobnost vzniku události, kterou lze z bezpečnostního hlediska považovat za nežádoucí. Riziko je odvoditelné z konkrétní hrozby a jeho míra, tedy pravděpodobnost škodlivých následků, vyplívající z hrozby a zranitelnosti zájmů lze posoudit pomocí analýzy rizik. (15)

Regionální rozvoj

Jedná se o proces, který vede ke zvýšení životní úrovně, kvality životů obyvatel a kvality životního prostředí dané lokality, k její konkurenceschopnost, ke snižování regionálních nerovností a vyrovnávání regionálních rozdílů. (16)

3.2 Specifika veřejné správy

Základní specifikem veřejné správy je skutečnost, že slouží občanům. Při plnění svých úkolů chrání tzv. veřejný zájem. (17)

Poskytovatelé veřejných služeb nazýváme souhrnně veřejným sektorem, jehož jádrem je veřejná správa. Veřejnou správu tvoří soustava institucí s centrální nebo územní působností. (18)

Dle klasifikace OSN COFOG tvoří veřejný sektor následující odvětví (18):

- Veřejná správa
- Obrana
- Veřejný pořádek a bezpečnost
- Ekonomické záležitostí (veřejná doprava, věda a výzkum, lesnictví atd.)
- Ochrana životního prostředí
- Bydlení a společenská infrastruktura
- Zdravotnictví
- Kultura, rekreace a náboženství
- Vzdělávání
- Sociální služby

Veřejný sektor se od soukromého odlišuje tím, že není založen na principu zisku. (18)

Dále mezi specifika využívání sociálních sítí ve veřejné správě oproti běžnému uživateli či firmám řadíme právní regulaci. Komunikaci mezi veřejnou správou a občanem upravují například Zákon o elektronických úkonech a autorizované konverzi dokumentů, nařízení GDPR, Zákon o zpracování osobních údajů, Zákon o Policii České republiky, Občanský zákoník a další.

3.2.1 Nařízení GDPR

Nařízení zásadně ovlivňuje práci organizací se sociálními sítěmi, není například přípustné, aby organizace veřejně či prostřednictvím soukromých zpráv na sociálních sítích sdílela osobní údaje klientů. Organizace se tímto nařízením musí řídit, je tedy vhodné se o něm v diplomové práci zmínit.

GDPR, celým názvem Nařízení Evropského parlamentu a Rady (EU) 2016/697 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti zpracováním osobních údajů a o volném pohybu těchto údajů. Cílem nařízení je ochrana fyzických osob při zpracování jejich v soukromém a veřejném sektoru. (19)

Nařízení umožnuje fyzickým osobám lépe kontrolovat svoje osobní údaje. Zahrnuje níže uvedené. (19)

- Snadnější přístup k osobním údajům
- Právo na přenos údajů mezi poskytovateli služeb
- Právo na výmaz osobních údajů
- Právo na informaci, že došlo k narušení osobních údajů

Dokument je platný po celém území EU, GDPR tak přebírá všechny doposud stanovené zásady v rámci ochrany a zpracování údajů, na nichž unijní systém ochrany údajů stojí a potvrzuje, že ochrana cestuje i přes hranice společně s údaji. K nařízení byly již vydány 3 tiskové opravy. První verze pochází z roku 2016, která se týkala pouze německé, estonské, italské a maďarské verze. Druhá verze z roku 2018 obsahovala 28 textových změn a třetí verze z března 2021 obsahuje také 28 textových změn. (20)

3.2.2 Zákon o eGovermentu

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů upravuje důležitý pojem datová schránka a autorizovaná konverze dokumentů. Zákon zvaný jako zákon o eGovernmentu nabyl účinnosti 1. 7. 2009. (21)

Cílem zákona je zajistit optimální podmínky pro komunikaci mezi úřady a občany, dále mezi úřady. Dle Ministerstva vnitra je hlavní myšlenkou eGovernmentu správa veřejných věcí za využitím informačních technologií, díky kterým bude systém veřejné správy k občanům dostupnější, rychlejší, efektivnější, levnější a přátelštější. (21)

Součástí eGovernmentu je také Czech POINT, který je právně zakotven v zákoně č. 365/2000 Sb., o ISVS. Jedná se o český podací ověřovací informační národní terminál, který snižuje byrokracii ve vztahu mezi občanem a veřejnou správou. V současné době musí občan navštívit několik úřadů, aby mohl vyřídit jednu záležitost. Czech POINT slouží jako asistované místo výkonu veřejné správy, které umožňuje vyřídit věc z jednoho místa, tedy aby „obíhala data, nikoliv občan“. (22)

Celý postup probíhá následovně. Občan navštíví českou poštu, vybraný zastupitelský úřad nebo další instituce stanovené vyhláškami. Na přepážce pracovník Czech POINT ověří údaje o žadateli nebo o předmětu jeho zájmu. Pracovník Czech POINT se připojí k centrále Czech POINT, a to zabezpečeným kanálem. Prostřednictvím centrály pracovník zadá dotaz a dostane odpověď, kterou vytiskne, orazítkuje a podepíše. Takto ověřený výpis má hodnotu

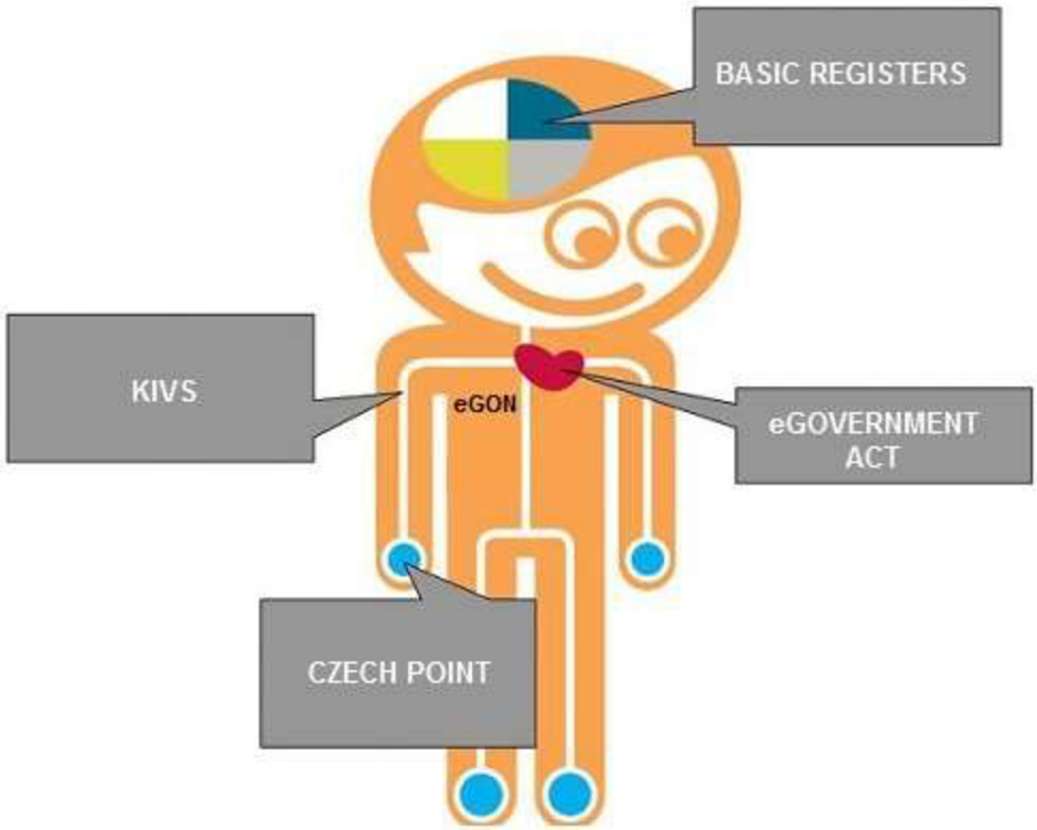
veřejné listiny. Na kontaktních místech Czech POINT lze zažádat o: výpis z obchodního rejstříku, katastru nemovitostí, rejstříku trestů nebo z živnostenského rejstříku. (22)

Symbolem eGovermentu je eGON viz obrázek níže. EGON je v přeneseném významu živý organismus, ve kterém vše souvisí se vším a fungování všech jeho částí se navzájem podmiňuje. (23)

Životní funkce eGONa zajišťují:

- Mozek, který tvoří základní registry veřejné správy. Mezi základní registry patří např. registr osob, registr obyvatel, registr práv a povinností, registr územní identifikace, adres a nemovitostí atd.
- Srdce - Zákon o eGovernmentu
- Oběhová soustava, kterou tvoří komunikační struktura veřejné správy (telekomunikační síť, KIVS)
- Prsty, výše zmiňovaný Czech POINT

Obrázek 4: EGON



Zdroj: (24)

Portál občana

Portál občana umožňuje všem občanům mít vlastní účet, ke kterému má přístup pouze on. Portál je bránou k elektronickým službám, jako je správa svých dokladů a jiných údajů ze základních registrů a databází. Prostřednictvím portálu lze také založit datovou schránku, pomocí níž může občan komunikovat s úřady. Portál odkazuje na další portály, jako je Finanční správa, ČSSZ, Očkovací portál, eRecept, Úřad práce atd. K přihlášení je nutné prokázat nejprve svojí totožnost a lze se do něj přihlásit prostřednictvím datové schránky nebo Identity občana. (25)

Portál občana nabízí například tyto služby:

- Žádost o nový řidičský průkaz
- Potvrzení o studiu
- Notifikace platnosti dokladů
- Přístup ke kontrole tachometru vozidla
- Přístup k podání daňového přiznání na portálu MOJE daně
- Výpis bodového hodnocení řidiče
- Přístup k registraci provozovatele dronu a online testu pilota dronu
- Přístup k portálu krajů měst a obcí
- Výpisy ze základních registrů
- Informace ze základních registrů
- Založit či přidat datovou schránku
- A mnohé další

Pro zasílání elektronického podání a komunikaci s veřejnou správou je nutné do Portálu občana přidat svojí datovou schránku. (25)

3.2.3 Zákon o zpracování osobních údajů

Předchůdcem zákona o zpracování osobních údajů byl zákon č. 101/2000 Sb., zákon o ochraně osobních údajů a o změně některých zákonů. K jehož zrušení došlo 24. 4. 2019. Např. § 4 písm. a) vymezoval osobní údaj jako jakoukoliv informaci, která lze subjekt 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. Sem spadá např. i SPZ. (26)

Policie ČR zveřejňuje na sociálních sítích, jako je např. Facebook příspěvky z dopravních nehod či nebezpečných manévrů řidičů. Tyto fotografie či videa mohou sloužit jako odstrašující příklad, nemůže však dojít k porušení zákona o zpracování osobních údajů. Na videu, kde figuruje dopravním prostředek, musí být SPZ cenzurována.

Zákon 110/2019 Sb., o zpracování osobních údajů (Adaptační zákon), který nabyl účinnosti 24. 4. 2019, zapracovává příslušné předpisy Evropské Unie, konkrétně Směrnici Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2017 a navazuje na přepis Evropské unie, konkrétně na Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 a k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů. (27)

Přijetím zákona o zpracování osobních údajů došlo k vymezení věkové hranice u dětí, které jsou způsobilé k udělení souhlasu se zpracováním osobních údajů. Zákon snížil hranici oproti Nařízení GDPR o 1 rok, tedy na 15 let. Od tohoto věku dítěte není nutný souhlas se zpracováním osobních údajů zákonným zástupcem. V některých případech může být udělený souhlas neplatný, např. souhlas, který je udělen k dlouhodobému zpracování osobních údajů. Adaptační zákon také například zmírňuje povinnost správce, která je stanovena v článku 35 Narážení GDPR. Povinnost spočívá ve vypracování posouzení vlivu na ochranu osobních údajů v případě pravděpodobnosti rizika při systematickém a rozsáhlém zpracování osobních údajů. Adaptační zákon z této povinnosti vylučuje správce, který zpracovává osobní údaje na základě zákonné povinnosti. (28)

3.2.4 Zákon o Policii České republiky

Zákon č. 273/2008 Sb. dává oproti jiným institucím veřejné správy možnost zveřejňovat osobní údaje. Policie České republiky je oprávněna tyto údaje zveřejňovat v rozsahu nezbytném pro plnění úkolů souvisejících např. s pátráním po osobách. Pokud se pátrá po fyzické osobě, je možné uveřejnit její fotografii na stránky Policie ČR nebo sociální sítě, především z úředních zdrojů, jako je evidence občanských průkazů nebo cestovních dokladů. Menší část fotografií pochází z veřejných nebo soukromých zdrojů. I přesto, že se na fotografie vztahuje autorské právo, na jejich použití se vztahuje ustanovení § 34 zákona č. 121/2000 Sb., Autorský zákon, které pojednává o úřední licenci. Podle této licence nezasahuje do autorského práva ten, kdo dílo využije v odůvodněné míře na základě zákona, a to například pro účely Policie České republiky. Dále je tato skutečnost upravena

v Občanském zákoníku, kde stojí, že s užitím fotografie musí majitel souhlasit, § 88 ale dodává, že může být fotografie použita pro úřední účely. (29)

3.3 Specifika komunikace veřejné správy

Specifika komunikace veřejné správy ovlivňuje:

Struktura subjektů veřejné správy

a) Subjekty veřejné správy
   - Stát
   - Jiné subjekty, o nichž to stanoví ústava nebo zákon
   - Veřejnoprávní korporace
   - Veřejné ústavy a veřejné podniky
   - Státní fondy
   - Nadace a nadační fondy
   - Obecně prospěšné společnosti
   - Veřejné výzkumné instituce (17)

b) Přímí vykonavatele veřejné správy
   - Prezident republiky
   - Vláda
   - Ministerstva
   - Jiné ústřední správní úřady
   - Jiné správní úřady
     - S celostátní působností
     - S územně vymezenou působností
   - Orgány samosprávy
     - Orgány územních samosprávných celků (obce a kraje)
     - Orgány profesních komor
     - Orgány vysokých škol
   - Veřejné bezpečnostní sbory (17)

Činností veřejné správy – cíle

- Podzákonné
- Výkonné
- Nařizovací (30)

3.3.1 Komunikace ve veřejné správě

Komunikace ve veřejné správě je založena především na komunikaci mezi veřejnou správou a občany. Mezi dva druhy komunikace patří komunikace povinná, neboli nutná a komunikace nepovinná, toto rozlišení je uváděno z hlediska dobrovolnosti. (31)

Povinná komunikace

Jedná se o standard chování, který vyplývá ze zákonů, vyhlášek a norem. Poskytuje tzv. „pravidla hry“, omezení, mantinely a sankce. Jde o záruku právního státu. Utváří předpoklady činnosti veřejné správy tak, aby umožňovala propojení veřejné správy s dalšími strukturami. Toto se týká především fyzických a právnických osob. Tyto osoby mají právo na informace, které mají orgány veřejné správy k dispozici. Překážky pro poskytnutí stanovuje legislativa. Povinností veřejné správy je zveřejňovat základní údaje o svých činnostech předepsaným způsobem tak, aby byly dostupné veřejnosti. (31)

Nepovinná komunikace

Tato rovina komunikace není ošetřena zákonem. Vychází z tradic, obecných zvyklostí, kultury a představ o slušném chování. Respektuje místní specifika a reaguje na problémy. Napomáhá k řešení těchto problémů a vytváří občanskou společnost. U nepovinné komunikace záleží, aby nedocházelo k obcházení zákona, nebo nebudou chybně interpretovány. Na nepovinné komunikaci záleží, do jaké míry je společnost demokratická, zda existuje prostor pro korupci a jestli dochází k zneužití moci. (31)

Veřejná správa ve vztahu k veřejnosti musí:

- Umět prezentovat hospodaření s majetkem a financemi
- Umět prezentovat výsledky činností orgánů veřejné správy
- Umět vysvětlit záměry a plány
- Vytvářet prostor pro iniciativu
- Všímat si potřeb veřejnosti (31)

Možnosti komunikace mezi úřady a občany

- Jednostranně
  - Úřední deska, rozhlas, zpravodaj, plakáty, letáky, webové stránky
- Oboustranně
  - Osobně, telefonicky, ankety na sociálních sítích (32)

Náležitosti elektronické komunikace ve veřejné správě upravuje především zákon č. 365/2000 Sb. o informačních systémech veřejné správy. (22)

Za informační systém veřejné správy můžeme považovat systém:

- o kterém zákon č. 365/2000 stanoví, že se jedná o ISVS
- který je zákonem označen jako registr, rejstřík nebo evidence
- o kterém zákon stanoví, že se jedná o ISVS, ale není u něj uveden odkaz na zákon č. 365/2000
- který je zákonem stanoven bez označení, že se jedná o ISVS
- který není upraven zákonem, ale prostřednictvím něhož vykonává orgán veřejné správy svěřenou činnost (informační systém o poplatcích za psy)

Elektronická komunikace mezi úřadem a občanem je velmi specifická. Mezi nástroje bezpečné elektronické komunikace patří elektronický podpis, což je zároveň nutnou podmínkou pro praktické využití elektronické komunikace. (22)

V současné sobě je elektronický podpis založen na kombinaci kryptografických metod, stěžejní je asymetrická kryptografie. Mezi faktory bezpečnosti a důvěryhodnosti elektronického podpisu patří délka šifrovacích klíčů užívaných pro asymetrickou kryptografii, typy algoritmů, kvalita nosiče a ochrany klíčů, způsob implementace atd. (22)

Např. tisková mluvčí ÚP ČR informuje o skutečnosti, že se na všech krajských pobočkách Úřadu práce otevírají ve spolupráci s Českou poštou s. p. kontaktní pracoviště Czech POINT. Lidé si zde mohou zřídit např. Mobilní klíče eGovernmentu. Dále vyzdvihuje výhody elektronické komunikace, prostřednictvím které mohou občané vyřídit žádosti o dávky, podpory či zprostředkování zaměstnání a zařazení do evidence uchazečů o zaměstnání, možné je také dokládat potřebné dokumenty pro konkrétní dávky. Formuláře lze zasílat prostřednictvím Identity občana. Nástroje, které mohou využívat, jsou: Bankovní identita, eObčanka, NIA ID či Mobilní klíč eGovernmentu. Další možnost je využití datové schránky nebo e-mailové komunikace s uznávaným elektronickým podpisem. (33)

Obrázek 5: Identita občana

Zdroj: (34)

Jelikož výše zmíněné prvky sociální sítě nezajišťují, veřejná správa komunikuje výhradně prostřednictvím informačních systému. Sociální sítě využívá pouze ke komunikaci, která souvisí se zodpovězením obecných dotazů a k informovanosti občanů.

O sociální sítě se v posledních letech začali zajímat také političtí vědci, jako jsou politologové, ale i psychologové, sociologové atd., a to v rámci politické komunikace. S využitím nových médií přicházejí pozitivní názory, jako je možnost politické participace a deliberace v kybernetickém prostoru, ale i negativní, jako je demobilizace obyvatel, zvětšování nerovností v přístupu nebo politická polarizace. Od 90. let se vědci začínají soustředit na jednotlivé online služby a aplikace. Na konci 90. let a začátku 21. století se věnují webovým stránkám, na začátku 21. století pak blogům, službám určeným ke sdílení videí (Youtube) a především sociálním sítím (MySpace, Facebook či Twitter). Jelikož nejsou sítě určeny pro vykonávání politiky, výzkumy se zabývají především sebeprezentací osob, soukromím na sociálních sítích a riziky, které s jejich využíváním souvisí. (35)

Zásadní vlna zájmu o sebeprezentaci na sociálních sítí přišla v roce 2008 v USA, kdy využil Barack Obama sociální síť Facebook a mobilní technologie pro svou kampaň. Sítě využíval ke komunikaci s organizacemi, podporovateli či blogery, ale i s různými skupinami

voličů, např. mladými lidmi, matkami apod. Úspěch Obamovy kampaně vedl k rychlému šíření sociálních sítí ve světe politických aktérů a odstartoval výzkum v oblasti využívání sociálních sítí v politické sféře. (35)

3.3.2 Historie komunikace

S rozvojem informačních technologií se vždy hovořilo o tom, jak jej prakticky využít ve veřejné správě. Například Masaryk tvrdil, že „nesnáze velikého množství lidu a jeho geografického prostorového rozdělení musí být podle možnosti překonány, značnou měrou pomáhají tu různé moderní komunikační prostředky“. Dle Hughese byla veřejná správa v období tradičního modelu lídrem využití moderních technologií, jako byl například telegram a telefon, což byly nástroje určené pro komunikaci mezi vnitřním a vnějším prostředím veřejné správy. Informační technologie se v minulosti využívaly především v oblasti financí, rozpočtů a uchování zaměstnaneckých dat. S příchodem internetu došlo k jejímu většímu využití pro účely komunikace a poskytování elektronický služeb. (36)

K posunu paradigmatu z tradičního modelu veřejného sektoru k manažerismu došlo v polovině 80. let. Změna souvisela s ekonomickými problémy, které se objevovaly v 70. a 80. letech. Tyto problémy vedly k tomu, že vlády začaly přehodnocovat své systémy byrokracie. Základní otázky, které si kladly, zněly následovně: Může nebo měla by být vláda menší? Jak může vláda dělat to, co dělá, lépe? Můžeme dělat více s menšími zdroji a zvýšit spokojenost občanů? Dalším důvodem těchto otázek byl vzrůst nedůvěry k veřejným institucím a politikům s nízkou legitimitou činností veřejných institucí. V rámci reformy veřejné správy byly organizace veřejné správy přinuceny využívat outsourcing, privatizovat zřízené organizace, včetně podniků a revidovat roli vlády dle soukromého sektoru. (36)

První zmínky o jazyce přišly již v době 10 000 let před Kristem. Vůbec nejstarší písemná zpráva, která se dochovala, pochází z roku 4 000 let před Kristem. Tisk byl vynalezen v roce 1450 Guttenbergem. Telegraf byl vynalezen v roce 1837. Telefon byl vynalezen v roce 1861. (11)

Ve 20. století došlo k objevu rozhlasu, televize, satelitu, počítače, optoelektroniky atd. Od 21. století se spíše zaměřujeme na prodej, uchování, nákup a získávání informací. (11)

Interpersonální komunikace, což je komunikace tváří tvář se již díky rozvíjejícím se technologiím daří realizovat mezi lidmi, kteří jsou od sebe tisíce kilometrů. Pro informace už v dnešní době neexistují bariéry, jejich přenos lze zajistit auditivně i vizuálně. (11)

3.3.3 Milníky

2010

V roce 2010 spustil Úřad vlády ČR svou oficiální prezentaci na Facebooku. Hlavním cílem účtu je informovat veřejnost o dění v Úřadu vlády ČR. Jedná se např. o tisková prohlášení, zajímavosti, fotografie při činnostech úřadu, vlády a jejího předsedy. (37)

Na facebookových stránkách Úřadu vlády můžeme dohledat záznamy z tiskových konferencí, informace o průběhu jednání, které probíhá například se zástupci Rady Asociace krajů ČR, informace o setkání odborníků z celé Evropy a zástupci Evropské komise a WHO na onkologické konferenci atd.

2013

Aktuality a užitečné informace začalo Ministerstvo práce a sociálních sítí nabízet občanům prostřednictvím facebookového profilu MPSV v roce 2013.

Ministerstvo práce a sociálních věcí založilo také profil pod názvem Důchodová reforma, kde občané najdou základní informace o třech pilířích reformy a kalkulačku, na které si lidé mohou vypočítat budoucí penzi. Dále se lze na profilu dozvědět, jaký fond či strategii spoření zvolit. (38)

2014

Úřad pro zastupování státu ve věcech majetkových se stal uživatelem twitteru v roce 2014. Úřad usiluje o informovanost občanů v oblasti majetkových věcí prostřednictvím krátkých zpráv, neboli tweetů. (39)

2017

V den Policie České republiky byl spuštěn provoz profilů Policie České republiky na sociálních sítích Facebook, Twitter a YouTube. Policie ČR uveřejňuje na svém YouTubovém kanálu preventivně zaměřená videa. Facebookový profil slouží ke sdílení zajímavých informací, komunikaci s občany a sdílení policejního života. Twitter slouží ke sdílení informací k bezpečnostním opatření, bezpečnostní situace a situaci v silničním provozu. (40)

2021

Od 1. 12. 2021 lze dohledat facebookový profil Ministerstva vnitra. Účelem profilu je informovanost veřejnost o aktuálním dění a zajímavostech týkající se agendy Ministerstva vnitra. Dále účet slouží ke sdílení blížících se akcí, které má pod svými křídly právě

ministerstvo. V neposlední řadě na stránkách lze dohledat informace o volných pracovních pozicích. (41)

Již několik měsíců využívá Nejvyšší kontrolní úřad sociální síť LinkedIn, kde zveřejňuje zajímavé informace ohledně hospodaření státu. Kontroluje jak příjmy, tak výdaje. Mimo novinek a zajímavostí úřad také zveřejňuje i pracovní nabídky v rámci úřadu. Na stránkách si lze dohledat zaměstnance, kteří na Nejvyšším kontrolním úřadě pracují. (42)

2022

Na stránkách LinkedIn můžeme najít také Nejvyšší soud, který sídlí v Brně a je vrcholným soudním orgánem v oblasti občanského soudního řízení a trestního řízení s výjimkou záležitostí, o kterých rozhoduje Nejvyšší správní soud či Ústavní soud. Soud zveřejňuje nejen informace ohledně soudnictví, ale také zveřejňuje informace o volných služebních a pracovních místech na Nejvyšším soudě. (43)

3.3.4 Soutěž zlatý erb

Smyslem soutěže je najít nejlepší webové stránky měst a obcí. V roce 2022 v soutěži uspěly města Litoměřice a Mnetěš. (44)

V roce 2014 proběhl rozhovor se starostou obce města Broumov, Královehradecký kraj ohledně webových stránek města. Starosta sdělil, že byly pro občané zpřístupněny v sekci Úřad online formuláře pro různé životní situace, které se aktualizují v návaznosti na novou legislativu. Město umožňuje občanům nahlížet do elektronického katalogu knih s možností rezervace konkrétní knihy, dále si mohou zkontrolovat vypůjčenou knihu. Občané mohou díky webovým stránkám hlásit závady, nedostatky a připomínky k území Broumova, například mohou nahlásit nepořádek v ulicích nebo parcích města, poškozené dopravní značení, komunikace, chodníky, nefunkční osvětlení nebo neposekanou trávu. Mezi další vychytávky webových stránek patří aplikace „Rozklikávací rozpočet“, kde se občané mohou dozvědět o hospodaření města, aktuálním stavu a vývoji rozpočtu, realizaci všech příjmů a výdajů obce. (44)

3.3.5 Statistiky

Veřejná správa on-line

Používání webových stránek je pro instituce veřejné správy nedílnou součástí. Ke konci roku 2010 je mělo 100% krajů, 97% všech obcí a 91% organizačních složek státu.

Pouze 199 obcí (s nejmenší rozlohou) v té době webovou prezentaci nevyužívalo. Přes 90% institucí poskytuje na svých stránkách informace k životním situacím, méně častou službou je poskytování formulářů ke stažení a jen v omezené míře je nabízena služba úplného elektronického podání. (45)

Otázkou je, do jaké míry tyto on-line služby lze vyřizovat. Například matriční záležitosti je nutné vyřídit osobně, žádost předložit na originálním formuláři a hlavně předložit potřebné doklady nebo fotografii. (45)

Internet ve službách veřejné správy

Internet ve vztahu k veřejné správě využívá pouze pětina jednotlivců, což je 22 % jednotlivců. Firmy využívají online služby veřejné správy podstatně více, jedná se o 9 z 10 podniků. Data jsou platná k roku 2011. (46)

Využívání ICT v organizacích veřejné správy

Využívání ICT v organizacích veřejné správy si klade za cíl optimalizaci činnosti veřejné správy, což vede k nabízení občanům a firmám rychlejší, srozumitelnější a profesionálnější služby. Předpokladem pro splnění tohoto cíle je vybavenost institucí veřejné správy informačními technologiemi, schopnost zpřístupnit online služby, dostatečně velký personál, který je schopný pracovat s informačními systémy a společnost, která má přístup k internetu a využívá ho. (47)

Od roku 2004 do roku 2011 probíhalo pravidelné šetření o využívání ICT veřejnou správou. Šetření se zabývalo výměnou dat s jinými organizacemi veřejné správy, on-line službami na webových stránkách organizací veřejné správy, obcí v krajích a okresech ČR, zabezpečením IT v organizacích veřejné správy atd. (47)

Zpřístupnění informací a on-line služeb na webových stránkách sledoval průzkum webových stránek organizací veřejné správy, a to do roku 2013. (47)

Nejnovější data z roku 2020 vycházejí ze šetření o využívání ICT v domácnostech a mezi jednotlivci a šetření o využívání ICT v podnikatelském sektoru společně s převzatými údaji ohledně eGovernmetu v ČR. (47)

Šetření týkající se vydaných výstupů prostřednictvím kontaktních míst Czech POINT ukazuje, že v roce 2007 bylo díky této službě vystaveno celkem 54 výpisů, autorizovaných konverzí dokumentů a ostatních výstupů, kdežto v roce 2019 se toto číslo vyšplhalo na 2045 celkem. (47)

Šetření týkající se vydaných výstupů prostřednictvím rozhraní CzechPoint@office (agendy matrik, ohlašoven, soudů, evidence přestupků, výpisy z rejstříků atd.) ukazuje, že v roce 2007 nebyl vydaný žádný výstup, v roce 2019 bylo vydáno 6094 výstupů. U rozhraní CzechPoint@home (výpisy z rejstříků) nebyl v roce 2007 vydán žádný výstup, v roce 2019 bylo vydáno 29,2 tisíců výstupů. (47)

3.4 Rizika využívání sociálních sítí

V kapitole rizika využívání sociálních sítí budou charakterizována rizika, jako je kybernetická kriminalita, porušení zabezpečení, falešná tvrzení a agrese na sociálních sítích.

3.4.1 Kybernetická kriminalita

Kybernetické války doprovází téměř každý politický, vojenský, či náboženský konflikt. Internet v dnešní době propojuje nespočet serverů a uživatelských stanic, díky čemuž se stává virtuálním bojištěm. Mezi nejznámější metody patří defacement, kdy dochází k nahrazení původních stránek novými, které obsahují politické nebo sociální poselství. (48)

Mezi hlavní střety patří útoky během války v Jugoslávii a čínsko americká hackerská válka. Při Kosovské válce, která byla poslední válkou 20. století a zároveň první válkou NATO, docházelo ke zmatení moderních zbraní NATO, které se snažily o vyhledání a zničení srbských obrněných jednotek v Kosovu. Střely s plochou dráhou letu, které byly zamířeny na radary systému protivzdušné obrany, byly jednoduše zmateny srbskou taktikou. Srbové radar na pár vteřin zapnuli a poté opět vypnuli, což vedlo k dezorientaci raket, které nakonec skončily v Bulharsku. Dále Srbové lákali NATO na falešné lákací mosty z umělé hmoty, pece na dřevo, jejichž komíny vypadaly jako hlavně atd. Opakem těchto primitivních akcí zaměřených na vyspělou technologii protivníka byly kybernetické útoky na infrastrukturu NATO, které probíhaly po celou dobu bombardování a vyřazovaly tak z provozu důležité servery. Po zásahu čínské ambasády zasílali čínští hackeři na americké vládní stránky vztahy typu „Nepřestaneme útočit, dokud neskončí válka!“ (48)

S kybernetickou kriminalitou úzce souvisí termín „softwarová policie“, který se vyskytuje v českých novinách a na internetu. Ta ve skutečnosti neexistovala a kybernetickou trestnou činnosti v 90. letech vyšetřoval Kriminalistický ústav v Praze. V roce 1998 vznikl Úřad služby kriminální policie a vyšetřování, oddělení informační kriminality. Do náplně práce spadalo softwarové pirátství, postupně byla tato činnost převedena na základní útvary služby kriminální policie. (48)

V roce 2006 došlo ke strukturální změně a vzniklo nové pojetí oddělení informační kriminality. Předpokladem bylo zřízení specializovaných míst operativních detektivů. První místo vzniklo v roce 2005 na pracovišti PČR v hlavním městě Praze. Hlavním úkolem oddělení je odhalovat, vyšetřovat, monitorovat, zajišťovat důkazy na Internetu a zajišťovat servis a podporu útvarům kriminální policie. Zjištěné poznatky ve většině případech předává na věčně a místně příslušné orgány, vyšetřování provádí sám pouze v náročných případech. (48)

Informační válka

Informační válku je nutné oddělit od kriminálních aktivit na internetu, je jim však velmi podobná. Jakákoli nelegální operace, která probíhá v kyberprostoru, která vede k porušení zákona, označujeme počítačovou kriminalitou. Může ji vykonávat jednotlivec či skupina, organizovaně či neplánovaně. U informační války se většinou nejedná o náhodný proces, ale o koordinovanou činnost mnoha složek. Informace je v této válce zbraň, která se využívá ve dvou úrovních, a to státní a vojenské. (48)

Významnou vlastností prostředků těchto válek je dosah, útočník je schopný napadnout cíl z jakéhokoliv místa, kde je připojení k síti. Dále jsou prostředky vynaložené na spuštění informační války v porovnání se škodami zanedbatelné. Útočník si vystačí s minimálními prostředky a vybavením, kdežto náklady na obranu jsou poměrně vysoké, jelikož je zapotřebí ochranné kroky provádět plošně a ve velkém rozsahu. (48)

Cílem informačních válek je oslabit jiné státy, podvrátit jejích státní základy a narušit státní zřízení, tomu útočník docílí při působení na politickou, diplomatickou, ekonomickou a sociální sféru prováděním psychologických operací a dalšími protiprávními jednáními v kyberprostoru. (48)

3.4.2 Porušení zabezpečení

Jedná se o takové porušení zabezpečení, které může mít za následek riziko pro práva a svobody fyzických osob. Může se jednat o útok proti počítači, ve kterém se uchovávají osobní údaje. Důsledkem je jejich únik, úprava nebo jiné zneužití. Může se také jednat o ztrátu listinných dokumentů, které obsahují osobní údaje. (49)

Využíváme obrovské a integrované úložiště, neboli databáze osobních údajů, které komunikují online s ostatními servery na internetu. Riziko je tedy jednoznačně vysoké. Data, která v databázích uchováváme: (22)

Anonymní údaje – jedná se o údaje, které se nevážou k dané osobě. Příkladem je „Jan Novák“. Z této informace nelze odvodit, o jakou konkrétní osobu jde, informace je tedy anonymní. (22)

Osobní údaje – jedná se o údaje, díky kterým lze identifikovat konkrétní fyzickou osobu. Příkladem je rodné číslo nebo jméno a příjmení v kombinaci s trvalou adresou za předpokladu, že na dané adrese nebydlí dvě osoby se stejným jménem a příjmením. Příkladem je „Jan Novák, Hradecká 1, Hradec Králové“. (22)

Citlivé údaje – jedná se údaje, které mají národnostní, etnický nebo rasový původ, vypovídají o politických postojích, náboženství, odsouzení za trestný čin, zdravotním a sexuálním životě osoby atd. Dále se může jednat o jakýkoliv biometrický nebo genetický údaj, jako je moč, vlas, slina, fotografie, DNA, hlas, otisk, vlastnoruční podpis, scan duhovky atp. (22)

Únik dat v době COVID-19

V době, kdy se v České republice začal šířit COVID-19 se zároveň začaly šířit útoky na nemocnice. Útočníci se snažili během této doby shromažďovat zdravotnické údaje občanů. Se ztrátou osobních a zdravotních údajů si člověk většinou spojí hackerské útoky na počítačové systémy. V době Covidu bylo ale nejjednodušším způsobem odcizit vytištěnou dokumentaci a informace. Ve chvíli, kdy zdravotník vytiskl dokumentaci, mohl ji u tiskárny vyzvednout kdokoliv s bílým pláštěm. Dle dotazníkového šetření společnosti Quocirca Print 2025 uvedlo 60% dotazovaných, že v důsledku nezajištěného tisku došlo k alespoň jednomu odcizení nebo porušení dat. Takováto skutečnost může mít pro společnost fatální následky, jak z hlediska nákladů, tak z hlediska reputace. (50)

Řešení správy tisku integrovaná do systému elektronické lékařské dokumentace zdravotnické organizace zajišťuje nejvyšší zabezpečení proti odcizení údajů. Pomocí tohoto řešení zdravotník odesílá tisk do fronty, nikoliv přímo do tiskárny. Pro vyzvednutí dokumentaci je nutná autentizace pomocí otisku svého jedinečného odznaku zaměstnance. Po autentizaci se dokument ihned vytiskne. V tomto případě neexistuje příležitost k odcizení dokumentu a dat. (50)

Nástroje pro bezpečný tisk:

- Zabezpečená služba Pull-printing – tiskové zařízení je uzamčeno, dokud uživatel neověří svojí identitu
- Reporting a tracking – sledování a rozpoznání, co se v organizaci kopíruje, skenuje a tiskne, dále kdy, kde, kdo a na jakém zařízení
- Zabezpečení komunikace – softwarové komunikace napříč organizací, které spolu komunikují
- Modelováni hrozeb – brainstorming s cílem určit a zmírnit rizika ve fázi designu
- Statická analýza zdrojového kódu – automatické kontroly, které se provádějí každou noc a zjišťují potenciální nebezpečí
- Bezpečnostní školení pro inženýry

3.4.3 Falešná tvrzení

Jelikož lze na sociálních sítích ve většině případech komentovat příspěvky, které jakýkoliv uživatel zveřejní, dochází v případě využívání sociálních sítí ve veřejné správě k šíření falešných tvrzení.

Např. v roce 2022 kolovala na sociálních sítích Úřadu práce České republiky falešná informace o vyhlášení STOP stavu kvůli uprchlíkům z Ukrajiny. Hoax zněl: “Dnes přišlo emailem: Paní po mateřské se šla zeptat na pracák na práci. A toto je výsledek: "Úřednice mi sdělila, že pro české občany je zatím vyhlášen STOP stav kvůli mnoha uprchlíkům z Ukrajiny, které potřebují zařadit do pracovního procesu, a tudíž jim musí dát práci přednostně. Tak rozhodla vláda!!! Prý se mám zkusit ve fabrikách zeptat osobně a domluvit si práci sama. Šla jsem tedy do místních fabrik, abych nějaké to zaměstnání našla. K mému překvapení jsem znovu a znovu narazila na podobnou odpověď jako na pracovním úřadě o tom, že přednostně budou dávat přednost utečencům z Ukrajiny. Bohužel dodnes jsem nenašla firmu, která by o mně projevila zájem a nabídla mi nějakou práci. Češi se nyní stávají drahou a nežádoucí pracovní silou, o kterou nebude zájem. Dokonce jsem se dozvěděla, že propouští české brigádníky a přijímají výhradně brigádníky z Ukrajiny." (51)

Proti tomuto tvrzení se Úřad práce České republiky ohradil a informoval občané prostřednictvím tiskové zprávy o tom, že služby občanům ČR nadále poskytuje. (51)

3.4.4 Agrese na sociálních sítích

Prostřednictvím sociálních sítí se nešíří jen falešná tvrzení, ale také negativní, někdy až agresivní komentáře jednotlivců vůči názorům politiků, politických stran či jednotlivých institucí.

Být agresivní v online světě je mnohem jednodušší, než v reálném světě, jelikož v online prostředí lze skrýt svou identitu. Tato možnost nám umožňuje si dovolit mnohem víc, než v offline světě a dovoluje nám tak dělat věci, které bychom v reálném životě nikdy neudělali. Na sociálních sítích můžeme jednat agresivně bez jakéhokoliv postihu. S tím souvisí odvázanost, která se označuje jako „disinhibice“, člověk při ní ztrácí zábrany (je schopný vyhrožovat, urážet, rozesílat videa se sexuálním podtextem atd.) Dále na sociálních sítích dochází k pocitu, že jsme si všichni rovni. Jelikož nevíme, jaký společenský titul má osoba na druhé straně, obavy z otevření se mizí. (52)

Hating – síření nenávisti vůči skupině mezi ostatními členy internetu. (52)

4 Vlastní práce

V praktické části je zkoumáno, jaké sociální sítě jednotlivé instituce veřejné správy využívají, za jakým účelem tyto sítě využívají a jaké zkušenosti s jejich využíváním mají. Dále je zkoumáno, s jakými riziky se instituce veřejné správy v souvislosti s využíváním sociálních sítí setkávají, jaké řešení pro tyto rizika měli nebo mají a jakou nastavili v instituci prevenci proti těmto rizikům. V neposlední řadě je provedena komparace využití sociálních sítí mezi vzorkem č. 1 a vzorkem č. 2. viz vysvětlení níže.

4.1 Metodické zpracování

V této části bude uvedeno, jakým způsobem došlo k výběru respondentů, jakým způsobem došlo k jejich oslovení a jak byla následně získaná data zpracována.

Výběr respondentů

V rámci praktické částí diplomové práce bylo osloveno celkem 70 správců sociálních sítí institucí veřejné správy v Královehradeckém kraji, a to ve dvou vzorcích. Osloveny byly pouze takové instituce, které nemají nadřízenou instituci (např. Okresní správy sociálního zabezpečení nebo kontaktní pobočky Úřadu práce, jelikož za OSSZ spravuje sociální sítě ČSSZ a za kontaktní pobočky Úřadu práce spravuje sociální sítě Úřad práce ČR), ty sídlí zpravidla mimo Královehradecký kraj.

Ve vzorku č. 1 byly osloveny obecní úřady, městské úřady a úřady městyse v Královehradeckém kraji. Královehradecký kraj má 387 obecních úřadů, 13 úřadů městyse, 47 městských úřadů a 1 magistrát města. Do vzorku bylo vybráno 55 obecních úřadů, 1 úřad městyse a 8 městských úřadů, celkem 64 úřadů. Jejich seznam najdete pod textem. Šedé vyznačení znázorňuje obecní úřady, modré úřad městyse a žluté městské úřady.

- Obecní úřad
  - Adršpach
  - Barchov
  - Červený Kostelec
  - České Meziříčí
  - Dobřenice
- Úřad městyse
- Městský úřad
  - Dolní Kalná
  - Dolní Radechová
  - Doubravice
  - Broumov
  - Habřina

- Heřmanice
- Hřibiny-Ledská
- Hořičky
- Chlumec nad Cidlinou
- Chotěvice
- Chvaleč
- Jaroměř
- Jánské Lázně
- Kosičky
- Kovač
- Kvasiny
- Kyje
- Lázně Bělohrad
- Ledce
- Libčany
- Libníkovice
- Libňatov
- Lochenice
- Lužany
- Markvartice
- Maršov u Úpice
- Mlékosrby
- Mokré
- Nechanice
- Nový Hrádek
- Nový Ples
- Ohařice
- Orlické Záhoří
- Osek
- Otovice
- Pěčín
- Pilníkov
- Podbřezí
- Praskačka
- Provodov-Šonov
- Račice nad Trotinou
- Rohoznice
- Rokytňany
- Roudnice
- Rychnovek
- Skřivany
- Sloupno
- Soběraz
- Staré Hrady
- Studnice
- Suchovršice
- Trnov
- Tutleky
- Úbislavice
- Vilantice
- Vítězná
- Výrava
- Zaloňov
- Zdelov

Ve vzorku č. 2 byly osloveny jiné instituce, než obecní úřady, městské úřady a úřady městyse. Jedná se o instituce státní správy. Jejich seznam najdete pod textem.

- Agentura ochrany a krajiny ČR
- Česká obchodní inspekce
- Hasičský záchranný sbor Královehradeckého kraje
- Inspekce životního prostředí
- Krajská hygienická stanice
- Správa Krkonošského národního parku

Šetření

Instituce byly osloveny prostřednictvím e-mailové komunikace, která je u jednotlivých institucí uvedena na stránkách statnisprava.cz. V záložce úřady byl vybrán Královehradecký kraj, dále úřady se sídlem v Královehradeckém kraji - např. záložka městské a obecní úřady, Hasičský záchranný sbor ČR atd., po jejichž rozkliknutí se zobrazí seznam všech úřadů spadající pod uvedenou záložku – např. Městský úřad Červený Kostelec, Obecní úřad Adršpach, Hasičský záchranný sbor Královehradeckého kraje atd. Po rozkliknutí konkrétních institucí je k dispozici e-mail, na který byl zaslán dotazník s prosbou o předání e-mailu osobě, která spravuje dané instituci sociální sítě. Instituce, které sociální sítě nevyužívají, nemají ani správce sociálních sítí. Instituce, které sociální sítě využívají, mají pověřenou osobu, která sociální sítě spravuje, jedná se především o starosty, tajemníky, administrativní pracovníky nebo tiskové mluvčí. V emailu byli správci sociálních sítí vyzváni k vyplnění níže uvedeného dotazníku. Otázky byly sestaveny v závislosti na hlavním a dílčích cílech celé práce. Na email odpovědělo všech 70 institucí.

Obrázek 6: Dotazník

1. **Otázka:** Jaké sociální sítě Vaše instituce využívá?

Sociální síť	**Facebook**	**Twitter**	**Instagram**	**TikTok**	**YouTube**	**LinkedIn**	**...**	**...**
Využíváme								
Hlavní účel								
Počet uživatelů								
Negativní zkušenosti								
Pozitivní zkušenosti								
Zhodnocení využití								

2. **Otázka:** Uvažuje instituce nasadit další sociální sítě, které nebyly doposud implementovány? Jaké a za jakým účelem?
   Odpověď:

3. **Otázka:** Od kdy instituce jednotlivé sociální sítě využívá a jak probíhalo jejich nasazení?
   Odpověď:

4. **Otázka:** S jakými riziky se instituce setkala?

Riziko	**Phishing**	**Hoaxy**	**Vulgární, agresivní, negativní reakce**	**Kybernetické útoky**	**Ztráta osobních údajů**	**...**	**...**
Setkala se s ním instituce?							
Jaké bylo řešení ze strany instituce?							
Jaká opatření instituce zavedla?							

5. **Otázka:** Jaká prevence je v instituci zavedena proti rizikům, která jsou spjatá s využíváním jednotlivých sociálních sítí?
   Odpověď:

Zdroj: vlastní

Zpracování dat

1. Zhodnocení využití sociálních sítí ve veřejné správě prostřednictvím grafů a tabulek
2. Zhodnocení rizik využívání sociálních sítí ve veřejné správě prostřednictvím grafů a tabulek
3. Komparace využití sociálních sítí mezi státní správou a samosprávou prostřednictvím grafů a tabulek

4.2 Využití sociálních sítí ve veřejné správě

Z dotazovaných 70 institucí nevyužívá celkem 37 z nich žádné sociální sítě, konkrétně se jedná o Krajskou hygienickou stanici Královehradeckého kraje a 36 obecních úřadů.

Instituce, které sociální sítě nevyužívají:

- Krajská hygienická stanice Královehradeckého kraje
- Obecní úřad Adršpach
- Obecní úřad Dobřenice
- Obecní úřad Dolní Radechová
- Obecní úřad Doubravice
- Obecní úřad Habřina
- Obecní úřad Heřmanice
- Obecní úřad Hřibiny-Ledská
- Obecní úřad Chotěvice
- Obecní úřad Kosičky
- Obecní úřad Kovač
- Obecní úřad Kyje
- Obecní úřad Ledce
- Obecní úřad Libčany
- Obecní úřad Libníkovice
- Obecní úřad Lochenice
- Obecní úřad Markvartice
- Obecní úřad Maršov u Úpice
- Obecní úřad Mlékosrby
- Obecní úřad Mokré
- Obecní úřad Nový Ples
- Obecní úřad Ohařice
- Obecní úřad Osek
- Obecní úřad Otovice
- Obecní úřad Pěčín
- Obecní úřad Rohoznice
- Obecní úřad Rokytňany
- Obecní úřad Skřivany
- Obecní úřad Sloupno
- Obecní úřad Soběraz
- Obecní úřad Staré Hrady
- Obecní úřad Studnice
- Obecní úřad Suchovršice
- Obecní úřad Tutleky
- Obecní úřad Úbislavice
- Obecní úřad Vítězná
- Obecní úřad Zdelov

Sociální sítě nevyužívají především obecní úřady, které se nachází v tzv. „malé obci“, která má méně než 500 obyvatel.

Tabulka 1: Nevyužívají sociální sítě (dle počtu obyvatel)

Počet obyvatel	Nevyužívá celkem
0-100	4
101-500	22
501-1000	6
1001-1500	4

Zdroj: vlastní

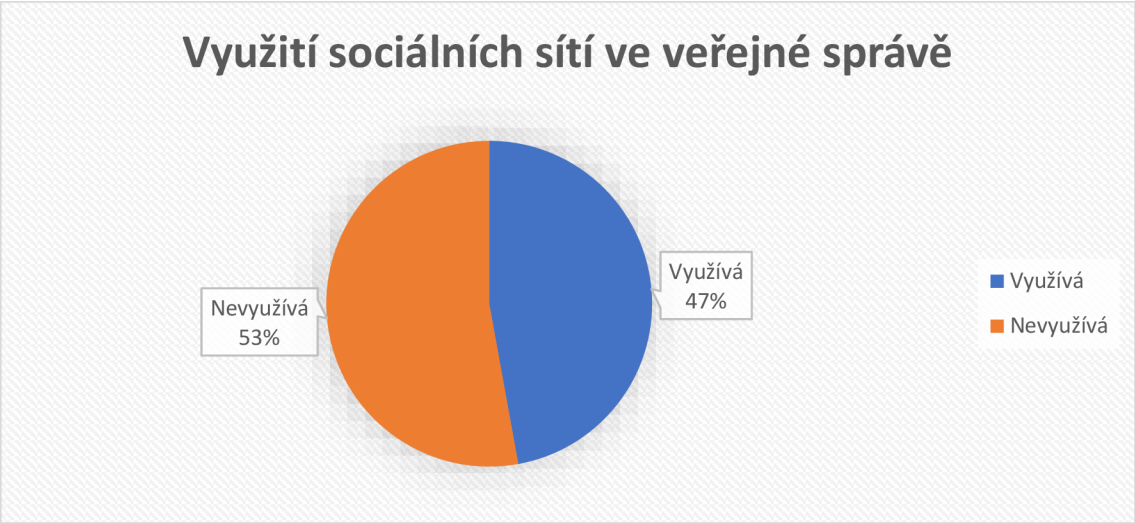
Tabulka 2: Názvy obcí, které dle počtu obyvatel nevyužívají sociální sítě

Počet obyvatel	Název obce
0-100	Hřibiny, Kyje, Ohařice, Soběraz
101-500	Rokytňany, Kovač, Libníkovice, Mokré, Maršov u Úpice, Staré Hrady, Mlékosrby, Osek, Zdelov, Rohoznice, Habřina, Kosičky, Ledce, Nový Ples, Tutleky, Doubravice, Otovice, Suchovršice, Heřmanice, Úbislavice, Adršpach, Pěčín
501-1000	Sloupno, Dobřenice, Lochenice, Markvartice, Dolní Radechová, Libčany
1001-1500	Chotěvice, Skřivany, Studnice, Vítězná

Zdroj: vlastní

Sociální sítě finančních úřadů, inspekce práce, úřadů práce, krajské hygienické stanice a krajské veterinární správy spravují nadřízené úřady, které sídlí zpravidla v Praze, nejsou tedy součástí uvedených dat.

Obrázek 7: Kolik procent institucí veřejné správy využívá sociální sítě?



Zdroj: vlastní

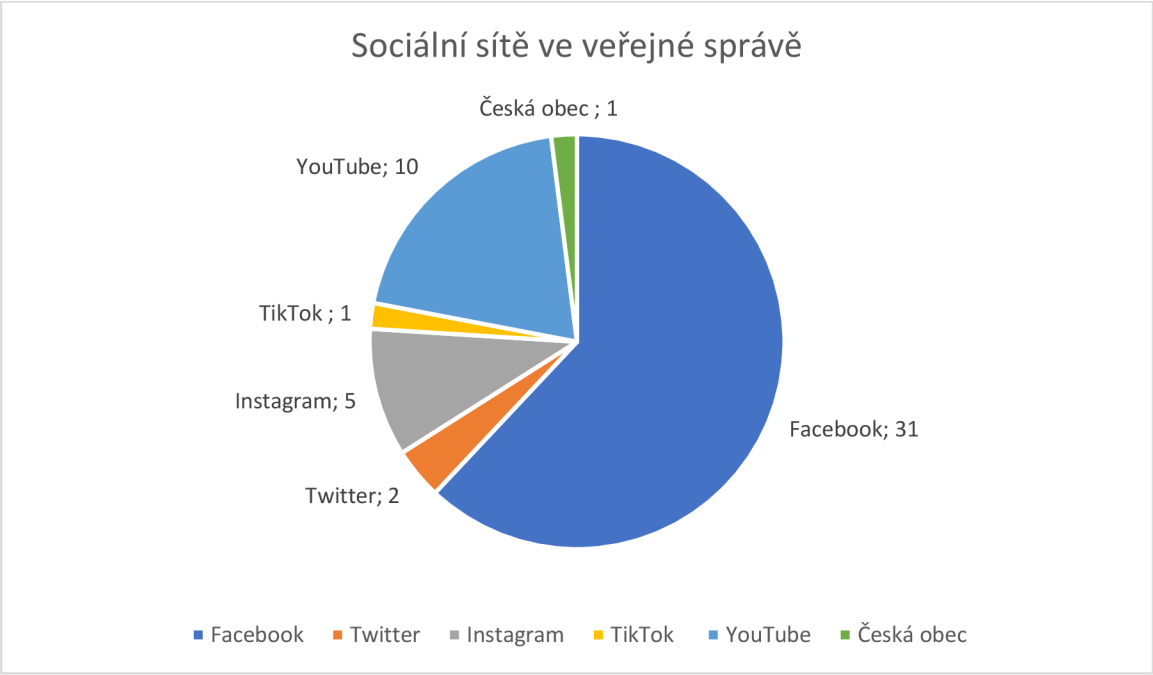
Z výše uvedeného grafu vyplývá následující. Z dotazovaných 70 institucí nevyužívá žádné sociální sítě více jak polovina, konkrétně 53%. Tyto instituce využívají pouze webové stránky, emailovou komunikaci, sms atd. 47% dotazovaných sociální sítě využívá.

Tabulka 3: Využití konkrétních sociálních sítí ve veřejné správě

Facebook	Twitter	Instagram	TikTok	YouTube	LinkedIn	Česká obec
31	2	5	1	10	0	1

Zdroj: vlastní

Obrázek 8: Sociální sítě ve veřejné správě



Zdroj: vlastní

Z tabulky a grafu výše vyplývá, že nejvíce využívaná sociální síť ve veřejné správě je Facebook, tu spravuje celkem 31 institucí. Úspěch má také YouTube, který využívá 10 institucí. Intagram a TikTok zůstává trendem mladých lidí, ve veřejné správě jsou však tyto sociální sítě využívány zřídkakdy. LinkedIn nevyužívá ani jedna z dotazovaných institucí. Jedna z obcí zmínila, že využívá sociální síť Česká obec, která v dotazníku nebyla zmíněna.

Tabulka 4: Rok nasazení sociálních sítí v institucích veřejné správy

	Facebook	Twitter	Instagram	TikTok	YouTube	Česká obec
2012	1	x	x	x	x	x
2014	2	x	x	x	x	x
2015	6	x	x	x	2	x
2016	1	x	1	x	x	x
2017	1	x	x	x	x	x
2018	8	x	x	x	3	x
2019	5	x	x	x	x	x
2020	5	1	3	x	1	x
2021	2	1	1	x	1	1
2022	x	x	x	1	3	x

Zdroj: vlastní

Sociální síť Facebook instituce veřejné správy zakládají od roku 2012, nejvíce institucí účet založilo v roce 2018, a to celkem 8, v roce 2015 účet na Facebooku založilo 6 institucí. Twitter a Instagram instituce zakládají od roku 2020. TikTok založila první instituce veřejné správy v Královehradeckém kraji až v roce 2022. Dvě instituce založily účet na YouTube v roce 2015, tři instituce v roce 2018 a 2022. Účet na sociální síti Česká obec si založila jedna instituce v roce 2021.

Tabulka 5: Zavedení nových sociálních sítí

Zvažování zavedení dalších sociálních sítí?	
ANO	3
NE	30

Zdroj: vlastní

Celkem 30 institucí se vůbec nechystá nasadit další sociální sítě, které nebyly doposud implementovány. 3 instituce uvažují nasadit Instagram, který má velký dosah na mládež, dále Facebook a WhatsApp.

Tabulka 6: Počet uživatelů sociálních sítí ve veřejné správě

Počet uživatelů	Facebook	Twitter	Instagram	TikTok	YouTube	Česká obec
1-100	2	x	1	x	4	x
101-500	13	x	x	x	x	1
501-1000	7	x	1	1	3	x
1001-5000	7	2	3	x	x	x
10000-50000	2	x	x	x	x	x

Zdroj: vlastní

Počet uživatelů na sociálních sítích, které spravují instituce veřejné správy, se pohybuje celkově mezi 1-5000 osob. U Facebooku je nejčastější počet uživatelů mezi 101-500, tento počet eviduje 13 institucí. 7 institucí eviduje počet uživatelů mezi 501-100 a 7 mezi 1001-5000. Pouze dvě instituce evidují počet uživatelů 10000-50000 a další dvě 1-100. U Twitteru evidují počet uživatelů mezi 1001-5000 dvě instituce. U sociální sítě Instagram evidují 3 instituce počet uživatelů mezi 1001-5000, jedna 1-100 a další jedna 501-1000. TikTok využívá jedna instituce, která eviduje počet uživatelů mezi 501-1000. Počet uživatelů u sociální sítě YouTube dosahuje u čtyř institucí počtu mezi 1-100 a u třech institucí 501-1000. Sociální síť Česká obec využívá opět pouze jedna instituce, počet uživatelů se pohybuje mezi 101-500.

Tabulka 7: Hlavní účel sociální sítě

Facebook	Twitter	Instagram	TikTok	Youtube	Česká obec
Informovanost obyvatel	Propagace činnosti instituce	Prezentace fotografií	Propagace činnosti instituce	Poskytování informací	Komunikace s obyvateli
Prezentace akcí	Sdílení informací	Sdílení informací		Sdílení videí	

Zdroj: vlastní

Hlavním důvodem, proč si instituce založily Facebook byl ten, aby mohly informovat obyvatele o změnách, aktuálním dění, budoucích i proběhlých akcích, výběrových řízeních atd., dalším zmiňovaným důvodem je pak prezentace proběhlých akcí, sdílení fotografií a videí. Twitter dle nejčastějších odpovědí slouží k propagaci činnosti instituce a opět k sdílení informací. Instagram slouží ve veřejné správě k sdílení fotografií, pod kterými jsou sděleny důležité či méně důležité informace. TikTok slouží k propagací činnosti instituce, stejné jako Twitter. Youtube instituce využívají k poskytování informací prostřednictvím videí, či živého vysílání, dále slouží k sdílení a záloze videí z akcí instituce. Poslední sociální síť, a to Česká obec je využívána jako sdělovací prostředek, tedy ke komunikaci s obyvateli.

Tabulka 8: Negativní zkušenosti při využívání sociálních sítí ve veřejné správě

Negativní zkušenosti	Facebook	Twitter	Instagram	Youtube
Automatické sdílení/retweet	x	1	x	x
Negativní komentáře	10	x	x	x
Časová náročnost	1	x	x	x
Diskuse mimo téma	1	x	x	x
Žádné	17	x	5	4

Zdroj: vlastní

Na otázku, zda se instituce setkala, či setkává s negativními zkušenostmi při využívání sociálních sítí, drtivá většina odpověděla, že ne. Překvapivě 17 institucí nemá žádné negativní zkušenosti s využíváním Facebooku, 5 s Instagramem a 4 s YouTube. Mezi nejčastější negativní zkušenosti se sociální sítí Facebook patří negativní, až vulgární komentáře pod sdílenými příspěvky. Jedna z obcí byla např. při likvidaci drůbeže při výskytu nákazy ptačí chřipkou soustavně osočována ze strany aktivistickým skupin, další se setkávají s negativní zpětnou vazbou spojenou s nevhodným výběrem obsahu. Jako další negativní zkušenost spojená s využitím Facebooku byla zmíněna časová náročnost obsluhy sociální sítě a diskuse mimo projednávané téma. Mezi negativní zkušenosti s využíváním sociální sítě Twitter bylo zmíněno nastavení automatického sdílení příspěvků jinými profily, což není pro instituce pokaždé žádoucí. K sociální síti TikTok se žádná z institucí nevyjádřila.

Tabulka 9: Pozitivní zkušenosti s využitím sociálních sítí ve veřejné správě

Pozitivní zkušenosti	Facebook	Twitter	Instagram	Youtube	Česká obec
Vyšší účast na akcích	5	x	x	x	x
Rychlá informovanost veřejnosti/ široký dosah	23	1	3	x	1
Pozitivní zpětná vazba	2	1	2	x	x
Sdílení větších videí, jednoduchost	x	x	x	1	x

Zdroj: vlastní

Z výše uvedené tabulky vyplývá, že pozitivní zkušenosti s využitím sociálních sítí ve veřejné správě převyšují negativní zkušenosti. Většina institucí si chválí rychlost a dosah informovanosti veřejnosti, u Facebooku tuto výhodu zmínilo 23 institucí, u Instagramu 3 instituce, u Twitteru a České obce po jedné instituci. Mezi další benefity využívání sociálních sítí patří vyšší účast na akcích, které dané instituce pořádají a propagují na svých sítích, což souvisí s rychlou informovaností a širokým dosahem. Tuto výhodu zmínilo

u Facebooku 5 institucí. Jako další pozitivní zkušenost byla uvedena pozitivní zpětná vazba od uživatelů, u Facebooku a Instagramu mají tuto zkušenost 2 instituce, u Twitteru 1. U sociální sítě YouTube jedna z institucí vyzdvihla pozitivní zkušenost se sdílením objemově větších videí a celkově s jednoduchostí jejich sdílení. K sociální síto TikTok se žádná z institucí nevyjádřila.

Tabulka 10: Celkové zhodnocení využití sociální sítě Facebook

Celkové zhodnocení	Facebook
Pozitivní	20
Negativní	x
Spíše pozitivní	9
Spíše negativní	2

Zdroj: vlastní

I přes negativní zkušenosti, jako jsou negativní komentáře pod příspěvky, instituce hodnotí využití sociální sítě Facebook především pozitivně nebo spíše pozitivně. Ve dvou případech se institucím zdá využití Facebooku spíše negativní, a to například z důvodu časové náročnosti, kterou obsluha sociální sítě vyžaduje.

Tabulka 11: Celkové zhodnocení využití sociální sítě Twitter

Celkové zhodnocení	Twitter
Pozitivní	1
Negativní	x
Spíše pozitivní	1
Spíše negativní	x

Zdroj: vlastní

Využití sociální sítě Twitter je ve veřejné správě méně rozšířené. Prozatím je na ní nahlíženo pouze doplňkově. Dle oslovených institucí je využití této sociální sítě spojováno spíše s pozitivními zkušenostmi.

Tabulka 12: Celkové zhodnocení využití sociální sítě Instagram

Celkové zhodnocení	Instagram
Pozitivní	5
Negativní	x
Spíše pozitivní	x
Spíše negativní	x

Zdroj: vlastní

S využíváním sociální sítě Instagram jsou instituce veřejné správy velmi spokojené, 5 z 5 institucí uvedlo, že mají s touto sítí velmi pozitivní zkušenosti.

Tabulka 13: Celkové zhodnocení využití sociální sítě TikTok

Celkové zhodnocení	TikTok
Pozitivní	1
Negativní	x
Spíše pozitivní	x
Spíše negativní	x

Zdroj: vlastní

TikTok využívá pouze jedna instituce, která je s jejím využitím nad míru spokojená. Instituce doposud žádné negativní zkušenosti neshledala.

Tabulka 14: Celkové zhodnocení využití sociální sítě YouTube

Celkové zhodnocení	YouTube
Pozitivní	5
Negativní	x
Spíše pozitivní	2
Spíše negativní	x
Neutrální	3

Zdroj: vlastní

Co se týče sociální sítě YouTube, ohlasy institucí veřejné správy jsou pozitivní nebo spíše pozitivní. Negativní zkušenosti nebyly shledány. Ve třech případech se instituce nechtěla k celkovému zhodnocení vyjádřit, jelikož sociální síť využívají teprve krátce.

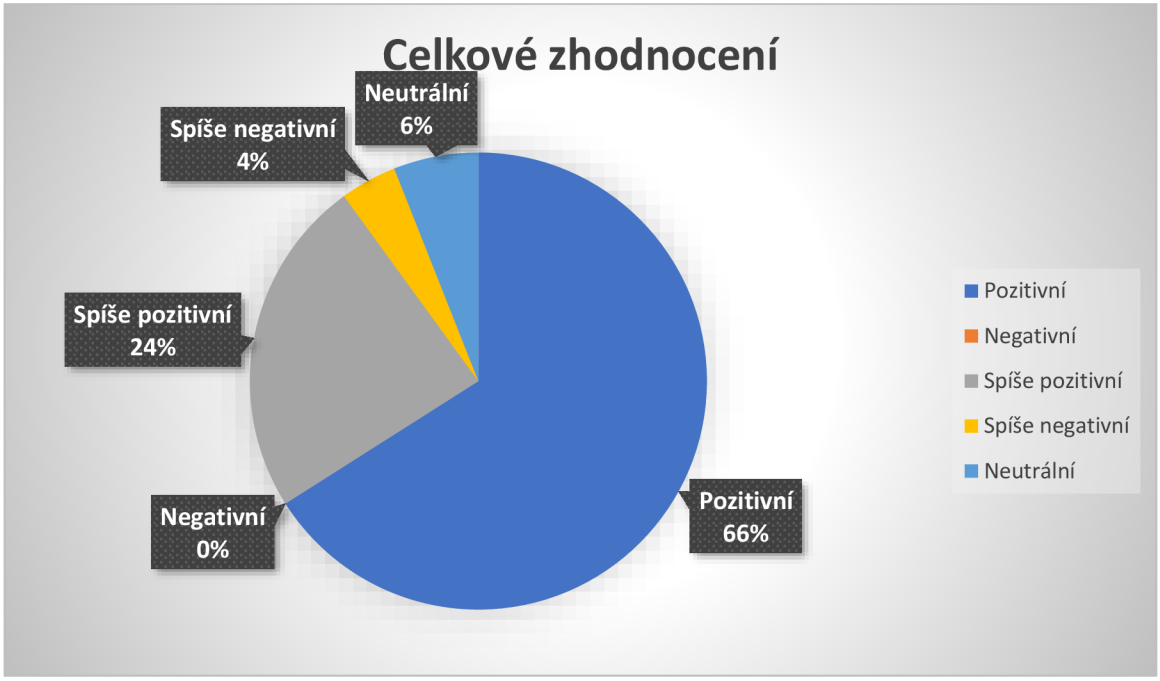
Tabulka 15: Celkové zhodnocení využití sociální sítě Česká obec

Celkové zhodnocení	Česká obec
Pozitivní	1
Negativní	x
Spíše pozitivní	x
Spíše negativní	x

Zdroj: vlastní

Sociální síť Česká obec využívá pouze jedna z dotazovaných institucí, která má s touto sítí výborné zkušenosti a byla doporučena dalším institucím veřejné správy.

Obrázek 9: Celkové zhodnocení využití sociálních sítí ve veřejné správě



Zdroj: vlastní

Z grafu je zjevné, že pozitivní zhodnocení převládá nad negativním. Instituce mají spíše pozitivní zkušenosti a negativním nepřikládají nijak velkou váhu. Z dotazníků vyplývá, že se jedná spíše o zanedbatelné záležitosti.

4.3 Rizika využívání sociálních sítí ve veřejné správě

Tabulka 16: Rizika spojená s využíváním sociální sítí ve veřejné správě

Phishing	Hoaxy	Vulgární, agresivní, negativní reakce	Kybernetické útoky	Ztráta osobních údajů
6	7	16	3	x

Zdroj: vlastní

Na základě vyplněných dotazníků bylo zjištěno, že se instituce v rámci využívání sociálních sítí nejčastěji setkávání s vulgárními, agresivním, či negativními reakcemi uživatelů, tuto zkušenost má 16 ze 70 dotazovaných. Negativní reakce jsou obvykle zpětnou vazbou na výběr sdíleného obsahu, občané buď nereagují vůbec, nebo tento výběr kritizují. Dále se instituce často setkávají s Phishingem a Hoaxy.

Tabulka 17: Řešení rizik ze strany instituce

Jaké bylo prvotní řešení rizika ze strany instituce?	Phishing	Hoaxy	Vulgární, agresivní, negativní reakce	Kybernetické útoky
IT řešení/SPAM filtr	3	1	1	3
Odstranění/ignorace	3	3	10	x
Reakce, odpověď	x	3	5	x

Zdroj: vlastní

Instituce se nejvíce setkávají s vulgárními, agresivními a negativními reakcemi pod příspěvky, které sdílí. Většina z nich tyto situace řeší buď ignorací, odstraněním, či skrytím nevhodných komentářů. Některé z institucí komentář skryjí a následně zahájí soukromou komunikaci s dotyčným útočníkem. Další možností, jak instituce toto riziko řeší, je tedy odpověď na nevhodný komentář. Cílem je uvést věc na pravou míru a upozornit útočníka na nevhodné vyjadřování. Dále se instituce setkávají s Phishingem, který řeší pouhým odstraněním, ignorací či přesunutím do spamu. Hoaxy instituce řeší podobně jako negativní reakce. Buď riziko zcela ignorují, nebo se snaží nepravdy vyvracet, popř. dochází k odstranění nepravdivého komentáře. Kybernetické útoky jsou řešeny IT zásahem.

Tabulka 18: Zavedená opatření

Jaké opatření instituce zavedla?	Phishing	Hoaxy	Vulgární, agresivní, negativní reakce	Kybernetické útoky
Školení	5	3	x	2
IT opatření	1	x	x	1
Sledování komentářů, následná reakce	x	3	5	x
Filtr vulgárních výrazů	x	x	3	x
Blokace útočníků	x	1	3	x
Schvalovací proces příspěvků	x	x	3	x

Zdroj: vlastní

Následná opatření, která byla zavedena po vzniku rizik, jsou následující. Po objevení vulgárních, agresivních, či negativních reakcí se 5 institucí rozhodlo sledovat všechny komentáře a příspěvky, které jsou zveřejňovány osobami mimo instituci, následuje reakce či odstranění/skrytí. Další 3 instituce rozšiřují filtr vulgárních výrazů, 3 instituce blokují útočníky a 3 instituce nejprve schvalují příspěvky, které chtějí lidé mimo instituci na stránkách instituce zveřejnit. Hoaxy jsou řešeny podobně, příspěvky a komentáře jsou hlídány, popř. dochází k reakci či odstranění, v některých případech k blokaci dotyčného uživatele. Co se týče Phishingu, 5 institucí zahájilo povinné školení na toto téma a jedna instituce riziko řeší IT opatřením, a to nastavením SPAM filtru. Kybernetické útoky jsou ošetřeny IT zabezpečením a školením zaměstnanců.

Tabulka 19: Prevence proti rizikům využívání sociálních sítí

Prevence proti rizikům	
Přístup k sociálním sítím – pouze vybraní zaměstnanci	8
Obezřetnost	5
Schvalování obsahu administrátorem	1
IT zabezpečení/bezpečná hesla	8
Školení	1
Žádná	7

Zdroj: vlastní

Prevence proti rizikům využívání sociálních sítí ve veřejné správě řeší 8 institucí omezeným přístupem. Sociální sítě spravuje zpravidla jedna či dvě odpovědné osoby, které dohlíží na bezpečnost obsahu, který se na sociálních sítích vyskytuje apod., ostatní zaměstnanci jsou např. blokování proxy serverem. Používání sociálních sítí instituce je v některých institucích přísně zakázáno využívat na osobních počítačích a mobilních telefonech, naopak soukromé sociální sítě se nesmí využívat na pracovních počítačích a mobilních telefonech. Dále se 8 institucí zaměřuje na IT zabezpečení, najímají k tomu určené externí pracovníky, investuje do bezpečnostních programů, dbá na školení bezpečnosti, nastavování bezpečných hesel apod. 7 institucí preventivní opatření vůbec neřeší a 5 institucí spoléhá na zdravý rozum a obezřetnost.

4.4 Komparace využití sociálních sítí a jejich rizika mezi státní správou a samosprávou

V kapitole komparace využití sociálních sítí a jejich rizika mezi samosprávou (dále jen vzorek č. 1) a státní správou (dále jen vzorkem č. 2) dojde k porovnání využití sociálních sítí a rizik, se kterými se instituce potýkají.

Porovnání využití sociálních sítí mezi vzorkem č. 1 a vzorkem č. 2

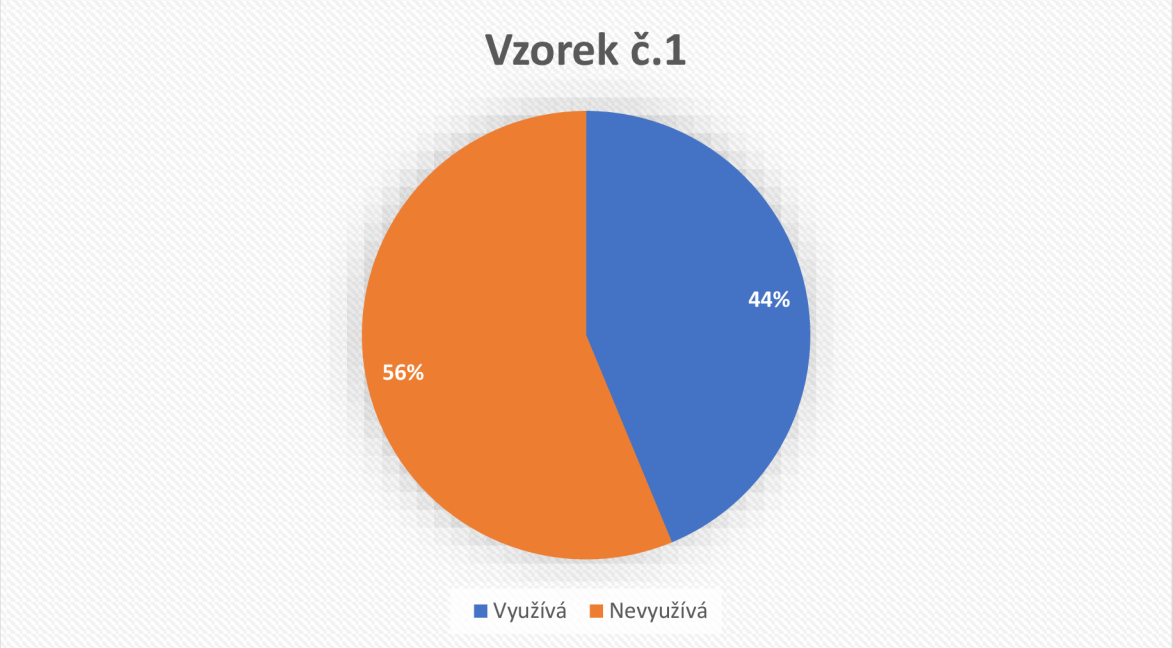
Tabulka 20: Porovnání využívání sociálních sítí mezi vzorkem č. 1 a vzorkem č. 2

Využití sociálních sítí	Vzorek č. 1	Vzorek č. 2
Využívá	28	5
Nevyužívá	36	1

Zdroj: vlastní

Na základě výše uvedené tabulky jsou níže zpracovány grafy s procentuálním vyjádřením institucí, které využívají a které nevyužívají sociální sítě.

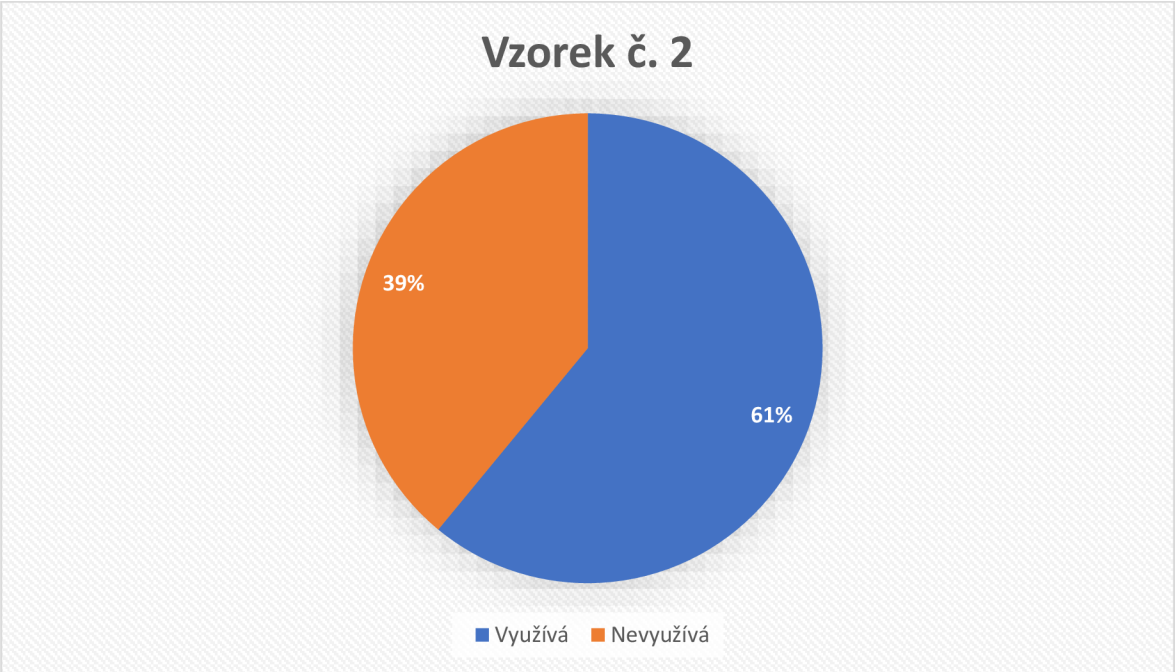
Obrázek 10: Využití sociálních sítí - vzorek č. 1



Zdroj: vlastní

Z grafu výše vyplývá, že vyšší počet institucí ze vzorku č. 1 sociální sítě nevyužívá, jedná se celkem o 56% dotazovaných institucí, 44% z nich sociální sítě využívá.

Obrázek 11: Využití sociálních sítí - vzorek č. 2



Zdroj: vlastní

Z grafu výše vyplývá, že vyšší počet institucí ze vzorku č. 2 sociální sítě využívá, jedná se celkem o 61% dotazovaných. Pouze 39% sociální sítě nevyužívá.

Z obou grafů plyne, že instituce vzorku č. 2 využívají sociální sítě více, než instituce ze vzorku č. 1.

Tabulka 21: Využívané sociální sítě - komparace

	Facebook	**Twitter**	**Instagram**	**TikTok**	**YouTube**	**Česká obec**
Vzorek. č. 1	28	0	3	0	7	1
Vzorek. č. 2	3	2	2	1	3	0

Zdroj: vlastní

Na základě výše uvedené tabulky je zřejmé, že žádná instituce ze vzorku č. 1 nevyužívá sociální síť Twitter a TikTok. Státní správa jde tedy oproti samosprávě s dobou a tyto sociální sítě začíná využívat. Twitter využívají 2 instituce a TikTok využívá jedna instituce ze vzorku č. 2.

Tabulka 22: Sociální sítě využívané ve vzorku č. 1 a č. 2 - procentuální vyjádření

Procentuální vyjádření	Facebook	Twitter	Instagram	TikTok	YouTube	Česká obec
Vzorek. č. 1	100%	0%	10,7%	0%	25%	3,6
Vzorek. č. 2	60%	40%	40%	20%	60%	0%

Zdroj: vlastní

Z důvodu nevyváženého počtu institucí ve vzorku č. 1 a vzorku č. 2 byl počet institucí, které využívají danou sociální síť převeden do procentuálního vyjádření.

Vzorek č. 1 využívá sociální sítě v tomto pořadí:

1. Facebook
2. Youtube
3. Instagram
4. Česká obec

Vzorek č. 2 využívá sociální sítě v tomto pořadí:

1. Facebook a YouTube
2. Twitter a Instagram
3. TikTok

Z komparace dat vyplývá, že vzorek č. 2 využívá více sociálních sítí, než vzorek č. 1. U vzorku č. 1 dominuje sociální síť Facebook, kterou využívá 100% dotazovaných. U vzorku č. 2 jsou na prvním místě sociální sítě Facebook a YouTube, které využívá 60% dotazovaných.

Tabulka 23: Nasazení dalších soc. sítí - vzorek č. 1 a č. 2

Nasazení dalších soc. sítí	Ano	Ne
Vzorek č. 1	3	25
Vzorek č. 2	0	5

Zdroj: vlastní

Z základě tabulky výše vyplývá, že většina institucí vzorku č. 1 nepřemýšlí o nasazení dalších sociálních sítí. U vzorku č. 2 o této možnosti neuvažuje ani jedna instituce. Vzhledem k nepoměru institucí mezi vzorkem č. 1 a vzorkem č. 2 byla vytvořena níže uvedena tabulka v procentuálním vyjádření.

Tabulka 24: Nasazení dalších soc. sítí - vzorek č. 1 a č. 2 procentuální vyjádření

Nasazení dalších soc. sítí - procentuální vyjádření	Ano	Ne
Vzorek č. 1	10,7%	89,3%
Vzorek č. 2	0%	100%

Zdroj: vlastní

89,3% institucí vzorku č. 1 nechce zavádět další sociální sítě, pouze 10,7% plánuje nasadit sociální sítě jako je Facebook, Instragram nebo WhatsApp. 100% institucí vzorku č. 2 další sociální sítě nasazovat nechce.

Tabulka 25: Celkové zhodnocení: Facebook - vzorek č. 1 a č. 2

Celkové zhodnocení - Facebook	Vzorek č. 1	Vzorek č. 2
Pozitivní	60,7%	100%
Negativní	x	x
Spíše pozitivní	32,1%	x
Spíše negativní	7,1%	x

Zdroj: vlastní

Z tabulky celkového zhodnocení využití sociální sítě Facebook vyplývá, že instituce vzorku č. 1 mají s touto sociální sítí pozitivní nebo spíše pozitivní zkušenosti, dohromady se jedná o 92,8%. Pouze 7,1% má spíše negativní zkušenosti. Instituce vzorku č. 2 mají s využíváním sociální sítě Facebook pouze pozitivní zkušenosti.

Tabulka 26: Celkové zhodnocení: Twitter - vzorek č. 1 a 2

Celkové zhodnocení - Twitter	Vzorek č. 1	Vzorek č. 2
Pozitivní	x	50%
Negativní	x	x
Spíše pozitivní	x	50%
Spíše negativní	x	x

Zdroj: vlastní

Z tabulky celkového zhodnocení využití sociální sítě Twitter vyplývá, že 100% institucí vzorku č. 2 mají s touto sociální sítí pozitivní nebo spíše pozitivní zkušenosti. Instituce vzorku č. 1 sociální síť Twitter nevyužívá, zkušenosti s ní tedy nemají.

Tabulka 27: Celkové zhodnocení: Instagram - vzorek č. 1 a č. 2

Celkové zhodnocení - Instagram	Vzorek č. 1	Vzorek č. 2
Pozitivní	100%	100%
Negativní	x	x
Spíše pozitivní	x	x
Spíše negativní	x	x

Zdroj: vlastní

Z tabulky celkového zhodnocení využití sociální sítě Instagram vyplývá, že 100% institucí vzorku č. 1 a vzorku č. 2 mají s touto sociální sítě pozitivní zkušenosti.

Tabulka 28: Celkové zhodnocení: TikTok - vzorek č. 1 a č. 2

Celkové zhodnocení - TikTok	Vzorek č. 1	Vzorek č. 2
Pozitivní	x	100%
Negativní	x	x
Spíše pozitivní	x	x
Spíše negativní	x	x

Zdroj: vlastní

Z tabulky celkového zhodnocení využití sociální sítě TikTok vyplývá, že 100% dotazovaných institucí vzorku č. 2 má s touto sociální sítí pozitivní zkušenosti. Instituce vzorku č. 1 tuto sociální síť nevyužívá, nemá s ní tedy žádné zkušenosti.

Tabulka 29: Celkové zhodnocení: Youtube - vzorek č. 1 a č. 2

Celkové zhodnocení - YouTube	Vzorek č. 1	Vzorek č. 2
Pozitivní	57,1%	33,3%
Negativní	x	x
Spíše pozitivní	28,6%	x
Spíše negativní	x	x
Neutrální	14,3%	66,7%

Zdroj: vlastní

Z tabulky celkového zhodnocení využití sociální sítě YouTube vyplývá, že 85,7% institucí vzorku č. 1 má s touto sociální sítí pozitivní nebo spíše pozitivní zkušenost, zbývajících 14,3% nahlíží na YouTube neutrálně. U vzorku č. 2 se jedná o 66,7% institucí, které mají s využitím sociální sítě YouTube neutrální zkušenosti, zbylých 33,3% má s touto sociální sítí pozitivní zkušenosti.

Tabulka 30: Celkové zhodnocení: Česká obec - vzorek č. 1 a č. 2

Celkové zhodnocení – Česká obec	Vzorek č. 1	Vzorek č. 2
Pozitivní	100%	x
Negativní	x	x
Spíše pozitivní	x	x
Spíše negativní	x	x

Zdroj: vlastní

Z tabulky celkového zhodnocení využití sociální sítě Česká obec vyplývá, že 100% institucí vzorku č. 1 má s touto sociální sítí pozitivní zkušenosti. Vzorek č. 2 sociální síť Česká obec nevyužívá, nemá s ní tedy žádnou zkušenost.

Porovnání rizik sociálních sítí, se kterými se vzorek č. 1 a vzorek č. 2 potýká

Tabulka 31: Rizika využití sociálních sítí - vzorek č. 1 a vzorek č. 2

	Phishing	Hoaxy	Vulgární, agresivní, negativní reakce	Kybernetické útoky	Ztráta osobních údajů
Vzorek č. 1	4	6	12	1	x
Vzorek č. 2	2	1	4	2	x

Zdroj: vlastní

Vzorek č. 1 se potýká s riziky v tomto pořadí

- Vulgární, agresivní, negativní reakce
- Hoaxy
- Phishing
- Kybernetické útoky

Vzorek č. 2 se potýká s riziky v tomto pořadí

- Vulgární, agresivní, negativní reakce
- Phishing a kybernetické útoky
- Hoaxy

Obrázek 12: Rizika využívání sociálních sítí u vzorku č. 1 a č. 2 - procentuální vyjádření

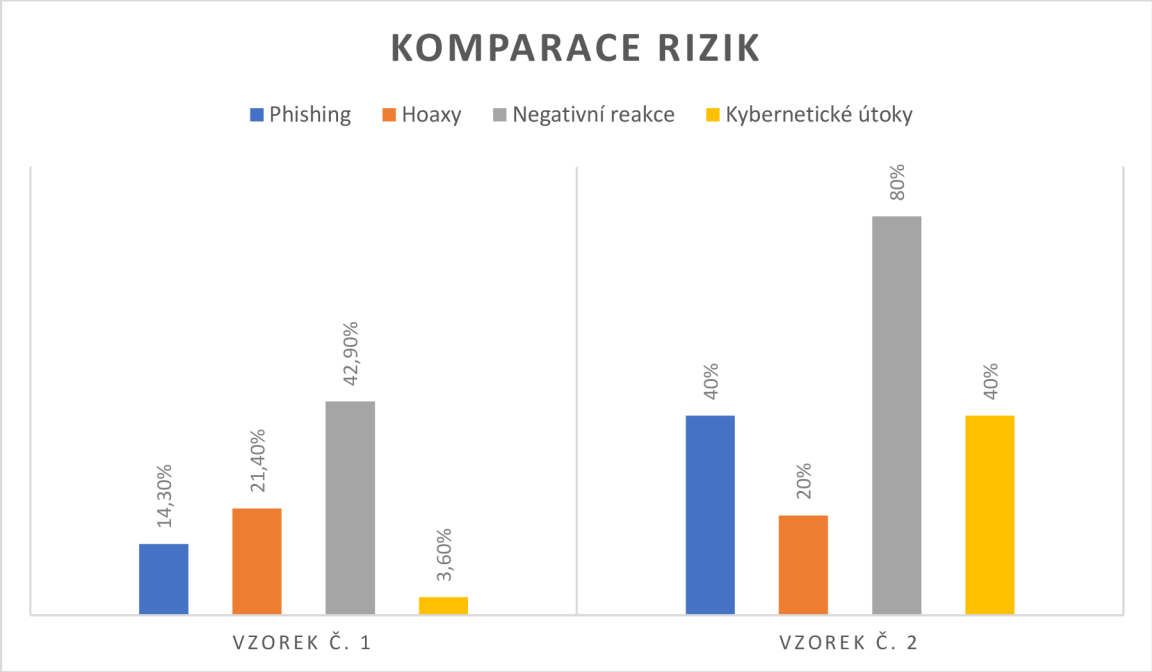
Procentuální vyjádření	Phishing	Hoaxy	Vulgární, agresivní, negativní reakce	Kybernetické útoky
Vzorek č. 1	14,3%	21,4%	42,9%	3,6%
Vzorek č. 2	40%	20%	80%	40%

Zdroj: vlastní

Vzhledem k nižšímu počtu institucí ve vzorku č. 2 byla tabulka s počtem institucí, které se setkávají s jednotlivými riziky převedena do procentuálního vyjádření. Z tabulky nyní vyplývá, že jsou největším problémem v obou vzorcích vulgární, agresivní a negativní reakce. Celkem 42,9% institucí vzorku č. 1 se potýká s tímto rizikem, u vzorku č. 2 je to 80%, tedy drtivá většina. U vzorku č. 1 jsou pak druhým největším rizikem hoaxy, se kterými

se potýká 21,4% institucí. Phishing a kybernetické útoky jsou v rámci vzorku č. 1 zanedbatelnými riziky, se kterými se setkává méně jak 15% dotazovaných. U vzorku č. 2 jsou druhým největším problémem kybernetické útoky spolu s phishingem. S těmito riziky se setkává 40% dotazovaných institucí. S hoaxy se setkává 20% institucí vzorku č. 2.

Obrázek 13: Komparace rizik mezi vzorkem č. 1 a č. 2 - procentuální vyjádření



Zdroj: vlastní

Z grafu vyplývá, že se s riziky setkávají více instituce vzorku č. 2, nežli instituce vzorku č. 2. Pouze v jednom případě se vzorek č. 1 setkává s daným rizikem častěji, jedná se o hoaxy. V tomto případě je procento institucí vyrovnané, u vzorku č. 1 se jedná o 21,4% dotazovaných institucí a u vzorku č. 2 se jedná o 20% dotazovaných institucí.

5 Výsledky

V praktické části bylo zkoumáno, jaké sociální sítě instituce veřejné správy v Královehradeckém kraji využívají, jaké s nimi mají zkušenosti a s jakými riziky se v rámci využívání sociálních sítí setkali.

Na základě provedeného šetření bylo zjištěno několik následujících poznatků. Instituce veřejné správy využívají převážně sociální síť Facebook. Tuto sociální síť využívá 44,3% institucí z celkových 70 dotazovaných a 93,9% z těch, které využívají alespoň jednu sociální síť. Dále se data odvíjí od počtu institucí, které využívají alespoň jednu sociální síť. Facebook je nejdéle využívaná sociální síť ve veřejné správě Královehradeckého kraje, některé instituce ji využívají již od roku 2012. Mezi hlavní účely využití Facebooku patří dle institucí informovanost obyvatel a prezentace akcí, což úzce souvisí s pozitivními zkušenostmi, jako je vyšší účast na organizovaných akcích, rychlejší informovanost veřejnosti a široký dosah. Mezi negativní zkušenosti využívání sociální sítě Facebook patří negativní komentáře, diskuse mimo téma a časová náročnost. Více jak polovina, konkrétně 54,8% institucí se nesetkalo se žádnou negativní zkušeností spjatou s využíváním Facebooku. Co se týče celkového zhodnocení, 93,5% institucí nahlíží na využití sociální sítě Facebook pozitivně nebo spíše pozitivně, pouze 6,5% institucí má s Facebookem spíše negativní zkušenosti a nevidí v jejím využití přínos. Z těchto dat je zřejmé, že je sociální síť ve veřejné správě velmi oblíbená a v podkapitole „Návrhy na implementaci sociální sítí" o ní bude dále diskutováno.

Druhou nejčastěji využívanou sociální sítí ve veřejné správě je YouTube, Tuto síť využívá 14,3% z celkových 70 dotazovaných a 30,3% z těch, které využívají alespoň jednu sociální síť. Dále se data odvíjí od počtu institucí, které využívají alespoň jednu sociální síť. Účty na sociální síti YouTube začaly instituce veřejné správy zakládat a využívat o něco déle, než Facebook, konkrétně tedy od roku 2015. Mezi hlavní účely sociální sítě řadí instituce šíření informací prostřednictvím sdílení videí. Jako pozitivní zkušenost instituce shledaly sdílení objemově větších videí a jednoduchost jejich publikace. 40% institucí uvedlo, že se při využívání YouTube nesetkalo s negativní zkušeností. Zbytek institucí se ke konkrétním zkušenostem nevyjádřil, jelikož využívají YouTube pouze doplňkově. Co se týče celkového zhodnocení využití sociální sítě YouTube, 70% institucí nahlíží na síť pozitivně nebo spíše pozitivně, zbylých 30% má na využívání sítě neutrální pohled. Přesto,

že není sociální síť až tak moc využívána, je na ní nahlíženo spíše pozitivně, v kapitole „Návrhy na implementaci sociální sítě“ o ní bude také diskutováno.

Třetí nejčastěji využívanou sociální sítí ve veřejné správě je Instagram. Tuto síť využívá 7,1% z celkových 70 dotazovaných a 15,2% z těch, které využívají alespoň jednu sociální síť. Dále se data odvíjí od počtu institucí, které využívají alespoň jednu sociální síť. Instagram využívají Instituce teprve krátce, a to od roku 2020, pouze jedna z institucí si založila účet už v roce 2016. Za hlavní účely Instagramu považují instituce šíření informací pod sdílenými fotografiemi, což opět souvisí s pozitivními zkušenostmi, jako je rychlá informovanost veřejnosti, široký dosah informací a pozitivní zpětná vazba, která je důležitá pro motivaci instituce v pokračování obsluhy sociální sítě. Negativní zkušenost s touto sociální sítí nemá ani jedna instituce. Jak je z výše uvedeného zřejmé, celkové zhodnocení je jednoznačné. Všechny instituce nahlíží na Instagram pozitivně a jedná se o velmi přínosnou síť. V kapitole „Návrhy na implementaci sociální sítě“ o ní bude zmíněno.

Další sociální sítě, jako je Twitter, TikTok a Česká obec nejsou téměř využívány, instituce jejich účty zakládá teprve od roku 2020, pozitivní a negativní zkušenosti nelze prozatím hodnotit. Tyto sociální sítě jsou využívány pouze doplňkově. Z výše uvedených důvodu nepovažuji za důležité, aby byly tyto sociální sítě ve veřejné správě nasazeny.

Mezi rizika spojené s využíváním sociální sítí, se kterými měli instituce veřejné správy v minulosti zkušenost, patří phisting, hoaxy, negativní reakce a kybernetické útoky. Téměř polovina, přesněji 48,5% institucí se setkala s negativními, vulgárními, až agresivními reakcemi pod zveřejněným obsahem či v soukromých zprávách na sociálních sítích, 21,2% institucí se setkala s hoaxy, neboli falešnými zprávami, 18,2% s phishingem a 9,1% s kybernetickými útoky. Za nejčastější hrozbu jsou tedy považovány negativní reakce, které instituce řeší především odstraněním, ignorací nebo domluvou. Odstraněním a ignorací tuto situaci řeší 62,5% z těch, kteří toto riziko zaznamenali. Mezi opatření, která instituce proti těmto reakcím zavedla, patří sledování komentářů, blokování útočníků, filtr vulgárních výrazů, aby nedocházelo ke zveřejnění negativních reakcí a schvalovací proces příspěvků.

V rámci komparace využívání sociálních sítí mezi státní správou a samosprávou bylo zjištěno, že sociální sítě využívá spíše státní správa, než samospráva. U státní správy využívá sociální sítě 61% dotazovaných, sociální sítě tedy nevyužívá 39%. U samosprávy využívá sociální sítě 44% dotazovaných institucí a nevyužívá je 56%. Doporučení nasazení

sociálních sítí se v kapitole 5.1 bude věnovat především samosprávě, a to z důvodu, že sociální sítě nevyužívá více jak polovina dotazovaných. Na otázku, zda daná instituce uvažuje o nasazení další sociální sítě, které nebyly doposud implementovány, odpovědělo 89,3% institucí vzorku č. 1, že tuto možnost nezvažuje, u vzorku č. 1 tuto možnost nezvažuje 100% institucí.

Co se týče komparace rizik spojených s využíváním sociálních sítí mezi státní správou a samosprávou, největším rizikem jsou pro všechny instituce vulgární, agresivní a negativní reakce. 42,9% institucí samosprávy a 80% institucí státní správy se setkává s těmito reakcemi. Kapitola 5.2 se bude věnovat návrhem na eliminaci tohoto rizika. 21,4% institucí samosprávy se dále potýká s hoaxy. 14,3% těchto institucí se dále setkává s phishingem. Kybernetické útoky nedosahují ani 4%, lze je tedy považovat za zanedbatelné. U institucí státní správy je to o dost jiné, 40% institucí se setkává s phishingem a kybernetickými útoky, což je oproti institucím samosprávy o dost více. Zato s hoaxy se setkává 20% institucí státní správy, podobně jako u institucí samosprávy. Zatímco instituce samosprávy by se měli mimo hlavní riziko vulgárních, agresivních a negativních reakci věnovat také minimalizaci výskytu hoaxů, státní správa by se měla zaměřit spíše na phishing a hybernetické útoky.

5.1 Doporučení nasazení sociálních sítí

Drtivá většina institucí veřejné správy není nakloněna zavádění sociálních sítí. Instituce, které nevyužívají žádnou sociální síť, tuto možnost ani nezvažují. Celkem 90,9% institucí, které využívají alespoň jednu sociální síť, nechce nasazovat další sociální sítě, pouze 9,1% institucí tuto možnost zvažuje. Doporučením je nad nasazením sociálních sítí uvažovat, a to vzhledem k velmi pozitivním ohlasům a pouze ojedinělým výskytům rizik, která jsou spojená s využíváním sociálních sítí ve veřejné správě.

Instituce, které nevyužívají žádnou sociální síť.

Každá instituce v České republice by měla využívat alespoň jednu sociální síť, a to Facebook, která je ve veřejné správě nejvyužívanější sociální sítí.

Doporučení směřuje především k institucím samosprávy, konkrétně k obecním úřadům v obcích s nízkým počtem obyvatel (tj. pod 500 obyvatel), které ve většině případech na základě výše uvedených výsledků nevyužívají žádnou sociální síť. Zavedení sociálních sítí by mělo přilákat mladší generace, které žijí v i mimo danou obec.

Přínosy zavedení sociálních sítí v malých obcích:

- Zvýšení účasti na pořádaných akcích (vyšší zisk stánkařů, vstupné atd.)
- Příliv turistů (pokud má obec co nabídnout, dochází ke zvýšení rekreační atraktivity)
- Snadný přístup k informacím
- Otázky regionálního rozvoje (podílení se místních obyvatel na rozhodování)
- Potenciální vnitrostátní migrace

Mále obce, kde převládá příroda, zemědělství a nízká hustota zalidnění, prezentaci na sociálních sítích mnohdy neřeší, což je ale škoda. Pokud tyto obce pořádají například pravidelné trhy, které navštěvují pouze místní, je možné díky sociálním sítím účast navýšit. S účastí se pojí vyšší zisk, podpora malých podnikatelů a vyšší povědomí o existenci dané obce. Sdílení různých akcí bude mít mnohem větší dosah, než vylepování letáků. Sdílení fotografií zajímavých míst v obci může zajistit příliv turistů, čímž opět dochází k podpoře malých podnikatelů a zvýšení rekreační atraktivity obce. Dalším důvodem, proč by měly mít tyto obce sociální sítě, jsou informace pro veřejnost na dosah ruky, jelikož hlavním účelem sociálních sítí institucí veřejné správy je právě informovanost veřejnosti. Pro mladší generace bude příjemnější informace získávat prostřednictvím sociálních sítí, než webových stránek, navíc lze informace jednoduše sdílet a vyjadřovat se k nim. Dále je možné díky sociálním sítím řešit otázky regionálního rozvoje, které by měly být řešeny v souladu s představami místních obyvatel, o těch se lze jednoduše dozvědět prostřednictvím anket nebo příspěvků na sociálních sítí. Sociální sítě mohou být také nástrojem, jak přilákat do obce nové lidi, a to kvalitní prezentací obce, sdílením informací o možnostech pronájmu obecních bytů, či prodeji pozemků ve vlastnictví obce.

Instituce, které využívají alespoň jednu sociální síť

Doporučením pro instituce, které využívají alespoň jednu sociální síť je nasazení další sociální sítě, kterou instituce prozatím nevyužívá, a to v tomto pořadí.

1. Facebook
2. Youtube
3. Instagram
4. Twitter
5. TikTok

Doporučení se týká všech institucí státní správy a samosprávy.

Na základě analýzy obdržených dat od jednotlivých institucí je zřejmé, že jsou pro ně sociální sítě spíše přínosné. Sociální sítě jim zlepšují image, zvyšují účast na akcích, či usnadňují informovanost veřejnosti. Tento přínos lze násobit sdílením na více sociálních sítích. Implementace dalších sociálních sítí by měla být uskutečněna s odstupem minimálně jednoho roku od zavedení z důvodu sžívání se s novou sociální sítí. Nelze tedy nasadit všechny sociálních sítí v jeden čas. Tato skutečnost by mohla zapříčinit časovou náročnost správy sociálních sítí, odkládání zveřejnění příspěvků atd., což by zapříčinilo nenaplnění záměru využívání sociálních sítí.

Pro nejčastější riziko, se kterým se instituce setkávají a které je odrazuje od nasazení další sociální sítě, uvádím návrh na jeho minimalizaci v kapitole 5.3.

5.2 Návrhy na minimalizaci rizik

Obsah nesplnil účel/obsah byl nahlášen a odstraněn

Většina institucí vzorku č. 1 a č. 2. se potýká pod svými příspěvky s negativními ohlasy občanů. Negativní ohlasy nebo žádné ohlasy jsou na základě analýzy dat v některých případech dopadem chybně prezentovaného obsahu. Pod nevhodně prezentovaným příspěvkem se seběhne lavina negativních komentářů, které jsou pro instituci velmi důležitou zpětnou vazbou. Žádný komentář je pro instituci také zpětná vazba, kterou není ideální přehlížet. Pokud převažují negativní reakce nad pozitivními, je zapotřebí uvažovat nad obsahem, který instituce na sociálních sítích zveřejňují a nad tím, co může ve čtenářích vyvolávat negativní emoce vedoucí k vulgarismu a agresivitě pod danými příspěvky.

V některých případech dochází ze strany občanů k nahlášení příspěvku a následné odstranění ze strany správce sociální sítě. Instituce tuto situaci řeší buď ignorací, nebo odstraněním nevhodných komentářů. V pár případech došlo také k nahlášení a odstranění celé sociální sítě, řešením bylo dále nevystupovat na žádné sociální síti.

Návrhem na minimalizaci těchto rizik je jasně definovaná politika využívání sociálních sítí, dle které se bude instituce řídit. Doporučení, jaké typy příspěvků, v jakém čase, frekvenci a jaké vizuály by měly instituce sdílet, je uvedeno v tabulce níže. Tato doporučení povedou k spokojenosti čtenářů, jelikož jim ve většině případů bude dávat možnost výběru obsahu a také možnost se vyjádřit. Jelikož jsou na základě analýzy dat nejčastěji využívanými institucemi Facebook, Instagram a Youtube, budou zmíněny doporučení pro využití těchto sociálních sítí.

Tabulka 32: Návrh na minimalizaci rizika - obsah nesplnil účel/obsah nahlášen a odstraněn

	Facebook	Instagram	YouTube
Typy příspěvků	Akce pořádané institucí, ankety, časté dotazy, důležité informace	Prezentace uplynulých akcí, důležité informace	Zodpovězení častých dotazů, prezentace akcí, projektů atd.
Časy a frekvence zveřejňování	2x týdně příspěvek, 1x měsíčně anketa (13-16 hodin)	Každý den 3-5 stories, 1x týdně příspěvek nebo reels (v 17 hodin odpoledne)	1x měsíčně video, 1x týdně reels (v odpoledních hodinách)
Vizuály	Min. 1 fotografie u každého příspěvku	Příspěvky s několika fotkami, carousels	Reels, kvalitní videa - dialog s publikem, dát publiku možnost rozhodovat o obsahu
Zabezpečení	Zákaz přidávání příspěvků občany popř. schvalování těchto příspěvků, kontrola komentářů, sdílení příspěvků s upozorněním na etický kodex komunikace na soc. sítí, zabezpečení účtu	Kontrola komentářů, blokace falešných profilů, reagování na nevhodné soukromé zprávy – upozornění na etický kodex komunikace na soc. sítích, zabezpečení účtu	Kontrola komentářů, blokace falešných profilů, zabezpečení účtu

Zdroj: vlastní

Na základě výše uvedeného doporučení by měly instituce na svém Facebookovém účtu sdílet následující příspěvky. Příspěvky o plánovaných akcích, a to alespoň 1 měsíc dopředu s připomenutím 1 týden a 1 den před akcí. Pokud instituce organizuje akci několik měsíců dopředu, vytvoří událost bezprostředně a upozorní sdílením události 1 týden a 1 den před

akcí. V příspěvku o události sdílené nejméně 1 měsíc předem musí být informace typu: kde, kdy, vstupné, program. 1 týden před akcí by měla být sdílena akce s informací navíc, která zaujme a přitáhne další účastníky. 1 den před akcí je zapotřebí akci sdílet pro připomenutí a informací, že se instituce na návštěvníky akce těší. Mezi další příspěvky je vhodné zahrnout často pokládané dotazy, např. prostřednictvím datové schránky, telefonicky nebo osobně. Tímto způsobem lze minimalizovat vytíženost osob zaměstnaných v institucích a předcházení kumulace stejných dotazů. S tím se pojí sdílení novinek, důležitých informací a např. návodů – jak žádat o dotace atd. Další součástí správy sociální sítě Facebook je doporučeno sdílení anket, které je vhodné zapojit v rámci rozvoje regionu a řešení důležitých otázek, které se přímo dotýkají obyvatel. Pokud se např. obec rozhoduje, zda investovat do nové sportovní haly nebo rekonstrukce divadla, je namístě se zeptat svých občanů. Anketa může a nemusí ovlivnit rozhodování při plánování regionálního rozvoje, nicméně se jedná o nejjednodušší způsob, jak se dostat k názoru obyvatel. Časy a frekvence zveřejňování se odvíjí od časové vytíženosti správce sociálních sít, nicméně doporučuji sdílet minimálně 2 příspěvky týdně, a to mezi 13. a 16. hodinou. Spamováním příspěvky každý den by instituce docílila poklesu sledujících. U každého příspěvku by neměla chybět fotografie, která na první pohled ukáže, o čem příspěvek je a inspiruje tak publikum obsah přečíst.

Co se týče Instagramových účtů, zaměřeny by měly být na sdílení fotografií a důležitých informací, které lze popsat ve zkratce, např. se může jednat o uplynulé akce, jako jsou konference, ale i akce pro občany. Pod těmito příspěvky by měl být pokaždé krátký komentář s nejdůležitějšími informacemi – co bylo účelem akce, kde se akce odehrávala, co je přínosem akce. Na rozdíl od uplynulých akcí by měla instituce o akcích, které se budou teprve konat přidávat spíše krátké stories, alespoň 1 měsíc dopředu o tom, kde, co, pro koho, za jakým účelem bude instituce akci pořádat. 1 týden a 1 den před akci znovu připomenout prostřednictvím stories. Tyto stories je zapotřebí ukládat do výběrů a pojmenovávat je tak, aby bylo zřejmé, pro koho jsou tyto akce pořádané. Lidé se tak budou věnovat výběrům, které se jich týkají a nepřehlédnou akci, která je vhodná zrovna pro ně. Např. obce mohou vytvořit výběr s názvem „Plánované akce – děti do 12 let“, „Plánované akce – senioři“, „Plánované akce – starostové/zastupitelé obcí/měst“ atd. Stejně tak může svoje výběry pojmenovat Hasičský záchranný sbor Královehradeckého kraje – př. „Plánované akce – hasiči Královehradeckého kraje“, „Plánované akce – hasiči ČR“ nebo „Plánované akce – milovníci hasičských závodů“. Pro efektivnější prezentaci těchto akcí lze využít Insta Stories

Carousel, což je rotující formát reklamy, která dává možnost sdělit více a lépe tak zaujmout. Součástí této funkce je proklik na web, kde se publikum dozví mnohem více informací, než je instituce schopna sdílet prostřednictvím stories nebo příspěvků. Instituce by měla sdílet každý den alespoň 3-5 stories a 1x týdně příspěvek nebo reels, a to především v odpoledních hodinách. Stories by se měly týkat zajímavostí, novinek a důležitých informacích, např. město může prostřednictvím nich upozornit, že ve velmi frekventované oblasti města bude probíhat oprava kanalizace nebo údržba silnic, lze takto minimalizovat dopravní komplikace. Za zajímavost lze považovat např. sázení alejí, otevření nového hřiště pro děti, za důležité informace např. poskytnutí informace, že daná instituce vypsala výběrové řízení na konkrétní pozici, stručné informace o možnostech čerpání dotací s odkazem na kompetentní osobu atd.

Sdílení obsahu na YouTube by mělo mít také svá pravidla. Jelikož je tato sociální síť určena ke sdílení videí a reels, zabere její správa hodně času. Doporučením je tedy sdílet videa pouze 1x měsíčně, a to pokaždé ve stejný den nebo nejbližší pracovní den a ve stejnou hodinu, nejlépe v odpoledních hodinách. Aby byla instituce neustále na očích, je vhodné 1x týdně nahrát krátké video „reels“, ve kterých zazní zajímavé informace, které lze sdělit ve zkratce. Videa vydávaná 1x měsíčně by měla být opět zaměřena na zodpovězení nejčastějších dotazů, prezentace uplynulých akcí, plánovaných projektů, prezentace činnosti a různých postupů pro veřejnost (např. krok po kroku, jak vyplnit žádost). Ve videích, která jsou zaměřena na představení jakéhokoliv plánu, který se týká veřejnosti, by měla instituce vést s publikem dialog. Instituce tak obdrží v komentářích zpětnou vazbu, která může být velmi přínosná. Správce sociální sítě by se měl na závěru videa ptát, jaká témata lidé chtějí, aby v příštích videích zazněla. Nestane se tak, že instituci dojdou nápady a zároveň dojde k uspokojení publika a mnohem vyšší sledovanosti.

Zabezpečení

Mezi možnosti, jak se vyhnout na všech výše uvedených sociálních sítích zveřejňováním nevhodného obsahu samotným občanem je zákaz přidávání příspěvků všem osobám mimo správce. Alternativou je schvalování příspěvků, které přidává jiná osoba, než je správce. Správce by měl pravidelně sledovat komentáře a účty, které se pohybují na sociálních sítích institucí. V případě, že se pod příspěvky objeví komentáře od podezřelého účtu, který se jeví jako falešný, je zapotřebí takový profil nahlásit a zablokovat. Stejně tak, pokud se po příspěvky opakují stejná jména, u kterých nelze zjednat nápravu je nejlepším

řešením nahlášení a blokace. Mezi další možnosti je filtr nevhodných výrazů, sníží se tak počet komentářů, které obsahují sprostá slova atd. V neposlední řadě je zapotřebí mezi své příspěvky zařadit i příspěvky o etickém kodexu vystupování na sociálních sítí. Lze pod každým příspěvkem zmínit, že budou nevhodné komentáře odstraněny a osoby odebrány ze skupin nebo rovnou blokovány, čímž jim bude odepřen vstup na sociální síť dané instituce.

Zabezpečení účtů:

- Všechny sociální sítě pojmenovat stejným názvem, kterou nese instituce
- Účty ve správě instituce, nikoli zaměstnance
- Omezený počet správců
- Registrace alternativních názvů
- Dvoufázová autentizace
- E-mail, který bude sloužit výhradně pro správu sociálních sítí
- Využívání zařízení instituce, nikoli soukromých zařízení
- Bezpečná hesla
- Přihlašovat se prostřednictvím Wi-Fi instituce
- Status ověřeného účtu
- Pravidelné kontroly a audity
- Odhlašování z účtu
- Plán pro případ ztráty přístupu

6 Závěr

Cílem této diplomové práce s názvem „Sociální sítě a jejich rizika v prostředí institucí veřejné správy v Královehradeckém kraji“ bylo zjistit, jaké sociální sítě vybrané instituce využívají, jaké zkušenosti s jejich využíváním mají a s jakými riziky se v rámci využívání těchto sociálních sítí setkávají.

Teoretická část práce je rozdělena na 4 kapitoly a několik podkapitol, které byly věnovány vymezení základních pojmů, jako je sociální síť, veřejná správa, komunikace, riziko atd. Následovala kapitola zaměřená na specifika veřejné správy, která má omezené možnosti vystupování na sociálních sítí oproti běžnému uživateli. Jelikož se veřejná správa musí při spravování sociálních sítí řídit zákony, podkapitoly se věnují nařízení GDPR, zákonu o eGovernmentu, zákonu o zpracování osobních údajů a pro zajímavost zákonu policie České republiky, který umožňuje Policii ČR zveřejňovat osobní údaje pachatelů nebo pohřešovaných osob. Další kapitolou jsou specifika komunikace veřejné správy, která souvisí se strukturou veřejné správy a jejími činnostmi, podkapitoly se věnují komunikaci ve veřejné správě, tedy jak lze s veřejnou správou komunikovat, dále historii komunikace, zásadním milníkům nasazení sociálních sítí nejznámějších institucí ČR, soutěži zlatý erb a statistikám. Čtvrtá kapitola je zaměřena na vymezení nejčastějších rizik využívání sociálních sítí, mezi které patří kybernetická kriminalita, porušení zabezpečení, falešná tvrzení a agrese na sociálních sítích.

Praktická část diplomové práce byla zaměřena na správce sociálních sítí institucí v Královehradeckém kraji. Vybráno bylo celkem 70 institucí, z toho 6 institucí státní správy a 64 institucí samosprávy. Prostřednictvím e-mailové komunikace byl správcům jednotlivých institucí rozeslán krátký dotazník, který zjišťoval následující: jaké sociální sítě instituce využívá, za jakým účelem, jak dlouho tyto sítě využívá, jaké má instituce s využíváním sociálních sítí negativní a pozitivní zkušenosti, jak celkově využívání sociálních sítí hodnotí a zda instituce přemýšlí o nasazení dalších sociálních sítí. Dotazník byl dále zaměřen na rizika, která souvisí s využíváním sociálních sítí. Správci byli dotazování, zda se setkali nebo setkávají s riziky jako je phishing, hoaxy, negativní reakce, kybernetické útoky, či ztráta osobních údajů, jak byly tyto situace ze strany instituce řešeny, jaké opatření instituce zavedla a jaká prevence je v instituci zavedena proti vzniku rizik.

Tato část byla rozdělena na základě cílů práce do 4 kapitol. První se zabývá metodickým zpracováním, tedy výběrem respondentů, šetřením a zpracováním získaných

dat. V kapitole využití sociálních sítí ve veřejné správě a kapitole rizika využívání sociálních sítí ve veřejné správě došlo k vyhodnocení získaných dat od správců sociálních sítí jednotlivých institucí. Ve čtvrté kapitole došlo k porovnání využití sociálních sítí a rizik mezi státní správou a samosprávou.

Ze získaných dat vyplynulo, že sociální sítě využívá především státní správa a nevyužívá je drtivá většina obecních úřadů v obcích s nízkým počtem obyvatel, proto bylo těmto obcím doporučeno využívat alespoň jednu sociální síť. Dále bylo zjištěno, že je největším rizikem, se kterým se instituce veřejné správy setkávají negativní reakce publika. Na základě slovního vyjádření správců ohledně vulgárních, agresivních a negativních reakcí bylo zjištěno, že se v některých případech jedná o chybu instituce, kdy zveřejňuje nevhodný obsah. Takový obsah vyvolává ve čtenáři negativní emoce. Z tohoto důvodu bylo navrženo doporučení, jakým způsobem by instituce měla příspěvky zveřejňovat, čeho by se měly týkat, v jaké frekvenci je ideální příspěvky zveřejňovat a jaké zabezpečení by instituce měla v rámci správy sociálních sítí dodržovat.

7 Bibliografie

1. BEDNÁŘ, Vojtěch. *Internetová publicistika.* Praha : Grada, 2011. ISBN 978-80-247-3452-1.

2. Twitter Facebook Instagram icon. *SSL.* [Online] 2015. [Citace: 17. 7 2022.] Dostupné z: http://ssl.edu/twitter-facebook-instagram-icon-6.

3. SCIRRI, Kaitlin. *How Facebook changed the world.* New York : Cavendish Square, 2018. ISBN 9781502641083.

4. DULING, Kaitlyn. *How twitter changed the world.* New York : Cavendish Square, 2019. ISBN 9781502641205.

5. About LinkedIn. *LinkedIn.* [Online] LinkedIn Corporation, 2022. [Citace: 17. 7 2022.] Dostupné z: https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl.

6. Teens, Social Media and Technology 2022. *Pew Research Center.* [Online] 10. 8 2022. [Citace: 17. 9 2022.] Dostupné z: https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

7. Snap Inc. *Snapchat.* [Online] Snap Inc., 2022. [Citace: 17. 9 2022.] Dostupné z: https://www.snap.com/en-GB?lang=en-US.

8. O aplikaci. *TikTok.* [Online] 2022. [Citace: 17. 9 2022.] Dostupné z: https://www.tiktok.com/about?lang=cs.

9. Aplikace TikTok představuje bezpečnostní hrozbu. *Národní úřad pro kybernetickou a informační bezpečnost.* [Online] 8. 3 2023. [Citace: 27. 3 2023.] Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1941-aplikace-tiktok-predstavuje-bezpecnostni-hrozbu/.

10. ŠKODA, Jan. Státní úřady i soukromé firmy ruší účty na TikToku, některé budou zákaz užívání aplikace kontrolovat. *Česká televize.* [Online] Česká televize 1996–2021, 17. 3 2023. [Citace: 27. 3 2023.] Dostupné z: https://ct24.ceskatelevize.cz/domaci/3572363-statni-urady-i-soukrome-firmy-rusi-ucty-na-tiktoku-nektere-budou-zakaz-uzivani.

11. Co je Česká obec. *Česká obec .* [Online] webhouse, 2022. [Citace: 10. 3 2023.] Dostupné z: https://www.ceskaobec.cz/.

12. KÁŇA, Pavel. *Základy veřejné správy: vybrané kapitoly veřejné správy pro studium žáků středních škol. 4., aktualiz. vyd.* Ostrava : Montanex, 2014. ISBN 978-80-7225-407-1.

13. MIKULÁŠTÍK, Milan. *Komunikační dovednosti v praxi 2., dopl. a přeprac. vyd. .* Praha : Grada, 2010, Manažer. ISBN 978-80-247-2339-6.

14. VYBÍRAL, Zbyněk. *Psychologie komunikace.* Praha : Portál, 2005. ISBN 807178-998-4.

15. TURECKIOVÁ, Michaela. *Klíč k účinnému vedení lidí: odemkněte potenciál svých spolupracovníků.* Praha : Grada, 2007. ISBN 978-80-247-0882-9.

16. DEVITO, Joseph A. *Základy mezilidské komunikace: 6. vydání.* Praha : Grada, 2008. ISBN 978-80-247-2018-0.

17. Riziko. *Ministerstvo vnitra České republiky.* [Online] Ministerstvo vnitra České republiky, 2023. [Citace: 20. 2 2023.] Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx.

18. BARTONĚK, Josef. Regionální rozvoj. *Rok v obci.* [Online] 10. 11 2015. [Citace: 15. 3 2023.] Dostupné z: http://www.rokvobci.cz/zpravy-redaktoru/detail/769-21-regionalni-rozvoj/.

19. Ministerstvo vnitra. *Vstupní vzdělávání následné, organizace a činnost veřejné správy.* [Online] 2022. [Citace: 13. 3 2023.] Dostupné z: https://www.mvcr.cz/.

20. SLAVÍK, Jakub. *Marketing a strategické řízení ve veřejných službách: jak poskytovat zákaznicky orientované veřejné služby.* Praha : Grada, 2014. ISBN 978-80-247-4819-1.

21. *Nařízení Evropského parlamentu a Rady (EU) 2016/679.* [Online] 27. dubna 2016. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32016R0679.

22. Obecné nařízení o ochraně osobních údajů (GDPR). *Úřad pro ochranu osobních údajů.* [Online] 2016. [Citace: 17. 7 2022.] Dsotupné z: https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr/ds-3938/p1=3938&rd=1000.

23. Co je eGovernment. *Ministerstvo vnitra České republiky.* [Online] 25. 6 2015. [Citace: 6. 7 2022.] Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx.

24. LIDINSKÝ, Vít. *EGovernment bezpečně.* Praha : Grada, 2008. ISBN 978-80-247-2462-1.

25. eGON. *Ministerstvo vnitra České republiky.* [Online] 2022. [Citace: 16. 7 2022.] Dostupné z: https://www.mvcr.cz/clanek/egon-66.aspx.

26. The eGON approach to modernise and connect Czech services and people. (eGON). *European Commission.* [Online] 22. 9 2017. [Citace: 16. 7 2022.] Dostupné z: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/document/egon-approach-modernise-and-connect-czech-services-and-people-egon.

27. Portál občana. *gov.cz.* [Online] Ministerstvo vnitra, 2022. [Citace: 16. 7 2022.] Dostupné z: https://portal.gov.cz/caste-dotazy/portal-obcana.

28. Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů a o změně některých zákonů. *In: ASPI.* Praha : Wolters Kluwer.

29. Zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů. *In: ASPI.* místo neznámé : Wolters Kluwer.

30. CHLEBUS, Tomáš. Nový zákon o zpracování osobních údajů. *epravo.cz.* [Online] 30. 5 2019. [Citace: 17. 7 2022.] Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html.

31. VOKUŠ, Jiří. Pátrání po osobách. *Policie České republiky.* [Online] 2015. [Citace: 16. 7 2022.] Dostupné z: https://www.policie.cz/clanek/zverejnene-informace-2015-patrani-po-osobach.aspx.

32. POSPÍŠIL, Petr. *Činnost veřejné správy.* [Online] 2020. [Citace: 13. 3 2023.] Dostupné z: https://is.slu.cz/osoba/pos0074#vyuka.

33. Komunikační strategie. *Komunikující město.* [Online] [Citace: 15. 3 2023.] Dostupné z: http://www.komunikujici-mesto.cz/index1.php?ukaz=000-016.

34. BOŘIL, Martin. Jak města a obce komunikují s občany? *Deník veřejné správy.* [Online] Triada, spol. s r. o., 1. 11 2021. [Citace: 15. 3 2023.] Dostupné z: http://denik.obce.cz/clanek.asp?id=6820905.

35. BERÁNKOVÁ, Kateřina. Nestůjte ve frontě, zřiďte si Mobilní klíč eGovernmentu a komunikujte s Úřadem práce ČR elektronicky. *Úřad práce ČR.* [Online] 10. 6 2022. [Citace: 16. 7 2022.] Dostupné z: https://www.uradprace.cz/-/nestujte-ve-fronte-zridte-si-mobilni-klic-egovernmentu-a-komunikujte-s-uradem-prace-cr-elektronicky.

36. Elektornická identifikace. *Identita občana.* [Online] 2022. [Citace: 16. 7 2022.] Dostupné z: https://www.identitaobcana.cz/Home.

37. MACKOVÁ, Alena. *Nová média v politické komunikaci: politici, občané a online sociální sítě.* Brno : Masarykova univerzita, Fakulta sociálních studií, Mezinárodní politologický ústav, 2017. ISBN 978-80-210-8745-3.

38. ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení.* Praha : C. H. Beck, 2012. ISBN: 978-80-7400-261-8.

39. Úřad vlády ČR na Facebooku. *Vláda České republiky.* [Online] 20. 1 2010. [Citace: 7. 16 2022.] Dostupné z: https://www.vlada.cz/cz/media-centrum/predstavujeme/urad-vlady-cr-na-facebooku-67049/.

40. FILIPOVÁ, Štěpánka. MPSV Nabízí informace i na sociálních sítích. *Ministerstvo práce a sociálních věcí.* [Online] 22. 5 2013. [Citace: 16. 7 2022.] Dostupné z: https://www.mpsv.cz/-/mpsv-nabizi-informace-i-na-socialnich-sitich.

41. Úřad pro zastupování státu ve věcech majetkových @uzscvm. *Twitter.* [Online] květen 2014. [Citace: 16. 7 2022.] Dostupné z: https://twitter.com/uzsvm?lang=cs.

42. BOCÁN, Jozef. Spouštíme komunikaci na sociálních sítích. *Policie České republiky.* [Online] 21. 6 2017. [Citace: 16. 7 2022.] Dostupné z: https://www.policie.cz/clanek/web-informacni-servis-zpravodajstvi-spoustime-komunikaci-na-socialnich-sitich.aspx.

43. DLUBALOVÁ, Klára. Ministerstvo vnitra je na facebooku. *Ministrestvo vnitra České republiky.* [Online] 1. 12 2021. [Citace: 16. 7 2022.] Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-je-na-facebooku.aspx.

44. Nejvyšší kontrolní úřad. *LinkedIn.* [Online] 2021. [Citace: 17. 7 2022.] Dostupné z: https://cz.linkedin.com/company/nejvy%C5%A1%C5%A1%C3%AD-kontroln%C3%AD-%C3%BA%C5%99ad?original_referer=https%3A%2F%2Fwww.bing.com%2F.

45. Nejvyšší soud. *LinkedIn.* [Online] 2022. [Citace: 17. 7 2022.] Dostupné z: https://cz.linkedin.com/company/nejvy%C5%A1%C5%A1%C3%AD-soud?trk=similar-pages.

46. Virtuálně, mobilně a na sociálních sítích. *Ministerstvo Vnitra České republiky.* [Online] 2014. [Citace: 16. 7 2022.] Dostupné z: https://www.mvcr.cz/clanek/virtualne-mobilne-a-na-socialnich-sitich.aspx.

47. NĚMEČEK, Jiří. Veřejná správa on-line. *Český statictický úřad.* [Online] 27. 3 2012. [Citace: 17. 7 2022.] Dostupné z: https://www.czso.cz/csu/czso/verejna_sprava_on_line20120327.

48. SIONOVÁ, Kristýna. Internet ve službách veřejné správy. *Český statistický úřad.* [Online] 31. 3 2011. [Citace: 17. 7 2022.] Dostupné z: https://www.czso.cz/csu/czso/internet_ve_sluzbach_verejne_spravy20110331.

49. WICHOVÁ, Jitka. Informační technologie ve veřejné správě. *Český statistický úřad.* [Online] 27. 11 2020. [Citace: 17. 7 2022.] Dostupné z: https://www.czso.cz/csu/czso/verejna_sprava.

50. JIROVSKÝ, Václav. *kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada, 2007. ISBN 978-80-247-1561-2.

51. Porušení zabezpečení. *Úřad pro ochranu osobních údajů.* [Online] 2013. [Citace: 16. 7 2022.] Dostupné z: https://www.uoou.cz/poruseni-zabezpeceni/ds-5020.

52. WIESER, Jim. Prevence úniku dat v nemocnicích v období COVIDu. *Centrum kybernetické bezpečnosti.* [Online] 24. 6 2020. [Citace: 17. 7 2022.] Dostupné z: https://centrumkyberbezpecnosti.cz/prevence-uniku-dat-v-nemocnicich-v-obdobi-covidu/.

53. BERÁNKOVÁ, Kateřina. ÚP ČR se distancuje od falešných tvrzení na sociálních sítích – občanům ČR své služby poskytuje. *Úřad práce ČR.* [Online] 23. 3 2022. [Citace: 16. 7 2022.] Dostupné z: https://www.uradprace.cz/web/cz/-/up-cr-se-distancuje-od-falesnych-tvrzeni-na-socialnich-sitich-obcanum-cr-sve-sluzby-poskytuje.

54. MIKULCOVÁ, Klára. Můžeme se v online prostředí setkat s agresí? *e-bezpečí.* [Online] 10. 11 2018. [Citace: 17. 7 2022.] Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybersikana/1412-muzeme-se-v-online-prostredi-setkat-s-agresi.