**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**


**Bakalářská práce**

# Digitální stopa

**Jana Turoňová**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jana Turoňová

Systémové inženýrství a informatika
Informatika

Název práce

**Digitální stopa**

Název anglicky

**Digital Footprint**

---

**Cíle práce**

Hlavní cíl práce je poukázat na problematiku digitální stopy a míru informovanosti o digitální stopě mezi uživateli.
Dílčím cílem je charakterizování jednotlivých typů digitální stopy. Upozornění na využití i zneužití datové stopy a možnosti ochrany dat.

**Metodika**

Teoretická část práce se zabývá digitální stopou a seznámení s danou problematikou, je zpracována dle studia doporučené literatury a jiných odborných informačních zdrojů.

Praktická část bakalářské práce je sestavena pomocí dotazníkového šetření, které bude vytvořeno pomocí internetového a osobního dotazování. Na základě získaných dat, dle předem zvolených kritériích, bude průzkum vyhodnocen a výsledky formulovány v závěrech bakalářské práce.

**Doporučený rozsah práce**

30 – 40 stran

**Klíčová slova**

bezpečnost, digitální stopa, ochrana soukromí, sledování, vymazání dat

---

**Doporučené zdroje informací**

ECKERTOVÁ, L., DOČEKAL, D. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press, 2013, ISBN 978-80- 251-3804-5

J. PERRY, Disappear Without a Trace: How to Erase Your Digital Footprint, 2017, ASIN: B07572H5N8

KOŽÍŠEK, M. – PÍSECKÝ, V. *Bezpečně n@ internetu : průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. První vydání. Praha: Grada Publishing, a.s., 2015, ISBN 978-80-247-5453-6

M. FERTIK, D. C. THOMPSON, The Reputation Economy: How to Optimize Your Digital Footprint in a World Where Your Reputation Is Your Most Valuable Asset, Little, Brown Book Group, 2015, ISBN: 978-03-853-4760-0

Petrowski Thorsten, Sicherheit im Internet für alle, Rottenburg: Kopp, 2013, ISBN 978-38-6445-275-8

---

**Předběžný termín obhajoby**

2020/21 LS – PEF

**Vedoucí práce**

Ing. Mgr. Vladimír Očenášek, Ph.D.

**Garantující pracoviště**

Katedra informačních technologií

Elektronicky schváleno dne 29. 7. 2020

**Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

**Ing. Martin Pelikán, Ph.D.**

Děkan

V Praze dne 26. 02. 2021

**Čestné prohlášení**

Prohlašuji, že svou bakalářskou práci "Digitální stopa" jsem vypracovala samostatně pod vedením vedoucího bakalářské 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 bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 14.03.2021 _____

**Poděkování**

Ráda bych touto cestou poděkovala Ing. Mgr. Vladimíru Očenáškovi, Ph.D. za odborné vedení, přínosné rady a pomoc při zpracování této bakalářské práce.

# Digitální stopa

**Abstrakt**

Bakalářská práce se zaměřuje na problematiku digitální stopy a zjišťuje míru informovanosti o digitální stopě mezi uživateli internetu.

V teoretické části se zabývá vznikem a druhy digitálních stop. Upozorňuje na možná rizika zneužití digitální stopy a na její využití. Charakterizuje pravidla bezpečnosti a možnosti ochrany digitální stopy, pomocí ověřených a dostupných prostředků.

V praktické části poukazuje na problematiku a ochranu digitální stopy, kterou mohou ovlivnit svým chováním uživatelé. Navazuje dotazníkové šetření, ve kterém byli respondenti rozděleni podle pohlaví, věkové kategorie a nejvyššího dosaženého vzdělání. Otázky v dotazníku se zabývají znalostí digitální stopy, zneužití datové stopy, ochrany datové stopy a bezpečného chování. Jednotlivé kategorie dotazovaných jsou vzájemně porovnávány dle znalostí a uvědomování si digitální stopy. Výsledky byly hodnoceny pomocí metody pořadí z hledisek věku, pohlaví a vzdělání. Hodnocení bylo provedeno také v rámci ochrany dat a využití i zneužití datové stopy. Na základě získaných dat, které byly vyhodnoceny, byl zformulován závěr a doporučení.

**Klíčová slova:**

Bezpečnost, Digitální stopa, Ochrana soukromí, Sledování, Vymazání dat

# Digital Footprint

**Abstract**

The bachelor thesis is focusing on problematics of digital footprint, ensures the level of digital footprint awareness among internet users.

The theoretical part discusses origin and types of digital footprint. Highlights possible risks of misusing digital footprints and its use. It characterises rules of safety and possible protection of digital footprint with proven and available resources.

In the practical part it points out on problematics of digital footprint safety that could be influenced by user's behaviour. Its followed up by questionnaire survey where the respondents are divided by their gender, age and highest level of education attained. Questions in the survey are focusing on knowledge of digital footprint, misuse of digital footprint, its protection and safety behaviour. Individual categories of respondents are compared by their knowledge and awareness of digital footprint. Results are evaluated using ranking method in terms of age, gender and education. The next part of evaluation was also carried out as data protection, abuse and misuse of digital footprint. The conclusions and recommendations were made out of results based on data obtained.

**Keywords**:

Security, Digital footprint, Privacy protection, Tracking, Erase data

# Obsah

# Seznam obrázků



# Seznam tabulek

# 1 Úvod

Svět v dnešní době je svázán s digitálním světem, který nám poskytuje nepřeberné množství informací a také možností. Hlavním prostředkem digitálního světa je Internet, na kterém zanecháváme svou digitální stopu a digitální identitu.

Internet je celosvětová struktura, která je propojena pomocí počítačových sítí. Můžeme ho spustit na různých technologických vymoženostech, jako jsou chytré mobily, tablety, laptopy, notebooky, stolní počítače. Zajisté každý z nás určitě máme minimálně jedno takové zařízení, ze zde zmiňovaných.

Ráda bych přešla k části beletrie, kde zajisté náznakem pochopíte, co je to digitální stopa a jak nám může zkomplikovat život v reálném světě.

*„Snadný výdělek.*

*Na internetu jsem se dočetla, že existují stránky, kde si můžete vydělat nějaké peníze. Jsem učitelka, ve školství se moc neplatí a tak by se mi hodila každá koruna. Sháněla jsem proto víc informací, až jsem narazila na jednu cizí stránku, která měla několik tisíc online návštěvníků. Princip je jednoduchý. Pokud máte webkameru, zapnete ji, a když se budete někomu líbit, napíše vám. Může vás sledovat i více lidí. Vy si s nimi můžete psát nebo třeba dělat na webce to, co vám řekne. Ze začátku mi to přišlo divné, že já ty lidi nevidím, ale po čase jsem si zvykla. Protože to byla cizí služba, tak jsem se nebála, že by to viděl někdo od nás. Taky jsem si všimla, že většina těch lidí chtěla, abych se svlékla. Vysloveně mě hecovali, abych si svlékla triko a podprsenku. Váhala jsem, jestli to mám udělat, protože jsem to nikdy nedělala, ale peníze jsem si vydělat chtěla. Přešla jsem proto do placeného režimu a napsala, že jestli chtějí vidět striptýz, musí se dohromady složit na sto dolarů. Ze začátku se nic nedělo, ale najednou jsem je skutečně měla. Spočítala jsem si, že když se takhle ukážu jednou denně, budu mít plat pomalu jak ředitelka ve firmě. Takhle jsem to provozovala docela dlouho, měla jsem dokonce pravidelné návštěvníky a obdivovatele a dostala i nespočet nabídek na sex. To jsem ale vždycky odmítala, protože jsem si chtěla zachovat odstup, a i kdyby ten chlap dal milion, tak by mi to za to nestálo. Taky jsem si všimla, že tak jako já chodí na tu službu stejní lidé, kteří se nabízejí a časem jsem se s nimi i skamarádila. Nebyli jsme si konkurencí, každá nabízela něco jiného. Jedna Ukrajinka mi poradila, že jestli si chci vydělat opravdu veliký balík peněz, mám ukazovat i něco jiného než striptýz. To už prý dneska nefrčí, že mám zkusit třeba hrátky se svým tělem a používat různé pomůcky. Zkusila*

*jsem to a dokonce jsem si udělala takový vlastní rekord – sledovalo mě přes čtyři sta lidí! Penízky se sypaly a já byla spokojená. Ranní vstávání do práce bylo ale těžší, protože většinu brigády jsem provozovala do čtyř do rána. Jednoho dne jsem jako vždy přišla do své třídy, už ve dveřích jsem cítila, že něco není v pořádku, děti se mi různě posmívaly a bylo cítit napětí ve vzduchu. Zasedla jsem za stůl a otevřela třídnici. Málem se mi zastavilo srdce, když jsem v ní objevila svoje nahé fotografie. Vyběhla jsem za šíleného smíchu ze třídy a utekla ze školy. Musela jsem dát výpověď, informace se rozšířila velice rychle a já bych se hanbou propadla. Zajímalo by mě, jak to ti šesťáci objevili!*[1]

V případě paní učitelky se můžeme domnívat, že není možné vypátrat odkud je video nahráváno nebo že není možné, aby někdo viděl náš pohyb na Internetu. Každý uživatel ovšem zanechává za sebou svou digitální stopu a to i v případě když ji odstraníme. Na síti stále zůstává.

# 2 Cíl práce a metodika

## 2.1 Cíl práce

Hlavní cíl práce je poukázat na problematiku digitální stopy a míru informovanosti o digitální stopě mezi uživateli.

Dílčím cílem je charakterizování jednotlivých typů digitální stopy. Upozornění na využití i zneužití datové stopy a možnosti ochrany dat.

## 2.2 Metodika

Teoretická část práce se zabývá digitální stopou a seznámení s danou problematikou, je zpracována dle studia doporučené literatury a jiných odborných informačních zdrojů. Praktická část bakalářské práce je sestavena pomocí dotazníkového šetření, které bude vytvořeno pomocí internetového a osobního dotazování. Na základě získaných dat, dle předem zvolených kritérií, bude průzkum vyhodnocen a výsledky formulovány v závěrech bakalářské práce.

# 3 Teoretická východiska

## 3.1 Digitální stopa

Veškerý pohyb na webové stránce zanechaný uživatelem, se ukládá na Internet. Všechny příspěvky které napíšeme do diskusí pod články, internetové nákupy, i účty které založíme na sociálních sítích jako je Facebook, Instagram, Snapchat a dalších, včetně přístupového bodu na internetu. [2] Všechny tyto informace jsou ukládány bez našeho vědomí a často i bez našeho souhlasu. [3]

Digitální stopa je přehled všech dat zanechaných námi na Internetu. Je velmi jednoduché ji dohledat, ale složitější ji odstranit nebo minimalizovat. Zatímco my postupem času můžeme na některé věci zapomenout, internet si je bude vždy pamatovat. [4]

S neustálým zdokonalováním technologií a objevování nových, které rychle pronikají do veřejného i soukromého života, se množství dostupných informací o nás neustále zvětšuje a s tím i velikost našich digitálních stop. [5]

Z nahromaděných digitálních stop lze sestavit velice podrobnou digitální identitu každého uživatele moderních technologií. Digitální identita je podle definice ekvivalentem naší osobnosti v prostředí internetu. [2]

## 3.2 Typy digitálních stop

Digitální stopu můžeme dělit do několik skupin, nejčastěji se dělí do dvou hlavních skupin, které se nazývají Ovlivnitelná a Neovlivnitelná. [3]

### 3.2.1 Ovlivnitelná

Vzniká s vědomím uživatele, který poskytuje ostatním účastníkům internetu svoje osobní informace. Osobní informace se předávají na různých sociálních sítí například přispěním příspěvku v diskusi, na fóru nebo posíláním medií (fotky, video, audio aj.) atd. Do ovlivnitelné patří i různé registrace a využívání všech služeb jako jsou seznamky, emailové schránky, chaty, blogy, operační systémy a datová úložiště. [3]

Ovlivnitelná část naší digitální stopy nás může ohrozit při povolání anebo především u budoucích pohovorů. Náš budoucí zaměstnavatel si může vyhledávat informace o nás, našem chování a našich názorech. Určitě si nepomůžeme, pokud budeme přidávat výstřední či extremistické politické názory nebo nevhodné fotky. Vedle ověření profilu na sociálních

sítích se může pozornost zaměstnavatele zaměřit i na soulad koníčků a schopností, které uvádíme v životopise. [6] A i když se tato data budeme snažit odstranit (či je odstraní někdo jiný), k jejich reálnému a trvalému odstranění nikdy nedojde. Vždy bude existovat kopie počítačového systému nebo kopie od jiného uživatele i s vašimi daty. [7]

### 3.2.2 Neovlivnitelná

Neovlivnitelná digitální stopa je důsledkem naší aktivity na internetu, tedy vzniká bez našeho úmyslu, při vstupu do sítě až po vyhledávání na internetovém prohlížeči. [3] V případě dostatečně zkušeného uživatele je možnost celou řadu „neovlivnitelných" digitálních stop pozměnit nebo zamaskovat. [7] Už prostý anonymní režim v prohlížeči, který vypne cookies, zamaskuje aktivitu prováděnou na počítači. Cookies jsou textové souborové záznamy o aktivitě a přednastavení prohlížeče. Přesto nemůžeme tvrdit, že zcela všechna data se dají pozměnit či upravit. [5] Pohyb uživatele po internetu se dá sledovat nejrůznějšími způsoby. Zde jsou uvedeny některé příklady neovlivnitelné digitální stopy.

**IP adresa**

Při vstupu do sítě, se posílá naše digitální stopa za pomocí adresy internetového protokolu nebo MAC adresy, které předávají informace poskytovateli internetového připojení. IP adresa není obecně anonymní, neboť počítačový systém ji používá pro komunikaci s dalšími počítačovými systémy. Tedy stejně jako obyčejný poštovní dopis i zde se dozvíme informace, kam a odkud je dopis posílán. V případě IP adresy je tento údaj v číslicích oddělených tečkami. [8]

*„IP adresy jsou přidělovány hierarchicky, přičemž dominantní roli zde má ICANN, který rozdělil reálný svět na regiony, nad nimiž vykonávají správu regionální internetoví registrátoři (RIR – Regional Internet Registry). Tito registrátoři dostali od ICANN přidělen určitý rozsah IP adres, které přidělují LIRům v rámci svého regionu. Regionální registrátoři jsou rozděleni do následujících pěti teritorií:*

*1) „Euro-asijská" oblast – RIPE NCC: https://www.ripe.net/*

*2) „Asijsko pacifická" oblast – APNIC: https://www.apnic.net/*

*3) „Severo-americká" oblast – ARIN: https://www.arin.net/*

*4) „Jiho-americká" oblast – LACNIC: http://www.lacnic.net/*

*5) „Africká" oblast – AFRINIC: http://www.afrinic.net/"* [7]

**Elektronická pošta**

Veškeré verze elektronické pošty, ač by si někdo mohl myslet, rozhodně nejsou anonymní službou. Ve zprávě, kterou odešleme, se skrývají naše osobní informace. [5] Tím není myšlen obsah zprávy, tedy co je v ní napsáno, ale zdrojový kód zprávy. Zde se ukrývají celé řady informací, které mohou poskytovatelé služby tak i poskytovatelé připojení identifikovat. Jako například zjistit cestu přes servery, skutečného odesílatele, zdrojové jméno počítače, název počítače, čas odeslání zprávy (včetně časové zóny) používaný operační systém, mailového klienta a další. [7]

## 3.3 Zneužití digitální stopy

Digitální stopa jako taková se nedá jen tak lehce zneužít. Většinou je zapotřebí, aby uživatel internetu podnikl kroky, které hraničí s morálkou člověka. Na internet nepatří celá řada osobních informací. Jako například sdílení choulostivých fotografií, extrémních názorů nebo svěřování se „internetovým přátelům".

„*V roce 2019 bylo v oblasti kybernetické kriminality a kriminality páchané na internetu evidováno 8 417 trestných činů. Významné zastoupení má stále také mravnostní kriminalita, kde znepokojivě roste počet pachatelů do 18 let věku v poměru ke zletilým pachatelům.*" [9]

*„Internet jako takový je bezpečný, nebezpeční jsou na něm jen lidé."* [1]

### 3.3.1 Sexting

Jedna z nejnebezpečnějších forem digitální stopy. Tento pojem tvoří spojení dvou slov a to „sex" a „texting". Sextingem se tedy rozumí zasílání či sdílení vlastních nebo cizích textových zpráv, fotografií nebo videí s erotickým a sexuálním obsahem. [7]

Mladí lidé dost často experimentují někdy až za hranicemi rozumného myšlení a právě tehdy můžou být následky tohoto jednání fatální. Často se sexting spojuje i s vydíráním, kterému oběti snadno podlehnou kvůli studu a možnému zesměšnění. [1]

Není to tak dávno, kdy se řešil případ „roztahovačky" v České republice. Jednalo se o facebookové stránky, na kterých byly zveřejňovány fotografie odhalených děvčat s „kousavým" komentářem. Fotky byly většinou bohužel staženy přímo z jejich profilu, který neměli dostatečně zabezpečený. Stránka měla pravděpodobně upozornit na povolná děvčata, zároveň tím ale upozornila i na bezpečnostní stránku celé věci.

Sexting pouze mezi dospělými není trestný čin, avšak riskuje se tím, že může dojít ke zneužití těchto dat. Pro minimalizaci rizika je důležité dodržovat určitá opatření.

- Nikdy nevytvářet fotky ani videa se svým obličejem.
- Za sebou mít vždy jednolité pozadí.
- Zakrýt tetování či jiné specifické prvky těla.
- Video vytvářet bez zvuků. [1] [7]

### 3.3.2 Kyberšikana

Kyberšikana vznikla přenesením šikany v reálném světě do světa internetových technologií. Šikana je tedy pojem, který označuje opakované psychické i fyzické týrání slabšího jedince v kolektivu nebo společnosti. Dochází k ní ve všech věkových skupinách.

Zatím co šikana probíhá v uzavřeném okruhu lidí, kyberšikana probíhá po celé síti, a má velmi často daleko težší následky pro oběti.

Útočník má velmi často utkvělou představu, že se schová pod anonimitou sítě a dostává tak falešný pocit bezpečí. K odhalení útočníka v dnešní době stačí, ale velmi málo. K odhalení především přispěje včasné nahlášení a dostatek důkazů, které lze získat pomocí digitální stopy.

Klasická šikana se skládá z několika jednotlivých útoků, které se opakují, ale vždy následuje konečný útok při včasném řešení, kterým to pro oběť končí. Bohužel u kyberšiny jsou oběti stále připomínány zážitky, které visí na síti. Oběť tak může žít v traumatu několik měsíců i let.[1] Ačkoliv se budeme snažit smazat stopy o těchto aktivitách, nikdy je nesmažeme úplně.

Častým prostředkem kyberšikany je zveřejnění natočeného fyzického nebo sexuálního útoku nic netušící oběti označovaného jako Happy slapping. Největší rozmach Happy slappingu je právě ve Velké Británii, kde do zvlaštní kategorie patří napadání bezdomovců velmi brutálním způsobem. Záběry slouží k zasvěcovacímu rituálu pro přijetí do různých skupin a gangů. [10]

Jeden z nejtragičtějších příběhů kyberšikany spojený s násilím se odehrál v Evropě v roce 2006 v Polsku. Obětí se stala teprve 14-ti letá studentka gymnázia, Anna.

„*Během vyučování, kdy musela učitelka na odvolání ředitele opustit na 20 minut třídu, Annu napadli a sexuálně obtěžovali 4 spolužáci. Strhali z ní šaty, osahávali ji a předstírali, že ji znásilňují. Jeden z nich ji chytil za hlavou a předstíral, že provádí orální sex. Další student, vše natáčel na svůj mobilní telefon. Útočníci Anně vyhrožovali, že pořízený záznam*

*umístí na internet, aby si ho mohli všichni prohlédnout, což také později udělali. Anně se nakonec podařilo vyprostit a utekla domů. O šikaně doma nikomu neřekla. Téhož dne večer sdělila kamarádce, která ji přišla navštívit, že už nevydrží to školní ponižování, že se chce zabít. Kamarádka při odchodu řekla Anninì matce, aby na ni dávala pozor. Další den Anna spáchala sebevraždu. Oběsila se na švihadle. Policejní vyšetřování ve škole odhalilo, že nešlo zdaleka o první útok, kterému byla Anna vystavena. Stejní útočníci ji napadali opakovaně několik týdnů od doby, kdy s jedním z chlapců odmítla chodit.*“ [11]

### 3.3.3 Kybergrooming

Kybergrooming je jednání, při kterém se útočník snaží vyvolat pocit důvěry a bezpečí ve své oběti za pomoci internetu či informačních a komunikačních technologií a přimět ji tak ke schůzce. [1]

Jako dopad této schůzky může být fyzické násilí, sexuální zneužití oběti, zneužití oběti pro prostituci nebo k výrobě pornografie apod. [7]

Útočník obvykle manipuluje se svou obětí velmi dloho v rámci měsíců až někdy několik let. Doba manipulace závisí na důvěřivosti oběti a útočníkovy vytrvalosti. Stávají se i případy, kdy agresor manipuluje dítě po dobu 2–3 let, než se setkají tváří v tvář a dojde k sexuálnímu zneužití.

Mezi nejčastější oběti patří :

a) děti s nízkým sebevědomím či nedostatkem sebedůvěry (lze je snadněji citově či fyzicky separovat od ostatních)
b) děti s psychickými problémy, oběti většinou nacházející se v těžké situaci
c) děti prostomyslné a přehnaně důvěřivé (jsou povolnější v on-line konverzaci a nerozpoznávají nebezpečí)
d) adolescenti/teenageři (velmi je zajímá sexuální život, jsou ochotni a někdy i sami chtějí o ní hovořit) [12]

Obětí kybergroomingu se může stát prakticky kdokoliv, i dospělý. Podle průzkumu se ale z pravidla jedná o dívky ve věku mezi 11 a 17 roky, tehdy právě vzrůstá zájem o neznámé a neprozkoumané oblasti života.

Některé vyobrazené příběhy kybergroomingu pomocí animace lze najít i na pornografických stránkách. Například příběh pod označením „Sweet Pink“. Jedná se o velmi mladou slečnu, která se až příliš objevuje na sociálních sítí. Jednoho dne ji osloví neznámý starší muž, vydávající se za velmi atraktivního mladíka. Slečna se zamiluje a muž získává

její důvěru. Na jeho žádost mu postupem času posílá i velmi intimní fotky. Nakonec příběhu se schází před jedním z bytů, kam ji zatáhne a znásilní.

### 3.3.4 Kyberstalking

Kyberstalking je dlouhodobé pronásledování, omezování a obtěžování za pomocí moderních technologií.

„*Původně bylo slovo stalking používáno lovci divoké zvěře a znamenalo stopování zvěře až k jejímu uštvání.* „[7]

Stalker neboli slídil [10] se snaží poškodit pověst oběti, očernit ji šířením nepravdivých informací nebo se snaží, jakkoliv ublížit. [1] Obětí se může stát kdokoli, bez vlastního zavinění.

Příklady Kyberstalkingu

- velmi časté posílání SMS zpráv nebo MMS obrázků
- telefonáty a prozvánění
- zasílání zpráv prostřednictvím sociálních sítí
- opakované komentování příspěvků oběti na sociálních sítích
- Napodobování oběti či vydávání se za ni **(**krádež identity)
- kontaktování oběti pod falešnou identitou (několika falešnými identitami)
- monitorování počítače oběti speciálními programy
- zveřejňování informací ze života oběti
- obtěžující kontaktování přátel oběti aj. [13]

Obtěžování se obvykle stupňuje a vyvolává u oběti strach o svoje soukromí, zdraví a také život. Nebezpečné pronásledování neboli stalking (kyberstalking) je velmi vážný zločin. Tento termín byl přidán do trestního zákoníku v roce 2010, pokud se tohoto zločinu někdo dopustí, hrozí mu až několikaleté vězení. Pokud se Kyberstalking neřeší včas, vede to až k dalším trestným činům, které můžou zahrnovat výrazné omezování osobních práv oběti nebo zneužití chování oběti k provedení krádeže, podvodu, vydírání a podobně. [5]

„*Aby mohla policie pachatele obvinit ze stalkingu, musí být dodrženy zejména tři podmínky:*

*1. Musí být jednoznačné, že pronásledovatel tak činí proti vůli oběti.*

*2. Pronásledování musí být intenzivní.*

*3. Pronásledování musí být dlouhodobé (min. 4-6 týdnů).“* [13]

### 3.3.5 Sledování návyků uživatelů

Sledování uživatelských návyků může probíhat dvěma způsoby přímo navštívenou stránkou anebo stránkami třetích stran, většinou v podobě sběratelů dat a reklamními společnostmi. Právě stránky třetích stran, které získávají o uživateli informace, mají z těchto informací největší výnos. Snaží se o neustálé zlepšení reklamního sdělení, reklamu cílenou, pomocí analyzování uživatelova chování na webu. [14]

Ohrožení soukromí může nastat, pokud je nahromaděno velké množství dat. Mohla by být odhalena uživatelova identita, geografická lokace, odhadovaný věk, rodinný stav či vlastnictví nemovitostí. Přestože jsou stále vymýšleny nejrafinovanější způsoby, jak skrytě zaznamenávat pohyb uživatele, stále se nejvíce používá datových souborů cookies a web beacons. [14] [15]

#### 3.3.5.1 **Cookies**

Cookies je malý datový soubor, který pomáhá uživatelům navázat v předešlé aktivitě na dané webové stránce. Zároveň si i pamatuje po nějakou dobu preference, které uživatel nastavil, například uživatelské jméno, preferovaný jazyk atd. Soubory cookies můžou uchovávat údaje o návštěvnosti a chování jednotlivých uživatelů. [15] [16]

Existuje několik typů souborů cookies:

1) Analytické soubory cookies

   Monitorují uživatele, jakým způsobem využívá webové stránky, o typu webové stránky, ze které byl uživatel přesměrován nebo kolikrát navštívil danou webovou stránku nebo aplikaci. Tyto informace slouží pro shromažďování statistik webové stránky.

2) Provozní cookies – nezbytné pro provoz stránek

   a. Technické cookies

      Slouží pro přenos komunikace prostřednictvím elektronické komunikační sítě.

   b. Autentizační cookies

      Personalizace neboli rozpoznání uživatele po ověření a přihlášení na daném webu dobu relace. [16] [17]

3) Trackingové cookies

   Tzv. sledovací, sledují pohyb uživatele na webu a jejich chování. V kombinaci s některými cookies mohou zaručit, že uživatel se stane zákazníkem webových stránek.

4) Cookies třetích stran

   Cookies jsou uloženy pomocí skriptu, který načítají domény jiných poskytovatelů služeb a je tak možné sledovat uživatele napříč různými doménami.

5) Trvalé cookies

   Tyto cookie jsou uloženy v počítači a po zavření prohlížeče nejsou smazány automaticky. Mohou být kdykoliv znovu přečteny.

Pro používání a ukládání cookies je vždy nezbytný souhlas uživatele. Většina prohlížečů může přijímat cookies automatiky ve výchozím nastavení. V nastavení prohlížeče je možné cookie odmítnou anebo nastavit užívání jen některých. [16] [17]

#### 3.3.5.2 **Web Beacons**

Též známé jako pixelové značky nebo pixelové tagy. Jedná se o malé skryté, průhledné, grafické obrázky s názvem GIF, avšak má podobu jakéhokoliv jiného obrázku. Mají podobnou funkci jako cookies. Oproti cookies jsou pevnými součástmi webových stránek. Sledují uživatelovo chování, když obdrží e-mail nebo navštíví konkrétní web a posílají tyto informace dál. [8] [18]

*„Někteří lidé jej mohou nazývat „spyware“ v tom smyslu, že se používá k zaznamenávání vašich online aktivit“* [8]

Web Beacons se často používá k rozesílání spamu nic netušícím uživatelům. Pokud tento spam uživatel otevře vyšle tím signál, že je připraven na další posílání spamu nebo nějakou jinou aktivitu. [18] [19]

### 3.3.6 Phishing a Pharming

V češtině se z angličtiny překládá phishing jako „rybaření“ a pharming jako „farmaření“. Podle jedné z mnoha teorií je slovo phishing zkratka pro souvětí „Password harvesting fishing“ – tedy doslovně přeloženo „sběr hesel rybařením“. [7]

„*Základní myšlenka původního phishingu je následující: Dostanete zprávu pocházející zdánlivě od vaší banky, z oblíbené sociální sítě nebo třeba internetového obchodu. Pod nejrůznějšími záminkami se z vás snaží vytáhnout přihlašovací údaje, hesla, PINy ke kartám a podobně.*“ [8]

„*Pharming je pokročilejší variantou phipingu, jde o útok, kdy je správná IP adresa změněna na IP adresu webu škůdce, napadený potom komunikuje s útočníkem v domnění, že se jedná o správnou instituci*.“ [20]

V roce 2016 byl zaznamenán případ malware Nemucod, který se šířil prostřednictvím infikovaných příloh e-mailových zpráv, které vypadaly opravdu realisticky. Většina e-mailových zpráv byly označeny jako výzva k zaplacení faktury nebo jako pozvání k soudu. Pokud uživatel otevřel infikovanou přílohu, tak se do počítače nainstaloval Nemucod, který umožňoval útočníkovi na infikovaný počítače posílat další škodlivý kód. V případě Nemucodu šlo o ransomware. Došlo tedy k zašifrování dat na počítači a požadavku na výkupné.

3 zásady ochrany:

1. Neposkytujte citlivé údaje – Pokud vás stránka znovu vyzve například k přihlášení na stránky, kde víte, že jste přihlášeni nebo se vás stránka ptá na osobní údaje, určitě tyto údaje neposkytujte.
2. Zkuste nejprve popřemýšlet – Zda není e-mail nebo webová stránka jen pokus o podvod, zda nemá některý ze základních symbolů phishingu.
3. Bezpečnostní antivirus – je základem pro jakýkoliv počítač. Kvalitní antivirus se dokáže vypořádat i s velkým množstvím phishingu. [21]

### 3.3.7 Spyware

Jedná se o velmi škodlivý software, spyware, který bez vědomí uživatele počítače, provádí špionáž. Tedy nějakým způsobem odposlouchává či zjišťuje data. [8]

Mezi symptomy spywaru může patřit pomalý start počítače, dlouhé načítání webových stránek, při prohlížení stránek na internetu vyskakují ve zvýšené frekvenci reklamy, změna domovské stránky, která byla náhodně provedena, časté pády, chyby systému a záhadné objevování nových ikon na ploše.

Spyware může odesílat:

1. Údaje o kreditních kartách
2. Přístupové údaje a hesla
3. Osobní informace, podrobnosti o smlouvách
4. Sériová a registrační čísla softwaru
5. Historie prohlížení stránek
6. IP adresa uživatele

Druhy spyware:

1. Adware - při brouzdání na internetu vidíme víc reklam
2. Browser helper object - umožňuje programátorům změnit a sledovat prohlížeč
3. Hijacker - mění domovskou stránku
4. Dialers - přesměrovává telefonní linku na drahé telefonní tarify
5. Keyloggers - zaznamenává každý stisk klávesy na klávesnici, odesílá uživatelská jména a hesla
6. Remote Administration - umožní vzdálenému uživateli ovládat PC [21]

### 3.3.8 Trojský kůň

Tento název pochází z historie od starověké Troje. Řečtí bojovníci darovali Troje dřevěného koně jako znak neporazitelnosti, ovšem v něm se ukrývali řečtí bojovníci a lstí dobyli starověkou Troju. [8]

Trojský kůň neboli „trojan“ [10] v dnešní digitální době uplatňuje stejný princip. Nejčastěji se schovává v programech, které si můžeme stáhnout zdarma nebo v programech ukradených, které se šíří internetem a jsou zdánlivě zdarma. Trojský kůň je sám o sobě program, který si stahujeme, nejčastěji jako součást užitečného programu.

Pokud se jedná o programy volně dostupné, můžeme jejich spolehlivost zjistit pomocí odborných časopisů, jakou jsou CHIP nebo c´t, a tak chránit své zařízení. Testování volně dostupných programů probíhá ve specializovaných laboratoří a odborníci rychle odhalí programy, které dělají nevyžádané operace. [8]

V případě programů ukradených a obohacených o trojského koně jsou nabízeny zdarma, což je pro mnohé uživatele internetu lákavé. Ovšem měli bychom brát na zřetel, že hackeři se nejen vykašlou na autorská práva, ale také si okopírují vaše soubory v počítači. Proti tomuto napadení se není možné bránit, a tak je potřeba se tomuto softwaru vyhnout. [8]

## 3.4 Využití digitální stopy

### 3.4.1 Behaviorální marketing

Behaviorální marketing označuje analyzování chování uživatele a následně pomocí statistik firmy či e-shopy upraví obsah svých stránek vzhledem k návštěvnosti jednotlivých skupin zákazníků. Z pravidla k sledování uživatelů využívají, již zmíněné, Analytické soubory cookies, pomocí kterých i využívají cílené reklamy. [14] [22]

### 3.4.2 Digitální stopy v personalistice

Uživatelé internetu dávají o sobě mnoho informací na internet. Sdílejí například své záliby, zkušenosti, názory a fotky z volnočasových aktivit. Z těchto informací tvoří personalisté profil uchazeče ještě dřív, než dojde k prvnímu setkání. Tyto informace následně i porovná s životopisem uchazeče. Díky těmto všem dostupným informacím mu personalista udělí hodnocení, „skóre“, které může rozhodnout, zda bude přijat do zaměstnání. [23]

Toto hodnocení na základě informací budou používat i všichni ostatní k zásadním rozhodnutím o uživatelově životě. Například ho použijí k tomu, jestli bude pojištěn nebo dokonce zda s ním někdo půjde na rande či se s ním bude někdo kamarádit. Proto je vhodné dbát na ochranu digitální stopy a chovat se podle pravidel etikety v prostředí internetu, která je dále popsána v kapitole 3.5. [23]

### 3.4.3 Forenzní vědy

Forenzní vědy zkoumají digitální stopu, pokud se uživatel dopustí protiprávního jednání, anebo je svědkem či objetí trestního činu. Digitální stopu lze poté využít jako důkaz, avšak musí splňovat určité náležitosti. Musí být například nepodjatá, přezkoumatelná, a musí mít detailní dokumentaci. [7][24]

## 3.5 Bezpečné chování na Internetu

Pro používání internetu existují pravidla tzv. „netiketa“ [20] tedy etiketa na síti. Net etiketa je soubor pravidel chování, podle kterých bychom se měli řídit.

**Pravidla netikety**

1. **Slušné chování** – Vyhýbejte se vulgarismům, nešiřte nenávist, nezveřejňujte choulostivé informace o sobě či ostatních aneb jak praví přísloví „Chovej se

k ostatním přesně tak, jak chceš, aby se oni chovali k tobě.“ Pokud vás něco v konverzaci rozčílí, rozdýchejte to, a odepište až za nějakou dobu.

2. **Gramatika a diakritika** – Snažte se psát bez chyb a s diakritikou, abyste předešli případným nedorozuměním. Pokud naleznete chybu v textu, nevysmívejte se, neupozorňujte na chyby, ani nikoho neurážejte.
3. **Vědomosti** – Nezneužívejte své vědomosti. Toto pravidlo se především týká tvůrců webových či sociálních sítí, kteří mohou mít přístup k velkému množství informací. Neboj se nabídnout pomoc a odpovědi lidem, kteří o ně žádají.
4. **Identita** – Zjistěte si, s kým mluvíte a chraňte si své soukromí. Lidi po celém světě se mohou připojit k internetu a každá země má jiné zákony a morální pravidla. Nevydávejte se za někoho jiného. Vydávat se za někoho jiného je velmi vážný trestný čin.
5. **Respektujte** – Respektujte soukromí jiných. Pokud vám přijde nějaká zpráva omylem, informujte o tom odesílatele a zároveň dodržujte diskrétnost. Respektuj čas jiných lidí. Neptej se na hloupé otázky, u nichž si můžete najít odpověď sami, nesnažte se naštvat lidi v diskuzi nebo skupinách. Respektuj názory jiných lidí.
6. **Nevyužívejte** – Nevyužívejte ani si nekopírujte software, za který jste nezaplatili, pokud se nejedná o volně šiřitelný software. Nevyužívejte zdroje ostatních uživatelů bez jejich svolení. Nevyužívejte počítače ke krádežím.
7. **Neposílejte** – Neposílejte spam, reklamu, hoaxy (klamavé zprávy), řetězové e-maily atd. Nerozesílejte lži a polopravdy. Nikdy neposílejte zprávy, které byste nebyli schopni vyslovit někomu do očí.
8. **Neporušujte** – Neporušujte autorská práva.
9. **Nedůvěřujte** – Nedůvěřujte lidem, které neznáte. Může se jednat o podvodníky, kteří se snaží z vás dostat citlivé údaje, anebo šprýmaře, kteří si z vás chtějí udělat legraci. Vždy trvejte na ověření osobnosti, fotografií s aktuálním datumem.
10. **Nekomunikujte** – Nekomunikujte s nikým po internetu při řízení, ve frontě u pokladny, během hodin ve škole, v kostele, při jednání s klienty, v restauraci, nebo když jsme s rodinou. [20] [25] [26]

## 3.6 Ochrana digitální stopy

Svoji digitální stopu bychom si měli chránit, protože nikdy nemůžeme s jistotou říct, že nikdo by nechtěl naše informace zneužít k vlastnímu zisku nebo pro svoje potěšení. Chránit naši digitální stopu můžeme hned několika způsoby.

### 3.6.1 Antivirové programy

Antivirový program je naprosto nezbytným základem pro bezpečnost dat a osobního počítače. Samozřejmě je důležité si vybrat ten správný antivirový program. Ne všechny antivirové programy jsou schopny před všemi viry ochránit. Více antivirů zároveň neznamená větší bezpečí, naopak to může způsobit problémy. Antivirové programy se můžou například přetahovat o kontrolu jednotlivých souborů. Je tedy důležité vybrat si jeden a ten používat. [7] [20]

### 3.6.2 Rodičovská kontrola

V angličtině Parental Control, jedná se o aplikaci v mobilním zařízení nebo program pro počítačová zařízení, který sleduje aktivitu dítěte, smíme nastavit limit doby strávené před počítačem nebo limit u her v telefonu, a může i blokovat obsah nevhodných stránek.

Ve většině programů nebo aplikací stačí zadat datum narození dítěte a sám se vyfiltruje obsah, kategorie webu, které jsou nevhodné tudíž budou blokované. Kategorie je možné upravit anebo nastavit blokování konkrétních adres.

### 3.6.3 Firewall

Jedná se o programové vybavení, které slouží jako ověření bezpečné komunikace mezi sítěmi. Brání před neoprávněnými průniky do sítě a zakazuje komunikaci, která není nezbytně nutná. [20]

Operační systém Windows má v sobě již Firewall zabudovaný. Najdeme ho v Ovládacích panelech v sekci Systém a zabezpečení a dále v podsekci Brána Windows Firewall. Můžeme používat i Firewall externí, který je součástí většiny antivirových programů. Opět, ale nesmíme zapomenout, že Firewall by měl být aktivní pouze jeden. [8] [20]

### 3.6.4 AntiTraking

Tracking Web je schopnost webu vědět, co jejich návštěvníci na svém webu dělají. To se provádí pomocí chybových hlášení nebo souborů cookies, které sledují každé kliknutí na webové stránce, a tyto informace hlásí webmasterům. Děje se to za předpokladu, že chcete vylepšit své prohlížení, ale ve skutečnosti to jsou způsoby, jak získat o vás co nejvíce informací, aby si mohli vytvořit váš profil. Na webu Panopticlick si můžete ověřit, které informace jste zanechali po sobě na internetu. Anonymitu na internetu si v žádném případě nezajistíte spuštěním prohlížeče v tzv. anonymním režimu. [8] [20] [27]

Informace, které tito sledovatelé mohou získat, zahrnují následující:

- Webové stránky, které jste navštívili
- Jak dlouho jste strávili na této webové stránce
- Vaše IP adresa (včetně vaší polohy)
- Historie prohlížení
- Položky, které jste vložili do nákupního košíku v internetovém obchodě [8]

Na druhou stranu, tyto kousky informací mohou být použity k tomu, aby vám ublížily. Pokud se tyto informace dostanou do nesprávných rukou, budete mít problém. To je důvod, proč se lidé na celém světě zajímají a používají AntiTrakingové programy a AntiTrakingové nástroje v prohlížeči.

Původně byly AntiTrakingové programy navrženy jako zcela bezplatné. Ovšem postupem času začaly být nabízeny za peníze. Například Avast AntiTrack Premium nebo AVG AntiTrack je nabízen k datumu 26.7.2020 za 1 180 Kč. V pozadí zůstávají i verze, které jsou zdarma, ovšem nejsou tak uživatelky přívětivé. Jedním z nich je Anti Tracks Free Edition, zde máme podporu češtiny pro verzi 9.0.1.107, jedná se, ale již o starší program, a tak o fungování programu v operačních systémech Windows 8 a vyšší, již můžeme jenom spekulovat. [7] [8] [19]

AntiTrakingové nástroje v prohlížečích jsou bezplatné, ale najdeme i placené verze. Bohužel velmi často chybí podpora českého jazyka. Například nástroj GHOSTERY nabízí obě verze, placenou i zdarma. Jako další příklad lze uvést uBlock Origin, který je též velmi rozšířený a zdarma.

Pokud si nejste jisti funkčností AntiTrakingového nástroje a chcete jistotu, zvolte raději AntiTrakingový prohlížeč – Tor, DuckDuckGo a další. V podstatě tyto prohlížeče umožňují

svým uživatelům zakrýt svoje identity online pomocí šifrování, aby byla jejich poloha neviditelná. Také izolují každý navštívený web, aby vás nemohly sledovat reklamy a sledovače třetích stran. [8] [28]

### 3.6.5 Bezpečnost hesel

K naší digitální stopě i digitální identitě se nejlépe lze dostat přes naše heslo, které ve většině případech nemáme dostatečně silné a chráněné. Mezi nejoblíbenější a nejčastější hesla patří například jména domácích mazlíčků, koníčky, rodné příjmení matky, vlastní narozeniny, jméno partnera, vlastní jméno, oblíbená barva, hudební kapela, fotbalový klub. Bohužel čím více máme elektronických služeb, tím více hesel si musíme zapamatovat, a to nás vede k pokušení vše si zjednodušovat.

Používání silných hesel je nezbytné pro ochranu naší bezpečnosti a identity. Hesla jsou stejně důležitá jako jiné nástroje, které používáme k ověření naší identity – jako jsou řidičské průkazy, karty sociálního zabezpečení a cestovní pasy.

Níže je uvedeno několik klíčových tipů, jak zjednodušit zabezpečení heslem, ale přesto uchovat jeho bezpečnost.

Nejsilnější hesla jsou dlouhá nejméně 12–15 znaků a obsahují malá a velká písmena, čísla a symboly. Můžeme si to udržet v paměti jednoduchým vytvořením krátké věty jako mnemotechnickou pomůcku, kterou si snadno zapamatujeme. Pro větší sílu hesla, nebo pokud to web vyžaduje, můžeme přidat specifické symbolu. [7] [8]

Pro účty, které obsahují citlivé nebo osobní identifikační údaje, použijme různá hesla. Právě tím zvýšíme bezpečnost našich dat. Pokud v těchto účtech použijeme stejné heslo, jakmile dojde k jeho prolomení, zranitelné budou všechny účty. Stejně jako používáme různé klíče k ochraně různých míst (poštovní schránka, domovní dveře, vrátka u zahrady, …), použijme různá hesla k ochraně důležitých účtů (e-mail, Facebook, Twitter, Skype, …). Většina z nás se vyhýbá použití různých hesel pro různé účty, protože je příliš těžké si je všechny pamatovat.

Nedopusťme, aby si prohlížeče pamatovaly vaše hesla. I když tato funkce v mnoha prohlížečích může usnadnit přístup k účtům, může to usnadnit také přístup někomu, kdo používá stejný počítač nebo zařízení, aniž by musel znát heslo. Naštěstí mohou pomoci správci hesel – nástroje, které ukládají a chrání hesla. Tyto nástroje mohou také vytvářet hesla, která jsou neuvěřitelně těžká. Všechna hesla, která jsme vytvořili sami, nebo to udělal správce hesel za vás, jsou uložena v šifrované úschovně, které lze otevřít pouze pomocí

hlavního hesla. Hlavní heslo by mělo být nejdelším a nejunikátnějším heslem, jaké jsme kdy vytvořili, a nemělo by být uloženo správcem hesel.

Použijme dvoufázové nebo vícefaktorové ověření. Funguje to takto: Po zadání hesla společnost okamžitě pošle krátký kód na něco, co máte: e-mailový účet, textovou zprávu nebo hlasové volání do telefonu nebo do aplikace, kterou jsme nainstalovali do svého zařízení. Poté zadáme tento kód na webu a máme přístup ke svému účtu. Některé nové technologie začínají používat novou autentizaci – skenování sítnice, skenování otisku prstu, skenování rozpoznávání obličeje atd.

Svá hesla nemusíme měnit tak často, jak si myslíme, stačí když si vytvoříme pořádné dlouhé a bezpečné heslo. Pak stačí změnit heslo jednou za půl roku. Uživatele internetu to aspoň odradí od jednoduché změny, jako je zvyšování čísla na konci hesla. [7] [8] [29]

### 3.6.6 Smazání digitální stopy

I když bychom si velmi přáli některé informace o sobě smazat, musím vás zklamat, nejde to. Bohužel se nikdy nemůžeme úplně odstranit z internetu, ale existují způsoby, jak minimalizovat naši online stopu. Což by mělo snížilo šanci, že se naše data vůbec dostanou na internet. [8]

*„Odstraňte se z webu a mějte nulovou digitální přítomnost“* [30]

Odstraňte nebo deaktivujte své účty v oblasti nakupování, sociálních sítí a webových služeb. Může se ale stát, že přes snahu data smazat, budou stále na internetu dohledatelná. V tomto případě je doporučeno kontaktovat webmastera stránky a požádat ho zdvořile o smazání dat. [2]

## 3.7 GDPR

Zkratka GDPR znamená v angličtině General Data Protection Regulation přeloženo Obecné nařízení na ochranu osobních údajů. Jedná se o soubor pravidel na ochranu dat jak v Evropské unii, tak i mimo ni. Osobními údaji se rozumí například jméno, příjmení, datum narození, adresa IP nebo údaje o zdravotním stavu. [31]

Osobní údaje je povoleno zpracovávat, pokud dotyčný dá souhlas se zpracováním údajů, nebo jsou údaje potřeba například z důvodu smluvní povinnosti, z důvodu právní povinnosti atd. Pokud se konkrétní osoba domnívá, že jeho údaje nejsou platné nebo správné má právo na opravu nebo jejich doplnění.

Pokud dojde k porušení zabezpečení údajů, kdy jsou osobní údaje zveřejňovány bez souhlasu nebo došlo k jejich pozměnění bez souhlasu, je nutné to nahlásit úřadu pro ochranu údajů do 72 hodin od objevení. [31]

### 3.7.1 Soubory cookies

Podle GDPR se ID cookies považují za osobní údaje. ID cookie je označení pro součást většiny souborů cookie při nastavení v prohlížeči uživatele.

*„GDPR vyžaduje, aby web shromažďoval osobní údaje od uživatelů pouze po výslovném souhlasu se zvláštními účely jeho použití.“* [32]

Souhlas se soubory cookies je nejčastěji udělován pomocí bannerů souborů cookies. Souhlas se soubory cookies musí být svobodný. To znamená, že by jednotlivec měl být schopen i svůj souhlas jednoduše odvolat. Mnoho webů obsahuje „centrum ochrany osobních údajů“ nebo ovládací panel, kde mohou uživatelé povolit, odmítnout a odvolat souhlas s různými typy souborů cookie. Souhlas musí být aspoň jednou do roka obnoven a bezpečně uchováván jako legální dokumentace. [32] [33]

### 3.7.2 Právo být zapomenut

„*Při používání informačních a komunikačních technologií a stále většímu objemu dat zveřejňovaných samotnými uživateli nutně došlo ke vzniku žádostí o potlačení či smazání dat, která nejsou aktuální, či která nějakým způsobem poškozují uživatele samotného. Pro tuto činnost se užívá pojem právo být zapomenut.“* [7]

První případ se stal v roce 2010, kdy Mario Costeja González podal stížnost proti společnosti La Vanguardia Ediciones SL. Po zadání jména M. Costeja Gonzáleze do internetového vyhledávače Google se objevuje odkaz na dvě strany deníku La Vanguardia, na kterých je oznámení uvádějící jméno M. Costeja Gonzáleze v souvislosti s dražbou nemovitostí zabavených v důsledku dluhů na sociálním zabezpečení.

M. Costeja González se domáhal, aby společnosti La Vanguardia bylo uloženo odstranění nebo změna uvedených stránek tak, aby se na nich neobjevovaly jeho osobní údaje. Stížnosti nebylo vyhověno, protože ke zveřejnění došlo na základě nařízení ministerstva práce a sociálních věcí. A také usiloval o to, aby společnosti Google Spain nebo společnosti Google Inc. dostala povinnost odstranit nebo utajit jeho osobní údaje tak, aby se již neobjevovaly ve výsledcích vyhledávání a přestaly být spojovány s odkazy na La

Vanguardia. Tomu bylo vyhověno. Provozovatelé vyhledávačů provádějí zpracování údajů, za které také odpovídají, a tak podléhají ochraně právní úpravy v oblasti ochrany údajů. [34] [7]

„*Google se přece jen musel adaptovat na GDPR, ale samotné důvody pro odstranění se naopak zpřísnily. Pro uložení povinnosti zlikvidovat osobní údaje, musí být splněna alespoň jedna z těchto podmínek:*

- *únik explicitních fotek,*
- *falešná nebo nedobrovolná pornografie,*
- *obsah, za jehož odstranění musíte zaplatit*
- *finanční informace nebo zveřejnění dokladu totožnosti,*
- *obsah, který pro vás představuje hrozbu ublížení na zdraví nebo obtěžování a zastrašování*
- *obsah je stále indexován v prohlížeči, ale na daných stránkách už byl smazán.* “ [35]

# 4 Vlastní práce

## 4.1 Problematika digitální stopy

Digitální stopa je v dnešním internetovém světě velmi důležitá, protože právě ona podává o uživatelích mnoho informací, které můžeme nalézt v podobě nevědomé i vědomé datové stopy.

V minulosti nebyl internet natolik rozšířen a svázán s běžným životem. Dnes je používání internetu téměř nutností, využívají a používají ho všechny věkové kategorie, již od malých dětí až po seniory.

Digitální stopa nevědomá vzniká již při prvním připojení uživatele k internetu. Vědomá stopa vzniká již s prvním slovem, které začnou uživatelé vyhledávat v prostředí prohlížeče.

Největším problémem je především neznalost vědomé části digitální stopy, s kterou zacházíme často neopatrně. Vkládáním fotografií, sdílení názorů a poskytování informací pomocí sociálních sítí. Při zjištění naší neopatrnosti se snažíme naši vědomou stopu smazat a zapomenout na ni, ovšem internet nikdy nezapomíná. Smazaná digitální stopa se dá kdykoliv obnovit.

Jak ale s naší digitální stopou zacházet? Můžeme minimalizovat vědomou digitální stopu, sdílet o své osobě co nejméně informací, nevyjadřovat politické a nevhodné názory a nesdílet kontroverzní fotografie. Nevědomou digitální stopu můžeme minimalizovat vhodným AntiTrakingovým webovým prohlížečem, mazáním cookies, a častým měněním uživatelského jména a hesla, abychom znemožnili dohledat naši stopu a s ní související digitální identitu.

### 4.1.1 Upozornění na využití i zneužití datové stopy

Nejčastěji se datová stopa využívá při cílených reklamách v souvislosti se soubory cookies, které monitorují veškerý pohyb uživatelů na internetu a zaznamenávají jejich preference na webových stránkách. Také pomáhá forenzním vědám jako důkaz například při protizákonném jednání. Digitální stopa může být zneužita, pokud je nahromaděno velké množství dat, roste riziko ztráty soukromí i identity.

Každému do podvědomí občas ze zpráv a dalších komunikačních zdrojů pronikne informace o kybernetickém útoku, kyberšikaně či kyberstalkingu. Velká většina uživatelů si neuvědomuje a ani si nepřipouští, že i jich se takové věci mohou týkat. Stačí neopatrné zadání údajů nebo nevhodné sdílení fotografií a náš současný život může být změněn, nebo i ohrožen.

### 4.1.2 Možnosti ochrany dat

Zabezpečit naši digitální stopu můžeme pomocí Firewallu, který ochrání naše zařízení před neoprávněními průniky do sítě. A také pomocí vhodného antivirového programu, který bude chránit náš počítač před škodlivými programy a chránit před hrozbami internetu. Pokud je v domácnosti i dítě, které bude používat internet, je vhodné nastavit rodičovskou kontrolu, která zablokuje nevhodné stránky. Důležité to je především v dnešní době, kdy i výuka probíhá online.

Jak jsou na tom se znalosti digitální stopy dnešní uživatelé? Zajímá se široká veřejnost o ochranu své digitální stopy, nakolik přišla do styku s internetovou kriminalitou? Zná a ví, jaká jsou pravidla chování v prostředí internetu? Tím se zabývá bakalářská práce v dotazníkovém šetření.

## 4.2 Dotazníkové šetření

Cílem dotazníkového šetření bylo zjistit, zda si respondenti uvědomují svou digitální stopu a znají následky svého jednání, jak v internetovém, tak i reálném světě. Následně se i dozvědět, jak chrání svoji digitální stopu.

Dotazník byl zasílán respondentům přes sociální sítě a elektronickou poštu a jen malé procento dotazníků bylo vyplněno při osobním kontaktu s respondentem. Respondenti byli uvědomění, že jejich odpovědi jsou anonymní. Byli vybíráni náhodně, pouze bylo dohlíženo, aby byl poměrný počet respondentů v každé věkové kategorii bez ohledu na pohlaví a všichni respondenti byli uživatelé internetu.

Dotazník byl použit pouze k účelům této bakalářské práce a celkový počet otázek činí 20, Viz Příloha 1. V dotazníku určenému pro širokou veřejnost se objevily čtyři typy uzavřených otázek, Dichotomické a trichotomické, Výčtové otázky a Výběrové otázky. Otázky byly rozděleny do podsekcí pro rychlejší orientaci v dotazníku, Obecné informace, sloužily pro rozřazení dotazovaných do jednotlivých kategorií. Dále následovaly podsekce Obecné informace o digitální stopě, Zneužití digitální stopy, Příběh paní Zuzany, Ochrana dat a Netiketa. Dotazník byl vytvořen online, pomocí webu.google.com/forms.

Odpovědi byly exportovány do textového souboru (.csv) a importovány a zpracovány v Microsoft Excel 2019. Zásluhou MS Excel bylo umožněno zpracovat velké množství dat, uvedených v řádcích pod sebou a rozdělených do několika sloupců, pomocí kontingenčního grafu. Každá otázka byla nejprve samostatně vyhodnocena a pak také znázorněna pomocí vlastního grafu. Následně pomocí získaných dat, bylo provedeno vyhodnocení pomocí Obecných informací napříč dotazníkem.

## 4.3 Dotazník

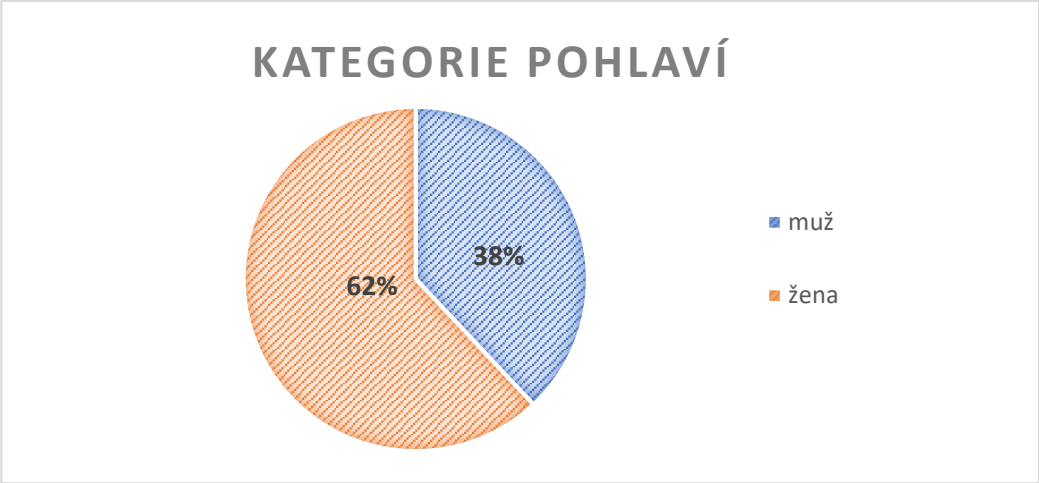
V následující kapitole jsou uvedeny výsledky dotazníkového šetření.

### 4.3.1 Obecné informace

Tato část dotazníků nám pomohla rozdělit respondenty do jednotlivých skupin podle pohlaví, věkové kategorie a nejvyššího dosažené vzdělání. Následně bylo možné jednotlivé kategorie mezi sebou porovnávat.

#### 4.3.1.1 Jaké je Vaše pohlaví?

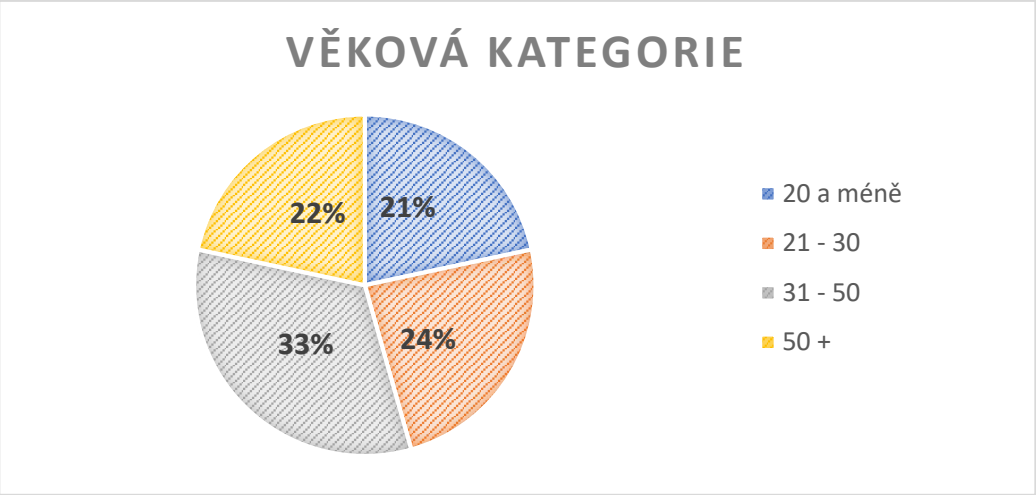
První otázka dotazníku rozdělila respondenty na muže a ženy. Z grafu je jasně patrné, že ženy se účastnily dotazníku častěji než muži a to z 62 % a z 38 % muži.




Obrázek 1 - Kategorie pohlaví

#### 4.3.1.2 Do jaké věkové kategorie spadáte?

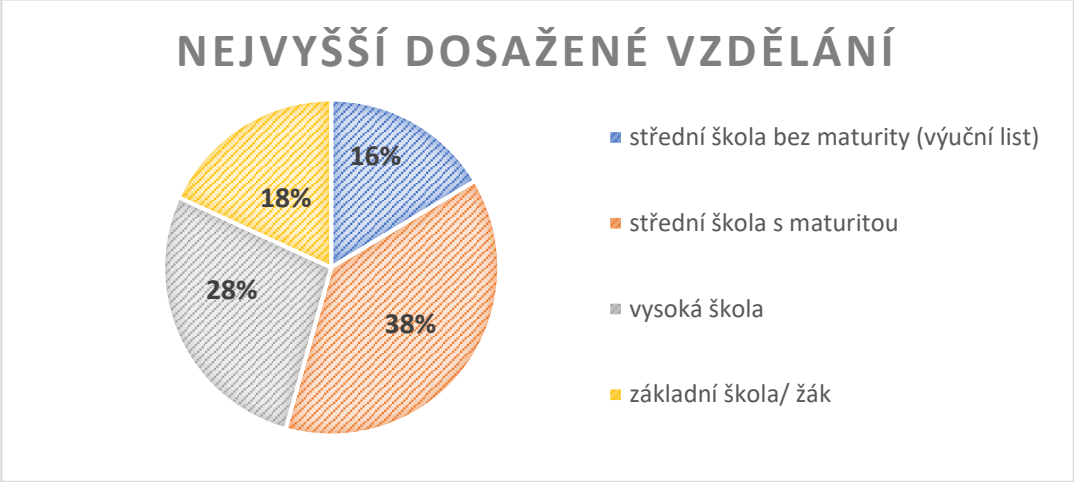
Druhá otázka je věk respondentů. Zde nejsilnější skupinou jsou lidé ve věku 31– 50 let 33 % respondentů. Na pomyslném druhém místě jsou mladí lidé ve věku 21–30 let 24 % všech dotazovaných. Ve věku 50+ let bylo 22 % dotázaných. Ve věku 20 a méně let bylo 21 % dotázaných.




Obrázek 2 - Věková kategorie

#### 4.3.1.3 **Jaké je Vaše nejvyšší dosažené vzdělání?**

Ve třetí otázce byli uživatelé internetu rozděleni dle nejvyššího dosaženého vzdělání, kde 18 % dotázaných ještě studuje na základní škole nebo mají dokončené pouze základní vzdělání a 16 % respondentů mají středoškolské vzdělání bez maturity. Největší zastoupení mají středoškoláci s maturitou 38 % dotazovaných. A 28 % účastníků výzkumu má vysokoškolské vzdělání.



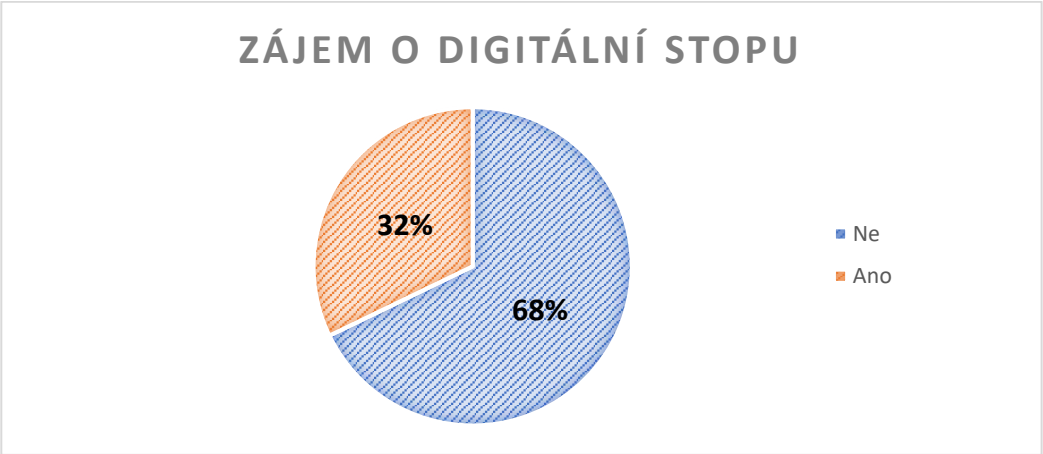

Obrázek 3 - Nejvyšší dosažené vzdělání

### 4.3.2 Obecné informace o digitální stopě

Následující oddíl výzkumné práce se zaměřuje na informovanost respondentů o obecných znalostech o digitální stopě.

#### 4.3.2.1 Zajímali jste se někdy o digitální stopu?

Zájem o digitální stopu v minulosti projevilo překvapivě jen poměrně malá část respondentů, a to pouze 32 % ze všech dotázaných.

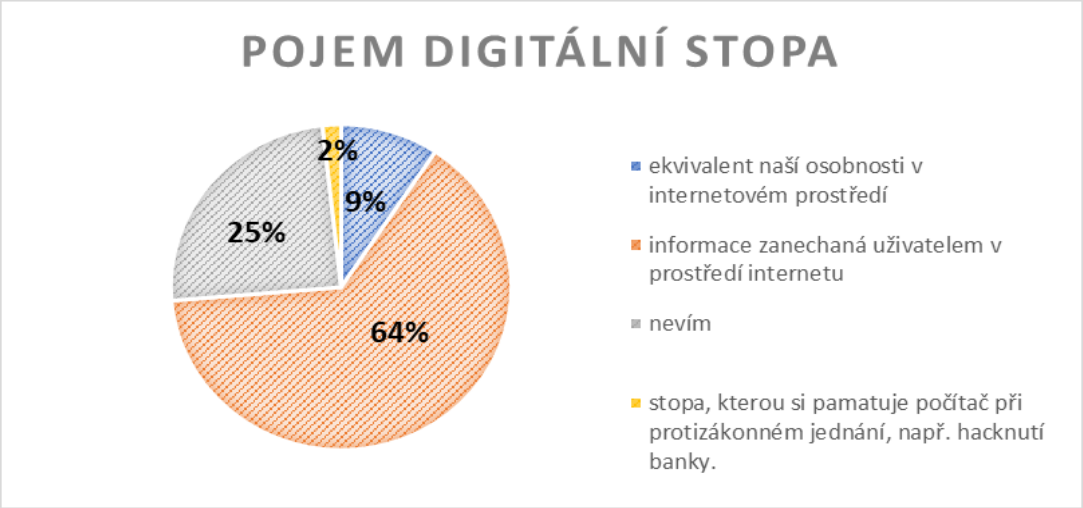



Obrázek 4 - Zájem o digitální stopu

#### 4.3.2.2 Co znamená pojem digitální stopa?

Vysvětlit co znamená pojem digitální stopa, někdy bývá opravdu složité, a proto byla otázka „Co znamená pojem digitální stopa?“ formou single-choice. Kdy respondenti vybírali jednu ze čtyř možných odpovědí. Naskytly se jim odpovědi typu: Ekvivalent naší osobnosti v internetovém prostředí, Informace zanechaná uživatelem v prostředí internetu, Stopa, kterou si pamatuje počítač při protizákonném jednání, např. hacknutí banky a odpověď Nevím. Odpověď „Ekvivalent naší osobnosti v internetovém prostředí“ nebyla správná, tato věta vychází z definice o digitální identitě. Digitální stopu s digitální identitou si plete 9 % respondentů. Odpověď „Informace zanechaná uživatelem v prostředí internetu“ je správná a zvolilo ji 64 % dotazovaných. Odpověď „Stopa, kterou si pamatuje počítač při protizákonném jednání, např. hacknutí banky“ nebyla správná, tuto odpověď zvolili 2 % respondentů. Jak již bylo v teoretické části bakalářské práce zmíněno, při jakémkoliv

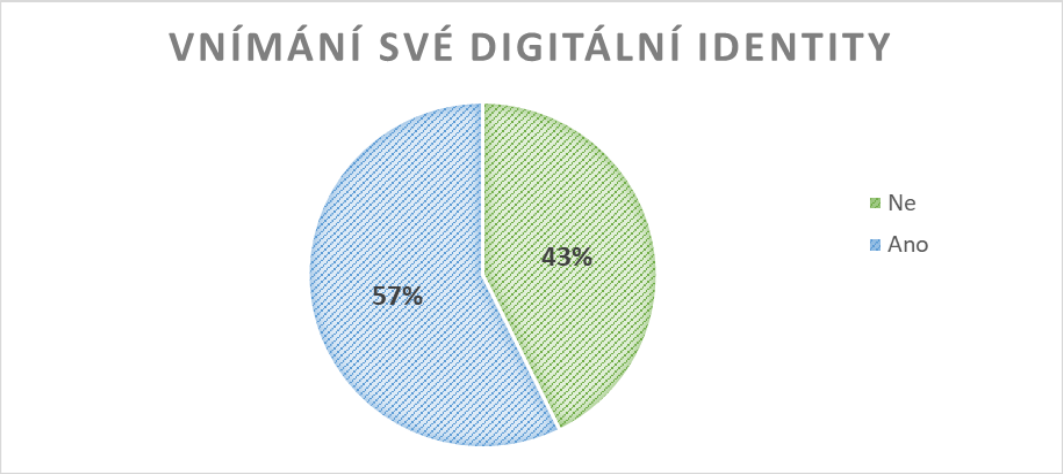
pohybu, nejen při tom protizákonném, je naše aktivita zaznamenávána. Poslední odpovědí byla neutrální odpověď „Nevím“, tu zvolilo 25 % dotazovaných.




Obrázek 5 - Pojem digitální stopa

#### 4.3.2.3 Je pro vás důležité, jak vás vnímají ostatní uživatelé internetu?

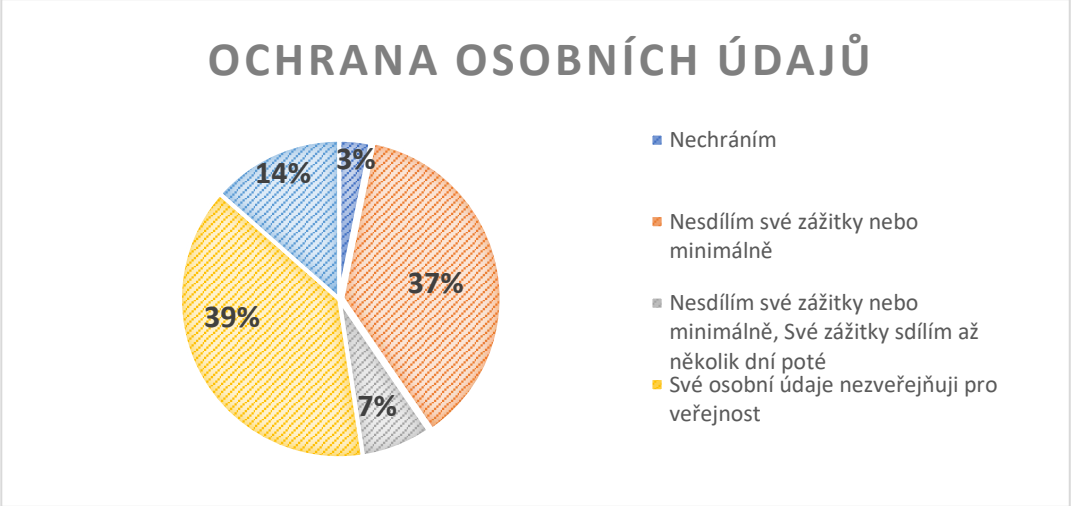
Respondenti byli také dotázáni, zda jim záleží, jak je vnímají ostatní lidé v prostředí internetu, tedy jak vnímají jejich digitální identitu. Můžeme tedy tvrdit, že přesně 57 % se opravdu zajímá o svoji digitální identitu tedy o to, jak působí na ostatní uživatele.




Obrázek 6 - Vnímání digitální identitu

#### 4.3.2.4 Jak chráníte své osobní údaje na profilech (účtech) před cizími lidmi?

Všem dotázaným byla položena otázka, jak chrání své osobní údaje na profilech (účtech) před ostatními účatníky internetu, otázka byla typu multiplechoice. Ze 39 % respondenti vybrali, že své osobní údaje nezveřejňuje pro veřejnost, 37 % dotázaných nesdílí své zážitky nebo minimálně, 14 % vybralo, že své osobní údaje nezveřejňuje pro veřejnost a své zážitky sdílí až několik dní poté, 7 % nesdílí své zážitky nebo minimálně a své osobní údaje nezveřejňuje pro veřejnost a ze 3 % účastníků výzkumu nechrání své osobní údaje.

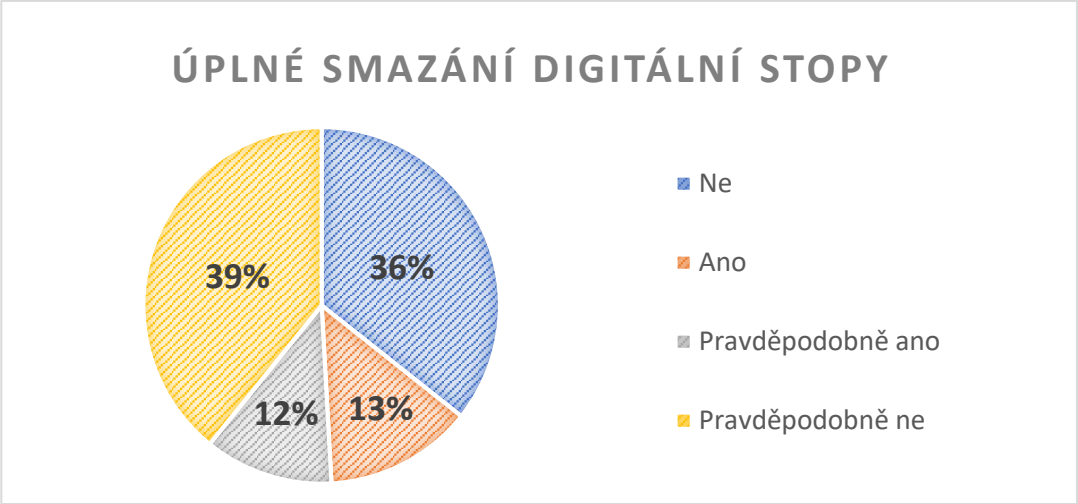



Obrázek 7 - Ochrana osobních údajů

#### 4.3.2.5 Myslíte si, že se dá Vaše digitální stopa ÚPLNĚ smazat?

Smyslem této otázky bylo zjistit, zda účastníci výzkumu mají povědomí o mazání digitálních stop. Zda si jsou vědomi, že jejich stopy můžou být dohledatelné a znovu obnovitelné. (Viz. Kapitola 3.6)

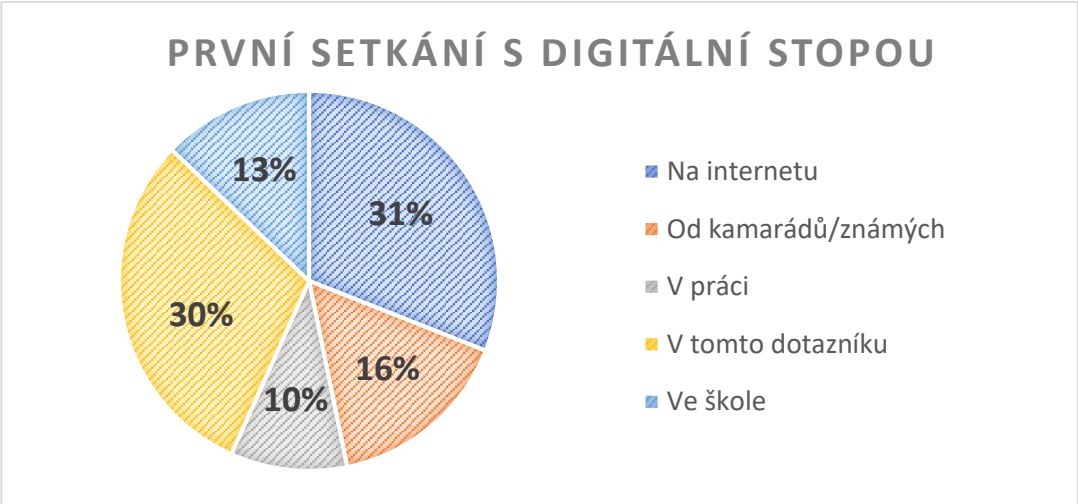
Z respondentů odpovědělo 36 %, že digitální stopu nelze úplně smazat, 39 % se domnívá, že se smazat pravděpodobně nedá, 12 % si myslí, že se digitální stopu pravděpodobně lze smazat. Ostatní účastníci výzkumu, konkrétně 13 %, věří, že se dá digitální stopa úplně vymazat.




Obrázek 8 - úplné smazání digitální stopy

#### 4.3.2.6 **Kde jste poprvé slyšel(a) o digitální stopě?**

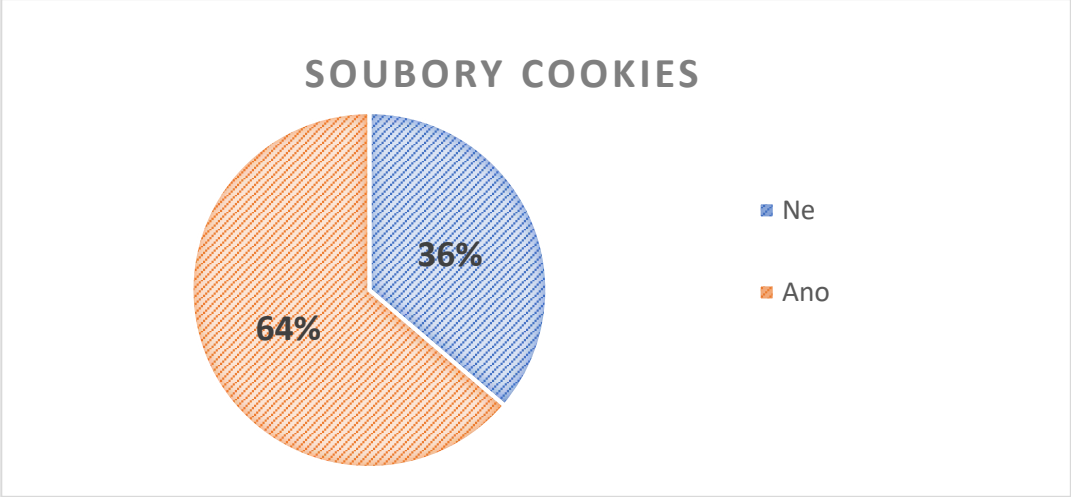
Dále bylo zjišťováno, kde poprvé se respondenti setkali s pojmem digitální stopa. Nejčastější odpovědí bylo „Na internetu“, to označilo 31 % dotazovaných, druhou častou odpovědí k velkému překvapení bylo „V tomto dotazníku“, což označilo 30 %. Od kamarádů známých, což zahrnovalo i rodinné příslušníky, se dozvědělo 16 % účastníku výzkumu. Ve škole se o digitální stopě dozvědělo 13 % a 10 % se o ní dozvědělo až v práci.




Obrázek 9 - první setkání s digitální stopou

#### 4.3.2.7 Víte, co jsou to soubory cookies, a kdo k nim má přístup?

Soubory cookies, malé datové soubory, jsou nedílnou součástí datové stopy, jak již bylo toto téma rozebíráno v kapitole 3.3.5. Respondenti byli, právě dotazováni, zda ví, co je to cookies a zda ví, kdo k těmto cookies má přístup. Více něž polovina, přesně 64 %, si je jisto, že ví, co je to cookies a kdo k nim má přístup. Ostatní dotazovaní buď netuší, co je to cookies, nebo neví, kdo k nim má přístup.

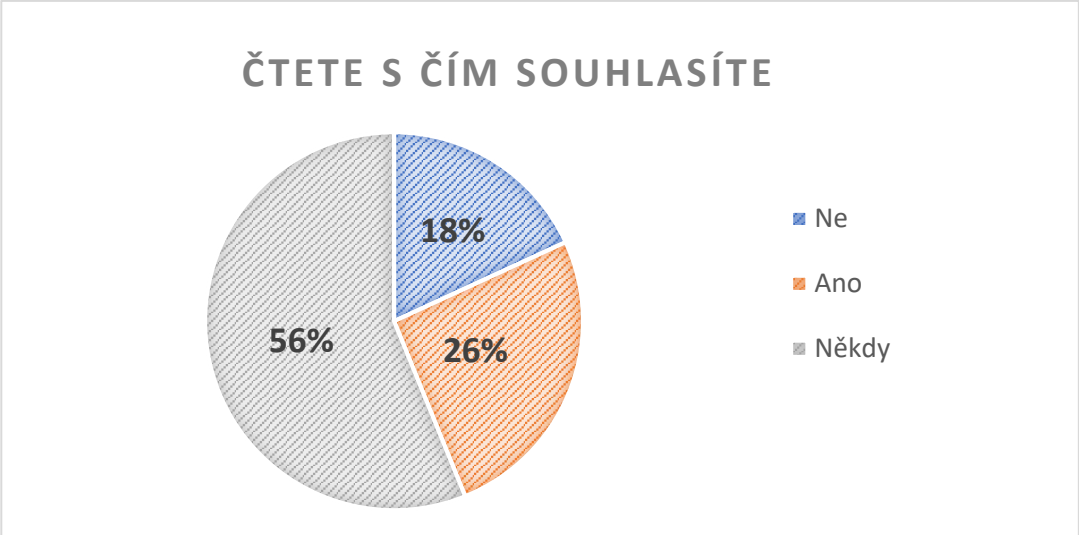



Obrázek 10 - soubory cookies

#### 4.3.2.8 Čtete, s čím dáváte souhlas na webových stránkách?

Účastníci výzkumu měli sdělit, jestli čtou vše, s čím dávají souhlas na webových stránkách. Jedná se tedy nejen o již zmiňované soubory cookies, ale například i souhlas se zpracováním osobních údajů a souhlas s provozními podmínky webové stránky při zakládání účtu.

Víc jak polovina dotazovaných se přiznává, že informace, s kterými udělují souhlas čtou jenom někdy. Víc než 1/4 respondentů tvrdí, že vždy čtou, s čím dávají souhlas na webových stránkách a 18 % nečte s čím dává souhlas.



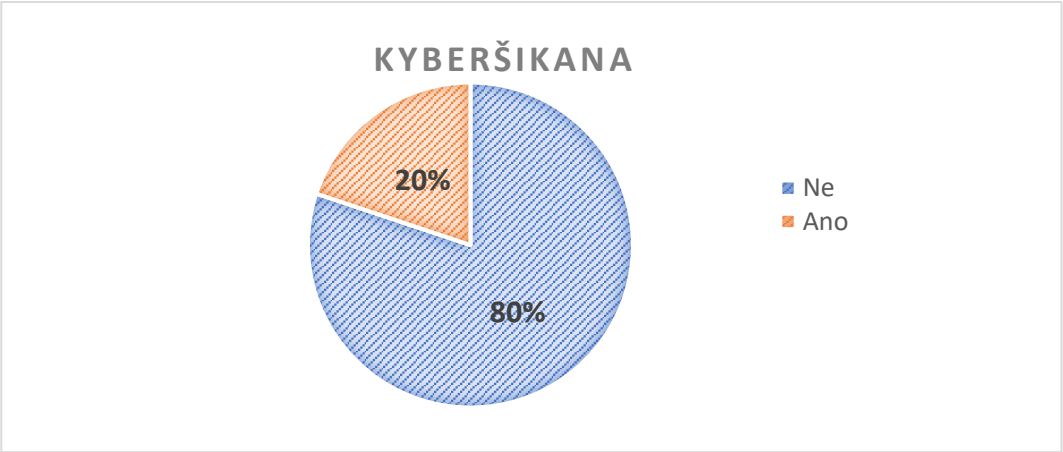

Obrázek 11 – čtete s čím souhlasíte

### 4.3.3 Zneužití digitální stopy

V této kapitole se zabýváme, kolik respondentů, bylo svědky zneužití digitální stopy v rámci kyberšikany a stalkingu, a jak by byli dotazovaní ochotni se zachovat v případě jejího nalezení.

#### 4.3.3.1 Zažil jste nebo byl jste svědkem Kyberšikany (= šikana v prostředí internetu)?

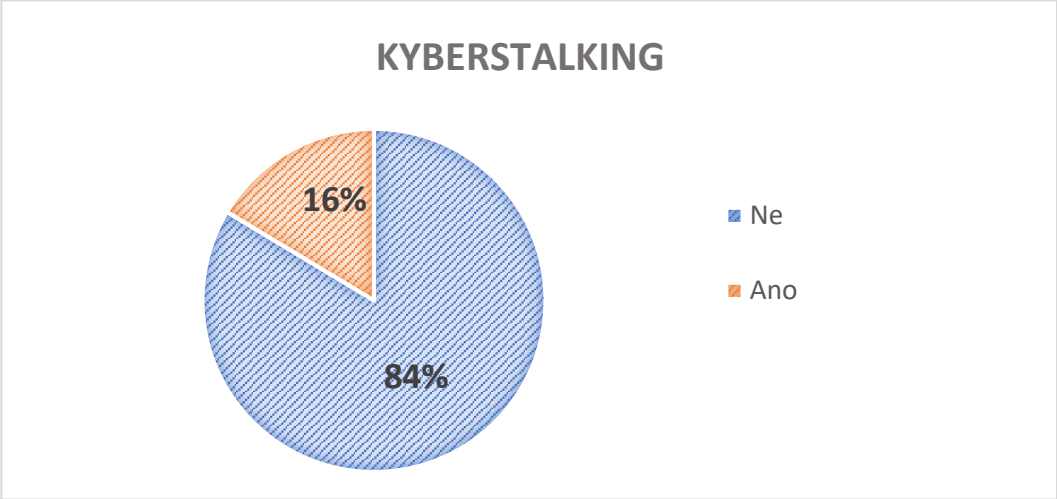
V dotazníku byla položena otázka „Zažil jste nebo byl jste někdy svědkem kyberšikany?“ Na tuto otázku odpovědělo 20 % lidí kladně. Překvapivě tedy 1/5 dotázaných se s kyberšikanou již setkalo.




Obrázek 12 – Kyberšikana

#### 4.3.3.2 Zažil jste nebo byl jste svědkem Kyberstalkingu (= nebezpečné pronásledování)?

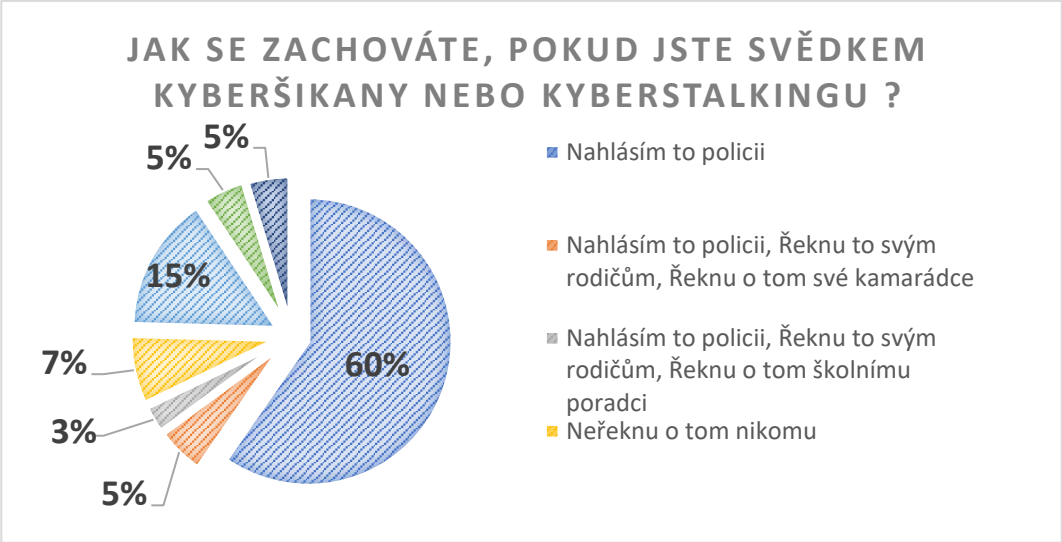
Byl položen i dotaz, zda někdo zažil či se stal svědkem nebezpečného pronásledování tedy Kyberstalkingu. Celkem 16 % všech dotazovaných odpovědělo kladně. Největší podíl na kladných odpovědí měly ženy a to z 64 %. Z dotazníku tedy vyplývá, že každá pátá žena zažila nebo byla svědkem nebezpečného pronásledování skrz internetové technologie.




Obrázek 13 - Kyberstalking

#### 4.3.3.3 Jak se zachováte, pokud jste svědkem Kyberšikany nebo Kyberstalkingu?

Incident by nahlásilo policii 60 % dotazovaných, pokud by se stali svědky kyberšikany nebo Kyberstalkingu, dalších 5 % by to oznámilo nejen polici, ale řekli by to svým rodičům a podělili by se o tuto zkušenost i se svými kamarády. Ve 3 % by to respondenti sdělili policii, řekli o tom svým rodičům a řekli o tom i školnímu poradci. V 5 % by to dle výzkumu bylo řečeno školnímu poradci a ve zbylých 5 % by to bylo řečeno rodičům. Bohužel 22 % účastníků výzkumu by nepodniklo žádné kroky k zabránění v těchto činnostech. Z těchto 22 % dotazovaných by 7 % to neřeklo nikomu a 15 % by to řeklo pouze své kamarádce.




Obrázek 14 - Jak se zachováte?

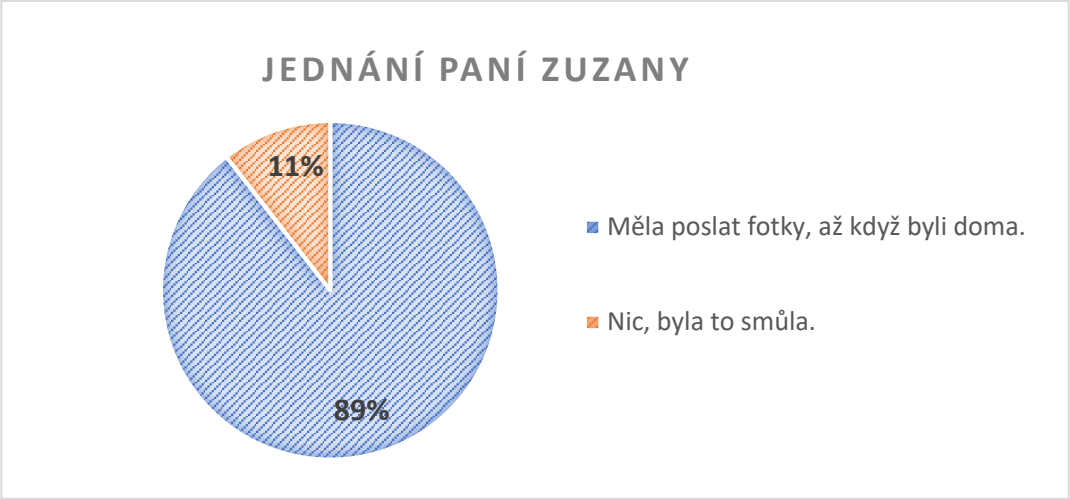
### 4.3.4 Příběh paní Zuzany

Tato část oddílu se zaměřuje na smyšlený příběh paní Zuzany, která si nechránila svoji digitální stopu a vše zveřejňovala a sdílela s celým světem. Až jednoho dne toho využili zloději, kteří jim vybílili celý dům.

Je nutno dodat, že ačkoliv je tento konkrétní příběh smyšlený vychází z příběhů, které autorka této bakalářské práce slýchala mezi lidmi.

#### 4.3.4.1 Co si myslíte, že paní Zuzana měla udělat?

Respondenti měli za úkol vybrat jednu z možných odpovědí. Přes 10 % účastníku výzkumu jsou toho názoru, že to byla smůla a paní Zuzana to nemohla nijak ovlivnit. Z těchto jedenácti procent má tento názor především 5 % dotazovaných ve věku 20 a méně let. Ze zbývajících procent se tento názor dělí mezi zbylé věkové kategorie tedy 3 % ve věkové skupině 21 až 30 let, 2 % respondentů s věkem 31 až 50 a 1 % zvolili účastníci výzkumu s věkem 50 a více.



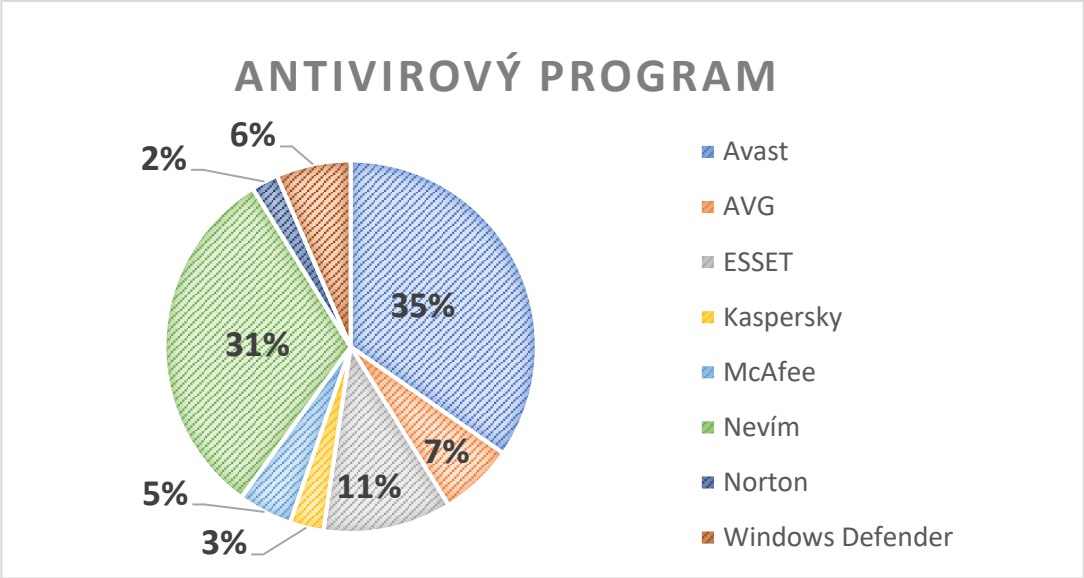

Obrázek 15 - Příběh paní Zuzany

### 4.3.5 Ochrana dat

V tomto oddílu se zaměřujeme na ochranu datové stopy pomocí nejrůznějších antivirových programů, respondenti jsou dotazováni, jak uchovávají svá hesla, tedy jak je chrání a kolikrát svá hesla mění za daný časový úsek.

#### 4.3.5.1 **Jaký antivirový program používáte?**

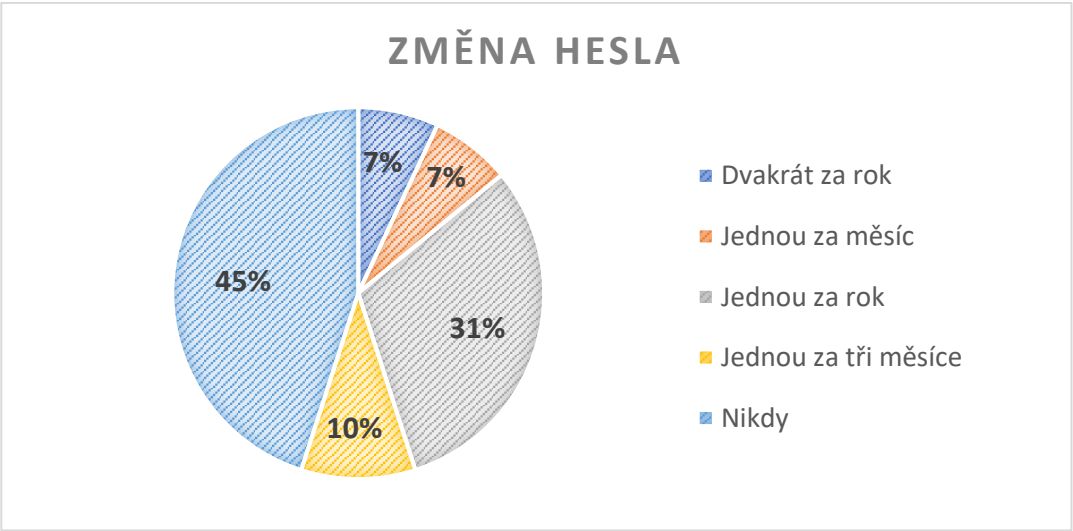
Z 35 % je používán antivirový program Avast, 31 % neví co používají za antivirový program. Třetí nejsilnější skupina je antivirový program ESSET s 11 % a až na čtvrtém místě se 7 % je antivirus AVG. Hned za AVG se drží Windows Defender, který je jako integrovaná součást počítačových systémů Windows Vista/7/8/8.1/10. S 5 % podílem se v dotazníku umístil McAfee a na zbylých dvou umístění máme Kaspersky a Norton.




Obrázek 16 - Antivirový program

#### 4.3.5.2 **Jak často si měníte svá hesla?**

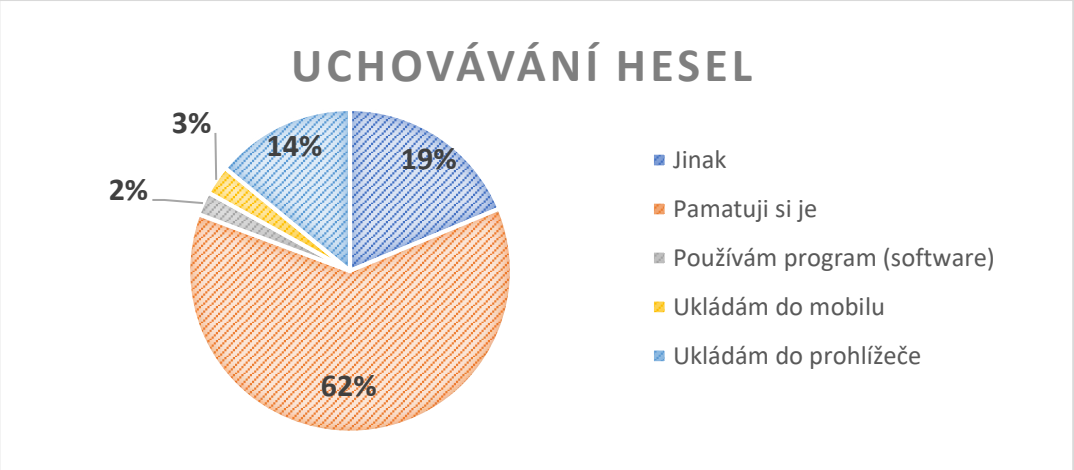
Změnu hesla bychom měli dělat ve většině za účelem ochrany dat na sociálních sítí. Bohužel v tomto dotazníkovém výsledku ze 45 % respondenti odpověděli, že nemění svá hesla. Pravděpodobně se domnívají že jejich hesla jsou naprosto bezpečná a jejich soukromá data jsou v bezpečí. Jednou za rok mění svá hesla 31 %, dvakrát za rok 7 %, jednou za tři měsíce 10 % a 7 % jednou za měsíc.




Obrázek 17 - Změna hesla

#### 4.3.5.3 Jak uchováváte svá hesla?

Respondenti dále uvedli, že nejčastěji svá hesla uchovávají ze 62 % ve své paměti a z 19% je uchovávájí jinde. Můžeme se domnívat, že je například píší do diáře nebo si je zapisují do kalendáře či jinak. Ze 14 % jsou hesla ukládána do prohlížeče, což může být problém ve chvíli, kdy se nacházíme na veřejném počítači například v knihovně nebo internetové kavárně. Pokud jsou hesla uložena do prohlížeče, bylo by tedy dobré vymazat ne jenom historii, ale i zaškrtnout políčko pro vymazaní Hesel a dalších přihlašovacích údajů. Ve 3 % jsou hesla uchovávána v mobilním telefonu uživatele. Takže v případě krádeže se do rukou zloději dostane nejen telefon, ale rovnou i klíč ke všem osobním informacím. Ve zbylých dvou procentech, dotazovaní používají speciální softwarové programy na úchovu hesel.



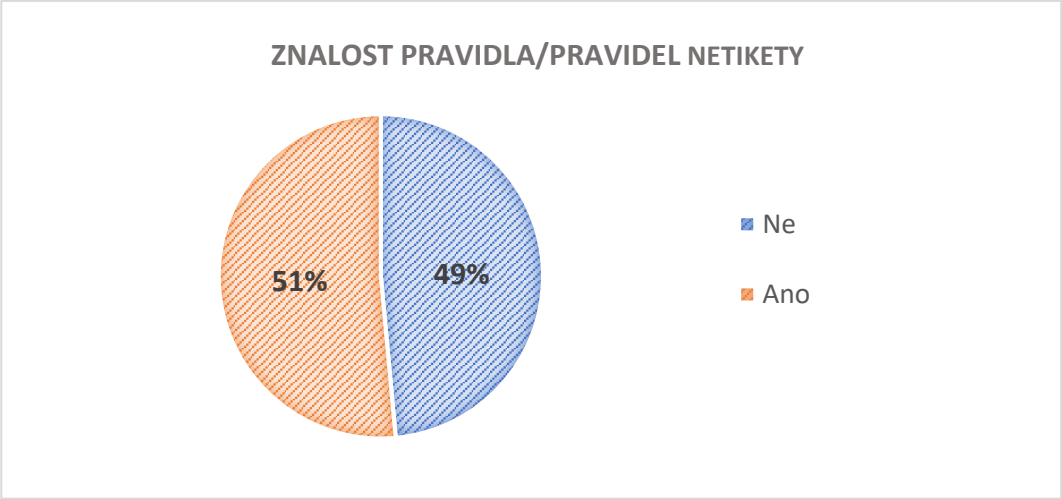

Obrázek 18 - Uchovávání hesel

### 4.3.6 Bezpečné chování na internetu – Netiketa

V tomto oddíle se zabýváme netiketou, tedy etiketou v prostředí internetu. Otázky v této části zkoumají, kolik účastníků výzkumu je schopno si uvědomit, jak se mají v prostředí internetu chovat a kolik z nich dodržuje podmínky netikety.

#### 4.3.6.1 Znáte nějaké(á) pravidlo(a)?

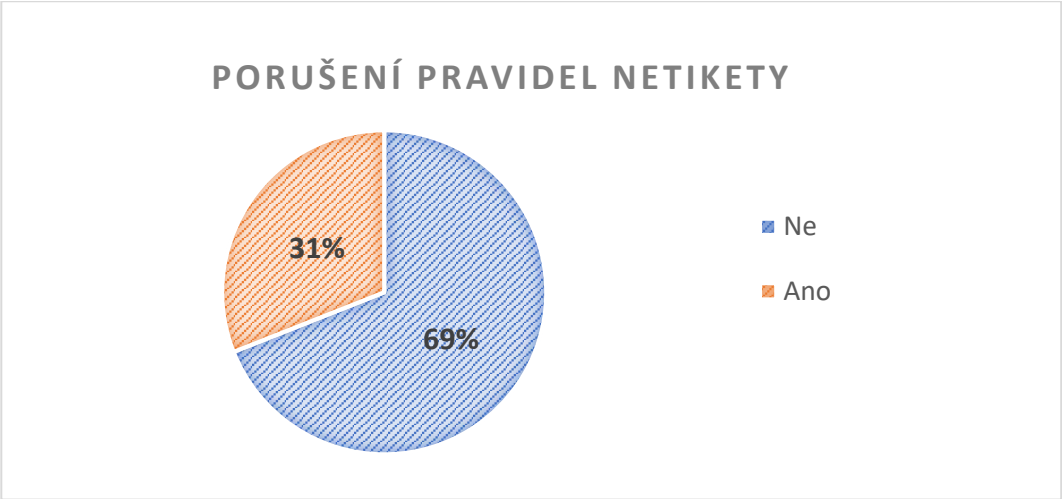
V této otázce jsme se ptali na znalost aspoň jednoho pravidla netikety, 51 % odpovídajících bylo schopno si aspoň vzpomenout na jedno pravidlo, bohužel 49 % si nevzpomnělo ani na jedno ze základních pravidel nebo opravdu žádné neznají.




Obrázek 19 - Znalost netikety

#### 4.3.6.2 **Porušili jste někdy některé z těchto pravidel?**

V další otázce bylo vyjmenováno pár základních pravidel netikety. Dotazovali jsme se respondentů, zda některé z těchto pravidel někdy porušili. Víc něž polovina odpověděla, že žádné z pravidel neporušili. Ve zbylých 31 % odpověděli, že ano, největší podíl má na tento výsledek věková kategorie 21–30 let.




Obrázek 20 - Porušení netikety

# 5 Vyhodnocení

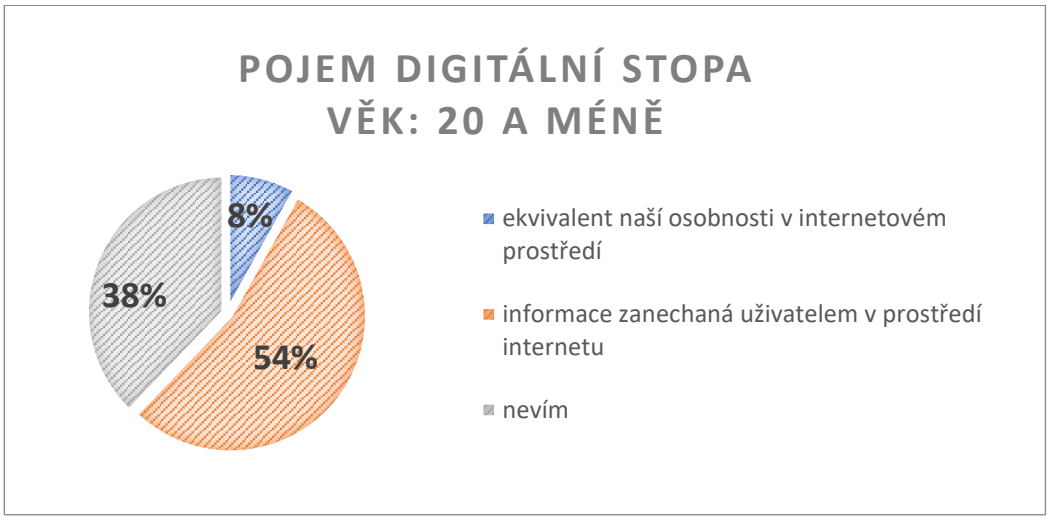
Získaná data od respondentů byla roztříděna podle pohlaví, věkové kategorie a nejvyššího dosaženého vzdělání, jednalo se o Obecné informace. Po přenesení dat do tabulek byly jednotlivé kategorie respondentů mezi sebou porovnány. Data jsou porovnávána v každé otázce pomocí metody pořadí mezi jednotlivými kategoriemi.

Z vyhodnocení byly vyloučeny otázky číslo 4, 12, 13 a 16. Účelem těchto otázek bylo dodatečné dotazování účastníka k jednotlivým kapitolám digitální stopy. Tyto otázky nemají charakter vyhodnocovací, ale vypovídající. Tyto otázky měly vzbudit zájem účastníka výzkumu o dané téma.

## 5.1 Vyhodnocení podle věkové kategorie

Hodnocení čtyř věkových skupin proběhlo na základě správných odpovědí jednotlivých otázek. Za jednu z nejdůležitějších otázek je považována otázka číslo 5, v ní jsme se ptali účastníků výzkumu, co znamená pojem digitální stopa.

Dotazovaní ve věku 20 a méně odpovídali ze 54 % správně ze 38 % si nebyli jistí odpovědí nebo skutečně nevěděli. Ze zbývajících 8 % si spletli digitální stopu s digitální identitou.




Obrázek 21 - Pojem digitální stopa ve věkové kategorii 20 a méně

Účastnici výzkumu ve věku 21 až 30 let odpověděli správně z 68 %, 20 % nevědělo co znamená pojem digitální stopa, 10 % si spletlo digitální stopu z digitální identitou a ze dvou procent se domnínají že digitální stopa vzniká pouze z nezákonné činnosti.


Obrázek 22 - Pojem digitální stopa ve věkové kategorii 21 až 30 let

Věková kategorie třicet jedna až padesát let odpověděla ze 71 % správně na otázku „Co je to digitální stopa?“, 13 % respondentů označilo odpověď nevím, 12 % se mýlí o tom, co je to digitální stopa. 4 % dotazovaných že digitální stopa vzniká pouze protizákonně.


Obrázek 23 - Pojem digitální stopa ve věkové kategorii 31 až 50 let

Respondenti ve věkové skupině 50 + let z 60 % odpovídali správně. Z 35 % neví, co je to digitální stopa nebo si nebyli odpovědí jisti. Ze zbývajících 5 % starší lidé padesáti let zaměňují význam pojmů digitální stopa a digitální identita.


Obrázek 24 - Pojem digitální stopa ve věkové kategorii 50+ let

Z těchto grafů můžeme vyčíst, že nejlépe informovanou věkovou skupinou je 31-50 a nejhůře informovanou skupinou je 20 a méně

Stejným způsobem bylo provedeno vyhodnocení i u ostatních otázek dotazníkového šetření. Vyhodnocení podle metody pořadí je zaznamenáno v tabulce.

| číslo otázky v dotazníku | 20 a méně | 21-30 | 31-50 | 50+ |
|---|---|---|---|---|
| 5 | 4 | 2 | 1 | 3 |
| 6 | 1 | 2 | 3 | 4 |
| 7 | 3 | 1 | 2 | 4 |
| 8 | 4 | 3 | 2 | 1 |
| 9 | 3 | 2 | 1 | 4 |
| 10 | 2 | 1 | 4 | 3 |
| 11 | 4 | 1 | 2 | 3 |
| 14 | 4 | 3 | 2 | 1 |
| 15 | 4 | 3 | 2 | 1 |
| 17 | 2 | 1 | 4 | 3 |
| 18 | 4 | 3 | 2 | 1 |
| 19 | 3 | 2 | 1 | 4 |
| 20 | 3 | 4 | 1 | 2 |
| **Vyhodnocení** | 41 | 28 | 27 | 34 |

**Tabulka 1 - Vyhodnocení podle věkové kategorie**

Ve věkové kategorii 20 a méně odpověděli pouze v jediné otázce nejlépe ze všech věkových skupin. Jednalo se o otázku, zda je zajímá, jak je vnímají ostatní uživatelé internetu.

Respondenti ve věku 21-30 se nejlépe vyznají v souborech cookies a zároveň čtou s čím souhlasí na webových stránkách. Nejlépe chrání své osobní informace na sociálních účtech a taky si nejčastěji mění heslo.

Věk 31-50 zná nejlépe definici pojmu digitální stopa a taky se poprvé setkali s digitální stopou mimo tento dotazník. Zároveň mají povědomí o pravidlech netikety a snaží se tyto pravidla dodržovat.

Lidé starší 50 let, kteří se účastnili tohoto dotazníkového šetření, by se nejlépe zachovali v případě zneužití digitální stopy a byli by schopni pomoct. Zároveň nejbezpečněji uchovávají svá hesla.

### 5.1.1 Závěr vyhodnocení podle věkové kategorie

Na závěr hodnocení pořadí v jednotlivých věkových kategoriích sečteme. Věková kategorie, která má nejmenší číslo, se stává podle tohoto vyhodnocení nejlepší věkovou skupinou ve znalosti digitální stopy a je i o digitální stopě nejlépe informovaná.

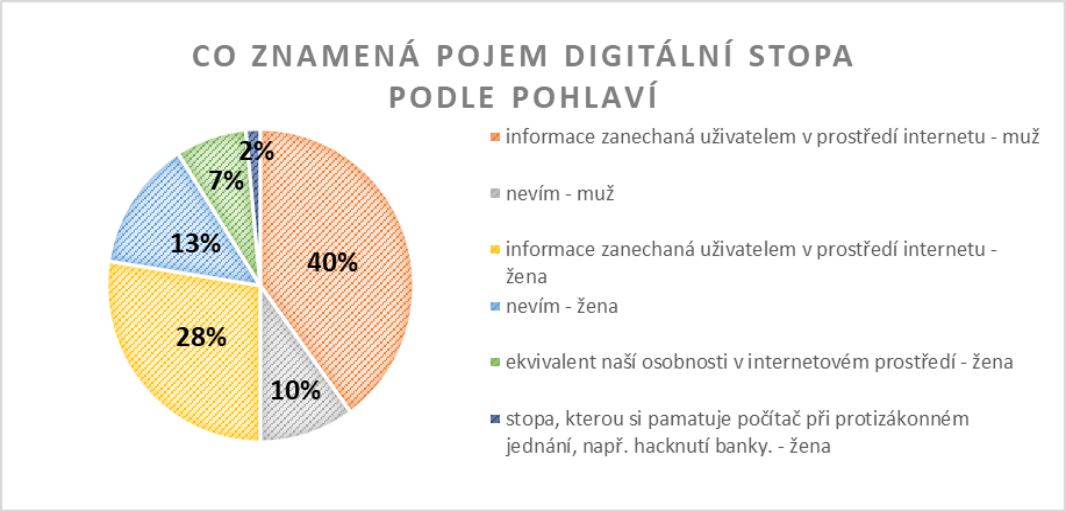
Nejlépe informovanou věkovou skupinou o digitální stopě je podle těchto kritérií věk 31 až 50. Nejhůře informovanou věkovou skupinou je paradoxně věk 20 a méně, přestože právě oni vyrůstají v digitálním světě od narození.

## 5.2 Vyhodnocení podle pohlaví a vzdělání

### 5.2.1 Vyhodnocení podle pohlaví

Hodnocení podle pohlaví proběhlo na základě správných odpovědí jednotlivých otázek. Příklad zpracování otázky číslo 5 vzhledem k pohlaví.

V procentuální porovnání mužů a žen jsou na tom lépe muži a to s 40 % správných odpovědí na otázku „Co znamená pojem digitální stopa?“ Ženy končí až na druhém místě s 28 %. Pouhých 13 % žen a 10 % mužů přiznává, že neví, co znamená pojem digitální stopa. Z grafu také vyplívá, že ženy si častěji pletou pojmy digitální stopa a digitální identita, a to z celých 7 %. Zbylá 2 % žen neznají přesnou definici digitální stopy.




**Obrázek 25 - Pojem digitální stopa podle pohlaví**

Všechny následující otázky byly vyhodnoceny stejným principem. Výsledky jsou zaznamenány v tabulce.

| Číslo otázky v dotazníku | ženy | muži |
|---|---|---|
| 5 | 2 | 1 |
| 6 | 2 | 1 |
| 7 | 1 | 2 |
| 8 | 2 | 1 |
| 9 | 2 | 1 |
| 10 | 1 | 2 |
| 11 | 1 | 2 |
| 14 | 2 | 1 |
| 15 | 2 | 1 |
| 17 | 2 | 1 |
| 18 | 2 | 1 |
| 19 | 2 | 1 |
| 20 | 1 | 2 |
| **Vyhodnocení** | 22 | 17 |

**Tabulka 2 - Vyhodnocení podle pohlaví**

Zdroj: vlastní

Ženy v porovnání s muži správně odpověděly jen v pár otázkách tématu základních informací o digitální stopě a dále pouze v jedné otázce tématu Bezpečného chování na internetu – Netiketě. Muži excelovali především v tématech Ochrany dat, Zneužití digitální stopy a v Příběhu paní Zuzany.

### 5.2.2 Vzdělání

Třetím kritériem, které bylo v dotazníku obsaženo je nejvyšší dosažené vzdělání, které jsme vyhodnotili podle pohlaví.

| Nejvyšší dosažené vzdělání | ženy | muži |
|---|---|---|
| základní škola/ žák | 19 % | 17 % |
| střední škola bez maturity (výuční list) | 13 % | 22 % |
| střední škola s maturitou | 38 % | 38 % |
| vysoká škola | 30 % | 23 % |

**Tabulka 3 - Nejvyšší dosažené vzdělání podle pohlaví**

U nejvyššího dosaženého vzdělání můžeme vidět, že procenta respondentů u žen převažují nad muži především u dokončeného vysokoškolského vzdělání. Střední školu s maturitou ukončilo shodný počet žen i mužů. U mužů převládají procenta výrazně u středoškolského vzdělání bez maturity oproti ženám.

### 5.2.3 Závěr vyhodnocení podle pohlaví a vzdělání

Vyhodnocování podle pohlaví bylo provedeno opět podle metody pořadí, následná pořadí byla sečtena a pohlaví s nižším výsledkem bylo určeno jako pohlaví, které má lepší znalost z oblasti digitální stopy a pravděpodobně je i lépe o digitální stopě informovaná.

Po sečtení jednotlivých pořadí ve vyhodnocování podle pohlaví jednoznačně mají větší informovanost o digitální stopě muži než ženy.

Hodnotíme-li výsledky respondentů podle pohlaví a dosaženého vzdělání, přestože muži celkově dosáhli nižšího vzdělání, jak vyplývá z tabulky č. 4, jsou víc informováni o digitální stopě než ženy.

## 5.3 Vyhodnocení dotazníku v rámci využití i zneužití datové stopy

V rámci využití digitální stopy jsme se zaměřili na cílené reklamy, které nejčastěji používají soubory cookies. Soubory cookies zaznamenávají preference, které uživatel nastaví jako například uživatelské jméno, preferovaný jazyk a jaké produkty si uživatel prohlíží. Dotazovali jsme se účastníků výzkumu, zda čtou souhlas s použitím souborů cookies. Víc, než jedna třetina respondentů nečte soubory cookies a nic o souborech nevědí. Udělíme-li povolení můžou se naše soubory cookies dostat k třetím stranám, které nás můžou sledovat napříč různými doménami a tím sbírat informace. Díky stopám, které za sebou zanecháváme, se můžeme stát snadno identifikovatelnými.

V rámci dotazníkového šetření byl položen dotaz na kyberšikanu a kyberstalking. Po vyhodnocení údajů se dozvídáme, že minimálně 28 % všech dotazovaných se setkali nebo byli svědky Kyberšikany nebo Kyberstalkingu. Dále jsme se ptali, jak by se uživatelé zachovali, kdyby spatřili na internetu kyberšikanu nebo kyberstalking. Většina dotazovaných by tento incident nahlásila policii. Zarážející je ale počet respondentů, kteří by nezabránili v páchání této internetové kriminality. Celkem 7 % by vůbec nereagovalo a 15 % by se pouze svěřilo kamarádovi či kamarádce.

Respondenti byli dotazováni na fiktivní příběh paní Zuzany, zajímalo nás, kolik dotazovaných si je vědomo, jak se mají chovat v případě sdílení informací na sociálních sítí. Na základě získaných dat si menší skupina respondentů myslí, že paní Zuzana neudělala žádnou chybu. Je důležité uvědomit si, že nevhodným sdílením informací ohrožujeme sebe i své blízké. Paní Zuzana mohla ochránit svá data pomocí vhodného nastavení svého profilu nebo nejlépe sdílet fotografie až, když byla s rodinou doma.

## 5.4 Vyhodnocení dotazníku v rámci ochrany dat

Hodnotíme-li ochranu dat na základě výsledků získaných z odpovědi respondentů zjistíme, že 31 % dotázaných uvádí, že neví, jaký je jejich antivirový program. Víme, že pokud používají operační systém Windows, jejich antivirus je integrovaný, Windows Defender. Znamená to ovšem, že doposud se o ochranu příliš nezajímali a neuvědomují si rizika.

Vhodný antivirus je jedním ze základních prostředků pro ochranu dat. Každý antivirus automaticky ale nezaručuje ochranu před všemi viry, je důležité vybírat jaký antivirus budeme používat a používat jeden. Použití dvou a více antiviru neznamená totiž větší ochranu, ale naopak souboj antiviru. Proto je nutné používat pouze jeden antivirus, který nám bude vyhovovat. Při používání počítače nezletilou osobou bychom měli zvážit používání rodičovské kontroly. Ovšem ne každý antivirus poskytuje rodičovskou kontrolu.

Při výběru antiviru je též důležité se rozhodnout, zda budeme používat antivirus placený nebo zdarma. Antivirové programy, které jsou nabízeny zdarma, často nemají ale všechny důležité ochrany, většinou chybí firewall, ochrana proti spamu či jiné ochrany.

Již zmiňovaný Windows Defender, který je integrovaný v systémech Windows, nemá ochranu proti spamu a ochranu bankovnictví. Dalším jeho problémem jsou méně časté aktualizace, tedy nemá ochranu proti novému škodlivému kódu.

| Název | Podporovaná čeština | Ochrana proti spamu | Ochrana proti phishingu | Ochrana Banky | Rodičovská kontrola | Firewall |
|---|---|---|---|---|---|---|
| Windows Defender | Ano | Ne | Ano | Ne | Ano* | Ano |
| Kaspersky | Ano | Ano | Ano | Ne | Ne | Ne |
| Avast! Free Antivirus | Ano | Ne | Ano | Ne | Ne | Ne |

**Tabulka 4 - Ukázka antivirových programů zdarma****

**Pouze v prohlížeči Microsoft Edge.*

***Jednotlivé informace byly zjištěny z oficiálních webových stránek.*

Z tohoto důvodu je vhodné zvážit používání placeného antiviru, ale i ten je důležitý správně vybrat a zjistit, co vše obsahuje.

Zde je stručné srovnání několika placených antivirových programů:

| Název | Cena /rok * | Podporovaná čeština | Ochrana proti spamu | Ochrana proti phishingu | Ochrana Banky | Rodičovská kontrola | Firewall |
|---|---|---|---|---|---|---|---|
| AVAST! Premium Security | 1 200 Kč | Ano | Ano | Ano | Ano | Ne | Ano |
| Kaspersky Internet Security | 1 000 Kč | Ano | Ano | Ano | Ano | Ano | Ano |
| AVG Internet Security | 1 600 Kč | Ano | Ano | Ano | Ano | Ne | Ano |
| Eset Internet Security | 1 500 Kč | Ano | Ano | Ano | Ano | Ano | Ano |
| McAfee | 1 200 Kč | Ano | Ano | Ano | Ne | Ano | Ano |
| Avira Antivirus Pro | 750 Kč | Ne | Ne | Ano | Ano | Ne | Ne |

**Tabulka 5 - Porovnání placených antivirových programů****

**Ceny jsou uvedeny k datumu 26/7/2020 a byly zjištěny z oficiálních webových stránek.*

***Jednotlivé informace byly zjištěny z oficiálních webových stránek.*

Při ochraně dat je také důležité dbát, k čemu udělujeme souhlas na webových stránkách. Na základě získaných dat z dotazníku 18 % účastníků výzkumu vůbec nečte a 56 % jen někdy čte s čím souhlasí na webových stránkách. U těchto účastníků výzkumu je velká pravděpodobnost, že jejich data již kolují po internetu bez jejich vědomí a ztratili tak své soukromí. Neuvědomují si, že i když své osobní údaje většina chrání, jak vyplívá z odpovědí v dotazníkovém šetření, jediným neopatrným udělením souhlasu mohli například sdílet své osobní údaje a činnosti na webových stránkách.

Významným prvkem v ochraně digitální stopy, tedy našich dat, jsou pravidla netikety, která byla popsána v kapitole 3.5. Podle výsledků z dotazníku zhruba polovina respondentů si nemohla ihned vybavit žádné pravidlo netikety, tedy etikety na síti. Přesto právě tyto pravidla a jejich dodržování můžou významně pomoct při ochraně digitální stopy.

# 6 Závěr

Teoretická část práce představuje úvod do tématu digitální stopy a seznamuje s možnostmi zneužití a využití datové stopy.

Ve vlastní práci je zpracován výzkum, který byl proveden dotazníkovým šetřením. Zúčastnit dotazníkového šetření se mohl každý člověk, který je uživatelem internetu. Zvlášť bylo dohlíženo na poměrný počet ve věkové kategorii bez ohledu na pohlaví.

Z dotazníkového šetření vyplynulo, že nejmenší znalosti z oblasti digitální stopy mají překvapivě uživatelé ve věkové kategorii 20 a méně let, víc než polovina dotazovaných neví, co znamená pojem digitální stopa a myslí si, že se dá digitální stopa úplně smazat. Přestože se již s pojmem datová stopa setkala ve škole, na internetu nebo si o tom povídali s přáteli. Nejlépe dopadli lidé ve věkové skupině 31 až 50 let, i když jejich znalost cookies je nedostatečná a nemění svá hesla pravidelně podle pravidel bezpečnosti, jak vychází z dotazníkového šetření. Hodnotíme-li znalosti, podle kategorie pohlaví a vzdělání, o digitální stopě, z dotazníkového šetření prokázali větší znalost muži, a to přesto že ženy mají celkově vyšší vzdělání. Respondenti často nečtou, k čemu uděluji souhlas na webových stránkách, o cookies nemají informace, a ani o antivirové programy se příliš nezajímají. Kyberšikana a kyberstalking je dnes velmi rozšířen a každý čtvrtý uživatel zažil nebo byl svědkem takového jednání, jak vyplívá z hodnocení dotazníku.

V dnešní době, kdy je internet rozšířen a prolíná se do všech stránek našeho života, je nutné posílit znalosti a uvědomění o digitální stopě mezi všechny uživatele. Jednou z možností je posílení a navýšení výuky informatiky na školách s důrazem na digitální stopu a její ochranu. Vzhledem ke zjištěným skutečnostem je navýšení hodin nutné nejen na školách základních, ale i středních. Zároveň v domácím prostředí by bylo vhodné zabezpečit internet pro nezletilé rodičovskou kontrolou pomocí antivirových programů, kde lze omezit návštěvnost nevhodných webových stránek. Pro zlepšení znalostí digitální stopy mezi všemi uživateli je možné využití médií. Rozhlasu, televize prostřednictvím šotů a reklam. V tištěné formě můžeme také upozornit na digitální stopu pomocí novin a časopisů.

Chránit své soukromí i svých blízkých je jedna z nejdůležitějších věcí v dnešním digitálním světě. Uvědomí-li si uživatelé jedinečnost digitální stopy, zjistí, jak výrazně ovlivňuje naše životy, zvýší i ochranu své datové stopy.

# 7 Seznam použitých zdrojů


[1] PÍSECKÝ, V. -- KOŽÍŠEK, M. Bezpečně n@ internetu : průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[2] ČERNÝ, Michal. Digitální stopy a digitální identita. *Metodický portál: Články* [online]. 26.08.2011 [cit. 26. 11. 2019] Dostupný na World Wide Web: https://clanky.rvp.cz/clanek/k/g/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html/

[3] Digitální stopa, 2019. Jak na Internet [online]. Praha: CZ. NIC, z. s. p. o. [cit. 2019-02-06]. Dostupné z: https://www.jaknainternet.cz/page/3651/digitalni-stopa/

[4] Dagmar Brechlerová, Digitální stopy a jejich odstraňování, SecurityWorld, 10. 07. 2016, [online] https://computerworld.cz/securityworld/digitalni-stopy-a-jejich-odstranovani-53197

[5] Kysela, Radek. Digitální stopy zanechávané na internetu [online]. c 2011 [cit. 26. 11. 2019] Dostupný na World Wide Web: http://www.kysela.info/digitalni-stopy.html

[6] Filip Sýkora, Před prvním pohovorem zameťte digitální stopy, 7. 9. 2017 [online] https://ekonom.ihned.cz/c1-65871270-pred-prvnim-pohovorem-zamette-digitalni-stopy

[7] KOLOUCH, Jan. CyberCrime. 1. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupný na World Wide Web: https://www.fd.cvut.cz/personal/barocvac/knihy/cybercrime.pdf

[8] PETROWSKI, Thorsten. Sicherheit im Internet: für alle. Rottenburg: Kopp Verlag, 2013. ISBN 9783864450662.

[9] Statistika kybernetické kriminality za rok 2019. E-Bezpečí [online]. Olomouc, 2020, 22. leden 2020 [cit. 2020-04-09]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-jinych-webu/1749-statistika-kyberneticke-kriminality-za-rok-2019

[10] ECKERTOVÁ, L., DOČEKAL, D. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press, 2013, ISBN 978-80- 251-3804-5

[11] Anna Halman (Polsko, 2006). E-Bezpečí [online]. Olomouc, 2020, 15. leden 2019 [cit. 2020-04-09]. Dostupné z:https://www.e-bezpeci.cz/index.php/72-kazuistiky/1426-anna-halman-polsko-2006

[12] KOPECKÝ, Kamil. Nebezpečí zvané kybergrooming I. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit.19.3.2014]. Dostupné z: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

[13] Internetem bezpečně: Kyberstalking [online]. b.r. [cit. 2020-06-26]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

[14] Что такое контекстная реклама? *WEBGAIN* [online]. 2019 [cit. 2021-02-08]. Dostupné z: https://webgain.ru/chto-takoe-kontekstnaya-reklama/

[15] Zásady pro používání souborů cookies. *Nový Web* [online]. Nový Web [cit. 2021-02-08]. Dostupné z: https://www.novy-web.cz/cookies.html

[16] Ochrana osobních údajů: Zásady používání souborů cookie. *Vláda České republiky* [online]. 1018 [cit. 2021-02-08]. Dostupné z: https://www.vlada.cz/cz/urad-vlady/o-serveru/ochrana-osobnich-udaju-167154/

[17] Používání cookies. *Evropská komise* [online]. [cit. 2021-02-08]. Dostupné z: https://ec.europa.eu/info/cookies_cs

[18] What is a Web Bug/Beacon? *What is my IP address* [online]. [cit. 2021-02-08]. Dostupné z: https://whatismyipaddress.com/web-beacon

[19] Pravidla pro užívání cookies. *MAP vzdělávání* [online]. [cit. 2021-02-08]. Dostupné z: https://www.mapvzdelavani.cz/?cookies=1&lang=cs

[20] KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. První vydání. Praha: Grada Publishing, a.s., 2015, ISBN 978-80-247-5453-6

[21] Phishing: Co je to phishing? *ESET software spol. s r.o.* [online]. North America, c2020 [cit. 2020-06-27]. Dostupné z: https://www.eset.com/cz/phishing/

[22] Behaviorální marketing. In: MediaGuru [online]. 2012 [cit. 2020-03-01]. Dostupné z: http://www.mediaguru.cz/medialni-slovnik/behavioralni-marketing/

[23] RECMANOVÁ, Alena. *Pravidla netikety* [online]. Masarykova univerzita: EDTECH KISK, 30.11.2017 [cit. 2020-07-14]. Dostupné z: https://medium.com/edtech-kisk/pravidla-netikety-ea92f7c3e58b

[24] Vlastnosti digitálních stop a jejich dopady na forenzní šetření. [online]. [cit. 2020-03-01]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf.

[25] Jste to, co píšete na internetu*.: Dodržujte netiketu, naučte ji své děti a jděte jim příkladem*[online]. redakce Rodiče vítáni, 2019 [cit. 2020-07-14]. Dostupné z:

https://www.rodicevitani.cz/trendy-ve-vzdelavani/digitalni-technologie/jste-to-co-pisete-na-internetu-dodrzujte-netiketu-naucte-ji-sve-deti-a-jdete-jim-prikladem/

[26] M. FERTIK, D. C. THOMPSON, The Reputation Economy: How to Optimize Your Digital Footprint in a World Where Your Reputation Is Your Most Valuable Asset, Little, Brown Book Group, 2015, ISBN: 978-03-853-4760-0

[27] DAN, Marina. *Anti Tracks Free Edition* [online]. 12.11. 2013 [cit. 2020-07-26]. Dostupné z: https://www.softpedia.com/get/Security/Secure-cleaning/Anti-Tracks-Free-Edition.shtml

[28] JANŮ, Stanislav a Vladislav KLUSKA. *Jak surfovat anonymně.* [online]. 04.02.2019 [cit. 2020-07-26]. Dostupné z: https://www.zive.cz/clanky/jak-na-internetu-surfovat-anonymne-osvedcene-zpusoby-na-zameteni-stop/sc-3-a-184471/default.aspx#part=1

[29] CLIFFORD, Colby a Sharon PROFIS. Strong passwords: 9 rules to help you make and remember your login credentials. *Cnet* [online]. CBS Interactive, c2020, 02.03.20120 [cit. 2020-07-29]. Dostupné z: https://www.cnet.com/how-to/strong-passwords-9-rules-to-help-you-make-and-remember-your-login-credentials/

[30] J. PERRY, Disappear Without a Trace: How to Erase Your Digital Footprint, 2017, ASIN: B07572H5N8

[31] Ochrana osobních údajů podle nařízení GDPR. *Oficiální internetová stránka EU* [online]. [cit. 2021-02-08]. Dostupné z: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_cs.htm

[32] GDPR AND COOKIE CONSENT. *Compliant cookie use* [online]. 27.10.2020 [cit. 2021-02-08]. Dostupné z: https://www.cookiebot.com/en/gdpr-cookies/

[33] KOCH, Richie. *Cookies, the GDPR, and the ePrivacy Directive* [online]. c2021, 27.10.2020 [cit. 2021-02-08]. Dostupné z: https://gdpr.eu/cookies/

[34] Blíže viz např. SLÍŽEK, David. Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost. [online]. [cit. 2020-08-02]. Dostupné z: http://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/

[35] PIŇOS, Eduard. *Co musíte podstoupit, když o sobě něco chcete smazat z Googlu* [online]. MediaRey, SE, c2020, 16.06.2020 [cit. 2020-08-02]. Dostupné z: https://www.forbes.cz/co-musite-podstoupit-kdyz-o-sobe-neco-chcete-smazat-z-googlu/

# 8 Přílohy

## 8.1 Příloha 1 - vzor dotazníku

Dobrý den,
dovoluji si Vás poprosit o pár minut Vašeho času k vyplnění následujícího dotazníku. Informace z dotazníku jsou anonymní a budou zpracovány v rámci bakalářské práce "Digitální stopa".

Prosím vyplňte každou otázku, jinak vás dotazník nepustí dál.
Po vyplnění dotazníku, Prosím nezapomeňte odpovědi ODESLAT.

Za Vaši ochotu a spolupráci Vám předem děkuji. :)
Jana Turoňová

**Obecné informace**

1. **Jaké je vaše pohlaví?**
    - Žena
    - Muž
2. **Do jaké věkové kategorie spadáte?**
    - 20 let a méně
    - 21–30 let
    - 31–50 let
    - 50+
3. **Jaké je Vaše nejvyšší dosažené vzdělání?**
    - Žák
    - Základní škola
    - Střední škola bez maturity (výuční list)
    - Střední škola s maturitou
    - Vyšší odborná škola
    - Vysoká škola

**Obecné informace o digitální stopě**

4. **Zajímali jste se někdy o digitální stopu?**
    - Ano
    - Ne

5. **Co znamená pojem digitální stopa?**
    - Ekvivalent naší osobnosti v internetovém prostředí
    - Informace zanechaná uživatelem v prostředí internetu
    - Stopa, kterou si pamatuje počítač při protizákonném jednání, např. hacknutí banky.
    - Nevím
6. **Je pro vás důležité, jak vás vnímají ostatní uživatelé internetu?**
    - Ano
    - Ne
7. **Jak chráníte své osobní údaje na profilech (účtech) před cizími lidmi?**
    - Nechráním
    - Své osobní údaje nezveřejňuji pro veřejnost
    - Nesdílím své zážitky nebo minimálně
    - Své zážitky sdílím až několik dní poté
8. **Myslíte si, že se dá Vaše digitální stopa ÚPLNĚ smazat?**
    - Ano
    - Pravděpodobně ano
    - Pravděpodobně ne
    - Ne
9. **Kdy jste poprvé slyšel(a) o digitální stopě?**
    - Ve škole
    - V práci
    - Od kamarádů/známých
    - Na internetu
    - V tomto dotazníku
10. **Víte, co jsou to soubory cookies, a kdo k nim má přístup?**
    - Ano
    - Ne
11. **Čtete, s čím dáváte souhlas na webových stránkách?**
    - Ano
    - Někdy
    - Ne

**Zneužívání digitální stopy**

**12. Zažil jste nebo byl jste svědkem Kyberšikany (= šikana v prostředí internetu)?**

- Ano
- Ne

**13. Zažil jste nebo byl jste svědkem Kyberstalkingu (= nebezpečné pronásledování)?**

- Ano
- Ne

**14. Jak se zachováte, pokud jste svědkem Kyberšikany nebo Kyberstalkingu?**

- Neřeknu o tom nikomu
- Nahlásím to policii
- Řeknu to svým rodičům
- Řeknu o tom školnímu poradci
- Řeknu o tom své kamarádce

**Příběh paní Zuzany**

Paní Zuzana se svou rodinou velmi ráda jezdila na výlety a cestovala. Vždy z výletů pořizovala fotografie a chlubila se s nimi svým kamarádkám a přátelům.

S příchodem moderní doby, ale přišla možnost nasdílet fotografie i uprostřed dovolené. Tak toho paní Zuzana využila, když byla u moře s celou rodinou, a to se jí stalo osudným. Nebyl žádný problém se podívat, kde právě všichni jsou.

Po příletu do země celou rodinu čekalo velmi nepříjemné překvapení. Celý dům byl vybílený. Gauč, skříně, elektronika, drahý porcelán, vzácné šperky, všechno bylo pryč.

**15. Co si myslíte, že paní Zuzana měla udělat?**

- Nic, byla to smůla.
- Měla poslat fotky, až když byli doma.

**Ochrana dat**

**16. Jaký antivirový program používáte?**

- Avast
- Windows Defender
- ESET
- AVG
- Norton
- McAfee
- Kaspersky
- Jiný/ Nevím

**17. Jak často si měníte své heslo?**

- Nikdy
- Jenou za rok
- Dvakrát za rok
- Jednou za tři měsíce
- Jednou za měsíc
- Jednou za týden

**18. Jak uchováváte svá hesla?**

- Pamatuji si je
- Ukládám do prohlížeče
- Ukládám do mobilu
- Používám program (software)
- Jinak

**Bezpečné chování na internetu – Netiketa**

I pro používání internetu existují pravidla tzv. „netiketa“ tedy etiketa na síti.

**19. Znáte nějaké(á) pravidlo(a)?**

- Ano
- Ne

Některá pravidla netikety:

1. Běžná pravidla slušnosti z běžného života platí i na internetu. To, co napíšeš do počítače, bys možná do očí nikdy nikomu neřekl.
2. Odpouštěj ostatním chyby. I ty je děláš. Nevysmívej se ostatním a nenadávej na ně.
3. Respektujte názor druhých i jejich soukromí.
4. Nedůvěřujte lidem, které neznáte. Může se jednat o podvodníky.
5. Nešiř hoaxy. Nerozesílej spam a reklamu.
6. Neporušuj autorská práva.

*Zdroj: https://bezpecne-online.saferinternet.cz/surfuj-bezpecne/komunikace-se-svetem/item/53-netiketa*

**20. Porušili jste někdy některé z těchto pravidel?**

- Ano
- Ne