ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

SOCIÁLNÍ SÍTĚ A DATA UŽIVATELŮ

BAKALÁŘSKÁ PRÁCE

Marie Hušáková

Informatika, technická výchova

Vedoucí práce: Mgr. Jan Bezděka

Plzeň, 2021

Prohlašuji, že jsem diplomovou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 1. června 2021

.....

vlastnoruční podpis

PODĚKOVÁNÍ

Ráda bych poděkovala Mgr. Janu Bezděkovi za cenné rady, věcné připomínky, věnovaný čas a vstřícnost při konzultacích při vypracování této bakalářské práce.

OBSAH

ÚVOD

Sociální sítě zažívají v posledních letech velký vzestup. Slouží pro zábavu, práci i k usnadnění každodenního života. S tím jde ruku v ruce i častější zveřejňování osobních dat, což může přinášet mnoho rizik spojených s jejich, ať už oprávněným či neoprávněným, využitím. Cílem této práce je metodou analýzy zjistit, jaká data jsou sociálními sítěmi a jinými online službami sbírána s vědomím či bez vědomí uživatele a diskutovat možné techniky obrany před jejich únikem a zneužitím. Výstupy této práce by poté mohly posloužit jako edukativní podklad pro výuku či jako základní materiál pro orientaci v rizicích online prostředí úplným začátečníkům.

Struktura této práce je následující. V první kapitole je definován pojem sociální sítě, jsou zde popsána možná rizika spojená se sociálními sítěmi a jsou zde představeni zástupci sociálních sítí. Stěžejní částí práce je druhá kapitola, která je zaměřena na získávání uživatelských dat a následné nakládání s nimi. Nejprve jsou vymezeny základní pojmy z této problematiky a následně je formou analýzy stanoven rozsah a druh získaných uživatelských dat s vědomím a bez vědomí uživatele. V poslední části druhé kapitoly je diskutováno, k čemu jsou získaná uživatelská data využívána. Třetí kapitola je věnována výhodám, nevýhodám a rizikům spojeným se zveřejňováním dat. Předposlední kapitola seznamuje s nejčastějšími hrozbami na internetu a možnostmi, jak se proti nim aktivně či pasivně chránit. Poslední, pátá kapitola analyzuje jak aktuální, tak několik let staré kauzy týkající se zneužití uživatelských dat. V rámci této kapitoly je uvedena i osobní zkušenost autora se zneužitím jeho uživatelských dat.

1 SOCIÁLNÍ SÍTĚ

Rozvoj moderních technologií v posledních několika letech do značné míry ovlivnil náš každodenní život. V souladu s rychlým vývojem moderních technologií probíhá i vývoj aplikací a programů, mezi které patří také sociální sítě. Pohledem o pár let do minulosti zjistíme, že většina komunikace mezi lidmi probíhala převážně osobně. Například zážitky z dovolených si lidé vyprávěli tváří v tvář s fotografiemi v ruce. Dnes stačí jedním kliknutím odeslat zprávu či publikovat digitální fotografii ve virtuálním prostoru, tedy sociální síti, kde ji může v jeden okamžik sledovat současně stovka uživatelů. Sociální sítě do značné míry ulehčují život, ale přináší i celou řadu nezanedbatelných rizik.

Jako sociální sítě (anglicky social networks) označujeme internetové služby, které poskytují prostředky pro vytváření a sdílení svého digitálního profilu. Díky těmto službám je možné navazovat virtuální vztahy a komunikovat s ostatními uživateli. Součástí digitálního profilu jsou zejména osobní informace, fotografie, videa a jiné příspěvky. Dále zde lze plánovat události. Na sociálních sítích však platí, že většina obsahu sociálních sítí je tvořena uživateli samotnými (Havlová, 2003).

I když sociální sítě mohou být uživateli vnímány pouze jako prostor, kde mezi sebou mohou komunikovat a sdílet jejich životy, poskytují širokou škálu různorodých možností. Díky těmto možnostem vznikla řada nových profesí, které jsou dnes plnohodnotným způsobem obživy. Podrobněji se tomuto tématu věnuje jiná kapitola.

1.1 RIZIKA SOCIÁLNÍCH SÍTÍ

Ač se na první pohled může zdát, že sociální sítě přináší pouze pozitiva, existuje i mnoho rizik, která jsou s nimi spojená. Nadměrným užíváním sociálních sítí může vznikat závislost a existuje zde zvýšené riziko kyberšikany. Dále je zde uživatel vystavován stresu a z nadměrného příjmu modrého světla od monitoru či obrazovky mobilního zařízení mohou vznikat poruchy spánku. Jednotlivé problémy budou probrány v následujících kapitolách.

1.1.1 ZÁVISLOST

Společně s rozvojem moderních technologií se prohloubila i vznikající závislost s nimi spojená. Podle Vacka se závislost vzhledem k přístupu k našemu tělu a mysli řadí do

nelátkové, behaviorální závislosti. To znamená, že k vytvoření závislosti není nutné požít návykové látky. Kromě závislosti na internetu může být příkladem behaviorální závislosti také patologické hráčství (hazard), workoholismus, závislost na mobilních zařízeních, videohrách či na nakupování (oniománie či shopaholismus). Závislost může vzniknout také na cvičení nebo vztazích.

Závislost je definována jako chování, které přináší okamžité uspokojení a má tendenci být opakováno. Při častém opakování se pak z dlouhodobého hlediska stává zvykem či návykem i navzdory tomu, že nemá negativní následky (Vacek & Vondráčková, 2014).

Anglický psycholog ve svém článku uvádí model šesti základních příznaků, podle kterých lze rozpoznat závislého člověka. Jsou jimi: zaměření (salience), změna nálady (mood modification), tolerance, abstinenční příznaky (withdrawal symptoms), konflikt a relaps (Griffiths, Does Internet and Computer „Addiction" Exist? Some Case Study, 2000). Tyto příznaky v souvislosti se závislostí na internetu jsou diskutovány v následujícím odstavci.

- **Zaměření** (salience) nastává, pokud se konkrétní aktivita stává nejdůležitější v životě jedince. Závislý hledá způsoby, jak ji provádět a upřednostňuje ji na úkor ostatních věcí, aktivit a vztahů. Po vykonání aktivity, na které je jedinec závislý, přichází **změna nálady** (mood modification). Osoba pociťuje nabuzení a pocit štěstí.

- **Tolerance** podle Marka Griffitha nastává tehdy, když závislý jedinec prodlužuje čas strávený vykonáváním činnosti, na které je závislý. V případě závislosti na internetu tolerance znamená, že jedinec neustále prodlužuje dobu strávenou on-line.

- **Abstinenční příznaky** (withdrawal symptoms) nastávají, pokud se v našem případě jedinec nemůže dostat k počítači, připojit se na internet a podobně.

- **Konflikt** odkazuje na konflikt mezi závislým a okolím nebo na intrapersonální konflikt v jedinci samotném. Tento konflikt může vzniknout v důsledku upřednostňování aktivity, na které je jedinec závislý. Negativním důsledkem může být narušení osobního života (vztahů s přáteli, partnery, rodinou), pracovního života a podobně.

- **Relaps** neboli návrat k aktivitě, na které je jedinec závislý, i po neúspěšném pokusu se od ní oddělit.

1.1.2 KYBERŠIKANA

Kyberšikanu lze chápat jako agresivní chování, které není jednotlivcem nebo skupinou prováděno fyzicky, ale prostřednictvím informačních a elektronických médií, kde se oběť nemůže bránit. Kyberšikana se může zdát jako méně závažná než tradiční školní šikana, ovšem dopady má stejně závažné, ne-li závažnější (Černá, Dědková, Macháčková, Ševčíková, & Šmahel, 2013).

Mezi projevy kyberšikany patří například zasílání urážlivých a zastrašujících zpráv (skrze e-mail, zveřejňování na sociálních sítích), pořizování zvukových záznamů, videí či fotografií, jejich upravování a následné zveřejňování s cílem poškodit vybranou osobu (například natáčení učitele). Dalším příkladem může být vytváření internetových stránek, které urážejí, pomlouvají nebo ponižují konkrétní osobu, dále pronásledování či vydírání (Policie.cz: Víte co je kyberšina?, nedatováno).

1.1.3 STRES A DEPRESE

S rostoucím počtem aktivních uživatelů na sociálních sítích, kteří sdílí své fotografie a videa, se může zvyšovat i tendence se mezi sebou porovnávat. Většina uživatelů má tendenci prezentovat sama sebe na sociálních sítích z té nejlepší stránky. Pravděpodobně tedy spíše zveřejní fotografie z drahé dovolené, pochlubí se koupí nového auta, váhovým úbytkem či získaným akademickým titulem a novou prací, než aby veřejně sdíleli své problémy. S rozmachem sociálních sítí tedy vzniká více podnětů, se kterými je možné se srovnávat. Proto můžeme lehce nabýt dojmu, že jiný uživatel může mít lepší život než my, i přesto, že fotografie na sociálních sítích vždy nemusí odpovídat skutečnosti. Toto srovnávání může být příčinou vzniku nadměrnému stresu a depresí.

Fenomén FoMo (fear of missing out, v překladu „strach, že o něco přicházím“) je další příčinou stresu na sociálních sítích. Fear of missing out je strach jedince, že svou nepřítomností na sociálních sítích přichází o informace a zážitky. Získává pocit, že mu uniká dění ve virtuálním prostoru a nemá pod kontrolou to, co ostatní uživatelé sdílí, zda mu jiný uživatel neposlal zprávu a podobně. Tento strach je tedy přítomen v okamžiku, kdy sociální sítě využíváme pasivně (tzn., že nejsme právě online) a může být spouštěčem stresu a příznaků deprese (Burnell, 2019).

1.1.4 BLUE LIGHT

Mnoho uživatelů, kteří těsně před spaním tráví čas na mobilním telefonu nebo na počítači, může následně trpět nespavostí. Z monitoru či obrazovky mobilního zařízení vyzařuje modré světlo (v překladu blue light), které v nadměrném příjmu může být příčinou nespavosti.

Je to zapříčiněné tím, že zejména ve večerních hodinách má modré světlo negativní účinky na lidský organismus. Především díky vlivu na hladinu hormonu melatonin, který je díky modrému světlu potlačován a není vylučován do lidského těla. Výsledkem je, že se zvyšuje pozornost a další kognitivní činnosti. To se může zdát žádoucí při expozici modrým světlem během dne, ovšem s ohledem na spánek má modré světlo čistě negativní vliv (Šmotek, Kopřivov, & Šós, 2016).

1.2 NEJZNÁMĚJŠÍ PŘEDSTAVITELÉ SOCIÁLNÍCH SÍTÍ

Pokud se řekne „sociální síť“, většině lidí vyvstane na mysli pravděpodobně sociální síť s názvem Facebook. Ovšem Facebook není jediná sociální síť. Určit nejznámější sociální sítě je vcelku těžké, jelikož ty, které jsou dnes uživateli velmi oblíbené, mohou být zítra již naprosto zapomenuté. Proto zde sociální sítě nebudou uváděny podle jejich aktuální oblíbenosti, ale dle celkového počtu aktivních uživatelů. V následujících podkapitolách se práce bude věnovat sociálním sítím Facebook, YouTube, LinkedIn, Instagram a Twitter.

1.2.1 FACEBOOK

Facebook svým počtem aktivních uživatelů patří mezi nejznámější a nejrozšířenější sociální sítě. K podzimu roku 2020 měl 2,7 miliard aktivních uživatelů, čímž se řadí na první místo nejpoužívanějších sociálních sítí (Statista.com, 2020). Tato sociální síť byla založena v roce 2004 čtyřmi studenty Harvardské Univerzity: Markem Zuckerbergem, Eduardem Saverinem, Dustinem Moskovitzem a Chrisem Hughesem. Původně byla tato síť určena pouze pro studenty Harvardovy univerzity, ale v roce 2006 se rozšířila po celém světě a nabízela založení uživatelského účtu zdarma pro každého, kdo dovršil 13 let.

Od jeho spuštění v roce 2004 se Facebook stal fenoménem mezi sociálními sítěmi. Od mladých lidí, kteří jsou nejaktivnější skupinou na sociálních sítích (Facebook.com), se

Facebook rozšířil i mezi generaci rodičů a prarodičů. Všichni uživatelé mohou na Facebooku sdílet fotografie a zážitky či spolu komunikovat.

1.2.2 YOUTUBE

S počtem 2 miliard aktivních uživatelských účtu se mezi nejznámější sociální sítě řadí i YouTube (Statista.com, 2020). YouTube sice není sociální sítí jako například Facebook, kde mezi sebou jednotliví členové sdílejí příspěvky a posílají si zprávy, ale jedná se o největší internetový server pro sdílení videosouborů, založený v roce 2005 (Timixi.com, 2015).

Díky vysokému počtu videí, který se k roku 2020 počítá v řádech miliard, se YouTube stal pro většinu lidí nedílnou součástí života. Tato platforma poskytuje zdarma nahrávání i zhlédnutí videí všeho druhu - od zábavných, hudebních, až po edukativní videa.

1.2.3 LINKEDIN

O tom, že sociální sítě nejsou jen pro zábavu, svědčí sociální síť s názvem LinkedIn. LinkedIn je celosvětově největší profesní síť na internetu, která je využívána k nalezení pracovní pozice či stáže. LinkedIn rovněž umožňuje náborovým pracovníkům oslovit a nalézt vhodného kandidát pro danou pracovní pozici.

Princip sítě LinkedIn spočívá ve vytvoření uživatelského účtu, v rámci něhož uživatel vyplní základní osobní informace jako jméno, příjmení a věk. Uživatel může dále svůj profil obohatit o aktuální životopis, dovednosti, zájmy a současnou pracovní pozici. Pokud je jedinec nezaměstnaný, může si na svém profilu nastavit, že je otevřený nabídkám pracovních pozic, čímž zvýší své šance na nabídku nové pracovní pozice.

Na této sociální síti se dají vytvořením profilu posílit profesionální vztahy, naučit se dovednosti, které uživatel může uplatnit ve své kariéře, a mít na jednom místě uložený životopis (Linkedin.com, 2020).

1.2.4 INSTAGRAM

Instagram je bezplatná aplikace pro sdílení fotek a videí, která od doby svého vzniku (2010) zažila velký vzestup, jelikož se jednalo o první sociální síť, kde uživatelé mohli sdílet jen fotografie a videa. Na Instagramu mohou lidé nahrávat fotografie a videa a dělit se o ně

se svými sledujícími nebo s vybranou skupinou přátel. Mohou si také prohlížet, komentovat a označovat jako „To se mi líbí“ příspěvky, o které se na Instagramu podělili jejich přátelé (Facebook.com: Co je to Instagram?, 2020).

Od roku 2016 může uživatel Instagramu využívat také tzv. Insta Stories. Uživatel Instagramu má možnost sledovat (případně vytvářet) vlastní příběhy a následně je zveřejnit pro určitý okruh uživatelů, všem svým sledujícím nebo široké veřejnosti. Insta Stories jsou na Instagramu viditelná 24 hodin, a poté dochází k jejich smazání. Do Insta Stories se řadí jak natočené krátké filmové úseky zachycující každodenní momenty, tak i několikavteřinové koláže vytvořené z fotografií, často doplněné o texty, barevné kresby a emotikony všeho druhu (It-slovnik.cz).

1.2.5 TWITTER

Twitter, jehož název lze přeložit jako cvrlikání, je sociální síť, která o svém účelu velice napovídá svým názvem a logem (modrý ptáček). Tato sociální síť se od ostatních liší tím, že umožňuje uživatelům posílat textové příspěvky, známé jako tweety o délce maximálně 280 znaků. Kromě textových příspěvků lze sdílet i fotografie, videa, odkazy a podobně. Tyto příspěvky se zobrazují na uživatelově profilové stránce a na stránkách těch, kteří jej sledují (followers). Tento princip je podobný jako u Facebooku či Instagramu (Twitter.com, nedatováno).

Twitter vytvořil prostředí, které díky omezenému počtu znaků na textový příspěvek donutí uživatele sdílet příspěvky stručně a jasně. Proto většina lidí na Twitteru sdílí v textových příspěvcích převážně své krátké myšlenky, postřehy a názory. Díky tomu se z Twitteru stává jakýsi mikro blog, který využívá i řada českých a zahraničních politiků a veřejně známých lidí. Twitter měl k podzimu roku 2020 152 milionů aktivních uživatelů (Statista.com, 2020).

2 DATA UŽIVATELŮ

Pod pojmem data uživatelů si lze představit veškerý obsah, který jako uživatelé sdílíme na internetu. Jsou to například fotky, různé příspěvky či zprávy. Dále se mezi ně řadí i osobní údaje, u kterých nemusí být uživateli na první pohled zřejmé, že je také sdílí. Z tohoto důvodu jsou v následující kapitole nejprve vymezeny základní pojmy týkající se osobních údajů. Dále jsou zmíněny informace související s právy na ochranu uživatelských dat. Další podkapitoly se budou zabývat tím, proč je nezbytné naše data chránit a z jakého důvodu mohou být pro někoho cenná.

2.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

Termín data uživatelů je poměrně široký, a proto je důležité vymezit základní pojmy této problematiky. Mezi základní pojmy patří například osobní údaje, citlivá data, anonymizovaná data a uživatelská data jako celek. Také je dobré vědět o možnostech ochrany osobních údajů – GDPR, které budou probírány na konci kapitoly.

2.1.1 OSOBNÍ ÚDAJE

Osobní údaj lze chápat jako informaci, díky které lze identifikovat konkrétní osobu. V některých případech dojde k identifikaci až po spojení více jednotlivých osobních údajů. Obecně mezi osobní údaje řadíme základní informace jako jméno, věk, datum narození. Za osobní údaj lze ale považovat i e-mailovou adresu, telefonní číslo, fotografii a podobně.

Zákon o ochraně osobních údajů definuje osobní údaj v zákoně č. 101/2000 Sb. následovně: „Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“ (Zákon o zpracování osobních údajů, 2000).

Zákon o ochraně osobních údajů byl v roce 2019 nahrazen zákonem o zpracování osobních údajů č. 110/2019 Sb., ovšem pojem osobní údaj nebyl oproti předchozímu zákonu výrazně upraven.

2.1.2 CITLIVÁ DATA

Do speciální kategorie osobních údajů se řadí citlivá osobní data neboli také citlivé osobní údaje. Citlivá osobní data jsou jakákoliv osobní data, jejichž únik, neoprávněné užití nebo zneužití může poškodit konkrétní subjekt, a to například v zaměstnání či ve společnosti. Únik osobních data může být dokonce příčinou diskriminace jedince. Jedná se o údaje o rasovém či etnickém původu, sexuální orientaci, politickém, náboženském nebo filozofickém přesvědčení, členství v různých skupinách, zdravotním stavu a trestních provinění či odsouzení osob. Újma vzniklá jedinci může být finanční, majetková, psychická nebo také ve formě ztráty soukromí. Proto zpracování citlivých údajů podléhá mnohem přísnějšímu řádu, než je tomu u osobních dat.

2.1.3 UŽIVATELSKÁ DATA

Za uživatelská data lze považovat veškeré informace, které uživatel veřejně sdílí. Příkladem mohou být fotografie, různé příspěvky, zprávy, ale i informace jako poloha uživatele, náboženské vyznání, jazyk, kterým uživatel mluví, biografická data nebo sdílené odkazy.

Tato data mohou být velmi cenná pro marketingový trh, jelikož si marketingové firmy mohou díky mnoha poskytnutým informacím vytvořit velmi přesnou představu o zákaznících. Následně mohou na uživatele cílit reklamu na míru, čímž zvýší svůj prodej.

2.1.4 ANONYMIZOVANÁ DATA

Skutečnost, že naše data jsou cenná, byla zmíněna již v úvodu. Příkladem hodnoty našich dat jsou data anonymizovaná. Tato data totiž slouží k přeprodávání. Charakteristikou anonymizovaných dat je, že jsou poskytována bez klíčových údajů, kterými by bylo možné identifikovat konkrétního uživatele. Například ze získaných osobních údajů osoby jako jméno, věk a určitá záliba, by se měla odebrat informace o jméně. V tu chvíli vznikne pouze záznam o osobě v určitém věku se zálibou v konkrétní činnosti. Anonymitu tedy data získávají v momentě, kdy si nelze ostatní osobní údaje jakkoliv spojit s konkrétní osobou.

Tato data jsou nejčastěji používána při výzkumech, kde není důležitá identifikace konkrétní osoby, ale je nezbytný velký počet vstupních dat pro vytvoření konečných statistik a závěrů.

2.1.5 OCHRANA OSOBNÍCH ÚDAJŮ – GDPR

Obecné nařízení o ochraně osobních údajů, anglicky General Data Protection Regulation (zkratkou GDPR), nabylo platnost 25. května 2018. Nahradilo tehdejší zákon č. 101/2000 Sb., o ochraně osobních údajů. Hlavním smyslem tohoto předpisu je vrátit osobám právo rozhodovat o tom, jak bude nakládáno s jejich daty. To znamená, že každý subjekt má právo mít kontrolu nad tím, které osobní údaje o něm daný podnik či společnost vlastní. Uživatel musí mít možnost udělit či neudělit souhlas o tom, s kterými údaji jeho údaji bude společnost nakládat. Jedinec má také nárok na to být informován, za jakým účelem a jakým způsobem jsou jeho osobní údaje zpracovávána, jakými prostředky jsou chráněna a s kým a na jak dlouhou dobu jsou sdílena. Oproti tehdejšímu zákoníku má osoba právo požádat společnost (za splnění podmínek daných zákonem) o vymazání jeho osobních údajů.

V souvislosti se sociálními sítěmi je důležité si uvědomit, že se zákon GDPR nemusí týkat jen velkých společností a organizací, ale i uživatelů samotných. Příkladem toho jsou fotografie. Ač někteří uživatelé mohou mít pocit, že lze skrze tlačítko „přidat fotografii“ nahrát na sociální síť libovolnou fotografii, opak je pravdou. I toho se totiž dotýká zákon GDPR a nejenže nesmíme fotografovat jiné osoby bez výslovného souhlasu, ale také bez jejich souhlasu nelze veřejně sdílet fotografii, na nichž se objevují. To platí o to více, pokud se jedná o fotografii, která dotyčného může zkompromitovat, způsobit mu újmu či ohrozit jeho práva a svobodu.

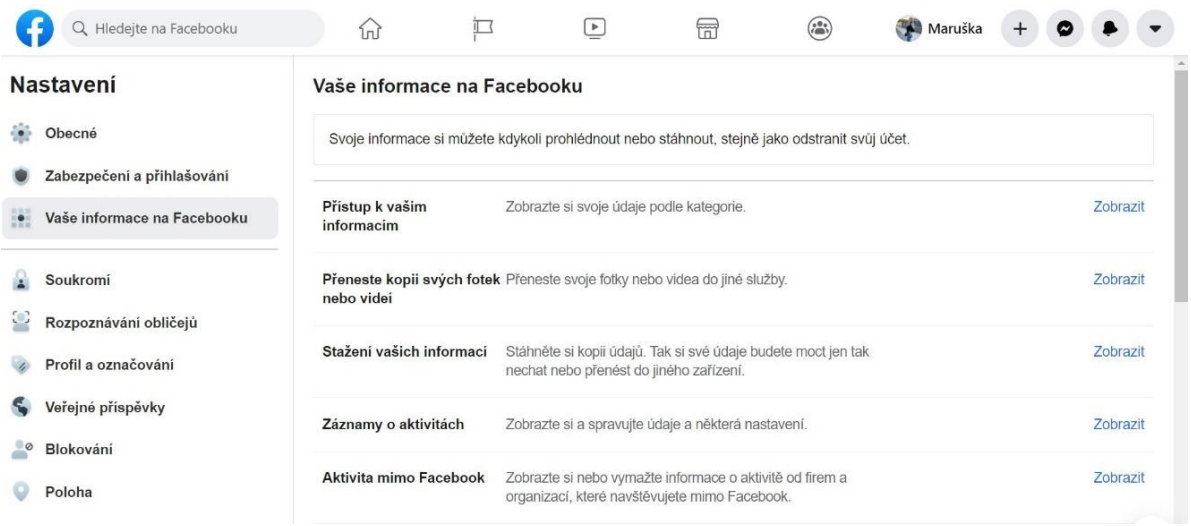
S těmito pravidly se mohou setkat zejména větší společnosti a organizace. Příkladem toho je příklad školství, kde bez souhlasu žáků či zákonných zástupců není možné fotografovat studenty a následně fotografie sdílet na sociálních sítích a webu. Stejně tak v zaměstnání je pro využití fotografií zaměstnanců na webu, sociálních sítích či v propagačním materiálu nutný souhlas zaměstnance. V opačném případě je nutné fotografii dané osoby anonymizovat (Úřad pro ochranu osobních údajů).

2.2 DATA ZÍSKÁVÁNA S VĚDOMÍM UŽIVATELE

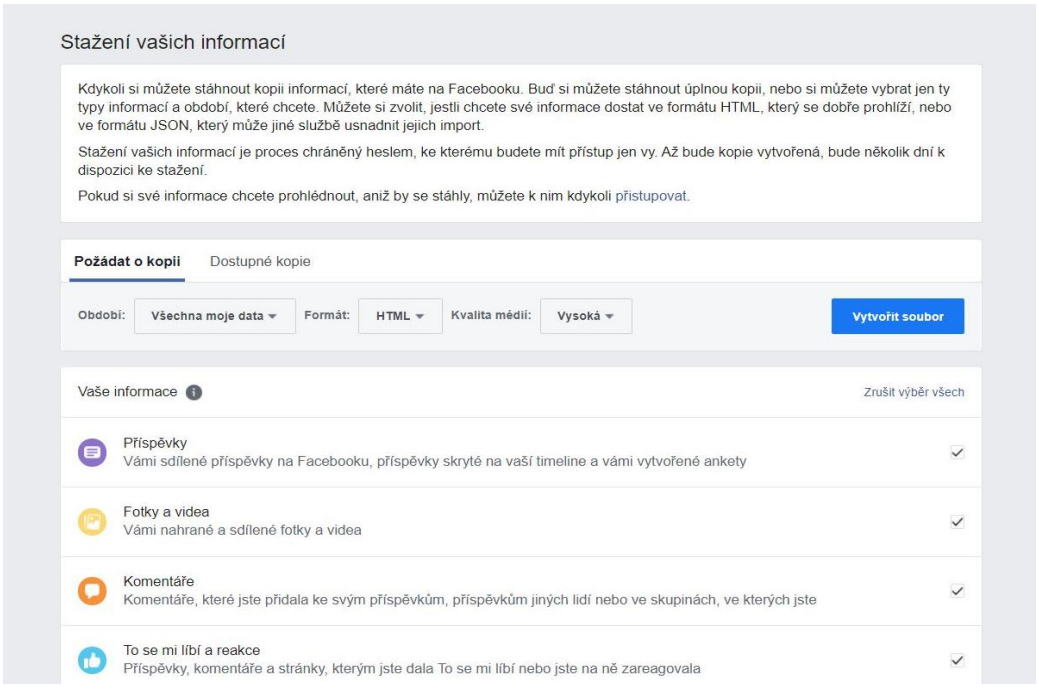
Data získávána s vědomím uživatele lze popsat jako taková data, která jsou uživateli vědomě poskytována dané sociální síti. Nejedná se o data sbíraná tajně, ale čistě o data, která zveřejníme, nahrajeme či vytvoříme na sociální síti. V následujících podkapitolách jsou

rozebrány jednotlivé informace, které o sobě sdílíme, včetně těch, které nejsou na první pohled zřejmá.

Analýza v této kapitole je realizována především na případu sociální sítě Facebook. Díky zákonu GDPR mají uživatelé právo požádat společnost o soupis dat, která jsou o nich uchovávána (obr. 1). V nastavení Facebooku se nachází možnost stáhnout si veškeré informace, které o daném uživateli Facebook získal na základě uživatelem vědomě poskytnutých dat (obr. 2). Tato data jsou podrobněji rozebrána ve zbytku kapitoly.



Obrázek 1 - Uživatelské informace na Facebooku. (Zdroj: Facebook.com.)



Obrázek 2 - Možnost stažení dat z Facebooku. (Zdroj: Facebook.com.)

2.2.1 PROFILOVÉ INFORMACE

Profilové informace jsou údaje, které sociálním sítím poskytujeme již při zakládání našeho uživatelského účtu. Veškeré informace o nás, jako například jméno, příjmení, kontaktní údaje, bydliště, zaměstnání, sexuální orientace, vyznávané náboženství, životní události, koníčky, hudba, profilová fotografie, heslo či z kterého zařízení a odkud se přihlašujeme, jsou data, která vědomě poskytujeme. Jelikož se jedná o osobní údaje (v některých případech i o citlivé údaje), je důležité zvážit, v jaké míře o sobě tato data na sociálních sítích chceme sdílet.

2.2.2 PŘÍSPĚVKY

Mezi data, která sociální sítě získávají s vědomím uživatele, nedílně patří veškeré příspěvky, které jako uživatelé nahrajeme na danou sociální síť. Pod příspěvkem si lze představit zveřejněnou fotografii nebo videozáznam, který sdílíme na sociální síti. V příspěvcích lze sdílet i text či hypertextové odkazy, vytvářet ankety nebo oznamovat polohu.

Jistým druhem příspěvků jsou i takzvané příběhy. Prostřednictvím těchto příběhů může uživatel nahrát a sdílet fotografie, videozáznamy, text či oznámit polohu. Čím se liší od klasického příspěvku, je skutečnost, že jsou viditelné pouze 24 hodin. Poté se uloží do archivu příběhů, který je dostupný jen samotnému autorovi. I přesto dále zůstává uložen v databázi dané sociální sítě.

2.2.3 AKTIVITY

Mezi data, která se mohou uživateli na první pohled zdát, že jím nejsou poskytována vědomě, patří veškerá aktivita uživatele. Pokud na sociální síti lajkujeme[1] či přidáváme komentáře k příspěvkům ostatních uživatelů, tak i tato data jsou sociální sítí zaznamenána a uložena. Stejně je tomu i v případě vyhledávání osob, stránek či událostí. Co se týče událostí, i z obyčejného potvrzení naší účasti na dané akci vědomě vytváříme data o nás, která mohou prozrazovat naše zájmy. Dalším podobným příkladem je i hraní her na sociálních sítích, ukládání příspěvků, provádění plateb či vyplňování anket a dotazníků.

[1] Lajkovat – Na sociální síti Facebook se provádí "lajkování" kliknutím na ikonu „To se mi líbí“, což vyjadřuje kladné mínění hodnotitele vůči danému příspěvku. Zdroj: It-slovnik.cz: Co je to Lajkovat? [online]. [cit. 2021-02-05]. Dostupné z: https://it-slovnik.cz/pojem/lajkovat

2.2.4 PŘÁTELÉ

Dalším příkladem dat získávaných s vědomím uživatele je seznam přátel daného uživatele. Tento seznam si může uživatel skrýt, ovšem pouze pro ostatní uživatele, nikoliv pro provozovatele sociální sítě. Vedle přátel poskytujeme i data o tom, koho na sociálních sítích sledujeme – ať už se jedná o oblíbeného umělce, školní či pracovní skupinu, nebo stránky sdružující uživatele se stejným zájmem. Nelze však opomenout i stránky, které sami jako uživatelé založíme.

2.2.5 ZPRÁVY

V neposlední řadě je nutné zmínit zprávy. Ač se může zdát, že cokoliv, co napíšeme ve zprávách na sociální síti, zůstane jen mezi zúčastněnými uživateli, není tomu tak. Jedná se opět o data, která dobrovolně vytváříme tím, že konverzaci vedeme skrze danou sociální sít. Veškerá historie zpráv, včetně sdílených obrázků, videozáznamů, odkazů, dokumentů na sociální síti, je stále uložena v databázi, a dokonce si ji můžeme sami prohlédnout.

2.3 DATA ZÍSKÁVÁNA BEZ VĚDOMÍ UŽIVATELE

Hranice mezi daty, která jsou získávána s vědomím a bez vědomí uživatele, je velice tenká. Data získávána s vědomím jsou informace, které vytváříme nebo poskytujeme dané službě. Naopak data získávána bez vědomí uživatele lze popsat jako informace, které daná služba shromažďuje, když jí využíváme. Následující kapitola se zaměřuje na jednotlivá data, která o nás sbírají sociální sítě a jiné služby, aniž by si to většina uživatelů uvědomovala. V první části jsou diskutovány zejména cookies, které hrají v této problematice zásadní roli. Následují další, neméně důležité způsoby sběru osobních dat uživatelů.

2.3.1 COOKIES

Cookies jsou drobné soubory, které slouží pro ukládání stavové informace, které jsou potřeba pro komunikaci mezi klientem a serverem. Tyto soubory jsou ukládány na disku uživatele a dnes jsou již podporovány většinou webových prohlížečů (Google Chrome, Internet Explorer, Safari, Mozilla Firefox a podobně). Díky těmto souborům dochází k tomu, že nás daná webová stránka dokáže identifikovat (McCarthey & Weldon-Siviy, 2013).

Tato identifikace pro uživatele znamená různé výhody i nevýhody. Výhodou je, že pokud webovou stránku opakovaně navštívíme, díky cookies si stránka zapamatuje uživatelské nastavení. Uživatel si tedy nemusí stránku nastavovat pokaždé, když ji navštíví. Další výhodou cookies je například nakupování přes internet, kdy si položky uživatelem vložené do košíku prohlížeč pamatuje i při obnovení stránky. Cookies tedy uživateli šetří čas a usnadňuje práci s webovými stránkami. Navíc dovolují webovému serveru samotnému uchovávat stavovou informaci, kterou by jinak vzhledem k bezstavovosti protokolu HTTP/HTTPS nebylo možné udržet.

Nevýhodou používáním cookies je pak ztráta anonymity uživatele. Tím, že webová stránka uživatele identifikuje, dochází k ukládání různých informací, které jsou s konkrétním uživatelem spojené. Příkladem je historie vyhledávání či projevení zájmu o určité produkty. Dále tak lze sledovat, jak často dané stránky uživatel navštěvuje či které části stránky při návštěvě uživatel nejčastěji použil. Z těchto informací těží internetové reklamy. To je důvodem, proč se uživatelům po vyhledání nějakého zboží v internetovém prohlížeči, začnou automaticky nabízet reklamy na daný produkt například na Facebooku.

Uživatel se ovšem může sám rozhodnout, zda chce cookies povolit či ne. Důvodem je směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Tato směrnice Evropské unie totiž uvádí, že každá webová stránka má ohledně souborů cookies následující povinnosti. Musí uživatele informovat, že využívá soubory cookies. Také musí získat souhlas uživatele ještě před tím, než bude s cookies nakládat. A v neposlední řadě musí uživateli nabídnout možnost odmítnout ukládání souborů cookies (Směrnice o soukromí a elektronických komunikacích, 2002).

Většina uživatelů mohla zaznamenat informační pruh na spodní části stránky, kde buď můžeme cookies sobory povolit nebo odmítnout. Odmítnutím cookies uživatel přijde o veškeré výhody výše zmíněné, což může vést k jistému nepohodlí při využívání webových stránek.

2.3.2 DEVICE FINGERPRINT

Device fingerprint (v překladu otisk zařízení) je další metodou, díky níž lze získat data o uživateli bez jeho vědomí. Jedná se o techniku sledování, kterou webové stránky

aplikují ke shromažďování informací o uživatelích. Výsledkem je identifikace jednak uživatele, ale i nastavení jeho zařízení.

Většina webových stránek vyžaduje aplikování skriptů – souvislé série příkazů (pokynů), které prohlížeči určí, co má dělat. Tyto skripty pracují na pozadí procesů. Mohou identifikovat spoustu informací o uživateli i jeho zařízení a prohlížeči. Po spojení těchto informací vytvoří jedinečný online otisk zařízení. Tento otisk zařízení pak lze vysledovat zpět k uživateli skrze internet a relace procházení (Avast.com: What Is Browser Fingerprinting?, 2020).

Rozdíl mezi cookies a otiskem zařízení je následující. Jak bylo popsáno v předchozí podkapitole, cookies spravuje směrnice Evropské unie. Z toho vyplývá, že podléhá přísnějším zákonům a uživatel musí s použitím cookies v jeho prohlížeči souhlasit. Oproti tomu otisk zařízení je méně známý způsob a lze s ním obejít omezení cookies. V současnosti se na této problematice začíná více pracovat a různé prohlížeče se snaží této technice získávání dat předcházet.

2.3.3 GOOGLE ANALYTICS

Google Analytics je bezplatný nástroj od společnosti Google, který slouží k podnikání na webových stránkách či e-shopu. Tento analytický nástroj získává data o uživatelích, kteří web navštívili. Ze změřených dat lze vyvodit závěry, které mohou pomoci s rozvojem dané webové stránky a se zacílením obsahu stránky vůči návštěvníkům.

Propojení webové stránky s Google Analytics je zcela zdarma a zvládne ho i méně zdatný programátor. Stačí pouze vložit tzv. globální značku webu – jedná se o několik řádek kódu, který je potřeba vložit na každou stránku webu, ze které chceme data měřit. Po nasbírání dostatečného počtu dat se po přihlášení do účtu Google Analytics zobrazí přehled. Zde vlastník webu či e-shopu dostane hned několik dat o svých zákaznících. Mezi ty patří následující údaje:

- Celkový počet návštěvníků za celou dobu.
- Míra okamžitého opuštění.
- Průměrná doba trvání návštěv.
- Věk, pohlaví, zájmy a jazyk uživatelů.

- Země a město, odkud pocházela zákazníkova aktivita.
- Zdroj, ze kterého se nový uživatel dostal na danou webovou stránku.
- Platforma, na které aplikace nebo web běžely.
- Operační systém používaný návštěvníky webu včetně operačních systémů mobilních zařízení.
- Prohlížeč, ve kterém si uživatelé zobrazili webovou stránku.
- Dokonce lze zobrazit data i o rozlišení obrazovky uživatelova monitoru.
- Model zařízení, který návštěvník využívá.
- V reálném čase si lze zobrazit uživatele za posledních 30 minut včetně všech informací výše popsaných.
- Pokud se jedná o e-shop, lze z přehledu vyčíst i data o tržbách, a z kterých položek vznikly.

Jak lze z výčtu vidět, Google Analytics nabízí opravdu mnoho dat o návštěvnících webové stránky. Tyto informace jsou velmi užitečné pro rozvoj webu, cílení obsahu pro danou skupinu zákazníků, ale i pro odhalování chyb. Pokud například z přehledu dat lze vyčíst, že nějaká stránka nemá žádné zobrazení na jednom prohlížeči (např. Safari), je možné, že web nebo obsah na něm uživatelům s touto platformou nefunguje.

2.3.4 FACEBOOK PIXEL

Podobně jako Google Analytics funguje i Facebook pixel. Jedná se o část kódu, která po přidání na webovou stránku poskytne analytické údaje o návštěvnících. Umožňuje měřit výsledky reklam, okruhy uživatelů a zvýšit prodej. Poskytuje informace o tom, kolik uživatelů web navštívilo, provedlo nákup či opustilo nákupní košík těsně před provedením platby.

Hlavním cílem Facebook pixelu je následné využívání těchto dat k cílení reklamy. Lze si vytvořit okruh uživatelů dle jejich preferencí a následně cílit placenou reklamu na míru uživatelům, kteří webovou stránku již navštívili. Stejně tak lze sledovat akce, které zákazníci udělali. Pokud například nedokončili svůj nákup, pomocí Facebook pixel je lze opětovně oslovit cílenou reklamou.

2.3.5 HEAT MAP

Dalším způsobem, jak získávat na webu data o svých zákaznících, jsou tzv. heat maps (v překladu tepelné mapy). Tyto mapy nesbírají o uživatelích informace jako například Google Analytics nebo ostatní způsoby výše uvedené, ale zaznamenávají chování uživatele na dané webové stránce. Reprezentace sesbíraných dat je poté graficky vykreslena do zbarvených oblastí, které mohou označovat například míru kliknutí na danou část webu. Tepelné mapy usnadňují vizualizaci složitých dat a usnadňují jejich pochopení na první pohled.

Tepelné mapy webových stránek vizualizují nejoblíbenější a nejméně oblíbené prvky na webové stránce pomocí barevné stupnice od červené po modrou barvu (obr. 3). Přitom červená, teplá barva, označuje nejoblíbenější prvky a ty nejméně oblíbené reprezentuje modrá, studená barva.

Obrázek 3 - Ukázka tepelné mapy. (Zdroj: https://upload.wikimedia.org/wikipedia/commons/5/50/Eyetracking_heat_map_Wikipedia.jpg.)

Tepelná mapa je tedy grafické zobrazení chování návštěvníka na webu. Což usnadňuje analýzu dat a poskytuje okamžité pochopení toho, jak návštěvníci interagují s jednotlivými částmi webové stránky – na co klikají, co procházejí nebo ignorují – což pomáhá identifikovat trendy a naopak odstranit nezajímavé prvky.

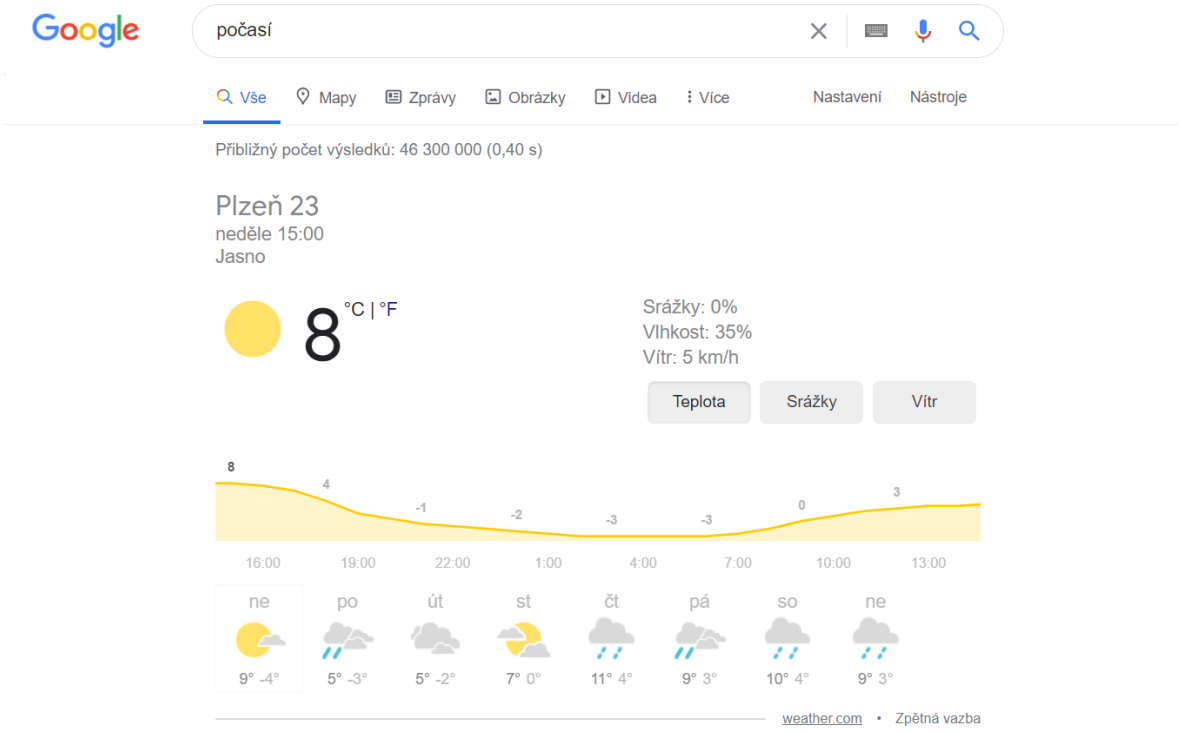
2.3.6 OSTATNÍ

K získávání dat bez vědomí uživatele může docházet i při využívání některých služeb. V tomto případě je vcelku těžké určit, kdy uživatel opravdu neví o tom, že svá data poskytuje. Nejen z hlediska právního – jelikož každá sociální síť či webová stránka musí uživatele informovat o tom, k jakým jeho datům má přístup, ale i z hlediska zkušeností uživatele. Uživatelé, kteří se na sociálních sítích a celkově na internetu pohybují již delší dobu, mohou zhruba vědět, kde jsou jejich data využívána. Uvedu tedy několik příkladů, kde to není tolik zřejmé.

Možnost **vyhledávání** je nedílnou součástí každého webového prohlížeče i většiny sociálních sítí. Skrze prohlížeč si lze vyhledat na internetu již téměř cokoliv. Od novinek ze světa, předpovědi počasí, až po zboží, které si lze přes internet koupit. Na sociálních sítích je vyhledávání zúženo na obsah, který se na nich nachází. Lze si vyhledat oblíbeného umělce, stránku, skupinu se stejným zájmem a také profil jiného uživatele. Ovšem ne každý uživatel ví, že i vyhledávání po něm zanechává stopy. Stopy ve formě vyhledávací historie. Vyhledávací dotazy se totiž ukládají do historie prohlížení a dochází ke shromažďování dat o uživateli.

Stejně tak je to v případě **sledování videí** na platformě YouTube, která také shromažďuje uživatelovu historii sledování. Na základně toho, která videa si sám uživatel vybral ke zhlédnutí nebo která dříve sledovali lidé s podobnou historií sledování, navrhuje YouTube na domovské stránce přihlášenému užívali videa. Tím si zajistí sledování i u jiných druhů videí a zvyšuje šanci, že uživatel zůstane na této sociální síti delší dobu.

V neposlední řadě je důležité zmínit se o **poloze** uživatele. Polohu prohlížeč získá souhlasem, tudíž se nemusí jednat přímo o data získána bez vědomí uživatele. Ovšem po udělení souhlasu může prohlížeč poskytnout polohu stránkám, které o ni požádají. Při využívání služeb map, které nabízí například Seznam.cz nebo Google, lze vidět označení aktuálního místa, což znamená, že služba dokázala uživatele lokalizovat. Stejně tak, pokud se do prohlížeče zadá slovo počasí, většině uživatelů se zobrazí rovnou místo, kde se nachází. Ukázkou je obrázek níže.



Obrázek 4 - Příklad lokalizace uživatele při zadání výrazu „počasí“. (Zdroj: vlastní.)

2.4 MARKETING JAKO VYUŽITÍ ZÍSKANÝCH UŽIVATELSKÝCH DAT

Předchozí kapitoly již lehce nastínily, k čemu se data uživatelů využívají a proč mohou být cenná. Anonymizovaná data například slouží pro výzkumy, data získaná z historie prohlížení slouží k přesnějšímu navrhování dalšího obsahu a data o návštěvnících webové stránky jsou cenným zdrojem pro jejich vylepšení. V této kapitole bude kladen důraz především na internetový marketing, jelikož zde dochází k největšímu využívání uživatelských dat. V následujících podkapitolách bude diskutován celý proces vytváření reklamy na bázi analýzy uživatelských dat.

2.4.1 INTERNETOVÝ MARKETING

Marketing hraje ve využívání získaných uživatelských dat největší roli. Pro lepší pochopení je nutné vymezit dva pojmy. Digitální marketing a internetový marketing. Digitální marketing je pojem, který zastřešuje veškerou marketingovou komunikaci, která využívá digitální technologie. Tato komunikace přitom může či nemusí být online. Internetový marketing (také online marketing) je podmnožinou digitálního marketingu. Označuje marketingové aktivity probíhající na internetu. Zabývá se marketingovými

strategiemi využívající internet a musí se přizpůsobit chování uživatelů na sociálních sítích či jiných mediích (Frey, 2011).

Cílem internetového marketingu je získání a udržení nových zákazníků, rozšíření povědomí o značce či službě, zvyšování návštěvnosti webové stránky a podobně. Dosažení těchto cílů je snazší právě na sociálních sítích, jelikož se jedná o místo, které většina uživatelů během dne minimálně jednou navštíví. Tvorba internetové kampaně však obnáší mnohem více než prosté vytvoření a sdílení finální podoby reklamního materiálu. Ty budou popsány v následujících kapitolách.

2.4.2 DATA BROKERS

Prvním krokem v internetovém marketingu je získání dat. Ta nemusí každá marketingová společnost shromažďovat sama, ale může využít takzvané „data brokers". Tento pojem, který lze dohledat i pod názvem „information brokers" (v překladu zprostředkovatelé dat), označuje společnosti, které shromažďují osobní údaje o uživatelích a ty dále přeprodávají nebo sdělují třetím stranám.

Datovým zprostředkovatelům napomáhá model dnešního internetu. Uživatelé za účelem využití bezplatné služby, jako například vyhledávače, sociální sítě, online hry či zpravodajské weby, poskytují své osobní údaje. Ne vždy vědomě. Právě díky tomu mohou zprostředkovatelé dat o uživatelích shromažďovat enormní množství informací. Rozsah získaných uživatelských dat sahá od běžných dat (to, co uživatel vyhledá, „lajkne", nakoupí na internetu) až po citlivé osobní údaje (Avast.com: Data Brokers, 2020).

Po shromáždění všech těchto dat o uživateli je datoví zprostředkovatelé roztřídí do kategorií. Data v rámci kategorie jsou pak prodána inzerentům nebo třetím stranám. Kromě celých kategorií si však lze zakoupit i data o konkrétních uživatelích na základě daných parametrů. Odkoupená data uživatelů se pak i nadále mohou zprostředkovávat třetím stranám. Surová či kategorizovaná data sama osobně nemají příliš vypovídající hodnotu. K zacílení reklamy je nejprve potřeba získaná data nějakým způsobem analyzovat – provést analýzu trhu, které se věnuje následující podkapitola.

2.4.3 ANALÝZA TRHU

Analýza trhu je proces, který má za cíl ze získaných dat (ať už zakoupených či získaných vlastním sběrem, např. pomocí Google Analytics) zjistit

preference určitých skupin uživatelů. Vstupní data mohou obsahovat informace jako pohlaví, věk, zájmy, a tak podobně. Ze získaných dat lze například vyčíst, že webovou stránku navštěvují více starší ženy se zájmem o vaření, než mladší muži se zájmem o sport. Tato informace tedy poskytuje důležité údaje pro vytvoření představy o cílové skupině. Místo reklamy a sortimentu mířeného na sportovně založené muže lze oslovit více zákaznic sortimentem pro vaření.

Získaná data tedy pomohou k analýze chování současných zákazníků a případně i zákazníků, kteří z webové stránky odešli nebo neuskutečnili svůj nákup. Motivem pro co nejpřesnější definování cílové skupiny je efektivní zacílení na zákazníky, s cílem zvýšit prodej či návštěvnost webu.

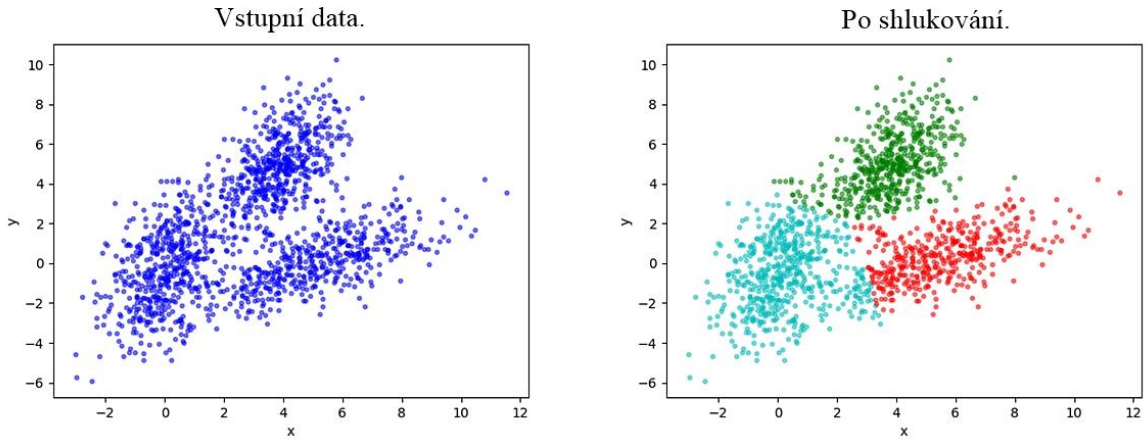
Výše popsaný způsob analýzy dat se nazývá **data mining** (přeložit lze jako dolování dat). Jedná se o analytickou metodu, pomocí níž se dá z objemného množství dat (nejčastěji z databází) získat užitečné informace. Funguje na principu matematické funkce, která analyzuje velké sady dat a hledá mezi nimi skryté souvislosti. Vzhledem k tomu, že metody data miningu mohou vyžadovat poměrně velké množství dat, se nejvíce využívají právě v oblasti internetového marketingu.

Pro lepší představu o metodě data miningu je zde uveden příklad, který výjimečně nepochází z oblasti internetového marketingu. Ve výzkumu, který nese název **beer and diapers** – v českém překladu pivo a plenky, se jedná o příklad využití data miningu na tržbách obchodu. Tento obchod skrze své účtenky zjistil, že muži mají tendenci kupovat pivo společně s plenkami, a to právě každý čtvrtek. Díky této informaci obchod postavil pivo a plenky vedle sebe a zvýšil tak prodejnost obou těchto produktů. Stejně tak to funguje i při data miningu na sociálních sítích – cílem je najít mezi daty určité souvislosti, které pomohou se zacílením reklamy (Golbeck, 2013).

Jedním ze způsobů získávání informací z uživatelských dat je algoritmus shlukování s názvem **K–means**. Obecně je cílem všech shlukovacích algoritmů nalézt takové skupiny uživatelů, kteří mají podobné zájmy či rysy chování. Díky tomu lze snadněji tyto vzorce chování identifikovat a využít k zacílení reklamy na danou skupinu uživatelů.

Obrázek níže ukazuje příklad rozdělení vstupních dat do tří shluků pomocí algoritmu K-means. Levá část obrázku představuje vstupní data, zatímco pravá část obrázku

vizualizuje výstup shlukové analýzy, kde každý z výsledných shluků je reprezentován jednou barvou.



Obrázek 5 - Vizualizace dat před a po použití algoritmu K-means. (Zdroj: vlastní z programu Python, pro vizualizaci Matplotlib.)

Následující kroky popisují princip algoritmu K-means (Raschka & Mirjalili, 2019):

1. Zvolí se číslo K, které udává žádoucí počet výsledných shluků.
2. Vybere se k-náhodných datových bodů (např. uživatelů) ze vstupní datové sady. Tyto body se označí jako centroidy.
3. Každý z datových bodů ve vstupní sadě se přiřadí ke shluku odpovídajícímu nejbližšímu centroidu.
4. V každém shluku se spočítá průměr hodnot jednotlivých souřadnic a tento průměr se použije jako nový centroid (nový centroid nemusí odpovídat žádnému bodu ve vstupní datové sadě).
5. Pokračuje se dále od bodu 3, dokud dochází k přesunu mezi shluky. Pokud k žádnému přesunu v posledním opakování algoritmu nedošlo, pokračuje se na krok 6.
6. Algoritmus končí.

2.4.4 REKLAMA

Po získání dat, jejich analýze a průzkumu trhu již dochází k realizaci reklamy samotné. Pro umisťování reklam je ideálním místem právě sociální síť. Uživatel může nabýt pocit, že sociální síť je vytvořena pouze pro dobro uživatele, ovšem dnes se již

jedná o prostor, kde převládá marketingový trh (Bolotaeva & Cata, 2011). Toho si díky nárůstu počtu reklam na sociálních sítích za poslední roky mohli uživatelé sami všimnout.

Umisťovat reklamy právě na Facebook, YouTube, Instagram či jiné sociální sítě přináší velkou výhodu oproti reklamám umístěných jinde. Například na Facebooku totiž dochází ke shlukování enormního množství lidí a je dnes spíše raritou nebýt uživatelem Facebooku. Z hlediska kvantity je tedy sociální síť ideální na umístění reklamy. Stejně tak je to i s počtem zobrazení reklam, jelikož většina uživatelů navštíví právě zmíněný Facebook minimálně jednou denně (Emarketer.com, 2019). Další velkou výhodou sociální sítě v oblasti reklamy je, že přirozeně disponuje velkým množstvím dat o uživatelích, kterým chce reklamu zobrazit. Uživatelé totiž tyto informace poskytnou již při své registraci, což vede k přesnějšímu zacílení reklamy. Dále také sociální sítě nabízejí řadu analytických nástrojů (viz. kapitola 2.3), které umožňují další optimalizaci vytvářené reklamy.

Výsledná reklama na sociální síti či webu může mít mnoho podob. Jedním z příkladů je **textová reklama**, která je realizována formou odkazu umístěného přímo v textu (hypertext). Dalším typem, se kterým se mohlo setkat mnoho uživatelů sociálních sítí, je **bannerová reklama**. Jedná se o reklamu ve formě obrázku či animace, která bývá umístěna na okraj stránky nebo přímo v příspěvcích na hlavní stránce. Tato reklama funguje na principu zakoupení prostoru na webové stránce či sociální síti na určité období, v průběhu kterého tam inzerent umístí svou reklamu. Výhodu této reklamy je libovolná velikost a grafické, animované či zvukové provedení, které uživatele upoutá.

Jak bylo zmíněno v úvodu této práce, díky rozmachu sociálních sítí vzniklo několik nových povolání. Mezi ně patří i tzv. **influenceři**. Influencer je osoba, která na internetu ovlivňuje velké množství lidí. Převážně se influencerem stává osoba, která je známá na sociálních sítích, nejčastěji Instagramu a YouTube. Influencer má zpravidla velké množství sledujících a svými příspěvky a názory tuto masu lidí ovlivňuje. Z toho důvodu již mnoho firem využívá influencery jako nepřímou formu internetové reklamy. Jedním způsobem reklamy je **placená spolupráce**. Při té influencer dostane zaplaceno za to, že ukáže výrobek či nějaký produkt svým sledujícím (na fotce či ve videu), čímž je přiměje ke koupi výrobku nebo jej minimálně dostane do podvědomí více lidí. Další forma spolupráce s influencery je **barter**. Spočívá ve stejné propagaci produktu, ovšem místo peněžní odměny dostane osoba zaplaceno tím, že si daný produkt po skončení spolupráce ponechá. Třetím

způsobem, který je také poměrně často využívaný, je **affiliate[2] kód**. Influencer dostane od inzerenta speciální unikátní kód, například „MARIE20“, který poskytuje slevu na produkty na dané webové stránce. Tento kód influencer propaguje prostřednictvím svého profilu na sociální síti, čímž naláká své příznivce ke koupi produktů. Po uplatnění kódu zákazníkem dostane zároveň influencer provizi z nákupu, čímž se pro něj tato forma reklamy stává výhodná (Šuľová, 2019).

[2] Jedná se o marketingový nástroj internetových firem, který závisí na provázanosti stránek prodejce se stránkami, které výrobek či službu, jež nabízí, propagují. Zdroj: Crescogroup.org: Význam slova: Affiliate [online]. [cit. 2021-03-01].

3 ZVEŘEJŇOVÁNÍ OSOBNÍCH DAT

Nahráním fotografie, videa či příspěvku na sociální síť o sobě uživatel zveřejňuje svá osobní data. Zveřejňování a celkově využívání sociálních sítí může přinášet mnoho výhod, ale i nevýhod. V této kapitole budou nejprve zmíněny výhody zveřejňování dat, ale stěžejní částí této kapitoly budou negativa související se zveřejňováním osobních dat a s tím budou představeny i možné následky. Obsahem této kapitoly je i diskuse o příspěvcích, které není na sociálních sítích vhodné sdílet.

3.1 VÝHODY ZVEŘEJŇOVÁNÍ DAT

Možnosti, které sociální sítě nabízejí, jsou pro potencionální uživatele velmi atraktivní. Vytvořit si profil na sociální síti totiž přináší mnoho výhod. Příkladem může být rychlejší komunikace s přáteli či rodinou a možnost sdílet jeden příspěvek (fotografie z dovolené, videa, odkazy a podobně) mezi více uživateli bez nutnosti rozesílat obsah individuálně. Kromě sledování novinek a zpráv ze světa lze sledovat i příspěvky našich přátel či veřejně známých osobností.

Motivací pro sdílení obsahu může často být i tzv. pocit štěstí, který uživatel může nabýt, pokud zveřejněním fotografie získá označení „To se mi líbí“ od ostatních uživatelů. Podle článku výzkumného pracovníka Harvardské univerzity Trevora Haynese za tento pocit štěstí může hormon dopamin, který vzniká v mozku a vylučuje se do těla. Příčinou je úspěšná sociální interakce (Haynes, 2018).

Prostřednictvím sociálních sítí lze v dnešní době absolvovat i pracovní pohovor, meeting nebo školní výuku skrze webkameru a mikrofon. Z toho plyne, že sociální sítě většině uživatelů ušetří čas. Nemusí se dopravovat na místo setkání, ale stačí se sejít na sociální síti. Tento neúplný seznam výhod využití sociálních sítí je příčinou toho, proč jsou dnes sociální sítě již nedílnou a také oblíbenou součástí života většiny uživatelů. Na sociálních sítích ovšem lze nalézt i negativa. Mimo rizika, která jsou blíže popsána v první kapitole, založením profilu na sociální síti ztrácíme kus našeho soukromí. Je to způsobeno tím, že o sobě sdělujeme mnoho informací osobám, které nemusíme ani osobně znát.

3.2 NEGATIVA ZVEŘEJŇOVÁNÍ DAT

Při používání sociálních sítí je velmi důležité si uvědomit, že cokoliv uživatel nahraje na internet, už většinou nejde vzít zpět. I když uživatel příspěvek – zprávu či fotografii smaže, vždy se může najít někdo, kdo si vytvořil screenshot[3]. Také smazání zprávy neznamená, že se definitivně odstraní z konverzace i druhému člověku. Proto je velmi důležité, aby si uživatel předem promyslel, co o sobě chce veřejně sdílet.

Lze oponovat tím, že některé sociální sítě – uvedu například Facebook, umožňují nastavit soukromí. Ovšem ne vždy toto nastavení opravdu zaručí, že sdílený obsah neuvidí nikdo jiný. Pokud se zkusíme sami zamyslet nad tím, zda jsme někdy ukázali či přeposlali screenshot příspěvku jiné osoby našemu známému, kamarádovi nebo rodině, určitě si minimálně na jeden takový případ vzpomeneme. Proto je pro používání sociálních sítí důležité pochopit, že i když si uživatel upraví soukromí příspěvku jen pro přátele, neznamená to, že není veřejně dostupný. Kdykoli uživatel digitálně sdílí příspěvek na sociální síti, měl by předpokládat, že by se mohl vymknout jeho kontrole.

3.3 NEVHODNÉ PŘÍSPĚVKY

Při sdílení příspěvků je důležité myslet na to, že se svými příspěvky uživatel prezentuje a vytváří druhým lidem obrázek o něm samotném. Ve společnosti je profil na sociální síti vnímán jako jakási vizitka. Navíc má k této vizitce díky virtuálnímu světu přístup kdokoliv – rodiče, prarodiče, pedagogové, nadřízení a podobně. Vždy je tedy důležité zvážit, jaké informace o sobě chce uživatel zveřejnit.

Existuje řada věcí, které by o sobě uživatel na sociálních sítích neměl nikdy sdílet. Na prvním místě to jsou veškeré citlivé i osobní údaje - adresa bydliště, čísla dokladů a bankovních karet, hesla, fotografie dokumentů, smluv a podobně. Tyto věci by měly být pro uživatele samozřejmé. Existuje ovšem řada uživatelských dat, jejichž sdílení se nemusí na první pohled zdát nikterak nebezpečné. Například nevinný příspěvek uživatele o tom, že odjíždí na dovolenou, může společně s předchozími fotografiemi bydliště vzbudit velký zájem zlodějů. Proto by uživatel neměl nikdy zveřejňovat

[3] Screenshot – grafický snímek obrazovky, fotografie zachycující obsah zobrazovaný na monitoru. Pořizuje se nejčastěji klávesou Print screen. Zdroj: It-slovnik.cz: Význam slova screenshot [online]. [cit. 2021-03-19]. Dostupné z: https://it-slovnik.cz/pojem/screenshot/?utm_source=cp&utm_medium=link&utm_campaign=cp

informace o jeho adrese či přímo fotografie bydliště, vchodových dveří, výhledu z bytu nebo domu a fotografie z dovolených sdílet nejlépe až zpětně.

3.3.1 DĚTSKÉ FOTOGRAFIE

Mezi nevhodné, ač na první pohled ne zřejmé, je sdílení fotografií dětí na sociálních sítích. Byť se může zdát, že se v žádném případě nemůže jednat o nevhodný obsah, existuje zde potencionální riziko, které si uživatel nemusí uvědomovat. Zveřejněním fotografie svého dítěte na sociální sítí dává uživatel souhlas s jejím šířením a zároveň riskuje možnost ukradení identity dítěte. V takovém případě může být identita dítěte použita například na dětských pedofilních či pornografických webových stránkách.

Problematika přehnaného sdílení dětských fotografií na internetu je již natolik rozšířená, že má svůj název **sharenting** – přílišné užívání sociálních médií rodiči, kteří sdílejí obsah týkající se jejich dítěte. Příkladem sharentingu je sdílení fotografií, videí či popisování činností a chování malého dítěte. Dítě tak získává online identitu, kterou nechtělo a ani po rodiči nepožadovalo (Kopecký, 2019).

3.3.2 CHOULOSTIVÉ FOTOGRAFIE

Dalším tabu na sociálních sítích je, aby uživatel sdílel jakékoliv jeho či cizí vyzývavé, odhalené nebo nahé fotografie. Některé fotografie se mohou na první pohled zdát jako nevinné. Například fotky dětí v plavkách nebo nahé fotografie dětí při koupání. Ovšem i zde je potencionální riziko, které by si měl uživatel zveřejňující fotografii uvědomit. Stejně tak to může být i u jedinců, kteří sdílí své choulostivé fotografie dobrovolně. Každá osoba užívající sociální sítě by měla být informována, že sdílet veřejně své choulostivé fotografie je naprosto nevhodné. Ať už kvůli následkům, které budou popsány v následující kapitole, ale také kvůli internetovým predátorům (kybergroomingu).

Termín **kybergrooming** označuje typ nevhodného chování osob na internetu (tyto osoby se označují jako predátoři). Takováto osoba si vyhlédne na internetu oběť a chce v ní vyvolat falešnou důvěru kvůli pocitu sblížení. Následně může například vyžadovat choulostivé fotografie, kterými může chtít oběť vydírat či může trvat na osobní schůzce. Následkem takovéto schůzky může být i sexuální zneužití oběti, fyzické násilí, nucení k dětské prostituci či výrobě dětské pornografie. Nejvíce ohroženou skupinou v této

problematice jsou dospívající děti, převážně dívky ve věku 11–17 let (Kopecký & Krejčí: Rizika virtuální komunikace, 2010).

3.3.3 NÁSILNÝ OBSAH, NEVHODNÉ VYJADŘOVÁNÍ

Ač tento obsah nemusí porušovat pravidla všech sociálních sítí, není vhodné sdílet veškeré fotografie či videa, na kterých je zachycené násilí a vulgární výrazy. Stejně tak je to v případě vyhraněných názorů na rasu, náboženství či na politiku.

Jak již bylo řečeno v úvodní části této kapitoly, takový obsah může zhlédnout kdokoli, např. pedagog nebo současný či budoucí nadřízený daného uživatele. Jednoduše řečeno, někdo, komu by takový druh obsahu nemusel být příjemný. Dále je potřeba zvážit i fakt, že na sociální sítě (i přes věkové omezení) mají přístup děti, a ne každý může být takové povahy, aby nějaké násilné, vulgární či urážlivé příspěvky unesl.

3.3.4 PRODEJ

Dalším nevhodným obsahem na sociálních sítích jsou nabídky k prodeji nevhodného či zakázaného sortimentu zboží. Ač sociální sítě v posledních letech zavedly možnosti prodeje a nákupu (například Facebook Marketplace), stále existují věci, které by uživatel na internetu nabízet a poptávat neměl. Facebook.com jako příklad uvádí různé druhy drog (marihuana a podobně), farmaceutická léčiva a střelné zbraně.

Zajímavostí je, že Facebook.com dovoluje vést diskuse o střelných zbraních. Dokonce lze střelné zbraně propagovat, ale k jejich zakoupení musí dojít mimo platformu Facebooku, a to za předpokladu, že splňují všechny příslušné zákony a nařízení.

3.4 NÁSLEDKY SDÍLENÍ NEVHODNÉHO OBSAHU

Sociální sítě jsou primárně místem pro komunikaci, sledování a sdílení obsahu mezi přáteli. Ovšem skrze zveřejněné informace a příspěvky jiného uživatele si lze vytvořit představu o jeho zájmech, názorech i životní úrovni. Z toho důvodu předchozí kapitola popsala několik druhů nevhodného obsahu, jehož sdílení může mít neblahé následky, které jsou popsány ve zbytku této kapitoly.

3.4.1 ZAMĚSTNÁNÍ

Většina lidí si před pracovním pohovorem připraví životopis, patřičné oblečení a vhodné fráze, které by mohly zvýšit šanci na přijetí na určitou pozici. Během pracovního pohovoru se snaží ukázat sami sebe v nejlepším světle. Na co ale může většina lidí zapomenout, jsou sociální sítě.

Pokud pohovor proběhl v pořádku, ale i tak uchazeč neuspěl, je zde možnost, že svou roli v nepřijetí hrál profil na sociálních sítích. Sociální sítě jsou veřejným místem a z příspěvků si lze vytvořit názor na danou osobu. Proto není překvapením, že si i náborový pracovník, nadřízený či kdokoliv jiný z firmy, může prohlédnout profil daného uchazeče. Pokud uchazeč sdílí na svém sociálním profilu příspěvky, které mohou být považovány za nevhodné, jako například vyhraněné názory (politické, rasové či náboženské) nebo choulostivé fotografie, mohou tyto skutečnosti způsobit nepřijetí jinak slibného uchazeče.

Stejně tomu tak může být ve stávajícím zaměstnání. Není raritou, že zaměstnanec tvrdí, že je nemocný a následně zveřejní fotografie z výletu či jiné aktivity. Stejně tak je tomu v případě příspěvků o aktuálním zaměstnanci, které by mohly danou osobu nebo firmu shazovat. I přes nastavené soukromí se příspěvek může dostat k nadřízeným a ohrozit tak stávající pracovní pozici jedince.

3.4.2 VZTAHY

Sociální sítě mají na seznamování ve 21. století velký vliv. Nabízí možnost seznámení, aniž by osoba musela vynaložit větší námahu. Lidé se nemusí náhodně potkávat a seznamovat, ale stačí si přidat někoho do přátel, začít protějšek sledovat či označit fotografii tlačítkem „To se mi líbí“. I z tohoto důvodu je opět důležité dbát na příspěvky, které uživatel sdílí. Dnes je totiž naprostou rutinou a samozřejmostí, že si lidé svůj potenciální protějšek prověřují právě na sociálních sítích a díky příspěvkům si o něm tvoří názor. Nevhodné příspěvky mohou potencionální partnery odradit.

4 ONLINE BEZPEČNOST

Internet je rozsáhlé veřejné místo, které se stalo nedílnou součástí každodenního života většiny lidí. Využívá se k práci, ke studiu, pro zábavu, odpočinek, ale i pro jiné osobní účely. Spolu s vyšší aktivitou uživatelů roste i riziko hrozeb na internetu. Tyto hrozby sahají od zneužití osobních dat, po nástrahy black hat hackerů[4] a podobně. Cílem této kapitoly bude informovat o možných hrozbách na internetu a poukázat na to, jak si zajistit větší bezpečnost během užívání internetu.

4.1 HROZBY

Uživatel by nejprve měl být informován o možných hrozbách, kterým by mohl v online světě čelit a v jaké podobě by na něj na internetu mohly čekat. Teprve potom se proti nim může začít efektivně bránit. Tato kapitola se na rozdíl od té předešlé nebude věnovat rizikům spojeným se zveřejňováním dat, ale bude se zabývat zbývajícími internetovými hrozbami – například malwarem, únikem a zneužití dat, hesel či čísel kreditních karet.

4.1.1 ZNEUŽITÍ HESEL

Heslo je řetězec znaků, který slouží k ověření totožnosti uživatele při přihlašování. S hesly se uživatel při plnohodnotném využívání internetu setká téměř všude. Například při přihlašování do e-mailové schránky, na sociální sítě nebo do školních či pracovních portálů. Z tohoto důvodu by heslo nemělo být uživatelem zveřejňováno. Navíc je heslo nutné volit tak, aby jej nešlo snadno prolomit. Slabé heslo, které například obsahuje datum narození uživatele, jméno mazlíčka, telefonní číslo a podobně, lze totiž velmi snadno uhádnout (ManagementMania.com, 2016).

Silné heslo samotné však nezabrání jeho zneužití. Častou chybou je využívat stejné heslo na každé webové stránce či aplikaci. Ačkoliv lze předpokládat, že velké sociální sítě, jako například Facebook.com, mají zabezpečení proti úniku hesel na nejvyšší úrovni, je zde stále možnost, že se přístupových údajů zmocní neoprávněná osoba. Může se to stát tak, že

[4] Black hat hacker – zločinec, který proniká do počítačových sítí, narušuje internetovou bezpečnost k osobnímu prospěchu. Zdroj: Kaspersky.com: What is a Black-Hat hacker? [online]. AO Kaspersky Lab [cit. 2021-03-23]. Dostupné z: https://www.kaspersky.com/resource-center/threats/black-hat-hacker

pokud je stejné heslo jako na Facebook.com použito i na jiné, mnohem menší a hůře zabezpečené stránce, na které dojde k úniku přihlašovacích údajů, zmocní se útočník automaticky i přihlašovacích údajů k již zmíněné sociální síti. Z tohoto důvodu je vedle silného hesla důležité i volit si ke každé webové stránce a aplikaci jiné heslo, které by nešlo spojit s žádným z dalších uživatelských účtů u jiných služeb. Nejvhodnější je využít některý z volně dostupných generátorů hesel, a pro zapamatování hesel využít program pro jejich správu – jako například KeePass (obr. 6).

V této oblasti se rozhodně vyplatí dbát zvýšené opatrnosti. Důsledkem úniku hesla může totiž být i například odcizení účtu, získání osobních údajů či čísel kreditních karet, což může vyústit až ve ztrátu finančních prostředků.

Obrázek 6 - Generátor náhodných hesel. (Zdroj: Avast.com.)

4.1.2 MALWARE

Malware (kombinace anglických slov malicious a software) je v informatice označením pro škodlivý software. Cílem je poškodit nebo zneužít zařízení, službu či síť. Malware používají black hat hackeři k získání osobních dat, krádežím financí, k nenávratnému poškození či vymazání počítače nebo mobilního zařízení.

Malware se nejčastěji objevuje v e-mailech a na sociálních sítích. Do zařízení se ale dostane chováním uživatele – otevírání odkazů s netypickou URL adresou, navštívením napadené webové stránky, stažením napadeného softwaru či jiného obsahu nebo například zadáním přihlašovacích údajů do elektronického bankovnictví na falešné webové stránce. Existuje mnoho druhů malwaru. Ty nejčastější z nich, jsou rozebrány níže na základě

článku o malwaru na stránkách Avast.com (Avast.com: Ochrana před hrozbami na Internetu.).

Trojský kůň je druh malwaru, který nese název díky antickému příběhu o dobytí Tróji, protože princip napadení cílového zařízení tímto typem škodlivého softwaru je mu velice podobný. Tento škodlivý software se totiž na venek tváří naprosto neškodně či naopak uživateli prospěšně. Trojský kůň se například může vydávat za bezplatný program (hra, spořič obrazovky) nebo dokonce za antimalwarový software. Po nainstalování ovšem skrytě začne uživateli způsobovat značné škody či sbírat jeho data.

Spyware je typ malwaru, který jde těžce odhalit. Uživatel totiž nijak nepozná, že jeho zařízení bylo napadeno, jako je to například u trojského koně. Spyware dokáže sbírat informace o chování uživatele na internetu. Například dokáže zachytit údaje o kreditních kartách, zadaná hesla či historii prohlížení.

Phishing se šíří skrze e-maily. Uživateli se e-mailová zpráva může jevit velmi věrohodně. Podvodný e-mail se může vydávat za zprávu od známé firmy, bankovní společnosti či jiné organizace jemu blízké. V takovém podvodném e-mailu zpravidla bývá odkaz s prosbou o doplnění osobních údajů či jejich aktualizaci nebo i informace o získání nějaké výhry. Po kliknutí na odkaz je uživatel přesměrován na falešnou webovou stránku, kde je vyzván k vyplnění osobních údajů, čísla kreditní karty či přihlášení do internetového bankovnictví. Design stránky přitom může vypadat shodně s oficiální stránkou. Po zadání informací data získá druhá strana.

Počítačový virus je část kódu nebo program, který se spustí na počítači bez vědomí a svolení uživatele. Díky tomu může získat kontrolu nad počítačem či provádět destruktivní akce. Virus se může šířit z počítače na počítač prostřednictvím různých sítí, stejně tak jako biologický virus přechází z člověka na člověka.

Spam není malwarem, který by ohrozil uživatelův počítač či data, ale jedná se o nevyžádanou poštu, která se masově šíří internetem. V této zprávě je převážně propagován nějaký produkt či služba. Nejčastěji lze na spam narazit v e-mailu. Bránit se mu uživatel může filtrací příchozí pošty.

4.1.3 VYDÍRÁNÍ

Mezi další hrozby na internetu patří vydírání. Vydírání má kromě klasické formy i svou malware podobu, která je záměrně zařazena do této samostatné podkapitoly. Uvedené informace opět čerpají ze stránky Avast.com (Avast.com: Ochrana před hrozbami na Internetu.).

Ransomware – tak se nazývá druh malwaru, který omezí či úplně zakáže uživateli přístup k jeho počítačovému systému nebo souborům. Za umožnění přístupu požaduje program zaplacení výkupného. Ne vždy je potřeba výkupné opravdu zaplatit, protože často se takový software dá odstranit specializovaným programem. I přesto je vhodné se proti takové hrozbě preventivně bránit.

Vydírání může probíhat i v případě **spamu**. Uživateli může například přijít e-mail, že někdo získal jeho osobní údaje, fotografie či videa pořízená z webkamery uživatele a pokud uživatel do časového limitu nepošle finanční obnos, rozešle je útočník celému jeho kontaktnímu adresáři. Jde pouze o vyvinutí tlaku na jedince a získání finančního obnosu. Ne vždy jsou takovéto výhružné zprávy podložené skutečným odcizením dat a lze proto takovou výhružku ignorovat. Existují však i případy, kdy se útočník skutečně zmocnil avizovaných dat a při nezaplacení je použil.

Vydírání může probíhat i na sociálních sítích či diskusních fórech. Vydírání na sociálních sítích bylo již letmo zmíněno v kapitole o sdílení nevhodných příspěvků. Tento problém však nemusí vždy souviset přímo s veřejně umístěnými informacemi. Pokud uživatel komunikuje s jinou osobou přes jakýkoliv komunikační kanál, měl by si dát pozor na informace či fotky, které s takovým člověkem sdílí. To platí obzvláště v případě, když uživatel nemá podložené informace o identitě druhé osoby. Na druhé straně komunikačního kanálu totiž nemusí být ten, za koho se vydává a může následně uživatele vydírat zveřejněním poskytnutých informací.

4.2 BEZPEČNOST NA INTERNETU

Jak na internetu chránit sebe i svá data je rozebráno v následujících dvou podkapitolách. Prvky bezpečnosti, kterými lze hrozbám předcházet, by uživatel měl mít v povědomí a aktivně je využívat. Pro přehlednost je zde bezpečnost rozdělena na dvě kategorie – aktivní a pasivní. Mezi aktivní bezpečnost se bude řadit chování uživatele,

kde k hrozbě může dojít neuváženým chováním na internetu. Mezi pasivní bezpečnost jsou pak řazeny prvky, které uživatele chrání bez jeho vědomí. Správným užitím metod jak aktivní, tak pasivní ochrany, se lze vyhnout následkům hrozeb, na které uživatel dříve nebo později narazí.

Následující zásady bezpečného chování na internetu vycházejí z obecně známých skutečností a internetových stránek Jaknainternet.cz a Bezpecnyinternet.cz.

4.2.1 PASIVNÍ BEZPEČNOST

Pro zachování bezpečnosti na internetu by měl uživatel pravidelně provádět preventivní kroky, které budou pasivně chránit jeho zařízení i osobní data. Tato pravidla hrozbám předcházejí, ale i minimalizují následky, pokud se uživatel stane obětí nějakého internetového útočníka.

- **Antivirový program** je počítačový software, který chrání zařízení před škodlivým softwarem (malware, viry). Dokáže identifikovat potencionální hrozbu a odstranit ji. Každý uživatel, který se chce byť jen připojit do internetové sítě, by měl mít zařízení chráněné právě antivirovým programem.

- Kromě antivirové ochrany je prevencí před hrozbami také pravidelné **aktualizování** operačních systémů a programů. Aktualizace v sobě mohou často obsahovat bezpečnostní vylepšení pro silnější ochranu zařízení.

- Důležitost ochrany **hesel** byla zmíněna již v předchozích kapitolách. Pro bezpečnost uživatelských dat je důležité mít silné heslo a nepoužívat stejné heslo v kombinaci s přihlašovacím jménem či e-mailovou adresou na všech webových stánkách a sociálních sítí.

- Používání **dvoufázového přihlašování** – nejprve se uživatel přihlásí heslem a poté mu přijde např. SMS s jedinečným kódem, který zadá do aplikace.

- **Firewall** v počítačové síti blokuje nebo povoluje komunikaci skrze internet. Brána firewall pomáhá zabránit hackerům a škodlivému softwaru v přístupu k počítači prostřednictvím sítě (Mcafee.com: Co je brána firewall?).

- Svou bezpečnost také uživatel může zdokonalit zvýšením pozornosti při nastavování **soukromí**. U každého příspěvku na sociální síti lze změnit, zda obsah mohou vidět jen přátelé nebo bude přístupný veřejnosti. Omezí se tak riziko poskytnutí osobních informací cizím lidem.

4.2.2 AKTIVNÍ BEZPEČNOST

Pro zajištění bezpečnosti musí uživatel aktivně přemýšlet, uvědomovat si rizika a věnovat pozornost možným nástrahám. Mít pouze ošetřeny všechny prvky pasivní bezpečnosti nestačí. Například antimalwarový program uživatele nezastaví, aby nesdílel své osobní informace s cizími osobami. Z toho důvodu je potřeba minimalizovat hrozby, které plynou z neuváženého chování tím, že budeme přemýšlet nad aktivitami prováděnými v online světě.

Hrozbám uživatel může předcházet tím, že bude rozumně **vyhodnocovat nebezpečí**. V případě neobvyklého e-mailu od neznámého odesílatele je důležité neotevírat a nestahovat přílohy. Neotevírat přiložené odkazy u podezřelých emailů. Nezadávat čísla svých kreditních karet nebo osobní údaje na stránkách, jejichž důvěryhodnost není ověřena platným certifikátem.

Potencionálně podvodný e-mail lze celkem snadno rozpoznat. Uživatel by měl nejprve vyhodnotit jméno a e-mailovou adresu odesílatele a doménu, ze které byl e-mail odeslán. Také je vhodné zaměřit se na gramatiku zprávy a její obsah. Pokud zpráva nedává smysl, mohl být text přeložen z jiného jazyka a může se jednat o podvodný e-mail. Věnovat svou pozornost je důležité hlavně přílohám a odkazům. Webové prohlížeče mají možnost po umístění kurzoru na odkaz zobrazit v levém spodním rohu celý název cílové adresy, což může napomoct odhalit potencionální hrozbu. Pokud se opravdu jedná o podvodný e-mail, zřejmě bude adresa dlouhá, složená z nesrozumitelných znaků a bude mít neobvyklou doménu. Je také třeba mít na paměti, že pokud naše banka bude vyžadovat doložení či aktualizaci osobních nebo přihlašovacích údajů, nebude nás o to žádat emailem.

Mezi aktivní bezpečnost tedy patří:

- Aktivně vyhodnocovat rizika.
- Umět rozlišit podvodné e-maily.
- Nesdělovat osobní údaje, hesla, čísla dokladů přes chat, diskusní fóra a nesdílet je nikdy veřejně. Ani s lidmi, které uživatel může znát osobně.
- Vždy zvážit, jaký obsah sdílet. Řeč je především o jakémkoliv materiálu, který by mohl vést k vydírání. Příkladem jsou například nevhodné fotografie, smlouvy apod.
- Zálohovat si důležitá data pro případ jejich ztráty.

5 KAUZY

V této kapitole jsou uvedeny příklady některých kauz týkajících se zneužití či úniku uživatelských dat. Zmíněna je kauza společnosti Cambridge Analytica, Avast, Mall.cz a WhatsApp. Závěrem je popsána i osobní zkušenost se zneužitím osobních dat autora této práce.

5.1 CAMBRIDGE ANALYTICA

Cambridge Analytica byla britská společnost zabývající se analýzou dat, založena v roce 2013. Jednalo se o dceřinou společnost firmy SCL Group, která uváděla, že se věnuje od výzkumu až přes protidrogové a politické kampaně. Cambridge Analytica se negativně proslavila díky zneužití více než milionu uživatelských dat z Facebooku v roce 2016. Svou činnost ukončila v roce 2018.

V souvislosti se společností Cambridge Analytica se hovoří převážně o zneužití uživatelských dat za účelem ovlivňovaní voličů v prezidentských volbách v roce 2016. Data uživatelů získala díky aplikaci vyvinuté vědeckým pracovníkem Aleksandrem Kogenem. Nesla název „This Is Your Digital Life“. Miliony uživatelů si tuto aplikaci stáhli, přihlásili se pomocí svých přihlašovacích údajů na Facebook a vyplnili otázky, které měly vytvořit psychologický profil uživatele. Aplikace ovšem shromáždila jednak data poskytnutá v aplikaci, ale i jejich osobní údaje z profilu na Facebooku. Kogen poté tato data poskytl společnosti Cambridge Analytica (Reuters.com: Who is Cambridge Analytica and what did it do?, 2013).

Cambridge Analytica následně v červnu roku 2016 využila tato data k ovlivňování potencionálních voličů v prezidentských volbách. Uskutečnila to tak, že díky získaným uživatelským datům mohla skrze Facebook provádět dezinformační kampaně pomocí cílených reklam. Uživatel mohl na sociální síti tedy narážet na reklamy na míru, kde inzerovaná politická strana rezonuje s jeho názory a zájmy (Niedermayer.cz: Únik dat na Facebooku – mysleli jste si, že vaše data jsou v bezpečí?, 2018).

5.2 AVAST

Avast Software s.r.o. je česká společnost, která byla založena v roce 1988. Zabývá se vývojem nástrojů pro počítačové zabezpečení a ochranu soukromí. Nejznámější produkt této společnosti je Avast antivirus. Tento antivirus má uživatele ochránit před hrozbami v podobě virů a malwaru a zařídit uživateli soukromí v online prostoru (Avast.com).

Koncem ledna 2020 webové stránky zaměřené na informační technologie PCMag a Motherboard zveřejnili, že antivirový program Avast rozprodává uživatelská data. Tyto stránky poskytly zdroji anonymitu. Avast měl údajně prodej dat provádět přes svou divizi Jumpshot. Prodaná data zahrnovala vyhledávání v prohlížeči Google, vyhledávání v Google Mapách i konkrétní shlédnutá YouTube videa. Uvádí se, že data byla anonymizovaná, ovšem několik odborníků uvedlo, že je možné odhalit identitu uživatele i zkombinováním získaných dat (Cox, 2020).

Úřad pro ochranu osobních údajů zahájil v této kauze společnosti Avast Software s.r.o. šetření. Předsedkyně Úřadu Ivana Janů uvedla: „V současnosti shromažďujeme informace k celému případu. Je zde podezření ze závažného rozsáhlého porušení ochrany osobních údajů uživatelů. Na základě našich zjištění učiníme další kroky, o kterých budeme veřejnost informovat.“ (Uoou.cz: Statement on Avast case, 2020). V době dopsání této práce není výsledek šetření znám.

5.3 MALL.CZ

Mall.cz je český, internetový obchod, který nabízí širokou škálu sortimentu. Například elektroniku, bílé zboží, počítače, mobilní telefony, hračky a sportovní potřeby. Kromě internetového obchodu provozuje Mall.cz i kamenné prodejny, které slouží především k výdeji objednaného zboží. V roce 2017 Mall.cz oznámil, že byl napadený hackery a došlo k úniku osobních údajů přibližně 750 000 uživatelských účtu. Jednalo se o jména, příjmení, e-mailové adresy a hesla uživatelských účtů. Soubor se všemi těmito údaji, včetně rozklíčovaných hesel, se objevil na portále Uložto.cz. Na vině bylo nedostatečné zabezpečení databáze a použití slabé hashovací funkce pro ukládání hesel. I přesto, že byl soubor ze stránky Uložto.cz později smazán, uniklá data mohou dodnes kolovat po internetu.

Michal Špaček, známý český webový vývojář, který se zabývá zejména zajištění bezpečnosti webových stránek, se zaměřil na to, jakým způsobem mohla být uniklá hesla v podobě hashů prolomena. Během 45 minut získal 165 tisíc hesel a po 12 hodinách z nich zůstalo neprolomených jen 935 (Špaček, 2018).

Úřad pro ochranu osobních údajů udělil společnosti Internet Mall, a.s. (Mall.cz) pokutu ve výši 1,5 milionu korun. Před neoprávněným přístupem nebyla data dostatečně chráněná v období minimálně od 31. prosince 2014 do srpna 2017. V důsledku toho došlo v době od 27. července do 25. srpna 2017 ke zpřístupnění uvedených osobních údajů na serveru Uložto.cz (Uoou.cz: Úřad udělil společnosti Internet Mall, a.s. pokutu 1,5 milionu korun., 2018).

5.4 WHATSAPP

Společnost WhatsApp Inc. založili v roce 2009 Jan Koum a Brian Acton. Název WhatsApp vznikl jako slovní hříčka vycházející z anglické fráze „What´s up?‘‘ v překladu „Jak se vede?“. Aplikaci, kterou společnost nabízí, používá již 2 miliardy lidí ve více než 180 zemích.

Aplikace WhatsApp nejprve sloužila jako alternativa k SMS zprávám. Dnes aplikace podporuje i výměnu hlasových zpráv, dokumentů, multimediálních souborů (fotografie, videa a audio soubory) a lze mezi uživateli sdílet i polohu. WhatsApp aplikaci jde využívat na smartphonu skrze telefonní číslo a je nutné, aby uživatel byl připojený k internetu (WhatsApp.com: O společnosti WhatsApp., 2021).

WhatsApp se v roce 2014 spojil s Facebookem. Cílem společnosti bylo i tak zůstat stále samostatnou aplikací se stejnými službami i zabezpečením komunikace. Přesto k 8. lednu 2021 došlo k aktualizaci zásad ochrany osobních údajů ze strany aplikace WhatsApp. Nové podmínky umožňují sdílet osobní data a informace s Facebookem a jeho přidruženými aplikacemi. Stejně tak WhatsApp může použít informace, které od Facebooku obdrží (Jonnalagadda, 2021).

Po zjištění obsahu této aktualizace zaznamenaly nárůst počtu nových uživatelů aplikace Signal a Telegram v důsledku odchodu uživatelů ze služby WhatsApp.

Signal a Telegram jsou komunikační aplikace, které využívají bezpečného koncového šifrování a nesledují data uživatelů.

5.5 OSOBNÍ ZKUŠENOST

Se zneužitím osobních dat mám i osobní zkušenost. Během koronavirové krize na jaře roku 2020 webová stránka Svetomat.cz zneužila mou starší fotografii na Facebooku. Použila ji u smyšlené recenze na podvodném e-shopu s rouškami. Tento e-shop nabízel koupi roušek pouze s platbou předem. Ovšem po zakoupení zákazníci neobdrželi žádné roušky, ani nedostaly peníze zpět.

Zneužití mé fotografie jsem se dozvěděla díky panu Januszovi Koniecznému, členovi České pirátské strany, který mě kontaktoval, zda se skutečně jedná o moji osobu. Po vysvětlení, že se jedná o mou starou fotografii a recenze není psaná mnou, mě požádal o spolupráci na podání trestního oznámení (obr. 7).

Obrázek 7 - Recenze s mou fotografií na podvodném e-shopu. (Zdroj: Svetomat.cz, webová stránka již není dostupná.)

ZÁVĚR

Cílem této práce bylo metodou analýzy zjistit, jaká data jsou sociálními sítěmi a jinými online službami sbírána s vědomím či bez vědomí uživatele. Dalším cílem bylo popsat hrozby v online prostoru, které nejčastěji zapříčiní zneužití uživatelských dat, a v návaznosti na ně diskutovat možné techniky obrany v podobě dodržování online bezpečnosti.

V teoretické části byly na základě uvedené literatury nejprve vymezeny podstatné pojmy týkající se sociálních sítí a dat uživatelů. To usnadní uvedení čtenáře do problematiky práce. V návaznosti na to se druhá kapitola zaměřuje na analýzu rozsahu a druhu získaných uživatelských dat s vědomím či bez vědomí uživatele. Tato část je přínosná v tom, že se podařilo odhalit mnoho metod, které jsou využívány k získávání uživatelských dat, a čtenář si tak může udělat obrázek o tom, jak je s jeho daty nakládáno. Příkladem sběru dat jsou cookies, device fingerprint, heat maps, Facebook pixel a Google Analytics. Otázka, k čemu tato data jsou užitečná, je zodpovězena v poslední části druhé kapitoly. Nejčastěji z těchto získaných dat těží internetový marketing za účelem přesného zacílení reklamy na uživatele.

V kapitole čtvrté, která se zabývá Online bezpečností, jsou popsány hrozby, se kterými by se uživatelé mohli v praxi setkat nejčastěji a mohli by zapříčinit únik či zneužití uživatelských dat. V návaznosti na to práce popisuje možné techniky obrany a zásady bezpečného chování na internetu. Tyto zásady jsou rozděleny na pasivní bezpečnost (antivirový program, aktualizace, silná hesla, dvoufázové přihlašování, soukromí) a aktivní bezpečnost (vyhodnocovaní rizik, rozlišování podvodných e-mailů, nesdělování osobní údaje, zálohování dat).

Po přečtení této práce by měl čtenář získat větší přehled o tom, kolik a jaká data jsou o něm sbírána a jakými způsoby to může být realizováno. Z tohoto důvodu by výstupy této práce mohly posloužit jako edukativní podklady pro výuku či jako materiál určený úplným začátečníkům pro orientaci v rizicích online prostředí.

RESUMÉ

The aim of this work was a methodological analysis to find out what data social networks and other online services collect with or without the user's awareness. The theoretical part defines the basic concepts related to social networks and user data. It also describes the possible threats in the online environment and possible ways of how to prevent them. The practical part of the work analyses the scope and type of user data obtained by the online services. This part can be beneficial since it also discusses a significant number of data collection methods that have been found. The outcome of the work could be used as an educational foundation, or as a guideline for orientation in the risks of the online environment dedicated to complete beginners.

SEZNAM LITERATURY

Avast.com [online]. Praha, 1988 [cit. 2021-03-27]. Dostupné z: https://www.avast.com/

Avast.com: Ochrana před hrozbami na Internetu. *AVAST Software s.r.o* [online]. [cit. 2021-03-23]. Dostupné z: https://www.avast.com/cs-cz/c-online-threats

Bezpecnyinternet.cz [online]. Praha, 2010 [cit. 2021-03-23]. Dostupné z: http://www.bezpecnyinternet.cz/

BOLOTAEVA, Victoria a Teuta CATA. Marketing Opportunities withSocial Networks. *Journal of Internet Social Networking and Virtual Communities* [online]. 2011, 1-8 [cit. 2021-02-28]. ISSN 21660794. Dostupné z: doi:10.5171/2011.409860

BURNELL, Kaitlyn, Madeleine J. GEORGE, Justin W. VOLLET, Samuel E. EHRENREICH a Marion K. UNDERWOOD. Passive social networking site use and well-being: The mediating roles of social comparison and the fear of missing out. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. 2019, **13**(3), 1 [cit. 2020-12-25]. ISSN 1802-7962. Dostupné z: doi:10.5817/CP2019-3-5

BURÝŠKOVÁ, por. Mgr. Lenka. *Víte co je KYBERŠIKANA?* [online]. 11. 12. 2009, 1 [cit. 2020-12-25]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

COX, Joseph. *Vice.com: Avast antivirus sells user browsing data investigation* [online]. Leden, 27, 2020 [cit. 2021-03-27]. Dostupné z: https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation

Crescogroup.org: Význam slova: Affiliate [online]. [cit. 2021-03-01].

ČERNÁ, Alena, Lenka DĚDKOVÁ, Hana MACHÁČKOVÁ a Anna ŠEVČÍKOVÁ. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0.

Facebook [online]. Dostupné z: https://www.facebook.com/

Facebook.com: *Facebook.com: Co je to Instagram?* [online]. [cit. 2020-11-27]. Dostupné z: https://www.facebook.com/help/instagram/424737657584573

EMarketer Reduces US Time Spent Estimates for Facebook and Snapchat. *Emarketer* [online]. Květen 27, 2019 [cit. 2021-03-01]. Dostupné z: https://www.emarketer.com/content/emarketer-reduces-us-time-spent-estimates-for-facebook-and-snapchat

FREY, Petr. *Marketingová komunikace: nové trendy 3.0*. 3., rozš. vyd. Praha: Management Press, 2011, s. 40-46. ISBN 9788072612376.

GOLBECK, Jennifer. *Analyzing the social web*. Waltham: Morgan Kaufmann, 2013, s. 223-235. ISBN 978-0-12-405531-5.

GRIFFITHS, Mark. *Does Internet and Computer "Addiction" Exist? Some Case Study Evidence* [online]. 2000, **3**(2), 211-218 [cit. 2021-04-04]. ISSN 1094-9313. Dostupné z: doi:10.1089/109493100316067

HAVLOVÁ, Jaroslava. Sociální síť. In: *Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* . [online]. Praha: Národní knihovna ČR, 2003 [cit. 2020-12-25]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000015947&local_base=KTD.

HAYNES, Trevor. Dopamine, Smartphones & You: A battle for your time. *Sciente in the news: Department of Neurobiology at Harvard Medical School.* [online]. Březen 1, 2018 [cit. 2021-03-19]. Dostupné z: https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/

Timixi.com: *Historie Youtube* [online]. 2015 [cit. 2020-11-27]. Dostupné z: https://www.timixi.com/cz/timeline/detail/1

INGRAM, David. *Reuters.com: Who is Cambridge Analytica and what did it do?* [online]. March 20, 2018 [cit. 2021-04-06]. Dostupné z: https://www.reuters.com/

It-slovnik.cz: Co je to Lajkovat? [online]. [cit. 2021-02-05]. Dostupné z: https://it-slovnik.cz/pojem/lajkovat

It-slovnik.cz: Instagram Stories [online]. [cit. 2020-11-27]. Dostupné z: https://it-slovnik.cz/pojem/instagram-stories

It-slovnik.cz: Význam slova screenshot [online]. [cit. 2021-03-19]. Dostupné z: https://it-slovnik.cz/pojem/screenshot/?utm_source=cp&utm_medium=link&utm_campaign=cp

Jak na internet.cz [online]. CZ.NIC, 2012 - 2014 [cit. 2021-03-23]. Dostupné z: https://www.jaknainternet.cz/

JONNALAGADDA, Harish. *Androidcentral.com: Whatsapp now requires you share data Facebook* [online]. 7 January 2021 [cit. 2021-03-27].

Kaspersky.com: What is a Black-Hat hacker? [online]. AO Kaspersky Lab [cit. 2021-03-23]. Dostupné z: https://www.kaspersky.com/resource-center/threats/black-hat-hacker

KOPECKÝ, Kamil. Jste rodiče? A jste aktivní v prostředí internetu? Možná i vy provozujete sharenting. *E-bezpeci.cz* [online]. Olomouc: Univerzita Palackého, 2019, **4**(1), 12-19 [cit. 2021-03-19]. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1405-jste-rodice-a-jste-aktivni-v-prostredi-internetu-mozna-i-vy-provozujete-sharenting

KREJČÍ, Mgr. Veronika a Kamil KOPECKÝ. *Rizika virtuální komunikace: (příručka pro učitele a rodiče)* [online]. Olomouc: NET UNIVERSITY, s.r.o, 2010, s. 14-22 [cit. 2021-03-19]. ISBN 978-80-254-7866-0. Dostupné z: https://www.zsmalse.cz/phprs/storage/enebezpeci_a5_3.pdf

LATOO, Nica. *Avast.com: Data Brokers: Everything You Need to Know* [online]. Říjen 29, 2020 [cit. 2021-02-26]. Dostupné z: https://www.avast.com/c-data-brokers

LATTO, Nica. *Avast.com: What Is Browser Fingerprinting and How Can You Prevent It?* [online]. Říjen 22, 2020 [cit. 2021-02-23]. Dostupné z: https://www.avast.com/c-what-is-browser-fingerprinting#topic-3

LinkedIn [online]. [cit. 2020-11-27]. Dostupné z: https://www.linkedin.com/

LÍVIA, Šuľová. *Affial.com: Influenceři a affiliate marketing* [online]. 28.1.2019 [cit. 2021-03-01]. Dostupné z: https://www.affial.com/influenceri-affiliate-marketing/

ManagementMania.com: Jak vytvořit silné, bezpečné heslo. [online]. 17.10.2016 [cit. 2021-03-23]. Dostupné z: https://managementmania.com/cs/heslo

Mcafee.com: Co je brána firewall? [online]. McAfee, 2021 [cit. 2021-03-23]. Dostupné z: https://www.mcafee.com/cs-cz/antivirus/firewall.html

Statista.com: *Most popular social networks worldwide as of November 2020, ranked by number of active users* [online]. [cit. 2020-11-27]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

RASCHKA, Sebastian a Vahid MIRJALILI. *Python machine learning: machine learning and deep learning with Python, scikit-learn, and TensorFlow*. Second edition. Birmingham: Packt, 2017, s. 348. ISBN 978-1-78712-593-3.

SKOUMALOVÁ, Sabina. *Niedermayer.cz: Únik dat na Facebooku – mysleli jste si, že vaše data jsou v bezpečí?* [online]. Praha: Kancelář europoslance Luďka Niedermayera, 10.04.2018 [cit. 2021-03-27]. Dostupné z: https://www.niedermayer.cz/aktuality/articles/unik-dat-na-facebooku-mysleli-jste-si-ze-vase-data-jsou-v-bezpeci

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací: Směrnice o soukromí a elektronických komunikacích. In: . 2002, ročník 2002, číslo 58. Dostupné také z: https://esipa.cz/sbirka/sbsrv.dll/sb?DR=SB&CP=32002L0058

ŠMOTEK, Michal, Jana KOPŘIVOVÁ a Petr ŠÓS. Vliv modrého světla na cirkadiánní systém spánek a kognitivní činnost. *Psychiatrie* [online]. 2016, **20**(1), 29-33 [cit. 2021-04-04]. Dostupné z: http://www.modresvetlo.cz/PDF/Vliv_modr%C3%A9ho_sv%C4%9Btla_na_cirkadi%C3%A1nn%C3%AD_syst%C3%A9m_sp%C3%A1nek_a_kognitivn%C3%AD_%C4%8Dinnost.pdf

ŠPAČEK, Michal. *Michalspacek.cz: Crackování hesel z úniku Mall.cz* [online]. 2. ledna 2018 [cit. 2021-04-06]. Dostupné z: https://www.michalspacek.cz/crackovani-hesel-z-uniku-mall.cz

Twitter.com: Help center: Using Twitter [online]. [cit. 2020-11-27]. Dostupné z: https://help.twitter.com/

Úřad pro ochranu osobních údajů: Statement on Avast case [online]. 11. 2. 2020 [cit. 2021-04-06]. Dostupné z: https://www.uoou.cz/en/vismo/dokumenty2.asp?id_org=200156&id=1896

Úřad pro ochranu osobních údajů: Úřad udělil společnosti Internet Mall, a.s. pokutu 1,5 milionu korun [online]. 3. 10. 2018 [cit. 2021-03-27]. Dostupné z: https://www.uoou.cz/urad-udelil-spolecnosti-internet-mall-a-s-pokutu-1-5-milionu-korun/d-31959

Úřad pro ochranu osobních údajů: Ze školství [online]. [cit. 2021-02-05]. Dostupné z: https://www.uoou.cz/ze-skolstvi/ds-5088/archiv=0&p1=1933

VACEK, Mgr. Jaroslav a Petra VONDRÁČKOVÁ. Behaviorální závislosti: klasifikace, fenomenologie, prevalence a terapie. *Česká a slovenská psychiatrie*. 2014, **110**(3), 144-150. ISSN 1212-0383. Dostupné také z: http://www.cspsychiatr.cz/detail.php?stat=960

WELDON-SIVIY, Denise a Linda MCCARTHY. *Buď pánem svého prostoru: Jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, 2013, s. 165-170. ISBN 978-80-904248-6-9.

Whatsapp.com: o společnosti WhatsApp [online]. 2021 [cit. 2021-03-27]. Dostupné z: https://www.whatsapp.com/

Zákon č. 110/2019 Sb.: Zákon o zpracování osobních údajů. In: Sbírka zákonů, 2019, ročník 2019, číslo 110. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ A DIAGRAMŮ