VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a
komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Dita Kubíčková

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

INFORMAČNÍ SOUKROMÍ A VOLNĚ DOSTUPNÉ ZDROJE INFORMACÍ
INFORMATION PRIVACY AND OPEN-SOURCE INTELLIGENCE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Dita Kubíčková**
AUTHOR

VEDOUCÍ PRÁCE — **JUDr. MgA. Jakub Míšek, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Dita Kubíčková ***ID:*** 202674
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Informační soukromí a volně dostupné zdroje informací

POKYNY PRO VYPRACOVÁNÍ:

Bakalářská práce Informační soukromí a volně dostupné zdroje informací bude věnována problematice ochrany soukromí v online prostoru s akcentem na informace, které jsou člověku volně dostupné. Teoretická část se zaměří na koncept informačního soukromí a provede jeho vymezení. Následně představí vybrané techniky a nástroje, které umožňují a usnadňují sběr volně dostupných informací o jedinci a zhodnotí jejich účinnost a rizikovost pro soukromí jedince. Poskytne rovněž doporučení, jak své soukromí online může člověk chránit. Praktickým výstupem práce bude program, který na základě získaných teoretických poznatků provede kontrolu vybraných online zdrojů a upozorní na rizika zásahu do soukromí.

DOPORUČENÁ LITERATURA:

[1] Koops, B.-J. et al. A Typology of Privacy. Rochester, NY: Social Science Research Network, 2016 [cit. 30. 6. 2019]. http://papers.ssrn.com/abstract=2754043

[2] Pastor-Galindo, J. et al. The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE Access. 2020, s. 10282–10304.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: JUDr. MgA. Jakub Míšek, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

Abstrakt

Bakalářská práce se zabývá problematikou konceptu soukromí a informačního soukromí v prostředí internetu. Teoretická část práce popisuje hlavní typologie a vyvozuje hodnotu, kterou informační soukromí představuje a proč je třeba jej chránit, přičemž představuje technické a právní nástroje této ochrany. Dále představuje problematiku OSINT a uvádí vybrané techniky a nástroje používané ke sběru volně dostupných informací o osobách. Praktická část je následně věnována popisu vývoje a funkcionalit aplikace pro automatizované vyhledávání informací na sociálních sítích.

Klíčová slova

Informační soukromí, soukromí, osobní informace, sběr informací, vyšetřování, OSINT, OPSEC, sociální sítě, nástroje

Abstract

The bachelor thesis deals with the issue of privacy and information privacy on the Internet. The theoretical part of the thesis describes main typologies and concludes the value of information privacy and why is it important to protect it. It presents technical tools and legal regulations used for protection. It also deals with an issue of OSINT and presents some techniques and tools for person‘s information gathering. In practical part of the thesis, there is described the development and functions provided by the application for automated information gathering from social networks.

Keywords

Information privacy, privacy, personal information, intelligence gathering, investigation, OSINT, OPSEC, social networks, tools

Bibliografická citace

KUBÍČKOVÁ, Dita. *Informační soukromí a volně dostupné zdroje informací.* Brno, 2021. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/133515. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Jakub Míšek.

Poděkování

Děkuji vedoucímu bakalářské práce JUDr. MgA. Jakubovi Míškovi, Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

V Brně dne: 24. května 2021 ----------

podpis autora

Obsah

SEZNAM OBRÁZKŮ

Úvod

S problematikou informačního soukromí se setkává dennodenně každý uživatel internetu a služeb, které jsou jeho prostřednictvím poskytovány. Dalo by se říct, že každým krokem v online prostředí se vzdáváme kousku naší identity, a že být stoprocentně anonymní a nevystopovatelný je téměř nemožné. A právě těchto informací, které o sobě člověk sděluje, ať už úmyslně nebo nevědomky, využívá proces Open Source Intelligence (OSINT). Na základě takto posbíraných veřejně dostupných dat je vytvořen profil cíle, který může sloužit pro účely vyšetřování po pohřešovaných osobách, v boji s organizovaným zločinem, teroristickými buňkami, v oblasti kyberbezpečnosti nebo v investigativní žurnalistice.

Hlavním cílem této práce je představit koncept informačního soukromí v prostředí internetu, možnosti jeho ochrany a uvést vybrané techniky a nástroje používané ke sběru volně dostupných informací o osobách. Cílem praktické části je pak vytvořit program, který toto vyhledávání informací zautomatizuje. K naplnění cílů práce přispívají kapitoly tak, jak je dále popsáno.

Mou motivací a cílem je uvést čtenáře do problematiky soukromí v online prostoru, na nějž má zákonné právo, a nabídnout možnosti, jak omezit nebo případně alespoň minimalizovat jeho narušení ze stran společností. Následně chci poskytnout pohled z druhé strany, tedy na proces získávání volně dostupných informací, na používané metody a nástroje a související zásady. Praktická část pak práci doplňuje o nástroj pro takového vyhledávání informací.

V první kapitole této práce je představen pojem soukromí, jak jej v průběhu let definovali nejrůznější autoři a jsou zde popsány hlavní typologie soukromí, v nichž se časem vynořilo informační soukromí jako jeho samostatná kategorie. V dalších podkapitolách je popsáno, jakou hodnotu informační soukromí má, proč je třeba jej chránit a jaké jsou technické a právní nástroje jeho ochrany.

Druhá kapitola se zaobírá cyklem OSINT. Je v ní přiblížen jeho historický vznik a postupný vývoj do dnešní podoby, v jaké je realizován, a také v jakých oblastech je využíván. Následuje popis průběhu každé fáze operačního cyklu, jak jej definuje CIA, od plánování a nasměrování, přes shromažďování, zpracování, analýzu a produkci až po rozšiřování. V dalších podkapitolách jsou představeny používané techniky a možnosti nástrojů pro získávání informací, z nichž nejpoužívanější jsou popsány podrobněji.

Třetí kapitola je věnována praktické části práce, v rámci níž bude vytvořen program pro automatizované vyhledávání informací pro účely OSINT o osobách na základě poskytnutého jména a příjmení. Výstupem programu pak bude výpis zjištěných dat s odkazy.

1. SOUKROMÍ

Soukromí je jedním ze základních předpokladů pro svobodnou demokratickou společnost a pro samotné uchopení identity jedince a formování jeho osobnosti [1, 40]. Přesto není vůbec snadné tento pojem vymezit. Filozofka Judith Jarvis Thomson ve svém textu The Right to Privacy z roku 1975 uvádí: *„Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.“* [2, 295] Důvod tohoto tvrzení nám začne být jasnější, když se podíváme, jak na soukromí pohlíží zákon. Právní úprava totiž nestanovuje, co soukromí je, ale jakým situacím dotýkajících se soukromí se dostane právní ochrany [3, 36]. V rámci České republiky došlo k zásadnímu zlomu na poli ochrany soukromí v roce 2011, kdy padlo rozhodnutí Ústavního soudu ve věci data retention. Soud shledal zákony implementující tuto směrnici neústavními a jako závažně zasahující do práva na soukromí a práva na informační sebeurčení [4].

1.1 Pojem soukromí a jeho informační část

O definici soukromí se v průběhu let pokoušela řada autorů. Například Jeffrey H. Reiman píše [5, 30], že soukromím rozumí stav, kdy mají lidé znemožněn přístup buď k nám nebo k nějakému s námi spojenému prožitku a dodává, že soukromí je více než prosté informace. Když si představíme modelovou situaci, kdy je někdo sledován během převlékání, tak sledující nutně nezískává žádné nové informace, ale přesto se jedná o zásah do soukromí, na které má daná osoba právo. Stejné je to i v případě, že by byl sledován blízkou osobou. Zkrátka jde o to mít možnost provádět dané úkony v soukromí a nezáleží na tom, zda osoba, která akt sleduje, jej vidí poprvé nebo už k tomu dříve měla svolení. Reiman tedy své tvrzení zakládá na podmínce znemožnění přístupu.

Naproti tomu filozof Charles Fried tvrdí [6, 482], že podmínkou je kontrola nad tímto přístupem a udává příklad: *„To refer for instance to the privacy of a lonely man on a desert island would be to engage in irony.“* Zde se však dostáváme k jasnému problému. Pokud bychom na soukromí pohlíželi tak, že do něj spadají jen ty činnosti, u nichž můžeme kontrolovat, kdo nás při nich bude sledovat, znamenalo by to, že do něj nespadají činnosti, u nichž sledování kontrolovat nemůžeme. Co když je někdo sledován, aniž by o tom věděl? Co když jsou o někom sbírány informace bez jeho vědomí a souhlasu? Navíc, neudělení souhlasu s přístupem ještě neznamená, že dané informace o osobě nemohou být zjištěny z jiných zdrojů. Člověk tedy může mít pocit kontroly, a přesto došlo k narušení jeho soukromí. Na druhou stranu vězeň na samotce nad svým soukromím kontrolu nemá, ale nelze tvrdit, že by soukromí v určité míře neměl. Stejně tak, pokud se vrátíme k příkladu Charlese Frieda s trosečníkem na pustém ostrově. Nevybral si to, nemůže kontrolovat, zda jej někdo sleduje nebo ne, protože tam zkrátka nikdo není, ale dle mého tvrdit, že nemá soukromí, je zde tou opravdovou ironií. Reiman [5, 30-31] upozorňuje na nutnost oprostit soukromí od podmínky kontroly a ke stejnému názoru

dochází i Ruth Gavison [7, 427] s velmi přesvědčivým argumentem. Podle ní, pokud se na soukromí díváme z aspektu podmínky kontroly, by to naznačovalo mít možnost si soukromí zvolit, a že tato volba bude respektována. Což samozřejmě takto nefunguje ani v demokratických státech, jelikož právo na soukromí není neomezené a jsou určité zákonné výjimky, kdy může být porušeno, nemluvě o totalitních státech nebo totálních institucích [8, 52].

Když se vrátíme zpět k definicím, tou pravděpodobně nejvýmluvnější je definice Judith Wagner DeCew [9, 62], podle níž je soukromím oblast, do které zákonitě nikomu nic není. Řada autorů popisuje soukromí výhradně jako množství informací známých o někom. Jsou to například A. Miller, Beardsley a Gross [7, 429]. Profesor Gerety [10, 19] tuto myšlenku ještě zužuje pouze na soukromé informace spojené s intimitou, identitou a autonomií.

Nyní se od obecného pojmu soukromí přesuneme k jeho informační sféře. Mohlo by se zdát, že informační soukromí je fenomén několika posledních let, kdy docházelo (a stále dochází) k nárůstu vlivu sociálních sítí, počtu jejich uživatelů a obecně komunikace přes internet. Ve skutečnosti je starší než internet sám a už od šedesátých let minulého století čím dál více roste zájem o jeho ochranu a ochranu dat [11, 487]. V literatuře se také můžeme setkat s označením „datové soukromí“ ve smyslu informačního soukromí, a to z toho důvodu, že někteří autoři považují slovo „informační“ za zavádějící a svádějící k chybné domněnce, že se vždy musí jednat o smysluplná data nebo data s jasným významem [11, 568]. Ve všech případech, kdy je zde řeč o informacích, jsou tím myšleny informace osobního rázu, fakta o osobě, jejichž zveřejnění by mělo být v režii pouze daného jedince. Například bydliště, kontaktní údaje, příjmy, zdravotní stav, medikace, nebo volební preference.

Zřejmě nejvýstižněji popsal informační soukromí Alan Westin ve své práci z roku 2003 [12, 431], kde soukromí definoval jako oprávnění jedince určit kdy, jakým způsobem a které informace týkající se jeho osoby budou známy ostatním. Z této definice vychází i Koops a rozšiřuje ji o zájem zabránit sbírání těchto informací [11, 568]. Ve světle toho, kolik informací je o uživatelích sbíráno a následně výhodně prodáváno korporacím, užíváno pro cílený marketing, ovlivnění politického smýšlení a k dalším účelům, je jasné, jak zásadní je Koopsův dodatek. Lidé by měli mít možnost rozhodnout, zda a jakým způsobem bude s jejich informacemi nakládáno. A to je základní premisa informačního soukromí.

1.2 Kategorie soukromí

Stejně jako se různí definice soukromí, vzniklo také mnoho různých typologií a taxonomií. Například Alan Westin [11, 496] v šedesátých letech představil čtyři základní druhy soukromí zaměřené na individuální prožívání každodenního života: samota, intimita, anonymita a rezervovanost. Každá z těchto sfér představuje odlišnou míru sdílení osobních informací a prožitků jedincem s jeho okolím. Samota je v pomyslném

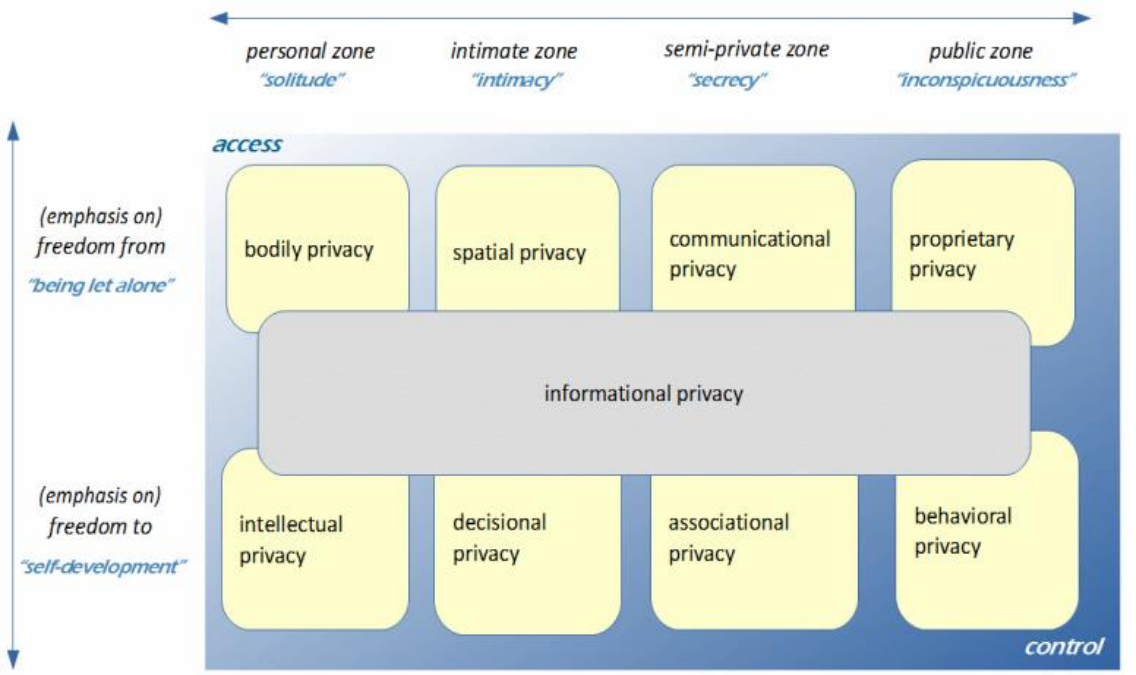
žebříčku nejvýše, člověk je sám jen se svými myšlenkami a vědomím, vyšší míry soukromí již nemůže dosáhnout. Intimita je ve Westinově pojetí rozsáhlejší, než jak ji běžně vnímáme. Týká se utváření blízkých vztahů mezi dvěma osobami nebo v malé skupině, tedy nejen mezi partnery, ale i členy rodiny, přáteli a spolupracovníky. V anonymitě se člověk nachází, pokud na veřejném místě není identifikován a soustavně sledován a touží po tom, čemu Westin říká „public privacy." Poslední sférou je rezervovanost a spočívá ve vlastním svobodném rozhodnutí jedince, jaké informace o sobě poskytne svému okolí nebo naopak odepře. Jde o vytváření psychologické bariéry, která brání zásahům do soukromí. Zároveň se jedná o sféru, do níž spadá informační soukromí [13, 29].

O třicet let později přišel Roger Clark s kategoriemi, které více reagují na současné požadavky na soukromí spojené s technologickým vývojem [11, 497]. Jeho přístup je založen na Maslowově pyramidě potřeb, kdy každou z nich přetvořil na potřebu spojenou se soukromím: osobní soukromí, soukromí jednání, soukromí komunikace, soukromí osobních dat a soukromí osobního prožitku/zkušenosti, kterou k ostatním zařadil až v roce 2013 s ohledem na další technologický vývoj a jeho dopad na soukromí [14]. V kontextu této práce je relevantní předposlední ze zmiňovaných. Kategorie soukromí osobních dat se u Clarka již velmi přibližuje dnešnímu konceptu informačního soukromí, ačkoliv zde jde spíše o ochranu obsahu komunikace, a ne komunikace jako takové, kterou Clark spojuje s informačním soukromím [11, 499]. Stále aktuálnější ochrana osobních údajů spadá do této úrovně také.

Odlišný přístup zvolila Anita L. Allen. V textu Unpopular Privacy [15] z roku 2011 vyjmenovává nemalé množství kategorií, které se navzájem překrývají nebo jsou „hybridní". V porovnání s ostatními autory do problematiky vnáší více právní a feministický úhel pohledu. U informačního soukromí, spíše než definici, uvádí situace, kdy je narušeno. Jedná se o případy odhalení nebo de-anonymizace dat, faktů nebo konverzací, u nichž si to jedinec nepřeje.

Nejvíce však dle mého mezi zmiňovanými vyčnívá práce Petera Bloka [11, 554], který nestaví informační soukromí vedle ostatních typů, ale pohlíží na něj jako na druhou stranu mince, jako na nedílnou součást každého fyzického typu soukromí, jelikož informační složku od nich nelze oddělit a je třeba ji chránit. S tímto argumentem souhlasí i Koops a dodává, že je třeba od sebe jasně odlišovat informační soukromí ve vztahu k osobním datům a fyzické soukromí v jeho širším smyslu [11, 555]. I on se k informačnímu soukromí ve své typologii postavil podobně a představil dvoudimenzionální model, kde se informační soukromí dotýká všech hlavních typů soukromí [11, 569], jak demonstruje obrázek 1-1 níže. Tyto ideální typy, jak je Koops nazývá, pokrývají základní druhy soukromí zmiňované v jiných odborných pracích, ale v žádném případě nemají představovat jediné formy, kterých může soukromí nabývat. Jsou jimi soukromí tělesné, prostorové, komunikační, majetkové, intelektuální, rozhodovací, sdružovací a chování, z nichž každé spadá do překryvu dvou zón. Ve směru

horizontální osy jsou umístěny zóny života jedince od osobní, přes intimní a polo-osobní až po veřejnou a na vertikální ose pak aspekty svobody, kterými jsou být nechán o samotě a osobní rozvoj [11, 566-567]. Dle mého názoru tato typologie nejlépe ukazuje propojení mezi informačním soukromím a ostatními aspekty každodenního života, tedy že nejde jen o další druh, ale o nedílnou součást všech typů soukromí a je proto nutné na něj tak nahlížet.



1-1 Typologie soukromí, převzato z Typology of Privacy, Koops

Tento výčet rozhodně není konečný, rozebírání dalších klasifikací je však nad rámec tohoto textu.

1.3 Hodnota soukromí a jeho ochrana

Na rozdíl od neshod ohledně toho, co vlastně soukromí představuje, je vědecká obec za jedno v nepopiratelné hodnotě jeho informační složky pro lidskou společnost a udržování mezilidských vztahů. Jak píše Charles Fried [16, 142], aby mezi lidmi mohl vzniknout intimní (přátelský nebo partnerský) vztah, musí spolu sdílet osobní informace, které nesdílejí se všemi, a tudíž je soukromí předpokladem a nutností pro tento vztah.

Například Reiman na soukromí pohlíží jako na velmi komplikovaný sociální rituál [1, 39-40], jehož nezbytnost spočívá ve vytváření sebe sama jako osobnosti. Své tvrzení podepírá studií Ervinga Goffmana, autora sociologického termínu totální instituce. Goffman ve své práci "On the Characteristics of Total Institutions“ poukazuje na to, jak je soukromí klíčové pro zachovávání lidské důstojnosti, a že jeho eliminace vede až

k naprostému pokoření a zlomení jedince [1, 40]. Z tohoto důvodu Reiman pokládá za nutné, aby všichni měli na své soukromí právo, a toto právo bylo chráněno [1, 41].

Další argument pro nutnost ochrany soukromí poskytuje Jeffery L. Johnson [17, 4], který nabízí více praktický pohled. Pokud čistě soukromé informace, jako je zůstatek na účtu, náboženské přesvědčení nebo menšinová sexuální orientace, už nebudou soukromé, tak již nejde o to, že tyto informace veřejnost má, ale jak se zachová. Možné odsouzení společností a diskriminace je důvod, proč by nás narušení soukromí mělo trápit. Stanley I. Benn [18, 226] zachází dokonce ještě dále, když uvádí možné zneužití soukromých informací pro účely vydírání, pronásledování nebo v rukou vlády tyranského režimu. Nutnost soukromí chránit je tedy nepopiratelná a zřejmě nejlépe ji vyjadřuje právě Benn ve své práci Privacy, Freedom, and Respect for Persons: *„The more one knows about a person, the greater one's power to damage him."*

Kromě výše uvedených následků stojí za zmínku také tzv. chilling effect, který uvádí ztrátu soukromí do souvislosti se ztrátou svobody jako takové. Pokud víme, že jsme sledováni a že naše chování by mohlo být považováno za nekonvenční, bude naše chování jiné, než by bylo v soukromí. Ze strachu z odsouzení a odmítnutí je tedy de facto omezena naše svoboda [5, 35].

Pro ucelenost argumentů je třeba poznamenat, že ve prospěch nezbytnosti soukromí mluví podle některých autorů i evoluce. Bruce Schneier na základě výroků biologa Petera Wattse formuloval myšlenku, že sledování v lidech vyvolává pocit kořisti [19, 127]. Z tohoto všeho je tedy jasné, jak je soukromí pro člověka důležité, ale jakou hodnotu představuje pro firmy, jež jsou ochotny za osobní informace platit, už není tak příjemné téma.

V současné ekonomice, kdy se vše dá ocenit, mají i osobní informace svou cenu. Profilování uživatelů je zcela běžné a děje se tak mnohdy, aniž by si to lidé uvědomovali. Je to legální? Ano. Je to morální? To už je diskutabilnější téma. Kdykoliv však uživatel přijme cookies a povolí na stránce sledovače třetích stran, dává k tomuto profilování své svolení. Osobní informace se tak staly artiklem, který vyměňujeme za služby, které jsou poskytovány „zdarma“. Gianclaudio Malgieri a Bart Custers [20, 9-11] uvádějí, že obecná informace jako věk nebo bydliště stojí v přepočtu přibližně 0,01 Kč. Čím jsou však data citlivější anebo pro potenciální kupující firmy poplatnější a mohou je tedy využít v obchodní strategii, tím více stoupá jejich cena. V praxi není obchodováno s jednotlivými kusými informacemi, ale s celými datasety, které o daných uživatelích již mají komplexnější vypovídací hodnotu a velikost, kompletnost a aktuálnost datasetu pak určuje jeho cenu. Zde se objevuje hlavní problém. Kompletní a přesný dataset představuje sbírku digitálních identit, u nichž se nedá mluvit o pseudonymitě a je možné je vystopovat. V tomto případě tak přímo souvisejí se soukromím daných osob [20, 11-18], které je jako jedno ze základních lidských práv nezcizitelné, nepromlčitelné a nezrušitelné a jako takové je právně chráněno.

1.3.1 Právní úprava soukromí

Termín „soukromí“ v kontextu ochrany soukromí zahrnuje nejen podstatu toho, co soukromí je, a jak by mělo být ceněno, ale také právo na soukromí, které definuje způsoby jeho právní ochrany [11, 491]. Jedná se tedy o oddělené pojmy, které by mezi sebou neměly být zaměňovány, ačkoliv spolu úzce souvisejí. Z hlediska historického vývoje z pohledu práva bylo soukromí vždy spojováno s jednotlivci, s respektováním soukromého života a právem žít dle vlastního přání beze strachu ze sledování, kontroly a odcizení od společnosti [11, 493]. Je tudíž logické, že právo na soukromí, které se poprvé jako pojem objevilo už ke konci 19. století v článku The Right to Privacy [21] autorů Warrena a Brandeise, staví na těchto základních konceptech soukromí, spolu s dalšími, jako je svoboda, individualita, osobnost a lidská důstojnost. Podobu ústavně chráněného práva však právo na soukromí dostalo až o mnoho let později [11, 793].

Tato práce se zaměřuje na současnou situaci v České republice a zohledňuje tedy jen právní úpravy k ní poplatné. Tou nejdůležitější je Evropská úmluva o ochraně lidských práv z roku 1950, kde se v článku 8 odstavci 1 praví: *„Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence* [22].“ Konkrétní výklady pojmů soukromý a rodinný život jsou ve velké míře dány soudy, především pak Evropským soudem pro lidská práva. Z právních úprav v mezinárodním prostředí je pak třeba zmínit i Článek 12 Všeobecné deklarace lidských práv: *„Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“* A nakonec na domácí půdě formulaci Listiny základních práv a svobod Článek 7 odstavec 1: *„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“*

Zásadní je pak v souvislosti s informačním soukromím právo na informační sebeurčení, které je garantováno Článkem 10 odstavcem 3 Listiny: *„Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“* Toto právo zajišťuje možnost svobodně se rozhodnout, jakým způsobem, v jaké míře, za jakých okolností a jaké informace bude o své osobě jedinec sdělovat svému okolí. Důležitost tohoto práva podpírá výrok Ústavního soudu v Data retention nálezu I., kde formuloval nezbytnost práva na informační sebeurčení nejen jako nástroje pro osobní rozvoj a seberealizaci, ale hlavně jako podmínku svobodného a demokratického komunikačního řádu [23].

Ve všech zmiňovaných ustanoveních je soukromí hojně skloňovaným pojmem, ale co je pod ním přesně myšleno, se tu už nedočteme. Je to dáno tím, že ať už se jedná o české nebo evropské právní úpravy, jsou práva týkající se soukromí formulována jako ochrana soukromého a rodinného života a konkrétní výklad je ponechán v rukou soudů, které pak mají ve vymezování soukromí hlavní slovo. Například v Evropské úmluvě o ochraně lidských práv nenalezneme formulace, co znamená právo na svobodu, na ochranu lidské důstojnosti a právo na sebeurčení. Jelikož je samotné soukromí v různých členských

státech zakořeněno odlišně, je rozhodující, jak se k tomu postaví příslušné soudy. Ku příkladu Evropský soud pro lidská práva zahrnul pod pojem soukromý život mimo jiné i formování mezilidských vztahů [24, 9-11].

1.3.2 Technické nástroje ochrany soukromí

Ochrana soukromí se v závislosti na pádivém vývoji technologií ukazuje být čím dál více důležitější, a proto je znepokojivé, jak je mnohdy komplikované své soukromí před zvědavýma očima všech sledovačů a cookies uchránit. Následující nástroje pro zmírnění zásahů do soukromí a potažmo zvýšení bezpečnosti na internetu jsou vhodné a dostačující pro potřeby běžného uživatele. Pokročilejším metodám zohledňující problematiku otisku prohlížeče je věnována kapitola 2.5 OPSEC.

Vše začíná a končí u bezpečných hesel. Nelze dostatečně zdůraznit, jak je pro soukromí nezbytné používat unikátní heslo splňující předpoklady pro bezpečnost pro každý účet. Obecně platí, že pokud si heslo dokážeme zapamatovat, není dostatečně bezpečné. Je proto doporučované využívat správců hesel, které dokážou generovat spolehlivá a silná hesla podle zadaných kritérií.

Během vyhledávání na internetu toho o sobě uživatel díky sledovačům může prozradit poměrně hodně a vyhledávače jako Google nebo Bing jsou známé tím, že tyto informace sbírají. Google navíc patří ke společnostem, které v minulosti postihly skandály v souvislosti se soukromím jejich uživatelů a slovy Edwarda Snowdena se jedná o nebezpečnou službu právě co se soukromí týče [25]. Náhradu poskytuje vyhledávač duckduckgo, který uživatelské soukromí respektuje a žádná data nesbírá. V případě volby samotného prohlížeče se ukazuje jako nejlepší možnost [26] Mozilla Firefox z hlediska nastavení míry soukromí.

Dále je vhodné instalovat rozšíření prohlížeče pro blokaci sledovačů jako je Privacy Badger, blokaci reklamních prvků uBlock Origin a nástroj pro kontrolu přístupu pouze k zabezpečeným webovým stránkám HTTPS Everywhere, který dokáže upozornit, pokud stránka používá nešifrovanou verzi HTTP.

K tomuto tématu by se dalo napsat mnohem více, bylo by to však nad rámec rozsahu práce a došlo by k odklonění od jejího hlavního cíle. Případné zájemce je možné odkázat na stránku Michaela Bazzella [27], jenž se ochraně soukromí a bezpečnosti věnuje ve své profesionální praxi.

2. OSINT

Open source intelligence neboli OSINT je proces spočívající v získávání informací z veřejně dostupných zdrojů legálními prostředky, jejich analýze a následném rozšiřování a třídění, kdy je hodnocena jejich relevantnost [28, 53]. Pojem „veřejně dostupné zdroje“ je zde zcela klíčový. Znamená to, že daná informace musí být přístupná kdykoliv, komukoliv a odkudkoliv [29, 1]. Zaheslované databáze, soukromé zprávy, nelegálně uniklá data nebo cracknuté uživatelské účty tedy do problematiky OSINT nespadají. Celý proces se musí odehrávat zcela v mezích platných zákonů dané země.

2.1 Vznik a vývoj

Poprvé se tento pojem objevil v 80. letech 20. století jako odpověď armády Spojených států na dynamicky se měnící požadavky na informace nezbytné pro plánování taktiky na bitevním poli [28, 54]. Historie OSINT však ve skutečnosti sahá až k roku 1939, kdy na popud vlády vytvořila britská stanice BBC (British Broadcasting Corporation) úřad pro zkoumání zahraničního tisku a rádiového vysílání, který funguje dodnes pod jménem BBC Monitoring. K dalšímu progresivnímu vývoji v této oblasti došlo za Studené války a to na obou stranách Železné opony. Stephen Mercado, analytik CIA, uvádí, že v této době se veřejně dostupné informace staly hlavním zdrojem pro určení vojenských dispozic nepřítele a pro předpověď možných hrozeb [28, 53]. Do podoby, která se již blíží dnešnímu chápání, byl OSINT vymezen v návrhu zákona Intelligence Reorganization Act amerického senátu z roku 1992. Mimo jiné jsou zde definovány jeho klíčové vlastnosti, tedy poskytování informací oproštěných od předsudků a zaujetí a získaných ze všech zdrojů, ať už veřejně dostupných nebo nikoliv [28, 54].

Od té doby se OSINT značně vyvinul a rozšířil i do nevojenských organizací, ale především se již zaměřuje pouze na legální veřejné zdroje informací, které jsou dostupné bez nutnosti za ně platit [30]. Těmi jsou v dnešní době hlavně internetové zdroje jako články, blogy, webové stránky, veřejné vládní dokumenty, sociální sítě, diskuzní fóra a metadata s nimi spojená. Není to však pravidlem, stejně tak je možné hledat informace v novinách a časopisech, v publikacích ve veřejné knihovně, nebo například na tiskové konferenci. Podobně, jako nezáleží na tom, odkud jsou informace získány (za předpokladu, že jsou dodrženy výše uvedené podmínky zákonnosti a volné dostupnosti), může být také jejich forma různorodá. Nemusí se jednat jen o text, stejně dobře je možné získávat informace z obrázků, videí, webinářů, map, rozhovorů nebo podcastů [30] [31].

2.2 Uplatnění

Jak již bylo zmíněno výše, OSINT dávno není výsadní záležitostí armády a zpravodajských služeb. Své uplatnění nachází při vyšetřování po pohřešovaných osobách, v boji s organizovaným zločinem a teroristickými buňkami, v oblasti kyberbezpečnosti,

lidských práv a v investigativní žurnalistice [32, 3]. Je také první fází každého cíleného útoku nebo penetračního testu [31]. Dále je třeba zmínit, že existuje početná skupina lidí na celém světě, kteří mají OSINT jako zálibu a tráví jím velkou část svého volného času. Jsou to lidé různých profesí, které spojuje zájem o geopolitiku, válečné konflikty, povstání a celkově aktuální dění.

Nezaleží na tom, zda je cílem jedna osoba, skupina nebo organizace, OSINT lze využít k profilování prakticky jakéhokoliv objektu zájmu. Dle získaných údajů je pak možno sestavit model hrozby, charakteristiku cíle a odhalit jeho zranitelnosti pro následné naplánování útoku, nebo alespoň zúžit oblast pro další pátrání. Je přitom kritické, aby celý proces probíhal opatrně, bez přímého kontaktování cíle a „potichu“. To znamená, že je nutné používat pouze nástroje, které jej neupozorní na sledování a sbírání informací [31]. Zároveň je však neméně důležité se během celého vyšetřování pohybovat v mezích zákonů příslušné země a vyvarovat se postupů nebo taktik, které by se daly obecně považovat za nemorální [33]. Také je třeba být diskrétní a dodržovat etické zásady vzhledem k objektu zájmu. Během profilování cíle je totiž možné narazit na informace velice osobního rázu, jako je náboženské přesvědčení nebo sexuální orientace, které by v případě zveřejnění mohly vést k šikaně nebo ublížení na zdraví [29, 2].

V současnosti je OSINT využíván hlavně v těchto třech oblastech:

1. společenské mínění a analýza názorů/postojů,
2. kyberkriminalita a organizovaný zločin,
3. kyberbezpečnost a kyberobrana.

Do první kategorie spadá sběr informací o uživatelích především ze sociálních sítí a to pro účely marketingu, politických kampaní, žurnalistiky a hledání potenciálních zaměstnanců HR odděleními nebo firmami. Relevantní jsou v tomto případě veškeré interakce uživatelů od příspěvků, reakcí, až po to, jaké mají preference a jaké účty sledují. Druhá kategorie se zabývá odhalením možné kriminální činnosti už v jejím počátku prostřednictvím analýzy veřejně dostupných dat. Je tak například možné sledovat aktivity teroristických organizací [29, 1] a extremistických skupin. Posledně jmenované jsou až překvapivě aktivní na sociálních sítích na dark webu (existuje zde i dark verze Facebooku), kde mají i své webové stránky. S rostoucím množstvím nelegálních aktivit v této části internetu se zvyšuje naléhavost zaměřit pozornost během vyšetřování i do těchto temných a mnohdy děsivých míst [34]. Třetí kategorie se zaměřuje na ochranu proti útokům na dostupnost služeb na internetu (Distributed Denial-of-Service Attack, neboli DDoS útok) a na zavádění preventivních opatření ve firmách a organizacích. Každodenní analýzy útoků pak pomáhají při rozhodování o obraně a urychlují reakce na útoky. Při zpětném vyšetřování takového incidentu dokáže OSINT poskytnout požadované informace a v kombinaci s digitální forenzní analýzou lze dohledat potřebné důkazy pro trestní stíhání [29, 2].

2.3 Postup

Postup OSINT vyšetřování se odvíjí v závislosti na organizaci a druhu cíle. Je zřejmé, že pátrání po zmizelé osobě se bude lišit od pátrání po pachateli trestného činu, jehož identitu neznáme. Nicméně jádro celého procesu zůstává stále stejné. Například model CIA obsahuje tyto kroky: plánování a nasměrování, shromažďování, zpracování, analýza a produkce, a rozšiřování. V knize Handbook of Intelligence Studies je uveden následující postup: shromažďování, zpracování, analýza a produkce, klasifikace, rozšiřování [35, 12]. Cílem této práce není dopodrobna představit celý proces tak, jak je v praxi realizován. Pozornost bude detailněji zaměřena pouze na fázi získávání informací a popis metod a nástrojů, které je k tomu možné využít. Ostatní kroky budou tedy pro ucelený obraz jen nastíněny. Na obrázku 2-1 je zobrazen celý průběh operačního cyklu.

2-1 Operační cyklus OSINT

Prvním krokem cyklu je plánování a nasměrování, kdy si vyšetřovatel musí položit čtyři základní otázky: co chce zjistit, jaké nástroje bude potřebovat, jak technicky způsobilý cíl je, a co má být výsledkem celého snažení. Odpověď na první otázku pomáhá držet vyšetřování v jasně vytyčených liniích a je tak eliminována tendence k hlubšímu zabředávání do informací, které nejsou relevantní. Volba nástrojů se odvíjí od typu cíle a od znalosti nebo předpokladů, na jakých sociálních sítích se zdržuje, jaké služby a technologie používá. S tím úzce souvisí volba, jaké uživatelské účty pod falešnou identitou (označovanou jako sock puppet) je nutné pro účely vyšetřování vytvořit. Určení technické způsobilosti cíle slouží k odhadnutí, jakých možných chyb se může dopustit a také definování modelu hrozby. Obecně je vždy lepší předpokládat o něco vyšší technickou způsobilost a podle toho se patřičně připravit, než cíl podcenit a riskovat

prozrazení. Zodpovězení poslední otázky, tedy co má být výsledkem, je mantinelem celého vyšetřování a rozhodujícím prvkem, kdykoliv se během kterékoliv fáze objeví potřeba rozhodnout, kterým směrem se dále vydat. Podcenění této přípravné fáze plánování a nasměrování může vést ke zdržení a v nejhorším případě se vyšetřování zasekne na mrtvém bodě nebo bude úplně zmařeno z důvodu kompromitace [36].

Druhým krokem je shromažďování informací souvisejících s cílem z veřejně dostupných zdrojů. Za použití technik a nejrůznějších nástrojů (popsáno v kapitole 3.4) dochází k rozšiřování datasetu o cíli a takto získané nové informace jsou dále použity jako vstupní data pro další vyhledávání [29, 5]. Této fázi je věnováno značné úsilí a velká časová dotace, protože od získaných informací se odvíjí celé další vyšetřování a analýza vytvořená na základě neúplných dat může být zavádějící a nepřesná a postrádat důležitá fakta. Aby tato část procesu byla efektivní, je dobré dodržovat několik zásad [37]. Zřejmě nejdůležitější zásadou je informace nejdříve posbírat a analyzovat je až později. Je to z toho důvodu, že některé příspěvky, články a podobně, které cíl publikuje, se mohou postupem času stát nedostupnými. Obecně je lepší mít více irelevantních informací, než nějakou důležitou opomenout. Druhou zásadou je začít vyhledávání spíše obecněji a zeširoka a až poté přidávat více specifická klíčová slova a výsledky zužovat postupně podle potřeby. Tím je omezen falešně negativní dojem, který by mohl vzniknout příliš konkrétními vstupy do vyhledávačů. Za třetí, nastavit si ve službách notifikace, které podle stanoveného filtru upozorní, že se objevila nová data nebo byla ta stávající změněna. To je užitečné zvláště v případě, kdy je předmětem vyšetřování probíhající událost a nové informace se vynořují postupně a jsou rovnou zpracovány a analyzovány. Čtvrtou zásadou je provádět pečlivou dokumentaci, kde a jak byla která informace získána, a to pro možné budoucí potřeby ze strany vedení nebo státních činitelů. A nakonec, nepoužívat vlastní soukromé účty pro účely OSINT. Ve chvíli, kdy se tak stane, je možné díky otisku prohlížeče (většina vyšetřovatelů má velmi unikátní otisk díky doplňkům, které běžní uživatelé nepoužívají) a datům, které různé služby sbírají, propojit všechny osobní účty a dostat se až k fyzické osobě, která za nimi stojí [37]. Tato poslední zásada spadá do problematiky OPSEC, která je více popsána v kapitole 3.5. Obecně sběr informací není jednorázovou záležitostí. V průběhu dalších fází mohou vyvstat nové otázky nebo potřeba některé věci upřesnit a cyklus tak začíná nanovo [37].

Třetím krokem je zpracování posbíraných informací pro účely analýzy tak, aby byly čitelné pro analytika. To zahrnuje dešifrování, dekódování, přepis videa a audia a překlad, pokud jsou informace v cizím jazyce. Následně je potřeba vyfiltrovat vše, co je pro vyšetřování nepodstatné a užitečná data logicky seskupit podle toho, jak spolu souvisejí nebo z nich vytvořit tabulku. Tu je poté možné využít jako vstup do některých vizualizačních nástrojů jako je Maltego, které je přiblíženo v kapitole 2.4.2. Vyřazené informace musí zůstat i nadále dostupné, kdyby v průběhu analýzy vyvstaly nějaké otázky nebo bylo potřeba ověřit překlad. Dále je vhodné vytvořit časovou osu

ze získaných informací k ujasnění, v jakém sledu k událostem došlo a k odhadnutí, kdy se odehrály události, u nichž jsou tyto údaje neznámé [38].

Čtvrtým krokem je analýza a produkce, kdy je zpracovaným informacím dán konkrétní význam pro vyšetřování. Výstupem této fáze je protokol nebo hlášení, které obsahuje objevené spojitosti, vzorce a trendy, často zobrazené v grafech nebo jinak vizuálně, a jsou doporučeny další postupy. Zároveň jsou zde zahrnuty odpovědi jednak na otázky stanovené během plánování a jednak na ty, jenž mohly vyvstat v průběhu. Pokud některé odpovědi nebylo možné získat, je to do protokolu zaneseno také, společně s uvedením dalších nejasností nebo trhlin v informacích. Všechna dokumentovaná data musí být zhodnocena z hlediska platnosti, důvěryhodnosti zdroje a jeho možné zaujatosti. Poslední zmíněné kritérium platí i pro vyšetřovatele/analytika, který nesmí být žádným způsobem zaujatý vůči cíli, ať už pozitivně nebo negativně, a nesmí upřednostňovat informace korespondující s jeho přesvědčením. Také je nutné brát na vědomí existenci desinformačních kampaní a možnost, že jimi vyprodukovaná data se mohla objevit ve zpracovaných informacích [39].

Pátým krokem je rozšiřování. Protokol, jenž byl výstupem analýzy a produkce, je předán patřičným autoritám, na jejichž popud vyšetřování začalo, a ty na jeho základě rozhodnou o dalším postupu. Tím může být i další hledání informací a rozšíření datasetu o cíli [40]. V tom případě pak protokol poslouží jako vstupní data, kruh se uzavírá a operační cyklus začíná nanovo.

2.4 Techniky a nástroje

V prostředí OSINT a kyberbezpečnosti jsou jako techniky označovány metody a postupy používané v procesu sběru informací k maximalizaci zisku užitečných dat, z nichž by později bylo možné vyvodit znalosti a konkrétní závěry. Jejich výběr závisí na druhu cíle a vyšetřovatel si musí položit otázky, co je jeho hlavním úkolem, jaká data hledá a jakým způsobem bude vyšetřování provádět. V závislosti na odpovědích je pak schopný určit nejvhodnější techniky k dosažení stanovených cílů.

Mezi nejpoužívanější techniky patří pravidelná kontrola výsledků vyhledávání na co nejvíce vyhledávacích platformách, sledování osobních blogů a stránek společností, určení používaných sociálních sítí a jejich prostřednictvím zajištění multimediálních dat, sběr telefonních čísel a emailových adres, pracovní pozice cíle a software, který sám nebo daná společnost používá, prohledávání starých dat uložených v cache Google nebo třeba používání map a satelitních snímků pro propojení geografických pozic cíle s dalšími skutečnostmi [30].

Nástroje slouží k rychlejšímu a snadnějšímu hledání potřebných informací. Spadají sem skripty, aplikace a rozšíření webových prohlížečů. Jejich množství je nepřeberné, orientovat se ve všech nemožné a stále přibývají nové a nové. S tím však souvisí jasné riziko: jsou všechny nástroje bezpečné? Odpověď není překvapivá, nejsou. A ty, které bezpečné jsou, jimi nemusí být navždy. Je proto důležité každý nový nástroj otestovat v

čistém virtuálním prostředí, kde nemůže napáchat škodu a například nás kompromitovat, „volat domů“ nebo jinak ohrozit probíhající vyšetřování [32, 3].

Odrazovým bodem mohou být sbírky nástrojů vytvořené odborníky, kteří se v této oblasti pohybují delší dobu, například OSINT Framework, jehož autorem je Justin Nordine [31]. Jedná se o strukturu nezpoplatněných nástrojů rozdělených podle zaměření na požadované výstupní informace, například záložka Email Address obsahuje nástroje pro vyhledávání emailů, ověření jejich platnosti, uniklých dat a vyhledávání v databázi emailů umístěných na blacklistu. Ne všechny nástroje jsou však v současnosti funkční, a to nejen v této struktuře. Obecně nelze zaručit, že nástroj, který použijeme dnes, budeme moci použít i zítra. Další užitečnou sbírkou je Kali Tools. Ta v sekci Information Gathering obsahuje veškeré dostupné nástroje přímo použitelné v Kali Linux a návody s příklady k jejich použití [31]. Ale zřejmě nejvíce vyčerpávajícím zdrojem je pravidelně aktualizovaná publikace švýcarské společnosti i-intelligence „Open Source Intelligence Tools and Resources Handbook“ [32], kde na více než pěti stech stranách (edice z roku 2020) nalezneme odkazy k nástrojům, které jsou k danému datu zveřejnění příručky funkční a prověřené (i když opatrnost je vždy na místě).

Výběr nástroje přímo souvisí s kvalitou a relevancí návratových hodnot a může být rozhodující pro to, zda jsou sbírány ty správné informace [32, 3]. Stejně jako není vhodné se omezovat pouze na jeden vyhledávač, protože různé vyhledávače zobrazují různé výsledky díky rozdílným algoritmům, bylo by neefektivní používat jen jeden nástroj pro daný typ hledané informace. Větší množství nástrojů znamená flexibilnější vyšetřování [32, 3].

2.4.1 Google Dorks

Google Dorks, také nazýváno jako Google hacking, je označení pro pokročilé vyhledávání za pomoci definovaných příkazů prostřednictvím vyhledávače Google. Tato technika využívá skutečnosti, že téměř každá část každé webové stránky je indexována, aniž by si toho její uživatelé museli být nutně vědomi, a tudíž lze dohledat teoreticky cokoliv. Výjimkou z tohoto pravidla jsou stránky, které administrátor daného webu zahrne do souboru robots.txt, čímž vyhledávačům sdělí, aby je neindexovali [41]. V praxi se však často stává, že je tento krok opomenut.

Nejpoužívanější příkazy, příklady jejich použití a výsledek vyhledávaného dotazu jsou zobrazeny následující tabulce 2-1.

Příkaz	Příklad použití	Výsledek
„“	„vysoké učení technické“	stránky, které obsahují přesně danou frázi
+	informační + bezpečnost	stránky, které obsahují daná dvě (a více) slova, ne nutně jako frázi
-	informační -bezpečnost	stránky, které obsahuje slovo

		informační, ale neobsahují slovo bezpečnost
|	informační | bezpečnost	stránky, které obsahují slovo informační nebo bezpečnost nebo oboje
*	jak naprogramovat *	zástupný znak, který znamená „cokoliv“
intitle:	intitle:VUT	stránky, v nichž je VUT obsaženo v názvu
inposttitle:	inposttitle:VUT	články a blogy, kde se VUT objevuje v názvu
inurl:	inurl:vutbr.cz	stránky, v nichž je vutbr.cz obsaženo v url adrese
allinurl:	allinurl: kontaktni informace	podobné jako inurl, ale pro více slov
intext:	intext:vutbr.cz	stránky, které mají někde v textech vutbr.cz
site:	site:vutbr.cz	všechny stránky spadající pod doménu vutbr.cz
	site:vutbr.cz aktuality	stránky spadající pod doménu vutbr.cz, v nichž se vyskytuje slovo aktuality
	site:*.vutbr.cz	vyhledá subdomény pod vutbr.cz
related:	related:vutbr.cz	stránky, které jsou podobné zadanému webu
info:	info:vutbr.cz	informace o dané stránce
filetype:	filetype:pdf	omezí výsledky hledání na daný typ souboru, lze hledat i více typů zároveň oddělením slov pomocí |
	filetype:pdf „The Prince“	vyhledá pdf The Prince
allintext:	allintext:kontakt	vyhledá kontakt v textu stránek (vynechá výsledky, kde je kontakt v linku a v nadpisu)
cache:	cache:vutbr.cz	cache kopie stránky, kterou má Google uloženou
link:	link:vutbr.cz	všechny linky, které vedou na vutbr.cz
intitle:"index of" inurl:ftp		všechny veřejné FTP servery
filetype:xls		excel soubory se seznamy emailů

inurl:"email.xls"		

2-1 Nejpoužívanější příkazy Google Dorks

2.4.2 Nejpoužívanější nástroje

Jak již bylo řečeno, množství dostupných nástrojů je obrovské a neustále narůstá. Na druhou stranu stejně tak dochází k jejich stahování z internetu, zablokování nebo nefunkčnosti z důvodu umístění captchy na prvky, na kterých jsou závislé. Následující nástroje by se v neustále se měnícím a vyvíjejícím světě OSINT daly považovat za jakési opěrné body a stálice, pravděpodobně každý vyšetřovatel se s nimi setkal a odkazy na tyto programy nalezneme ve většině článků věnující se této problematice.

Maltego představuje účinný nástroj pro data mining a sběr informací. To může být realizováno z veřejných zdrojů, z dat poskytnutých od partnerů Maltego Technologies a z vlastních vložených dat uživatele. Ze získaných dat dokáže automaticky vytvářet grafy podle souvislostí a obsahuje rozsáhlou knihovnu pluginů pro účely testování. Základní verze je dostupná ke stažení pod open source licencí [42].

Konzolová aplikace **Metagoofil** slouží k získání metadat z veřejných dokumentů. Na základě zadaných parametrů, jako je doména, typ souboru, a další, stáhne veškeré nalezené dokumenty a vrátí seznam uživatelských jmen, verzi softwaru a názvy serverů [43].

Recon-ng je dalším z nástrojů pro sběr informací a nalezneme jej předinstalovaný v Kali Linux. Skrze tzv. moduly lze vyhledávat nejrůznější typy dat, od sub-domén, obrázků, až po zranitelnosti. Pro nalezené informace je možné vygenerovat report a uložit do souboru ve formátu html [44].

Dalším nástrojem s mnoha případy užití je **SpiderFoot**. Dokáže vyhledávat informace na základě zadané IP adresy, e-mailu, jména nebo domény a nalezené výsledky zobrazí v souvislostech, podobným způsobem jako Maltego. Je často používán pro účely penetračního testování, jelikož je schopný odhalit možné úniky dat a zranitelnosti [45].

Poslední z nejpoužívanějších aplikací je **The Harvester**. Jeho prostřednictvím lze vyhledat informace o dané společnosti, jmenovitě e-mailové adresy, jména, subdomény, IP adresy a URL adresy. Obsahuje také integraci nástroje **Shodan**, který slouží k určení připojených zařízení k dané síti [46].

2.4.3 Sock puppet

Sock puppet, neboli loutka, je označení pro falešnou identitu na sociálních sítí, vytvořenou pro přiblížení se k cíli vyšetřování. Aby jako taková působila důvěryhodně, musí splňovat několik kritérií. Předně by měla mít přesvědčivou historii, včetně té profesní, a být aktivní na více sociálních sítích, zveřejňovat fotografie, komentovat články, a být v těchto aktivitách konzistentní. Pokud profil začneme vytvářet v době, kdy jej potřebujeme, je dávno pozdě. Nikdo neuvěří osobě, která se z ničeho nic objevila na

internetu před pár měsíci. Dokonalá identita je běh na dlouhou trať a začíná dávno předtím, než se naskytne příležitost ji použít [47].

Dříve, než skrz naši falešnou identitu začneme komunikovat s cílem, je nutné dostat se do jeho blízkosti, do jeho povědomí a nevzbudit přitom podezření. Jeden ze zkušených sock puppet tvůrců uvádí, že nejlepším způsobem, jak toho dosáhnout, je sledovat a interagovat s účty, které mají blízko k cíli a zbytek už nechat na algoritmech, které po nějakém čase tuto aktivitu našemu cíli ukážou, a pak už je jen otázkou času, než si nás všimne a naváže kontakt jako první [47].

Při samotné konfrontaci s cílem mají lepší výsledky ženské loutky, obzvlášť, pokud je tímto cílem muž. Podle všeho jsou muži méně obezřetní a obecně sdílnější při konverzaci s atraktivní ženou a spíše tak prozradí detaily například o své práci.

Existuje samozřejmě i druhá strana, kam patří „lovci“ falešných identit využívající metody strojového učení, jež dokážou odhalit, zda za danými dvěma účty stojí jedna osoba nebo zda je účet pravý [47]. Rozebírat však tento pohled na problematiku je nad rámec této práce.

2.5 OPSEC

Během OSINT vyšetřování je velmi snadné ocitnout se na druhé straně, tedy stát se sám terčem. Mitigace možného prozrazení identity vyšetřovatele je realizována dodržováním zásad OPSEC (operational security), jejichž cílem je znemožnit jakýkoliv únik nebo zveřejnění informací, které by vedly k osobě vyšetřovatele nebo prozrazovaly detaily jeho pátrací činnosti. Ačkoliv tento termín původně pochází z prostředí americké armády, v současnosti zahrnuje i metody a nástroje ochrany používané v civilní sféře. Při jejich výběru se pohlíží na model hrozby vyplývající z povahy účelu, za jakým je OSINT realizován [48]. Jinými slovy, jakému riziku může být vyšetřovatel potenciálně vystaven. Jako příklad lze uvést investigativního novináře, který odhalí korupci na vysokých místech a je tak možné, že se stane terčem vydírání a vyhrožování a v jistém nebezpečí se může ocitnout i jeho rodina. Tento model hrozby bude zcela odlišný od modelu někoho, kdo se snaží určit souřadnice místa podle fotografií. Aplikovat v obou případech stejná opatření by bylo buď nezodpovědné nebo naopak zbytečné. Existují však zásady, které je nutné dodržovat vždy bez ohledu na charakter vyšetřování.

Vše začíná už při výběru nástrojů pro sběr informací. Obezřetnost je zvláště na místě, pokud se jedná o takové, které vyšetřovatel sám nikdy dříve nepoužil nebo se na internetu objevily teprve nedávno. V obou případech je dobré nejdříve zjistit, kdo za aplikací stojí, jaké zkušenosti s ní mají ostatní členové OSINT komunity a zda je tedy důvěryhodná, před vložením jakýchkoliv dat. Jen tak na okraj lze pro ilustraci uvést aplikaci Lampyre, která na začátku roku 2019 oznámila plánovaný update a žádala mimo jiné i nejrůznější experty na poli OSINTu o vyzkoušení a zpětnou vazbu. Matthias Wilson ve svém článku Be careful what you OSINT with [49] popisuje, jak se mu s několika kolegy podařilo poodhalit, co se za údajně maďarskou společností, která měla tuto platformu vyvinout,

skrývá. Ukázalo se, že uvedená společnost existuje pouze na papíře, a co víc, dekompilace kódu a další vyšetřování odhalilo, že osoba označovaná za testera má pracovní minulost u FSB a v současnosti pracuje u firmy vyvíjející software pro ruskou vládu. Vyvozovat nějaké konkrétní závěry by sice nebylo úplně správné, ale minimálně fakt, že veškerá komunikace na ruském území musí být šifrována vládou schválenými a kontrolovanými metodami [50] a veškerá data vložená do aplikace Lampyr jsou s největší pravděpodobností posílána na ruské servery, je mírně znepokojivý a je tedy jasné, že stojí za uvážení, jaké nástroje použít.

Další z věcí, kterou je třeba se zabývat, je otisk prohlížeče. Jedná se o hodnotu vytvořenou na základě nastavení a verze prohlížeče, instalovaných pluginů a informací o hardwaru počítače, jako je operační systém, grafická karta, rozlišení, používané fonty a další. Otisk prohlížeče fakticky souvisí s informačním soukromím a to do té míry, že pokud jsou společnosti jako Google nebo Facebook schopny identifikovat uživatele na základě jeho unikátního otisku, mohou tak jednoduše zformulovat jeho digitální identitu v závislosti na jeho chování a stránkách, které navštěvuje a sledovat jej napříč online prostorem. Děje se tak hlavně za nemalého přispění sledovačů a cookies, jež dokážou propojit uživatelské aktivity z jedné webové stránky s dalšími, ať už se jedná o záležitosti pracovní nebo soukromé, a nástrojů běžících přímo v rámci kódu dané stránky. V kontextu OSINT to znamená, že pokusy o setrvání v anonymitě a distancování od sock puppet účtů jsou zcela marné, dokonce dochází k zablokování těchto falešných účtů ze stran služeb, a spíše než o anonymitu by se měl vyšetřovatel pokoušet o stav pseudonymity, což v této souvislosti znamená nevyčnívat z davu, tedy nemít unikátní otisk. V praxi toho lze dosáhnout použitím aplikací jako UBlock Origin, Privacy Badger a Cookie Auto-Delete (vše dostupné pro Firefox a Chrome) a rozšíření blokujících JavaScript, jelikož na něm běží většina nástrojů, kterými webové stránky sbírají identifikující data. Dalším problémem je, co na sebe prozrazuje sám prohlížeč. Druh a verze společně s informacemi o operačním systému jsou snadno zjistitelné, přesněji řečeno nejsou žádné pokusy o jejich skrytí, a jsou součástí tzv. User Agent String, které stránky používají pro optimální zobrazení obsahu. Pokoušet se o neposkytnutí této hodnoty by nadělalo v úsilí o pseudonymizaci více škody než užitku, protože upřímně, který běžný uživatel by toto dělal? Je tedy mnohem lepší použít například rozšíření User Agent Switcher, který vytváří dojem jiného typu prohlížeče a operačního systému. A nakonec je zde otisk plátna (canvas fingerprinting), který je pravděpodobně nejméně známou z uvedených metod pro identifikaci uživatele a zařízení. Spočívá ve vytvoření unikátního hashe na základě toho, jakým způsobem prohlížeč zobrazuje grafiku a fonty dohromady s údaji o operačním systému, grafické kartě, ovladačích, rozlišení a dalšími. Jelikož tato kombinace softwarových a hardwarových atributů je pro uživatele neměnná, ke změně hashe nestačí nastavit jinou IP adresu ani vymazat cookies a pokud vyšetřovatel na stejném zařízení přistupuje k sock puppet i ke svému osobnímu účtu, stránkám používajících canvas fingerprinting se jeví jako jedna osoba a některé služby toho

využívají k rozpoznání falešných profilů a jejich deaktivaci. Mitigace je možná opět skrz rozšíření prohlížeče, například Canvas Fingerpring Defender nebo Canvas Blocker, obojí kompatibilní s Firefox a Chrome [51].

Posledním ze základních bodů OPSEC je zabezpečení používaného zařízení. Spadá sem zablokování mikrofonu a webkamery, nastavení bezpečných hesel a jejich spravování ve správci hesel, případně použití tokenu pro vícefaktorovou autentizaci a skenování dokumentů před jejich stažením. Samozřejmostí je pak důvěryhodný antivirový software, VPN a pravidelné updaty celého systému [48].

Celý princip OPSEC podle mě jednoduše vystihuje rada, kterou dostal J. J. Luna [52], v současnosti konzultant specializující se na osobní soukromí a bezpečnost, od neznámého člena španělské tajné policie v roce 1960: „*Make yourself invisible.*“

2.6 Výhody a nevýhody OSINT

Předpokládá se, že množství dat, které vytvoří jedna osoba za sekundu, je 1,7 MB, což znamená, že v přepočtu se na internetu objeví 2,5 trilionu bajtů nových dat každý den [53]. I kdyby jen zlomek z nich představoval volně dostupné informace, lze s jistotou mluvit o tom, jak velký potenciál OSINT má, a že stále se zvyšující objem dat pracuje v jeho prospěch. Mimo běžnou rovinu internetu lze provádět vyšetřování i v rámci dark a deep webu, což se mnohdy ukazuje jako účinný nástroj v boji proti kyberkriminalitě a organizovanému zločinu. Vývoj výpočetní výkonnosti procesorů a grafických karet navíc v současnosti představuje možnost rychlejší analýzy i objemnějších dat a datasetů a aplikaci pokročilých metod zpracování. Možnost zapojit do procesu strojové učení je další podstatnou výhodou, protože dokáže odhalit komplexní souvislosti mezi velkým množstvím informací v rozměru, kterého by člověk nebyl schopen. Další výhodou je široké spektrum oblastí, v nichž lze OSINT využít, ať už se jedná o žurnalistiku, psychologii, ekonomii nebo sledování podezřelých a nebezpečných osob na poli kyberbezpečnosti a zločinu obecně [29, 4].

Na druhou stranu takto velké množství dostupných dat představuje i jisté problémy, už jejich samotné efektivní spravování může být komplikované. Dále je třeba vynaložit značné úsilí na jejich roztřídění a analýzu za účelem získat relevantní informace. S relevantností souvisí podle mého názoru nejpalčivější problém, kterému musí vyšetřovatelé čelit, a tím je důvěryhodnost zdroje. Pravdivé a spolehlivé informace jsou nezbytné pro další fáze cyklu. Pokud jsou zatíženy subjektivními názory, dezinformacemi a fake news, projeví se tato skutečnost negativně na závěrech vyšetřovatelů [29, 4].

2.7 Výzvy a budoucnost OSINT

Navzdory množství výhod a soustavnému vývoji, čelí OSINT řadě výzev a limitací a to, jakým způsobem se k nim komunita, vládní organizace a zákonodárná moc postaví, bude určovat jeho další podobu. Pastor-Galiando a jeho kolegové v práci The Not Yet

Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends identifikují hned několik takových výzev.

V rámci informačního cyklu se jedná o automatizaci sběru informací, zlepšení analýzy dat, začlenění více otevřených zdrojů a vyfiltrování irelevantních dat a dezinformací. Vše zmíněné souvisí s rostoucím množstvím volně dostupných informací. Lze předpokládat, že stále větší roli bude hrát automatizace v případě sběru informací (například za pomocí technik Web crawling a Web scraping), a různé typy strojového učení, které mají potenciál zefektivnit analýzu dat a urychlit tak klíčovou, avšak zároveň časově nejnáročnější fázi vyšetřování [29, 18]. Jako konkrétní příklad je možné uvést neuronové sítě, které se nabízejí pro rozeznávání objektů z fotografií a videí [54].

Co se týče relevantnosti dat, jak již bylo uvedeno výše, dezinformace mají negativní vliv a mohou vyústit ve falešně pozitivní výsledek, kdy bude za hrozbu označena nevinná osoba. Při současném vývoji umělé inteligence a deep fakes je tak více než kdy dřív kritické dokázat rozlišit, co je pravda a co ne. Už z tohoto důvodu je nutné využít co nejvíce dostupných zdrojů včetně sociálního inženýrství a také různé typy dat jako takových [29, 19].

Další výzvu představuje „zbourání“ hranic mezi státy. Spousta nástrojů je použitelná pouze na území některých zemí, ať už se jedná o aplikace pro prohledávání veřejných vládních dokumentů, nebo o neúplné databáze. To představuje problémy hlavně v případech, kdy cíl často mění místo pobytu ve světovém měřítku. Vyhledávání informací v konkrétní zemi pak samozřejmě přinese méně výsledků, než by poskytlo hledání celosvětové. Cílem by tedy mělo být modifikovat a vytvářet nástroje tak, aby tuto možnost poskytovaly [29, 19-20].

Nakonec je zde právní a morální hledisko, otázka soukromí a možné zneužití open source intelligence. I když jsou sbíraná data volně dostupná, je třeba brát v úvahu, že některé informace jsou citlivé a v závislosti na jejich povaze a místa, kde se cíl pohybuje, může jejich odhalení vést až k životu ohrožujícím situacím nebo zatčení dané osoby. Z pohledu práva nesmí být OSINT prováděn s nekalými úmysly a vždy musí být dodrženy zákony dané země, přičemž získané informace nesmí být nikde zveřejněny. Toto vše musí být při vývoji nástrojů zohledněno, ale především je nutné kontrolovat, aby účinnost nástroje odpovídala okruhu jeho uživatelů a neporušovala lidská práva, svobodu a soukromí. Při současném vzrůstajícím trendu kybernetické agrese se mohou jakákoliv osobní data stát prostředkem k šikaně, pomluvě a vyloučení na okraj společnosti, a proto by dle Galianda nejefektnější a nejsilnější nástroje měly být pouze v rukou orgánů výkonné moci a zpravodajských služeb [29, 20]. Na druhou stranu však nelze popřít, jak zásadní význam OSINT má pro novinářskou praxi, a že bez jeho praktik by velmi pravděpodobně nebylo možné uskutečnit taková odhalení, jakých jsme svědky například u Bellingcat [55], skupiny tvořené vyšetřovateli, výzkumníky a žurnalisty z celého světa.

3. PRAKTICKÁ ČÁST

Cílem praktické části je vytvoření programu, jenž by automatizoval vyhledávání pro potřeby Open Source Intelligence. Jelikož sbírání informací je časově velmi náročné, zautomatizování této části pomůže proces urychlit a ušetřený čas pak může být využit v dalších fázích cyklu. Existují různé typy dat, které lze použít jako vstupní parametr pro vyhledávání informací o cíli v závislosti na druhu cíle. Funkcionalitou vytvářeného programu je vyhledávání osob, relevantní vstupní hodnoty tedy budou jméno a příjmení hledané osoby.

Uživatel si v menu programu zvolí, podle kterého parametru chce zahájit vyhledávání a napíše jeho hodnotu. Program pak podle zvoleného parametru předá vstupní hodnotu patřičným funkcím a jejich výstupy, tedy nalezené informace o cíli, vypíše uživateli. Cílem programu tak bude nalézt v krátkém čase co největší množství informací týkajících se zadaných dat a na uživateli pak už bude jen odfiltrovat to, co nebude považovat za relevantní.

3.1 Rozbor řešení

Pro vytvoření aplikace byl zvolen programovací jazyk Python, a to nejen z důvodu jeho přívětivé syntaxe a intuitivnosti. Python je jeden z nejpopulárnějších jazyků, má širokou komunitu uživatelů a je tak snadné najít řešení problémů, které se během programování mohou vyskytnout. Dalším důvodem je jeho univerzálnost. Skripty vytvořené v Pythonu lze spustit na jakémkoli zařízení, ať už běží pod Windows nebo Linuxem a to bez nutnosti zdrojový kód upravovat. A nakonec, obsahuje nepřeberné množství knihoven a modulů, a je proto často využíván právě pro automatizování, datovou analýzu a strojové učení [56] a díky knihovnám podporujícím HTML, XML a JSON je ideální pro sběr informací z internetu [57].

Hlavním stavebním kamenem programu je Google Custom Search API, které umožňuje vytvořit Custom Search Engine (CSE). Jedná se o programovatelný vyhledávač, v němž lze nastavit prohledávané webové stránky, jazyk, oblast a další podrobnosti. Použitím tohoto přístupu není nutné používat vyhledávače příslušné přímo k dané stránce, například v případě sociálních sítí, ale je tak možné získat informace z těchto stránek bez potřeby je navštívit přímo. Každý takto vytvořený vyhledávač má svůj vlastní unikátní API Key a CSE Key. Ty jsou poté použity v samotném sestavení vyhledávače v kódu, jak je vidět v následujícím výpisu:

```
API_KEY = "xyz"
CSE_KEY = "123"
resource = build ("customsearch", "v1", developerKey = API_KEY).cse()
result = resource.list(q = dorks_dotaz, cx = CSE_KEY, start =
prvni_index).execute()
```

Uvedené hodnoty klíčů jsou pouze ilustrační. Skutečné jsou propojeny s mým jménem a školním emailovým účtem, nebudou tedy v tomto textu zobrazeny.

Parametr dorks_dotaz v proměnné result představuje řetězec složený ze vstupu od uživatele, tedy hledaného jména a příjmení, a operátorů Google Dorks (viz kapitola 2.4.1). Jde o jednoduchou konstrukci specifikující, na jakých sociálních sítích (Facebook nebo Twitter) má být osoba vyhledávána, jak je vidět dále:

```
dorks_dotaz = "site:" + sluzba + " intitle:" + "\"" + vstup_jmeno + "\""
```

Výsledky vyhledávání získané pomocí CSE jsou zpracovávány ve formátu JSON s pomocí Python modulu requests a vybrané návratové položky jsou vypsány uživateli v konzoli. Je to z toho důvodu, že kompletní výstup obsahuje spoustu „vaty“, jako informace o rozlišení stránky, a to nejsou údaje pro uživatele relevantní. Vypsanými položkami jsou titulek stránky, odkaz a popisek, odpovídá to tedy tomu, co by uživatel viděl ve vyhledávači v prohlížeči. Po vypsání nalezených prvních třiceti výsledků je (za předpokladu, že existují další výsledky) uživatel tázán, zda si přeje pokračovat v hledání. Tento počet je zvolen čistě z praktického hlediska. Odpovídá třem stranám výsledků vyhledávače v prohlížeči a dává uživateli rychlý přehled. Vypisovat vše naráz by zvláště u některých dotazů generujících velké množství výsledků nebylo efektivní.

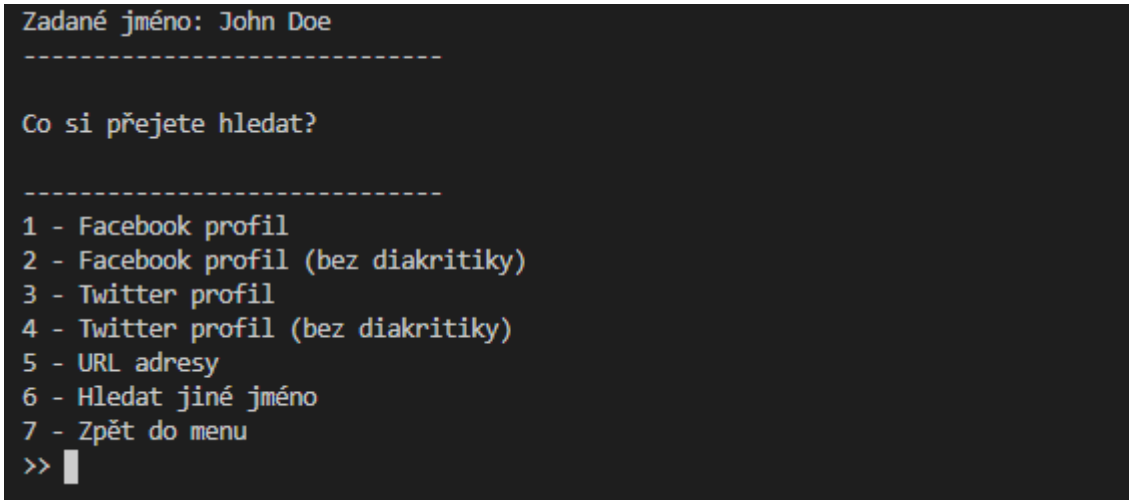
Pro případ, kdy by uživatel chtěl zjistit, zda hledaná osoba nemá blog nebo obecně neexistuje stránka s adresou obsahující její jméno, má program funkci pro hledání v URL adresách. V tomto případě je výstupem jejich seznam a údaj o počtu nalezených výsledků.

Samozřejmostí je pak funkce upozorňující na negativní výsledky hledání.

Celá aplikace je ve fázi prvotního návrhu a je zde prostor pro funkcionální i vzhledové vylepšení. V jejím vývoji plánuji pokračovat a mimo jiné vytvořit i grafické rozhraní, aby byla uživatelsky přívětivější.

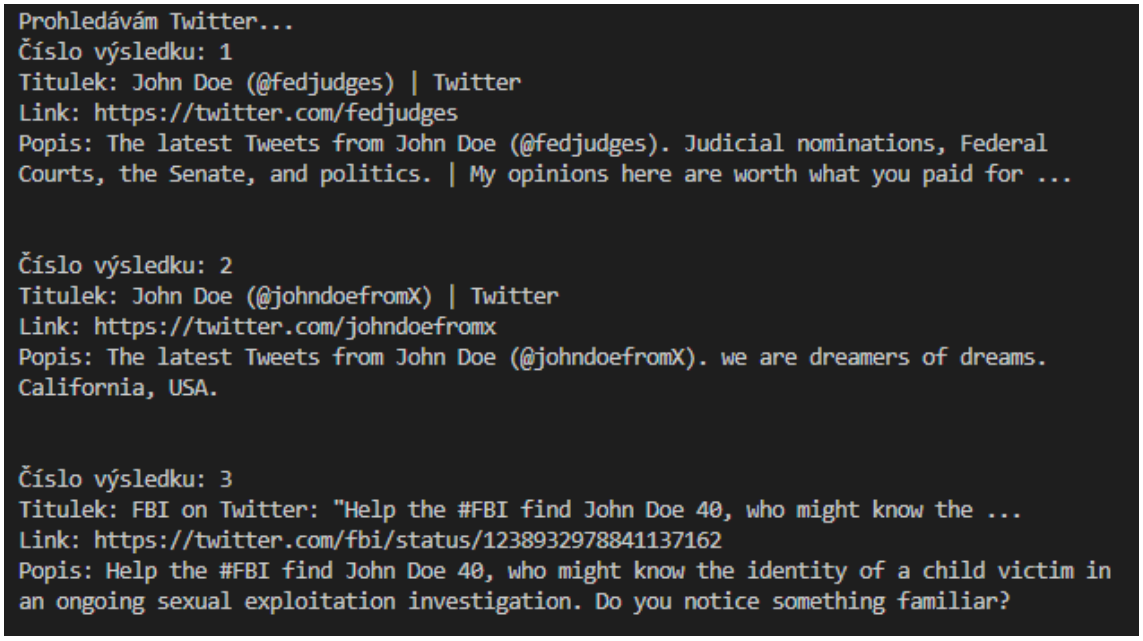
3.2 Příklad výstupu

Po spuštění aplikace a zvolení položky „1 – Jméno“ a vepsání jména a příjmení hledané osoby se uživateli zobrazí konzolové menu, kde si následně vybere, jaký dotaz chce uskutečnit. Náhled tohoto menu je na následujícím obrázku 3-1.



3-1 Náhled menu

Výpis výsledků vyhledávání pak ukazuje další obrázek 3-2.



3-2 Výsledky vyhledávání

4. ZÁVĚR

Mou motivací a hlavním cílem práce bylo představit problematiku soukromí, především pak jeho informační složky, v online prostoru, a uvést možnosti, jak lze soukromí chránit. Chtěla jsem také poskytnout náhled z druhého konce, tedy na proces získávání volně dostupných informací, na používané metody, nástroje a vytvořit aplikaci, na které by bylo možné vyhledávání informací demonstrovat. Tyto cíle byly splněny.

Na nejrůznějších typologiích byl ukázán vývoj, kterým pohled na soukromí v průběhu let prošel, a jak se z něj postupně stalo jedno ze základních lidských práv. Dále bylo řešeno, jakou hodnotu soukromí pro člověka má, jaká je jeho cena a jaké tedy plynou důvody jeho ochrany. V této souvislosti byly rozebrány právní normy upravující soukromí na území České republiky i v kontextu Evropské Unie a některé z hlavních technických nástrojů, kterými může uživatel přispět k ochraně svého soukromí na internetu.

V druhé kapitole práce byl poskytnut náhled do operačního cyklu OSINT, a to co se týče jeho historického vývoje, tak i dnešních způsobů uplatnění v široké škále oblastí vyšetřování. S důrazem na fázi sběru informací, jelikož ze své podstaty souvisí s informačním soukromím, byl popsán průběh cyklu a byly představeny nejpoužívanější techniky a některé z hlavních nástrojů užívaných právě pro sběr veřejně dostupných dat o cíli. S open source intelligence úzce souvisí OPSEC, tedy operational security, a jeho metody a zásady byly dále řešeny, stejně jako výhody a nevýhody samotného procesu OSINT a výzvy, kterým v současné době čelí. Nakonec byl v teoretické části poskytnut náhled do možné budoucnosti OSINT a možné role AI v jeho informačním cyklu.

V rámci praktické části práce bylo cílem vytvořit program pro vyhledávání volně dostupných informací o osobách. V poslední kapitole tohoto textu je popsán postup vývoje této aplikace, která umožňuje automatizovaný sběr informací na základě poskytnutého jména osoby, a jsou zde popsány funkcionality společně s ukázkami zdrojového kódu a ukázkou výstupu.

LITERATURA

[1] REIMAN, Jeffrey H. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*. 1976, **6**(1). ISSN 00483915.

[2] THOMSON, Judith Jarvis. The Right to Privacy. *Philosophy & Public Affairs*. 1975, **4**(4), 295.

[3] GROSS, Hyman. The Concept of Privacy. *New York University Law Review* [online]. 1967, **42**(34) [cit. 2020-11-30]. Dostupné z: https://heinonline.org/HOL/LandingPage?handle=hein.journals/nylr42&div=16&id=&page=

[4] Nález Ústavního soudu České republiky ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, publikován pod č. 94/2011 Sb. [cit. 2020-12-11]. Dostupné z https://nalus.usoud.cz/Search/ResultDetail.aspx?id=69635&pos=1&cnt=1&typ=result

[5] REIMAN, Jeffrey H. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara Computer and High-Technology Law Journal*. 1995, **27**(1). ISSN 2334-1610.

[6] FRIED, Charles. Privacy. *The Yale Law Yournal* [online]. 1968, **77**(3), 482 [cit. 2020-11-30]. ISSN 0044-0094. Dostupné z: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5894&context=ylj

[7] GAVISON, Ruth E. Privacy and the Limits of Law. *The Yale Law Journal* [online]. 1980, **89**(3), 427–429 [cit. 2020-11-30]. Dostupné z: https://ssrn.com/abstract=2060957

[8] GOFFMAN, Erving. *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates* [online]. 2nd printing. New Jersey: Transaction Publishers, 2009 [cit. 2020-12-11]. ISBN 978-0-202-30971-2. Dostupné z: https://books.google.cz/books?hl=cs&lr=&id=be3vAQAAQBAJ&oi=fnd&pg=PR1&dq=asylums+goffman&ots=JpGRHQUNpE&sig=qQDqmbr6wzRC4XTMiMF1xomc3FI&redir_esc=y#v=onepage&q=privacy&f=false

[9] DECEW, Judith Wagner. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca (NY): Cornell University Press, 1997. ISBN 9780801433801.

[10] GERETY, Tom. Redefining Privacy. *Harvard Civil Rights - Civil Liberties Law Review* [online]. 1977, **12**(2) [cit. 2020-11-30]. Dostupné z: https://heinonline.org/HOL/LandingPage?handle=hein.journals/hcrcl12&div=16

[11] KOOPS, Bert-Jaap. A Typology of Privacy. *University of Pennsylvania Journal of International Law* [online]. 2017, 24. 3. 2016, **38**(2), 487-569 [cit. 2020-11-30]. ISSN 483-575. Dostupné z: https://ssrn.com/abstract=2754043

[12] WESTIN, Alan F. Social and Political Dimensions of Privacy. *Journal of Social Issues* [online]. 2003, **59**(2), 431-434 [cit. 2020-11-30]. Dostupné z: https://spssi.onlinelibrary.wiley.com/doi/epdf/10.1111/1540-4560.00072

[13] MÍŠEK, Jakub. *Osobní údaje v čase a prostoru: Role performativní regulace v ochraně osobních údajů*. Brno, 2019. Disertační práce. Masarykova univerzita, Právnická fakulta, Právo informačních a komunikačních technologií, Ústav práva a technologií. Vedoucí práce Radim Polčák.

[14] CLARKE, Roger. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* [online]. 2013 [cit. 2020-11-30]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html

[15] ALLEN, Anita L. *Unpopular Privacy: What Must We Hide?* [online]. New York: Oxford University Press, 2011, 6-11, 25-26 [cit. 2020-11-30]. ISBN 978-0-19-514137-5. Dostupné z: https://books.google.cz/books?hl=cs&lr=&id=91NpAgAAQBAJ&oi=fnd&pg=PP1&dq=unpopular+privacy&ots=g4DSPkEiUd&sig=gojnCd0gqgVjBXKu6hlwe-Qlqmg&redir_esc=y#v=onepage&q&f=false

[16] FRIED, Charles. An Anatomy of Values: Problems of Personal and Social Choice. *Harvard University Press* [online]. 2013, 1970 [cit. 2020-11-30]. Dostupné z: doi:https://doi.org/10.4159/harvard.9780674332485

[17] JOHNSON, Jeffery L. A Theory of the Nature and Value of Privacy. *Public Affairs Quarterly* [online]. University of Illinois, 1992, **6**(3), 274-275 [cit. 2021-5-8]. ISSN 08870373. Dostupné z: https://www.jstor.org/stable/40435812

[18] BENN, Stanley I. *Privacy, Freedom, and Respect for Persons*. Cambridge: Cambridge University Press, 1984. Dostupné z: doi:https://doi.org/10.1017/CBO9780511625138.009

[19] SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* [online]. New York: W. W. Norton & Company, 2015 [cit. 2021-5-8]. ISBN 978-0-393-24482-3. Dostupné z: https://ciberativismoeguerra.files.wordpress.com/2017/09/bruce-schneier-data-and-goliath_-2015.pdf

[20] MALGIERI, Gianclaudio a Bart CUSTERS. Pricing Privacy: The Right to Know the Value of Your Personal Data. *Computer Law & Security Review*. [online]. 2018, 2017, **34**(2), 9-18 [cit. 2021-5-8]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047257

[21] WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review* [online]. The Harvard Law Review Association, 1890, **4**(5) [cit. 2020-12-11]. ISSN 0017811X. Dostupné z: https://www.jstor.org/stable/1321160

[22] Úmluva o ochraně lidských práv a základních svobod. Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících

[23] KOKEŠ, Marian. Judikatura ÚS: Ochrana soukromí v tzv. době internetové. *Soudní rozhledy* [online]. 2019, **2019**(6) [cit. 2021-5-8]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhfpxg4s7gzpxgxzrhaza#

[24] DE HERT, Paul a Serge GUTWIRTH, a , ed. Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action. GUTWIRTH, S., Y. POULLET, P. DE HERT, J. NOUWT a C. DE TERWANGNE. *Reinventing Data Protection ?* [online]. Dordrecht: Springer Science, 2009, 2009, s. 3-44 [cit. 2021-5-24]. Dostupné z: https://works.bepress.com/serge_gutwirth/10/

[25] KIM, Larry. 5 Online Privacy Tips From Edward Snowden: Protect your privacy with advice from the world's most infamous NSA whistleblower and privacy guru. *Inc.* [online]. c2021, 13. 1. 2015 [cit. 2021-5-8]. Dostupné z: https://www.inc.com/larry-kim/5-online-privacy-tips-from-edward-snowden.html

[26] COLE, Julie. Mozilla Firefox Review. *VPN pro* [online]. c2021, 18. 5. 2021 [cit. 2021-5-21]. Dostupné z: https://vpnpro.com/web/mozilla-firefox-review/

[27] *IntelTechniques: By Michale Bazzell* [online]. c2009-2021 [cit. 2021-5-8]. Dostupné z: https://inteltechniques.com/index.html

[28] SCHAURER, Florian a Jan STÖRGER. The Evolution of Open Source Intelligence (OSINT). *The Intelligencer: Journal of U.S. Intelligence Studies* [online]. 2013, **19**(3), 53-54 [cit. 2020-11-30]. Dostupné z: https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf

[29] PASTOR-GALIANDO, Javier, Pantaleone NESPOLI, Felix GOMEZ MARMOL a Gregorio MARTINEZ PEREZ. *The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends* [online]. 9. 1. 2020 [cit. 2020-11-30]. Dostupné z: doi:10.1109/ACCESS.2020.2965257

[30] BORGES, Esteban. What is OSINT? How can I make use of it? *SecurityTrails* [online]. Los Angeles, c2020 [cit. 2020-11-16]. Dostupné z: https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it

[31] What is OSINT? (And How Is It Used?). *SentinelOne blog* [online]. Mountain View, c2020, 17. 7. 2019 [cit. 2020-11-16]. Dostupné z: https://www.sentinelone.com/blog/what-is-osint-how-is-it-used/

[32] BIELSKA, Aleksandra, Noa Rebecca KURZ, Yves BAUMGARTNER a Vytenis BENETIS. *OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK 2020* [online]. Zurich, 2020 [cit. 2020-11-30]. Dostupné z: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

[33] Ethical Intelligence Analysis Is Not a Pipe Dream. *AaronCTI: Cyber Intelligence, Heavy Metal and Beer* [online]. c2020, 7. 9. 2020 [cit. 2020-11-16]. Dostupné z: https://www.aaroncti.com/staying-ethical-when-conducting-intelligence-analysis/

[34] CREPS, Jake. OSINT Tools for the Dark Web. *Jake Creps: Open Source Intelligence* [online]. 16. 5. 2019 [cit. 2020-11-16]. Dostupné z: https://jakecreps.com/2019/05/16/osint-tools-for-the-dark-web/

[35] WILLIAMS, Heather J. a Ilana BLUM. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* [online]. Santa Monica, Calif: RAND Corporation, 2018 [cit. 2020-11-30]. ISBN 978-0-8330-9883-2. Dostupné z:

https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf
[36] The OSINT Intelligence Cycle Part 1: Planning and Direction. *Secjuice: NON-PROFIT CYBER GOODNESS* [online]. c2020, 30. 8. 2020 [cit. 2020-11-16]. Dostupné z: https://www.secjuice.com/the-osint-intelligence-cycle-part-i-planning-and-direction/
[37] OSINT & The Intelligence Cycle Part II: Lets Talk About Collection. *Secjuice: NON-PROFIT CYBER GOODNESS* [online]. c2020, 6. 9. 2020 [cit. 2020-11-16]. Dostupné z: https://www.secjuice.com/osint-and-the-intelligence-cycle-part-ii-collection
[38] OSINT & The Intelligence Cycle Part III: Processing Raw Intelligence. *Secjuice: NON-PROFIT CYBER GOODNESS* [online]. c2020, 13. 9. 2020 [cit. 2020-11-16]. Dostupné z: https://www.secjuice.com/osint-the-intelligence-cycle-part-iii-processing-raw-intelligence/
[39] OSINT & The Intelligence Cycle Part IV: Analysis and Production. *Secjuice: NON-PROFIT CYBER GOODNESS* [online]. c2020, 8. 11. 2020 [cit. 2020-11-16]. Dostupné z: https://www.secjuice.com/osint-the-intelligence-cycle-part-iv-processing-raw-intelligence/
[40] How Intelligence Works: A dynamic process fueling dynamic solutions. *U.S. Intelligence Careers: The official source for careers in the U.S. Intelligence Community* [online]. [cit. 2020-11-30]. Dostupné z: https://www.intelligencecareers.gov/icintelligence.html
[41] BORGES, Esteban. Exploring Google Hacking Techniques. *SecurityTrails* [online]. Los Angeles, c2020, 5. 3. 2019 [cit. 2020-12-11]. Dostupné z: https://securitytrails.com/blog/google-hacking-techniques
[42] What is Maltego? *Maltego* [online]. c2021 [cit. 2021-5-8]. Dostupné z: https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego-
[43] Metagoofil: The metadata collector. *Edge-Security* [online]. [cit. 2021-5-8]. Dostupné z: http://www.edge-security.com/metagoofil.php
[44] What Is Recon-ng? How To Use Recon-ng | Best Guide. *Hacking Blogs* [online]. c2019, 25.5.2018 [cit. 2021-5-8]. Dostupné z: https://hackingblogs.com/learn-recon-ng/
[45] SpiderFoot Documentation. *Spiderfoot* [online]. c2021 [cit. 2021-5-8]. Dostupné z: https://www.spiderfoot.net/documentation/
[46] TheHarvester. *GitHub* [online]. c2021 [cit. 2021-5-8]. Dostupné z: https://github.com/laramies/theHarvester
[47] BULE, Guise. The Art Of The Sock. *Secjuice: NON-PROFIT CYBER GOODNESS* [online]. c2021, 12. 8. 2018 [cit. 2021-5-8]. Dostupné z: https://www.secjuice.com/the-art-of-the-sock-osint-humint/

[48] Basic OPSEC Tips & Tricks for OSINT researchers. *We are OSINTCurio.us* [online]. 18. 4. 2019 [cit. 2021-5-8]. Dostupné z: https://osintcurio.us/2019/04/18/basic-opsec-tips-and-tricks-for-osint-researchers/

[49] WILSON, Matthias. Be careful what you OSINT with. *Key Findings: Unlocking future trends in OSINT, investigations and intelligence* [online]. 23. 3. 2020 [cit. 2021-5-8]. Dostupné z: https://keyfindings.blog/2020/03/23/be-careful-what-you-osint-with/amp/?__twitter_impression=true

[50] PARKER, Tom. New Russian law will require all domestic traffic to be encrypted with government-controlled tools. *RECLAIM THE NET* [online]. 3. 4. 2019 [cit. 2021-5-8]. Dostupné z: https://reclaimthenet.org/russian-government-internet-encryption/

[51] Opsec for OSINT – Why You Need To Deal With Browser Fingerprinting. *NixIntel: OSINT, Linux, Digital Forensics, and InfoSec* [online]. 9. 7. 2019 [cit. 2021-5-8]. Dostupné z: https://nixintel.info/osint/opsec-for-osint-why-you-need-to-deal-with-browser-fingerprinting/

[52] LUNA, J. J. *How to Be Invisible*. New York: St. Martin's Press, 2004. ISBN 0-312-31906-1.

[53] BULAO, Jacquelyn. How Much Data Is Created Every Day in 2021? *Techjury: Business Software Solutions* [online]. c2020, 7. 5. 2021 [cit. 2021-5-8]. Dostupné z: https://techjury.net/blog/how-much-data-is-created-every-day

[54] MORRISON, Nidal. Artificial Intelligence & OSINT : Part 1. *Secjuice: NON-PROFIT CYBER GOODNESS* [online]. c2021, 25. 11. 2018 [cit. 2021-5-8]. Dostupné z: https://www.secjuice.com/artificial-intelligence-ai-and-osint/

[55] *Bellingcat* [online]. c2021 [cit. 2021-5-21]. Dostupné z: https://www.bellingcat.com/

[56] 12 Essential Advantages of Python: Why Learn Python on 2020. *Mikke Goes Coding* [online]. C2016-2021, 9. 10. 2020 [cit. 2021-5-8]. Dostupné z: https://mikkegoes.com/advantages-of-python/

[57] BODO, Lorand. Python, Your Friendly OSINT Helper. *We are OSINTCurio.us* [online]. 25. 12. 2018 [cit. 2021-5-8]. Dostupné z: https://osintcurio.us/2018/12/25/python-your-friendly-osint-helper/

SEZNAM SYMBOLŮ A ZKRATEK

Zkratky:

API	application programming interface
BBC	British Broadcasting Corporation
CIA	Central Intelligence Agency
CSE	Custom Search Engine
DDoS	distributed denial-of-service
FSB	Federální služba bezpečnosti
HR	human resources
OPSEC	operational security
OSINT	open source intelligence
VPN	virtual private network
VUT	Vysoké učení technické