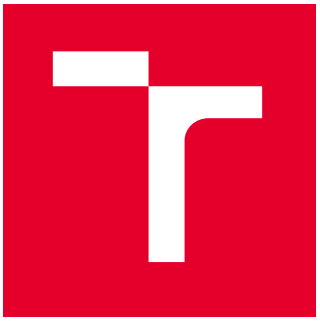

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

NÁSTROJE ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ, KLAMAVÉ ÚČTY A PRÁVNÍ LIMITY JEJICH VYUŽÍVÁNÍ V RÁMCI ETICKÉHO HACKOVÁNÍ

OPEN-SOURCE INTELLIGENCE TOOLS, SOCK PUPPET ACCOUNTS AND LEGAL LIMITS TO THEIR USE IN ETHICAL HACKING

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Filip Růžička

AUTHOR

VEDOUCÍ PRÁCE — Mgr. Jakub Vostoupal, Ph.D.

SUPERVISOR

BRNO 2025

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Filip Růžička ***ID:*** 247602

Ročník: 3 ***Akademický rok:*** 2024/25

NÁZEV TÉMATU:

Nástroje zpravodajství z otevřených zdrojů, klamavé účty a právní limity jejich využívání v rámci etického hackování

POKYNY PRO VYPRACOVÁNÍ:

Student v teoretické části práce analyzuje a kriticky zhodnotí nejpoužívanější nástroje zpravodajství z otevřených zdrojů (OSINT) a metod vytváření klamavých účtů. Paralelně se pak zaměří na právní limity, kterých musí výzkumník dbát, konkrétně na omezení pro etický hacking jako celek, a pak specifikované pro účely OSINT a používání klamavých účtů. Na základě závěrů analýzy pak student vytvoří nástroj, který bude unifikovat nejpoužívanější OSINT nástroje (příp. na základě konzultace s vedoucím práce a dle zjištěných nedostatků praxí využívaných nástrojů další funkce doplní), a nástroj na jednoduché a snadné vytváření klamavých účtů, které integruje dohromady (přičemž oba nástroje, zejména generátor klamavých účtů, je nutné přizpůsobit užívání v ČR a evropském prostoru). K těmto nástrojům připraví student právní dokumentaci, ve které specifikuje limity legálního použití.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání: 10.2.2025 ***Termín odevzdání:*** 3.6.2025

Vedoucí práce: Mgr. Jakub Vostoupal, Ph.D.

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

ABSTRAKT

Tato bakalářská práce se zaměřuje na analýzu nástrojů zpravodajství z otevřených zdrojů (OSINT), klamavých účtů a právních limitů jejich využívání v rámci etického hackingu. Popisuje jejich technické aspekty, možnosti využití v reálných scénářích a právní omezení se zvláštním zřetelem na český a evropský právní rámec. Součástí práce je také praktická část, ve které je vytvořen nástroj Puppint, který sjednocuje funkce pro OSINT analýzu a generaci klamavých účtů v českém prostředí.

KLÍČOVÁ SLOVA

Etický hacking, Kybernetická bezpečnost, GDPR, OSINT, Red Teaming, klamavé účty

ABSTRACT

This bachelor thesis focuses on the analysis of open source intelligence tools (OSINT), deceptive accounts and the legal limits of their use in the context of ethical hacking. It describes their technical aspects, possibilities of their use in real scenarios and legal limitations with special attention to the Czech and European legal framework. The thesis also includes a practical part in which the Puppint tool is created, which unifies the functions for OSINT analysis and generation of deceptive accounts in the Czech environment.

KEYWORDS

Ethical hacking, Cybersecurity, GDPR, OSINT, Red Teaming, Sock Puppet accounts

RŮŽIČKA, Filip. *Nástroje zpravodajství z otevřených zdrojů, klamavé účty a právní limity jejich využívání v rámci etického hackování*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2025. Vedoucí práce: Mgr. Jakub Vostoupal, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Filip Růžička
VUT ID autora:	247602
Typ práce:	Bakalářská práce
Akademický rok:	2024/25
Téma závěrečné práce:	Nástroje zpravodajství z otevřených zdrojů, klamavé účty a právní limity jejich využívání v rámci etického hackování

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Mgr. Jakubovi Vostoupalovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy a poznámky k práci. Také bych rád poděkoval mé rodině, přítelkyni a přátelům za podporu napříč celou prací.

Obsah

Úvod **9**

Cíle práce **10**

1 Etický Hacking **11**
1.1 Právní limity etického hackingu 13

2 OSINT **17**
2.1 Historie OSINT 18
2.2 Intelligence Gathering 19
2.3 Kde se v kybernetickém světě OSINT využívá 20
2.3.1 Internetové vyhledávání 21
2.3.2 Sociální sítě 22
2.3.3 Dark Web a Deep Web 25
2.3.4 Využití z pohledu etické osoby 26
2.3.5 Využití z pohledu neetické osoby 27
2.4 OSINT a jeho právní limity 30
2.4.1 GDPR 32
2.4.2 Duševní vlastnictví 35
2.4.3 Due Diligence 36

3 Klamavé účty **37**
3.1 Catfishing 39
3.2 Právní limity klamavých účtů 40

4 OSINT nástroj **43**
4.1 Návrh 43
4.2 PUPPINT 43
4.2.1 IPstack 43
4.2.2 Hunter 44
4.2.3 Shodan 44
4.2.4 Google Reverse Image Search a Google Dorking 44
4.2.5 Generace klamavého účtu 44
4.2.6 FullHunt 44
4.3 Tvorba nástroje 45
4.4 Návrhy na zlepšení 45

5 Právní rámec a limity legálního použití nástroje Puppint **47**
5.1 Úvod 47
5.2 Legální rámec využití 47

Závěr **50**

Literatura **51**

Úvod

Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný.[28]

S rozvojem digitální společnosti roste i důležitost nástrojů a metod, které umožňují efektivní sběr a analýzu informací z veřejně dostupných zdrojů. Jedním z takových přístupů je zpravodajství z otevřených zdrojů (OSINT), které se stalo nedílnou součástí moderní kybernetické bezpečnosti. Tato práce se věnuje problematice zpravodajství z otevřených zdrojů a jeho aplikaci v oblasti kybernetické bezpečnosti, konkrétně v rámci etického hackingu. OSINT představuje klíčový nástroj pro získávání veřejně dostupných informací, který využívají jak bezpečnostní experti, tak novináři nebo orgány činné v trestním řízení. Práce se zaměřuje na analýzu technik OSINT, využití klamavých účtů a na právní limity, které je třeba dodržovat, aby byla zachována etičnost a legálnost takových postupů.

Cílem práce je objasnit právní a technické aspekty OSINT a klamavých účtů v kontextu etického hackingu a navrhnout nástroj, který integruje vybrané OSINT služby spolu s generátorem klamavých účtů. Tento nástroj by měl umožnit efektivní provádění průzkumu a analýzy dat v souladu s právními a etickými pravidly platnými jak v České republice, tak v Evropské unii.

Práce je rozdělena do několika kapitol. Nejprve je popsán koncept etického hackingu a jeho právních limitů. Následuje kapitola zaměřená na techniku OSINT, kde je vysvětlena definice, příklady použití a typy Intelligence Gatheringu. Dále je popsána historie, aktuální možnosti využití například na sociálních sítích, a právní rámec, který je nutné při aplikaci techniky dodržovat. Třetí kapitola se věnuje problematice klamavých účtů, jejich rozlišení od jiných typů falešných profilů (např. botů), využití v rámci OSINT i fenoménu Catfishingu a následně analyzuje právní limity spojené s jejich vytvářením a používáním.

Na teoretickou část navazuje návrh a implementace nástroje Puppint, který unifikuje vybrané OSINT nástroje a umožňuje generaci klamavých účtů s přizpůsobením pro použití v českém prostředí. Závěrečné kapitoly se věnují jeho funkčnosti, technickému řešení a vymezení právního rámce pro jeho legální využití.

Cíle práce

Tato práce se zaměřuje na důkladné prozkoumání a objasnění právních, etických a technických aspektů spojených s používáním techniky OSINT (zpravodajství z otevřených zdrojů) a vytvářením klamavých účtů. Cílem je identifikovat hranice a podmínky, za kterých je možné tyto nástroje využívat legálně, a zároveň pochopit, jaké konkrétní zákony a regulace je třeba respektovat s ohledem na ochranu osobních údajů, soukromí a další právní normy, které se těchto činností dotýkají, zejména v kontextu českého a evropského právního rámce.

Součástí práce je také návrh a realizace nástroje Puppint, který propojuje vybrané OSINT služby a funkce pro generování klamavých účtů s důrazem na jejich legální a etické použití v českém prostředí. Praktická část práce tak doplňuje teoretický rozbor o konkrétní implementaci a ukazuje, jak lze navrhovat a používat podobné nástroje v souladu s platnou legislativou a zásadami etického hackingu.

1 Etický Hacking

Tato kapitola se zaměřuje na problematiku etického hackingu. K pochopení etického hackingu je nejdříve potřeba vysvětlit, co je to hacking.

Hacking je zneužití slabých míst a nedostatků v počítačovém systému nebo v sítí takového systému.[1] Hacky dokážou mít devastující následky, kdy firmy čelí únikům dat, výpadkům systémů a dalším potížím, které následně vedou ke ztrátě zákazníků, menším výdělkům, poškození reputace nebo třeba i pokutám a jiným právním trestům, za které samotné společnosti nemůžou.[2] Podle dat od IBM, průměrný únik dat stojí firmu 4,88 milionu dolarů.[2]

Oproti tomu, etický hacking je použití hackovacích technik spřátelenými stranami ve snaze odhalit, pochopit a opravit slabá místa zabezpečení v síti nebo počítačovém systému před tím, než těchto slabin zneužije někdo jiný.[3] Etičtí hackeři používají obdobné nástroje, jako hackeři, ale za cílem zlepšení síťového zabezpečení, aby nedošlo k žádnému narušení od nežádoucích útočníků.

Etické a neetické hackery je od sebe možno rozlišovat na základě jejich motivace, jelikož obě skupiny na ně nahlíží z opačné perspektivy. Hackeři útočí na oběti z mnoha různých důvodu jako např. osobního zisku a to ať už peněžního, reputačního, pomsty nebo čistého nutkání hackovat.[4] Na základě těchto motivací modifikují, odstraňují a kradou data obětem, aby dosáhli toho po čem touží.[5]

Etičtí hackeři mnohdy začnou vykonávat činnost etického hackingu díky své zvědavosti, a proto zvědavost dokáže být velkou motivací, za účelem zjištění, jak věci fungují na nejnižší úrovni a jak tyto věci řeší jednotlivé společnosti.[7] Zvědavost je jen jedna z mnoha motivací etických hackerů. Mezi další motivace patří snaha o zlepšení kyberbezpečnosti, prosadit své jméno v hackerské komunitě (získat reputaci), učit se řemeslu, kariérně postupovat a samozřejmě i peněžní zisk (i přesto, že bývá ve většině případů druhořadou motivací).[8] V neposlední řadě, mnoho etických hackerů vnímá svou činnost jako druh „digitálního aktivismu“ a vnímají sami sebe spíše, jako ochránce proti kybernetickým hrozbám, než jen jako technické odborníky.[9]

Uvedené motivace mohou etičtí hackeři uplatnit v činnostech, jako jsou Bug Bounty programy, Red Teaming, penetrační testování a další.

Před samotným vysvětlením Bug Bounty programů je vhodné zmínit jejich evoluční předstupeň a tím je Odpovědné zveřejňování zranitelností (Responsible Vulnerability Disclosure). Odpovědné zveřejňování zranitelností se zaměřuje na to, jakým způsobem by měl identifikátor zranitelností předávat informace správným osobám ve vhodný čas a prostřednictvím odpovídajících kanálů, aby se co nejvíce omezily negativní dopady spojené se zranitelnostmi a jejich zveřejňováním.[10]

K hledání těchto zranitelností poté povzbuzují etické hackery zmíněné Bug Bounty

programy, které nabírají na popularitě z důvodu přístupu, kdy za identifikaci slabin v aplikacích, společnosti nabízejí odměny bezpečnostním specialistům v rámci crowdsourcingu.[11] Tento systém je oboustranně výhodný pro společnosti a zároveň i pro hackera (v tomto případě dále bug huntera). Společnosti využívají platformy, jako BugCrowd, Cobalt, HackerOne, Intigri a další, aby nabídli odměnu v podobě, jak finanční, tak reputační[11]. Na oplátku bug hunteři hledají chyby a zranitelnosti, které zaručí společnostem vyšší bezpečnost jejich aplikací.

Bug Bounty nabídky se dělí na veřejné a soukromé.[12] Na veřejných nabídkách může pracovat každý, a proto je zde pro bug huntera velká konkurence v rámci nalezení zranitelností a získání odměn. Do soukromých nabídek musí být hacker pozván společností.[13] Soukromé nabídky poskytují společnostem větší kontrolu, jelikož na nabídce bude pracovat méně bug hunterů.[12] To je výhoda i pro bug huntery samotné, jelikož mají mnohem větší šanci najít nějakou slabinu bez obav, že ji někdo najde nebo nahlásí dřív a díky tomu mají také větší šanci získat zaslouženou odměnu.

Další činností je penetrační testování. Penetrační testování je typ testování zabezpečení informačních systémů se souhlasem vlastníka systému.[14] Díky těmto penetračním testům etický hacker doporučí firmě, jaké opatření musí učinit pro lepší bezpečnost proti hackerskému napadení. Často se pojmy *etický hacking* a *penetrační testování* používají zaměnitelně, ale je zde rozdíl.[15] Etický hacking je širší oblast kybernetické bezpečnosti, která zahrnuje jakékoliv využití hackerských dovedností za účelem zlepšení zabezpečení sítě, kdežto penetrační test je jedna z metod, kterou etičtí hackeři používají.[15]

Penetrační testy se rozdělují do několika typů:

- **Externí testování**, při kterém se penetrační tester zaměřuje na externě viditelné servery nebo zařízení, jako jsou například DNS servery, e-mailové servery, webové stránky a další.[16]
- **Interní testování**, kdy útočník simuluje útok, jako by byl uvnitř společnosti, jakožto neoprávněný uživatel se standardními uživatelskými právy.[16]
- **Testování průniku do sítě**, u kterého jsou testovány slabiny v rámci síťové infrastruktury.[17]
- **Bezdrátové testování** zpravidla testuje a prověřuje bezdrátové připojení k firemní WiFi mezi zařízeními, jako jsou notebooky, tablety a podobné.[17]
- **Slepé testování**, které simuluje akce a postupy skutečného útočníka tím, že společnost předem přísně omezuje informace poskytnuté osobě nebo týmu, který test provádí.[16]
- **Dvojitě slepé testování**, posouvá slepý test ještě dál a to tím, že o dění penetračního testu ví jen hrstka osob v dané společnosti.[16]
- **Fyzické penetrační testování** zahrnuje testování na prostory, jako jsou ser-

verovna nebo budova samotné organizace, přičemž toto testování je navrženo tak, aby identifikovalo slabá místa v zabezpečených oblastech a simulovalo způsoby reálného útočníka (např. sociální inženýrství) za účelem získat přístup do vyhrazených oblastí nebo k informacím.[18]

V neposlední řadě stojí za zmínku tzv. Red Teaming. Red Teaming je metodika, která využívá nezávislé, strukturované kritické myšlení a různé kulturní pohledy k tomu, aby zpochybňovala předpoklady a důkladně zkoumala alternativní možnosti, za cílem minimalizovat rizika a podpořit nové příležitosti.[19] Slouží k posouzení zabezpečení organizace a otestování, jak by organizace reagovala na skutečný útok.[20] Mezi typické nástroje a techniky Red Teamingu patří například:

- **Sociální inženýrství**, zde spadají phishing a podobné techniky za cílem získání informací nebo proniknutí do systému od nic netušícího zaměstnance.[21]
- **Fyzické testování zabezpečení** testuje společnost v rámci zabezpečení dohledových systémů a alarmů.[21]
- **Penetrační testování webových aplikací** za účelem hledání slabin v konfiguraci a navržení webových aplikací.[22]
- **Hrubé vynucení přihlašovacích údajů (Brute Force)**, jako systematické hádání hesel, testování běžných hesel a podobně.[21]

Rozdíl mezi penetračním testováním a Red Teamingem spočívá v tom, že hlavním úkolem penetračního testování je identifikovat zneužitelné zranitelnosti a získat přístup do systému.[21] Oproti tomu Red Teaming je činností zahrnující simulaci veškerých rozhodnutí nebo chování protivníka, jejichž výstupy jsou měřeny a využívány za účelem informování nebo zlepšení obranných schopností.[23] Rehberger také uvádí, že v rámci cybersecurity se pojem Red Teaming odkazuje na operace narušení za účelem měření a zlepšování procesu reakce na incidenty.[23]

1.1 Právní limity etického hackingu

Z výše zmíněných činností etického hackera, jako je Bug Bounty, Red Teaming nebo penetrační testování, vyplývá, že etický hacker může porušit jistá právní ustanovení a to i v případě, že činnost je vykonávaná s dobrým úmyslem a v rámci etiky. Proto z právního hlediska etického hackingu, je potřeba určit, jaká právní ustanovení mohou být touto činností potenciálně dotčena. V této kapitole se zaměřuji zejména na skutkové podstaty trestných činů, které se nejčastěji pojí s průběhem etického hackingu. Jednotlivé právní ustanovení jsou v textu strukturována podle typu zásahu. Nejdříve se jedná o právní ustanovení dotýkající se digitálního průniku (§ 230-232), poté na zásahy fyzického prostoru (§ 178 a § 205), činy s ochranou osobních údajů a duševního vlastnictví (§ 180, § 182 a § 270) a na závěr se kapitola věnuje i soukromoprávní rovině.

Jak již bylo naznačeno při definici penetračního testování, tak základním pilířem pro vykonání penetračního testu, eticky a bez obav ze spáchání trestného činu, je souhlas, který musí protistrana etickému hackerovi udělit. Díky tomuto svolení dává společnost etickému hackerovi povolení k proniknutí do systému, za účelem zjištění bezpečnostních slabin, proti kterým se firma musí následně opatřit. Právní souhlas jde definovat, jako „výslovný souhlas daný slovy nebo jednání" ze strany oběti nebo ze strany poškozeného obecně k potenciálnímu pachateli, přičemž § 30 trestného zákoníku stanovuje souhlas následovně: „trestný čin nespáchá, kdo jedná na základě svolení osoby, jejíž zájmy, o nichž tato osoba může bez omezení oprávněně rozhodovat, jsou činem dotčeny"[24] Tento souhlas se v souvislosti penetračního testu uděluje u tzv. *„Pravidel použití síly" (v angličtině Rules of Engagement).* Tyto pravidla použití síly nastavují hranice, které musí penetrační test dodržovat, nastavují také jaká bude komunikace mezi jednotlivými stranami a v neposlední řadě také právní aspekty a požadavky, jako je například udělení již zmíněného souhlasu k provedení testu.[25] Samotný souhlas by měl penetrační tester dostat od organizace dobrovolně, srozumitelně, vážně a před začátkem samotného pentestu.[26]

Pokud by penetrační tester nebo etický hacker nedostal souhlas a i přesto se rozhodl činnost vykonat, mohl by tím porušit několik ustanovení trestního zákoníku. Za klíčová v kontextu etického hackingu podle mého názoru považuji § 230, § 231 a § 232.

§ 230 trestního zákoníku se dotýká jakékoliv myslitelné činnosti etického hackingu mimo ty, které jsou zahrnuty v § 231 a § 232 trestního zákoníku. Aby došlo k porušení tohoto právního ustanovení, musel by etický hacker úmyslně překonat bezpečnostní opatření a získat neoprávněný přístup k počítači.[27] První odstavec chrání systém v rámci důvěrnosti systému, neboli jak bylo již zmíněno proti neoprávněnému přístupu k počítačovému systému. Druhý odstavec pojednává o integritě dat a jeho manipulací ať už se jedná o smazání, změně nebo neoprávněného užití daných dat.

Na to plynule navazuje § 231 trestního zákoníku, který pojednává o opatření a přechování přístupového zařízení a hesla k počítačovému systému.[27] Tím se má namysli, že pokud se etický hacker dostane do systému organizace, nesmí tento přístup sdílet s žádnou další stranou. Pokud se etický hacker do organizace dostane například za pomocí hrubé síly (brute force), tím následně zjistí i heslo k organizaci, tak toto heslo nesmí uchovat pro budoucí použití nebo ho sdílet a podobně. Totéž platí i pro nástroje, které by etický hacker využil k získání přístupu do systému dané organizace. Toto právní ustanovení může dopadat i na nástroj Puppint, vytvořený v rámci praktické části, pokud by byl použit k uchovávání nebo sdílení přístupových údajů získaných neoprávněným způsobem.

Pokud by za těchto okolností byl pachatel fyzická či právnická osoba, která vyko-

nává zaměstnání, povolání, postavení nebo funkci, nebo má jiné povinnosti mu uložené podle zákona nebo smluvně převzaté, může porušit § 232 trestního zákoníku, který pojednává o neoprávněném zásahu do počítačového systému nebo nosiče informací z nedbalosti.[27] Toto právní ustanovení se může zdát podobné s ustanovením § 230 odst. 2 písm. b) trestního zákoníku, ovšem subjekt je zde speciální, protože skutková podstata vyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení.[28]

Jak již bylo zmíněno v úvodu této kapitoly etický hacking nezasahuje pouze do digitálního prostoru, ale může zasahovat i fyzický prostor proniknutím do objektů za účelem testování jejich bezpečnosti. Právě v této oblasti mohou etičtí hackeři narazit na limity zákona, zejména na ustanovení § 178 trestního zákoníku, který upravuje neoprávněné vniknutí, a § 205 trestního zákoníku, jenž se týká krádeže.

V předchozí kapitole bylo zmíněno, že fyzický penetrační test se zaměřuje na prověření fyzické bezpečnosti objektu, zatímco v rámci Red Teamingu se hodnotí i funkčnost a účinnost technických prostředků zabezpečení, například kamerových systémů či alarmů. Aby bylo možné tyto zabezpečovací systémy otestovat, etický hacker musí proniknout do budovy ať už přímo a nebo diskrétně pomocí technik sociálního inženýrství, čímž se na etického hackera může vztahovat § 178 trestního zákoníku, což znamená, že etický hacker na pozemek nesmí vniknout neoprávněně.[27]. V návaznosti na proniknutí do budovy může nabýt své skutkové podstaty také § 205 trestního zákoníku. Toto právní ustanovení nabyde své skutkové podstaty v případě, kdy by došlo během útoku k odcizení majetku organizace.[26] Příkladem k naplnění znaků může dojít v okamžiku, kdy etický hacker odcizí majetek, jako důkaz, že do prostor zvládl proniknout.

Pokud by součástí dat, které byly získány proniknutím do systému, byly nějaké osobní údaje, které by určitým způsobem způsobily vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají tím, že by byli zveřejněny, sděleny, zpřístupněny, nebo by byly přisvojeny a to byť jen omylem, mohlo by se na takové jednání vztahovat ustanovení § 180 trestního zákoníku, který pojednává o neoprávněném nakládání s osobními údaji.[27] Je však nutné zdůraznit, že toto ustanovení se dle současné praxe uplatňuje zejména v souvislosti s výkonem veřejné moci a tehdy, pokud dané jednání skutečně vede k vážnému zásahu do práv subjektu údajů.[24]

V rámci proniknutí do systému, je možno také narazit na soukromé zprávy. Jelikož zprávy odeslané nebo rozepsané chráněny nejsou, byť jsou chráněny v soukromí, ale musí se jednat o zprávy neodeslané, které jsou chráněny tzv. **tajemstvím**, přičemž tajemstvím je chráněn obsah dopravovaných zpráv bez ohledu na jejich formu či hodnotu pro adresáta, odesílatele či pachatele.[28] Při *porušení tajemství* dojde k naplnění skutkové podstaty § 182 trestního zákoníku. Podle právního ustanovení,

kdo úmyslně poruší tajemství

(a) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

(b) neveřejného přenosu dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková data,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.[27]

Součástí získaných dat při průniku do systému, může být také autorské dílo. Příklad takového autorského díla by mohl být kus kódu programu, který společnost napsala. V případě distribuce chráněného autorského díla dojde k naplnění skutkové podstaty § 270 trestního zákoníku, který pojednává o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.[28] Toto právní ustanovení může hrát důležitou roli v situaci, kdy etický hacker ukončí spolupráci se společností, pro kterou pracoval a uchoval si informace ze získaných dat počítačového systému v podobě autorského díla a následně toto dílo zneužil.

Kromě trestněprávních ustanovení je důležité zmínit také soukromoprávní rovinu, která může být při etickém hackingu rovněž relevantní. Mezi nejčastější situace patří hrozby v podobě žalob za zásah do dobré pověsti, porušení smluvních povinností, porušení autorských práv nebo také porušení obchodního tajemství.[24]

Další kapitola pojednává o hlavním tématu této práce a tím jsou nástroje zpravodajství z otevřených zdrojů.

2 OSINT

Nástroje zpravodajství z otevřených zdrojů (dále jen OSINT) je technika pro získávání a analyzování informací, které jsou veřejně dostupné.[29] Otevřenými zdroji se mají na mysli zdroje, jako jsou webové stránky, články, noviny, časopisy a další těmto podobné. Dnes tuto techniku používají žurnalisté, etičtí hackeři, ale i orgány činné v trestním řízení pro dopadení osob, které překročili hranici zákona.[30] Příklad tohoto může být Mark Sokolovsky, který si žil bohatý, byť nelegální život a kvůli válce na Ukrajině a vyšetřovatelům, kteří využívali techniky OSINT, se mu tento bohatý život propadl pod rukama. Mark Sokolovsky byl Ukrajinec, který naprogramoval malware RaccoonStealer. Tento malware se zaměřuje na prohlížeč oběti a krade citlivá data, jako uložená hesla, uživatelská jména, kreditní karty a další.[31] Programátor po vypuknutí války na Ukrajině opustil stát a díky kamerovému systému, který ho vyfotil při cestě do zahraničí, a také díky příspěvku na Instagramu jeho přítelkyně, byl dopaden.[32]

Předešlý příklad ukázal, jak mohou Orgány činné v trestném řízení využít OSINT k dopadení pachatele za pomocí veřejně dostupných dat (v tomto případě příspěvěk na platformě Instagram). Ovšem dovolím si říct, že OSINT není ve většině případů tolik přímočarý. I přes to, že dnes existuje mnoho užitečných nástrojů a veřejných zdrojů, které ať už zjednodušují průběh techniky OSINT nebo umožňují upřesnit vyhledávané informace, většina OSINT operací zahrnuje více kroků, efektivní analýzu informací a kombinace různých zdrojů dat.

Pro vhodnější ilustraci a představu praktického využití techniky OSINT v krizové situaci, následující příklad simuluje pátrání po pohřešované osobě, ve kterém etičtí hackeři využívají analýzu sociálních sítí, práci s veřejnými kamerami, reverzní vyhledávání obrázků, hledání ve veřejných registrech a určení přibližné geolokace pomocí informací získaných z veřejných zdrojů.

Slečna je den nezvěstná a vyhlásí se pátrání. Etičtí hackeři se rozhodnou, že přiloží ruku k dílu a využijí OSINT k pátrání, zda lze o dívce získat nějaké informace z veřejně dostupných zdrojů. Jako první prozkoumají sociální sítě, kde zjistí, že slečna má veřejný účet a poslední příspěvek je z předešlého dne z kavárny, ve které byla se svými přáteli. Na základě interiéru byli vyšetřovatelé schopni určit lokaci této kavárny. V blízkosti této kavárny se nachází i online kamera, která ukazuje na náměstí poblíž kavárny a poskytuje i záznam. Zde vyšetřovatelé uvidí slečnu na cestě domů, když ji v tom okamžiku zastihne nějaký muž, se kterým začne vést konverzaci. Po chvíli muž odvede slečnu jiným směrem.

Vyšetřovatelé pomocí kamery zjistí, jak muž vypadá a díky jeho fotografii ho dokážou vyhledat na sociálních sítích a zjistit také jeho jméno a příjmení. Na základě profilu na LinkedInu zjistí, že muž je podnikatel. Z různých příspěvků a po ná-

sledném Reverse Image Search (který bude více vysvětlen v podkapitole *Internetové vyhledávání*), zjistí, že muž se v této lokalitě pohybuje pravidelně. Vyšetřovatelé následně využijí výpis veřejného rejstříku a vyhledají tohoto muže na základě již zjištěných informací. Zjistí, že muž má již kriminální minulost včetně trestů za únos a napadení. Po těchto nálezech se vyšetřovatelé vrátí zpět k online kamerám a příspěvkům na sociálních sítí z daných míst v čas, kde byla slečna s mužem. Na základě těchto informací dokázali lokalizovat přibližnou oblast, kde by se mohla dívka nacházet a tyto informace následně předali orgánům činným v trestném řízení.

Jak ukazují předchozí příklady, OSINT dnes hraje klíčovou roli od investigativní žurnalistiky až po pátrání po pohřešovaných osobách. Přitom tato technika není vynálezem moderního internetu. Její kořeny sahají hluboko do minulosti, kdy lidé poprvé začali systematicky využívat veřejně dostupné informace k dosažení svých cílů. Proto se další podkapitola bude věnovat tomu, kdy a jak OSINT vznikl.

Poznámka k terminologii
V textu bude pro zjednodušení používán termín *vyšetřovatel*, kterým se má na mysli osoba využívající techniku OSINT k získávání informací z veřejně dostupných zdrojů, pokud nebude uvedeno jinak.

2.1 Historie OSINT

Nyní bych se časově přesunul do minulosti a to konkrétně ke vzniku OSINTu. První výskyty pojmu OSINTu se obecně uvádí na počátku 2. světové války.[33] Jednalo se o BBC Monitoring ve Velké Británii vzniklé roku 1939 a Foreign Broadcast Monitoring Service (FBMS) z roku 1941 ve Spojených státech.[33] Co se týče techniky OSINTu, ty se začali prakticky využívat v dřívějších dobách. První známky OSINTu se našli už v raných dobách 16. století, kdy Council of Ten (jeden z hlavních řídících orgánů Benátské republiky, zpravodajský aparát) vysílal agenty, které pro ně získávali informace o politickém a obchodním vývoji. Agenti získávali informace z novin, ale zaměřovali se i na diplomaty a obchodníky, kde používali tzv. HUMINT, což je získávání informací z lidských zdrojů.[33]

OSINT takový, jaký je znám, začal hrát velmi důležitou roli v období světových válek. BBC Monitoring ve Velké Británii sloužil k monitorování rádiových vysílání.[34] Hlavní úkol bylo podávat britské vládě včasné a přesné zprávy, které nashromáždili ze zpráv, propagandy a také nepřátelského vojenského vysílání.[34] Naslouchání a analýza nepřátelských německých vysílání byla klíčovým prvkem v průběhu druhé světové války, díky kterému dokázali Britové získat informace o pohybu

nepřátelských jednotek, strategické plány a potenciální zranitelnosti, což dávalo Spojencům značnou informační výhodu.[34]

V této kapitole byl zmíněn HUMINT, což je jeden z typů tzv. zpravodajství, které je popsáno v následující kapitole.

2.2 Intelligence Gathering

Dle vlády USA je zpravodajství (anglicky Intelligence Gathering) definováno, jako shromážděné informace, které mohou způsobit ohrožení národa, jeho obyvatel, majetku nebo zájmů, vývoje, šíření nebo použití zbraní hromadného ničení a jakýchkoli dalších záležitostí týkajících se národní bezpečnosti nebo bezpečnosti vlasti.[35]

S posunem let se zpravodajství rozdělilo na několik dalších typů mezi, které spadá i samotný OSINT.

HUMINT (Human Intelligence) je získávání informací z lidských zdrojů. Používá se k výslechu svědků, vedení rozhovorů s podezřelými a zájmovými osobami.[36]

SOCMINT (Social Media Intelligence) se zaměřuje na sociální sítě. Snadný zdroj potřebných informací o jednotlivých lidech na jednom místě.[37]

SIGINT (Signal Intelligence) vzniká zachycením signálů, které mohou být získané z letadel, lodí, satelitů nebo pozemních míst.[38] SIGINT se dále dělí do třech pod-typů:

- **COMINT** (Communication Intelligence) slouží k zachytávání hlasových nebo textových zpráv.
- **ELINT** (Electronic Intelligence) analyzuje a sbírá informace z vysílání radarů a dalších elektromagnetických vysílání.
- **FISINT** (Foreign Instrumentation Signals Intelligence) dokáže zachytit dálkové měření zbraňového systému nebo vesmírného vozidla. Za pomocí analýzy dokážou je možné zjistit výkon zmíněných systémů či vozidla.[36]

IMINT analyzuje informace z fotografií a snímků (satelitních, radarových a podobné)(též zmiňovaný, jako PHOTOINT).[36, 38]

GEOINT vzniká skrze kombinací geolokace a IMINT, což je získávání informací z obrázků, satelitních snímků, radarových senzorů a dalších.[36]

MASINT je typ zabývající se zbraňovými schopnostmi a průmyslových činností.[38] Používá se k odhalování informačních vzorců, které dosud nebyli využity jinými systémy. MASINT se skládá z pěti dílčích typů:[36]

- **TELINT** (Telemetry Intelligence) se používá například pro označení údajů předávanými zbraněmi během testů. Během těchto testů se zároveň často používá společně s ELINT, jelikož může označovat elektronické emise zachycené moderními zbraněmi a sledovacími systémy.[38]

- **Radar MASINT** používá radar za účelem analýzy a měření vlastností. Neplést s ELINT, jelikož nesbírá informace[39]
- **Materiální MASINT** sbírá informace o materiálech, jako je voda, vzduch nebo o pevných materiálech, které jsou následně analyzovány[40]
- **Nukleární MASINT** detekuje, identifikuje a charakterizuje známky radiace a události, které ji zapříčinili[40]
- **Elektro-optický MASINT** se využívá k objasnění obrazu za pomocí vyzařování, objasňuje kontext a dokáže i identifikovat materiály v obraze prostřednictvím světelných senzorů[39]
- **Geofyzický MASINT** je kolekce fyzikálních jevů na Zemi, jako jsou různé energie a problémy, které ovlivňují různé sféry, oceány, povrch nebo oblasti zemské kůry a níže[40]

2.3 Kde se v kybernetickém světě OSINT využívá

Postupem času vznikly pro OSINT automatizační nástroje, které výrazně zefektivňují a urychlují proces vyhledávání informací. Tímto způsobem lze efektivně shromažďovat data a dále je spojovat. Řada moderních nástrojů obsahuje funkce pro agregaci dat, přičemž míra automatizace se liší podle konkrétního nástroje. Tyto nástroje obvykle deklarují, že jsou určeny k práci s daty a jejich analýze.[41] Nejdůležitějším nástrojem je tzv. **OSINT Framework** (*https://osintframework.com*), který můžeme chápat, jako databázi automatizačních nástrojů pro OSINT podle potřeby využití. V databázi je možno najít nástroje pro hledání na základě uživatelských jmen, telefonního čísla, prohledávání jednotlivých sociálních sítí, archivů a mnoho dalších.

Spoustu těchto nástrojů slouží také k tzv. Scrapingu. Data Scraping je proces, při kterém se získávají data z internetu nebo dokumentů.[37] Jedná se o shromažďování cenných informací z různých zdrojů.

Mezi nástroji se také nachází, z mého pohledu, největší nástroj pro OSINT obecně, čímž je nástroj Maltego. Maltego je platforma, která umožňuje rychlé vyšetřování OSINT pro digitální profilování pomocí, komplexní analýzu vazeb pro velké soubory dat, umožňuje vyšetřovatelům shromažďovat, monitorovat a uchovávat informace o sociálních médiích v reálném čase pro účely veřejné bezpečnosti, řízení rizik a právního stíhání.[42] Tento nástroj využívají, jak OSINT vyšetřovatelé, tak i zpravodajské týmy zabývající se kybernetickými hrozbami a orgány činné v trestním řízení.[42]

Další využívané OSINT nástroje představím v nadcházejících kapitolách, kde se věnuji konkrétním oblastem kyberprostoru, kde je OSINT nejčastěji aplikován.

2.3.1 Internetové vyhledávání

Internetové vyhledávače jsou nástroje používané na denní bázi. Ať už za účelem hledání odpovědí na otázky nebo vyhledání potřebných informací. Dnes tyto vyhledávače nabízejí rozšířené možnosti vyhledávání, které umožňují se co nejvíce přiblížit k požadovanému výsledku.

Google Dorking nebo také jinak nazývaný Google Hacking, je technika, která využívá pokročilé operátory za účelem filtrace výsledků, které by se jinak, při klasickém vyhledávání, nezobrazili.[43] Příkladem použití tohoto rozšířeného vyhledávání může být například: ***posudek bakalářské práce site:vut.cz filetype:pdf***. Výsledkem tohoto dotazu budou odkazy na posudky bakalářské práce na stránce *vut.cz* a pouze typu *pdf*. Operátory, které se dají použít, je mnoho, ale dá se také využít rozšířené hledání, tj. *www.google.com/advanced_search*, které plní stejnou funkci.

Mimo vyhledávání dnes vyhledávače umí zpracovávat i fotografie. Při nahrání fotografie, se vyhledávač snaží poskytnout výsledky, co nejvíce podobné nahrané fotografii. Pokud uživatel hledá určité místo, ze kterého má fotografii, ale nepamatuje si, kde tuto fotku pořídil, může jednoduše fotku nahrát na Google nebo jiný z vyhledávačů a vyhledávač uživateli následně ukáže co nejpodobnější fotografie, které se podobají danému místu. Toto vyhledávání se nazývá tzv. **Reverse Image Search**. Každý prohlížeč má v rámci Reverse Image Searchingu jiné výsledky a to kvůli tzv. indexaci. Jakmile uživatel nahraje fotografii do prohlížeče, tato fotografie se změří a analyzuje, prohlížeč poté prohledá databázi za účelem nalezení totožné fotografie, popřípadě poté hledá podobné fotografie ná základě fingerprintů, což jsou unikátní informace, které se nacházejí ve fotografii.[44] Při použití techniky OSINT a na základě poskytnutých fotografiích, je osoba využívající tuto techniku schopná identifikovat osoby, lokace nebo předměty, které dokážou značně pomoci při vyšetřování.[45]

Pro OSINT jsou také hojně využívané nástroje, které shromažďují a analyzují povrch internetu nebo zařízení připojené k internetu. Pro shromažďování informací o zařízeních připojených k internetu se využívá Shodan, který se dotazuje na různé veřejně dostupné informace, od malých stolních počítačů až po jaderné elektrárny.[46] Informace získané za pomocí nástroje Shodan, jsou jen těžko dohledatelné za použití běžného vyhledávače. Shodan totiž oproti vyhledávači Google prohledává celý internet, přičemž Google prohledává pouze World Wide Web, kde se nachází pouze nepatrný zlomek toho, co je připojené k internetu.[46]

Další nástroj, který zmíním a pracuje s veřejně dostupnými daty je nástroj Hunter. Hunter slouží k vyhledávání potenciálních zákazníků tím, že pomáhá profesionálům objevovat nové společnosti, vyhledávat a ověřovat e-mailové adresy, obohacovat kontakty a automatizovat personalizované e-mailové kampaně, a to vše při plném dodržování předpisů na ochranu osobních údajů, jako jsou GDPR a CCPA.[47] Vy-

hledávání e-mailových adres může být užitečné při testování technik sociálního inženýrství, například během simulace phishingového útoku.[48]

2.3.2 Sociální sítě

Sociální sítě jsou zlatý důl ke zjištění informací ke konkrétním osobám. Jelikož lidé rádi sdílí své zážitky a radosti mezi ostatní, dá se tohoto faktu lehce zneužít a zjistit tak o těchto osobách mnoho informací. Z tohoto důvodu vznikl dříve zmíněný SOCMINT.

Sociální sítě, které jsou dále popisovány, byly vybrány na základě počtu aktivních měsíčních uživatelů podle grafu poskytnutým webem *Statista*[49]. Mezi hlavní sociální sítě jsem tedy zařadil Instagram, Facebook, X (dříve Twitter), Reddit, Telegram a LinkedIn.

Instagram je bezplatná aplikace ke sdílení fotek a videí.[50] Sdílení těchto médií může být ať už veřejné, tak i soukromé. To znamená, že lidé, kteří se chtějí podívat na fotky osoby se soukromým profilem, musí dostat povolení ke sledování. Jelikož sdílení fotografií a videí jsou hlavní funkcionalitou Instagramu, tak již dříve zmíněný Reverse Image Searching, je u Instagramu velmi silným nástrojem. V podkapitole *Využití z pohledu neetické osoby* bude ukázáno, jak informace z těchto fotografií dokážou být pro některé jedince fatální.

Dalším velkým nástrojem pro získávání dat z Instagramu je tzv. Osintgram, což je nástroj, který dokáže získat data jako informace o sledujících dané osoby, stažení fotek a příběhů, dokáže získat seznam účtů, které komentovaly nějaký příspěvek dané osoby nebo seznam označených u příspěvků dané osoby.

Facebook je místo, kde miliony lidí přispívají své nápady, zájmy a kde se vyjadřují v rámci příspěvků.[37] Tyto příspěvky se rozdělují do několik kategorií a samotný Facebook udává, které z těchto kategorií je možno volně zobrazit a stáhnout. Jedná se o:

- **Aktivita na Facebooku:** Fotky, vytvořené příspěvky, účast ve skupinách, označení v příspěvcích a další.
- **Osobní údaje:** Informace poskytnuté při nastavování účtů a profilů.
- **Kontakty:** Informace o tom s kým je daná osoba v kontaktu, jaké má přátele a sledující.
- **Zaznamenané informace:** Informace, jako je historie vyhledávání.
- **Informace o zabezpečení a přihlašování:** Aktivita účtu a technické informace.
- **Aplikace a weby mimo Facebook:** Aktivita obdržená od aplikací mimo Facebook.
- **Předvolby:** Akce, pomocí kterých si uživatel přizpůsobil Facebook.

- **Informace týkající se reklam:** Interakce s reklamami a inzerenty na Facebooku.[51]

Facebook nabízí vcelku širokou škálu informací o uživatelích, které nám jsou volně dostupné. Na základě všech těchto kategorií, které určují rozsah, co je na platformě volně dostupné, vznikly různé OSINT nástroje, které těchto funkcí využívají. Jedním takovým nástroje je Whopostedwhat, což je nástroj, který za pomocí klíčových slov a času zobrazí výsledky, které obsahují toto klíčové slovo. To znamená, že pokud uživatel chce vyhledat všechny příspěvky, které obsahují slovo *VUT* a jsou z roku 2019, tak tyto informace zadá do nástroje a tato akce následně uživatele přesune na nový list, kde bude mít vyfiltrované výsledky na základě uvedeného klíčového slova a roku. Toto filtrování nabízí i samotný Facebook, ale tento nástroj, ulehčuje uživateli práci, jelikož nástroj nabízí určité přednastavené filtry, které stačí vyplnit a nástroj udělá zbytek.

Druhým užitečným nástrojem je Facebook Lookup ID. Ten nám umožňuje zjistit, jak je zřejmé z názvu, zjistit Facebook ID daného profilu. Pro vysvětlení, tento Facebook ID je řetězec čísel, které uživatele neidentifikují, ale je spojen s profilem uživatele a každý, kdo zná ID tohoto uživatele může vidět, jak jeho profil, tak i jeho veřejné informace.[52]

X (dříve Twittwer) je sociální síť, kde lidé sdílejí krátké příspěvky ať už ve formě textu, fotek, videí apod.[53] Těmto přpříspěvkům se nazývá tzv. tweety. Tato sociální síť je velice populární hlavně v Americe. Podle OSINT Frameworku, je na Twitter nejvíce OSINT nástrojů oproti všem ostatním sociálním sítím. Proto zmíním pár nástrojů pro vyhledávání, analýzu a geolokaci.

Na platformě X je možno najít přesné výsledky vyhledávání za pomocí pokročilého vyhledávání. Jedná se o funkci, která je zabudovaná přímo v X. Díky této funkci je uživatel schopen vyhledat příspěvky na základě, slov, hashtagů, účtů a dalších. Tato funkce by se dala přirovnat k Google Dorkingu, jelikož se dotazuje obdobným způsobem.

K analyzování existuje výborný nástroj TWINT, který slouží k Twitter Scrapingu, tedy získávání informací o účtech bez nutnosti přihlášení a použití Twitter API.[54] Tento nástroj vám ukáže, kdy je daný uživatel nejčastěji aktivní na síti, celkový počet tweetů, vytvoří seznam sledujících dané osoby a mnoho dalšího.

Jako poslední nástroj, který bych chtěl zmínit, se týká geolokace. Nástroj s názvem onemiliontweetmap, který lze nalézt na stránce *onemiliontweetmap.com*, umožňuje uživateli zobrazit, z jaké lokace byl příspěvek sdílen a od koho. Tento nástroj dokáže být také velice užitečný, jelikož můžeme zjistit z které oblasti daná osoba sdílí své příspěvky.

Telegram je cloudová desktopová a mobilní aplikace, která poskytuje bezpečné a rychlé zasílání zpráv.[55] Oproti ostatním sociálním sítím, jako je Facebook, X

a další, je Telegram hybrid mezi zasíláním zpráv a sociální sítí.[56] Díky tomu Telegram umožňuje uživatelům různé způsoby, kterými na platformě mohou komunikovat. Uživatelé mohou komunikovat skrz soukromé chaty, soukromé skupiny, veřejné skupiny a nebo tzv. kanály, které umožňují vysílat veřejné zprávy širokému publiku.[56] Jelikož Telegram si zakládá na soukromí, stal se místem mnoha ilegálních skupin prodávající drogy, zbraně a další.[57]

Telegram, stejně jako ostatní sociální sítě, disponuje jistými funkcemi, které je možné v rámci technik OSINT využít. Mezi tyto funkce patří například monitorování klíčových slov, jako například názvy různých malwarů, ransomwarových kampaní a podobné.[58]

Reddit je fórum, kde lidé mohou sdílet obsah, vytvářet komunity a v rámci těchto komunit se zapojují do diskuzí.[59] Tyto komunity si na Redditu vytváří tzv. subreddity, což se dá chápat, jako taková stránka plná příspěvků na dané téma. Tyto subreddity bývají často regulované administrátory a nastavují určitá pravidla chování.

Co se týče nástrojů pro Data Scraping Redditu, tak stojí za zmínku Reddit Comment Visualizer. Tento nástroj po zadání uživatelského jména zobrazí graf, kde následně po zadání data ukáže graf, kdy, co a kde uživatel komentoval.

Druhým nástrojem je *subreddits.org*. Jedná se o databázi 3 000 subredditů na různá témata.

Poslední sociální sítí je **LinkedIn**. LinkedIn je sociální síť, která je navržená hlavně pro podnikatele, firmy, manažery a osoby, které třeba hledají zaměstnání nebo spolupráce v rámci podnikání.[60]

LinkedIn dokáže být pro OSINT vyšetřovatele, velmi zásadním zdrojem obzvlášť v případě, kdy cíl, o kterém chce vyšetřovatel zjistit informace, je někdo ze společnosti, která LinkedIn využívá. Důvod je takový, že společnosti na této platformě rádi sdílejí fotografie nebo vieda například svých zaměstnanců nebo okolí firmy a podobně. Tyto fotografie můžou poskytovat vyšetřovateli citlivé informace, jako jsou visačky, které následně je jednoduché naklonovat a upravit, takže vyšetřovatel může předstírat, že je součástí firmy v rámci nějakého sociálního inženýrství.[45] V praxi by se tato taktika využila třeba u dříve zmíněného Red Teamingu.

Pokud vyšetřovatel bude chtít shromáždit informace, kteří zaměstnanci pracují pro cílenou společnost, může využít nástroj ScrapedIn. ScrapedIn je nástroj, který podle konkrétní zadané společnosti vytvoří podrobný seznam zaměstnanců, které pro danou společnost pracují.[61] Díky tomuto nástroji může vyšetřovatel zjistit informace o pracovnících v podobě jejich jména, příjmení, bydliště a dalších, které mají uvedené na svém profilu.

Tato podkapitola objasnila fungování OSINTu v rámci sociálních sítí, představila sadu různých užitečných nástrojů pro různé sítě. Další podkapitola se zaměří trochu

hlouběji do internetu a to konkrétně do Dark Webu.

2.3.3 Dark Web a Deep Web

Pojmy Dark Web a Deep Web jsou veřejně známy a spojovány s nelegálními nabídkami, jako nakupování drog, nájemných vrahů, poskytování dětské pornografie a dalších. Ovšem mnohokrát jsou tyto dva pojmy zaměňovány, přitom každý z nich znamená něco jiného.

- **Povrchová síť (Surface Web)** je klasický internet, jaký všichni znají. Podle zdroje *digitalsilk.com* byl v roce 2024 naměřen počet webových stránek a to přibližně 1.1 miliardy.
- **The Deep Web** jedná se o vrstvu webu, která není indexovaná a tudíž není přístupný tradičním vyhledávačům.[62] Deep Web může být například online bankovní účet, který je přístupný jen a pouze po zadání přihlašovacích údajů. Deep Web je nemožné měřit, respektive zmínit jeho velikost, jelikož se neustále rozrůstá, vytvářením nových účtů a podobně.[62]
- **Dark Web** označuje zašifrovaný online obsah, který není indexovaný standardními vyhledávači a uživatelé si tento obsah mohou zobrazit jen za pomocí specializovaných služeb, jako je vyhledávač Tor.[63] Dark Web je součástí Deep Webu, ale není známo, o jak velkou součást se jedná a kolik legálního a nelegálního obsahu se na Dark Webu nachází[62]

Než vyšetřovatel začne sbírat data na Dark Webu musí vědět, jak se na Dark Webu pohybovat. Aby tak mohl učinit, bude k prohlížení potřebovat prohlížeč Tor. Prohlížeč Tor je prohlížeč, který anonymizuje síťový provoz a tím umožňuje soukromé prohlížení webu.[64] Díky této anonymitě je široce používán pro přístup k Dark Webu. Tor funguje na principu, kdy skrývá IP adresy a aktivitu při procházení tím, že přesměrovává webový provoz přes řadu různých směrovačů, které jsou nazývány uzly.[64] Bohužel i tato komunikace dokáže být dnes narušena, jelikož Tor nedokáže zabránit sledování vstupních a výstupních uzlů sítě, a proto je doporučeno při vyhledávání používat i VPN.[64]

Díky této anonymitě je Dark Web ideální prostředí pro přenos informací, kterými můžou být například různé uniklé informace, zboží a služeb s potenciálně nelegálními úmysly, a proto zde orgány činné v trestním řízení mají velký zájem o shromažďování informací za pomocí OSINT.[65] Pokud vyšetřovatel začne OSINT vyšetřování na Dark Webu, musí si důkladně promyslet, zda chce sbírat informace o specifické osobě nebo o aktivitách a komunikaci určité stránky na Dark Webu.[65]

Na Dark Webu se nepoužívají klasické webové prohlížeče, jako jsou Google, Bing a podobně, jako na Surface Webu.[62] Uživatelé často k prozkoumávání Dark Webu využívají tzv. Hidden Wiki, která připomíná vzhledově Wikipedii, ale obsahuje od-

kazy na různé stránky nacházející se na Dark Webu.[62] Problém ovšem je, že většina z těchto stránek bývá ať už nefunkční nebo to jsou falešné stránky, za účelem okrádat nic netušící uživatele o peníze.

Pro pokročilejší vyhledávání, které využívají OSINT vyšetřovatelé na Dark Webu, slouží speciální vyhledávače a nejpopulárnějším z nich je *Ahmia.fi*, která vrací pouze výsledky související s Tor prohlížečem (až na dětskou pornografii, kterou filtruje).[63] Naproti tomu ještě existuje Grams, což je specifičtější vyhledávač podobný Googlu.[62]

Druhá technika, která se na Dark Webu používá je tzv. *Crawling*. Web Crawleři jsou softwarové programy, které prohledávají internet metodicky, automatizovaným způsobem za účelem objevování dostupných webových zdrojů a jsou obvykle používány vyhledávači, jako Google, Bing a další, pro objevování a indexování webových zdrojů.[66] Tyto Web Crawlery je možné aplikovat, také na samotný Dark Web, kde fungují podle následujících kroků:

1. Jakožto začínající bod pro procházení, začínají sadou výchozích adres URL
2. Načtou si nalezený obsah těchto URL a začnou analýzu
3. Extrahují hypertextové odkazy, které na daných URL adresách naleznou
4. Extrahované URL adresy uloží do fronty
5. Načte se každá URL adresa ve frontě a celý proces se opakuje[66]

Tyto techniky se používají pro hromadné hledání na Dark Webu. Hlavně kvůli nelegálním činnostem, jako jsou například materiály pro zneužívání dětí.

Jako poslední zmíním analýzu síťového provozu a de-anonymizaci. Orgány činné v trestním řízení kontrolují síťový provoz na Dark Webu a tzv. ho de-anonymizují využitím unikátních vlastností každé stránky na Dark Webu nebo na základě údajů získaných analýzou probíhajícího síťového provozu komunikace.[66] Síťový provoz na Dark Webu je analyzován pomocí již výše zmíněných Crawlerů, které analyzují jednotlivé darknety na základě tagů, textů apod.[67]. Zmíněná de-anonymizace, jak název napovídá, slouží k odhalení identity jednotlivců, kteří se na Dark Webu snaží skrýt díky své anonymitě. De-anonymizace uživatelů darknetu se provádí buď prostřednictvím specifických charakteristik dané sítě nebo analýzou síťového provozu vznikajícího při komunikaci v rámci darknetu.[66]

2.3.4 Využití z pohledu etické osoby

Tato kapitola se zaměřuje na to, jak využívají OSINT etické osoby. I přes to, že už jsem nějaké příklady využití zmínil v předešlých kapitolách, jako je například postup při hledání nezvěstné osoby, myslím si, že stojí za zmínku ještě pár dalších využití techniky OSINT a to ať už v rámci žurnalistiky, náboru zaměstnanců nebo třeba k poskytnutí pomoci při katastrofě.

Žurnalista je osoba, která sbírá, ověřuje a šíří informace. Pro novináře tento přístup digitálního vyšetřování a využití techniky OSINT umožnil nové možnosti pro investigativní žurnalistiku a také zpřístupnil novinářům informace, které byly dříve obtížné získat nebo byli přímo nedostupné.[68] Příklad online novinářů, kteří techniku OSINT využívají, jsou tzv. Bellingcat. Jedná se o skupinu, kterou tvoří civilní žurnalisté, výzkumníci, vyšetřovatelé a další, kdy za pomocí veřejných zdrojů a sociálních sítí zkoumají různá témata.[69]

Jelikož se digitální vyšetřování stalo nedílnou součástí žurnalistiky, novináři si museli osvojit dovednosti ať už v oblasti kódování, analýzy dat nebo třeba i kritické datové gramotnosti.[68]

Techniku OSINT si osvojili nejen novináři nebo etičtí hackeři, ale také recruiteři neboli náboráři, kteří se starají o nábor nových zaměstnanců do společnosti. Studie z roku 2012 ukazuje, že 13% společností Dax (německý burzovní index Frankfurtské burzy) zahájilo, při náboru potenciálních zaměstnanců, průzkum dostupných informací o zájemcích a jejich minulosti.[69]

V neposlední řadě bych chtěl zmínit využití OSINTu a SOCMINTu při přírodních katastrofách. Při takových událostech může být shromažďování informací pomocí techniky OSINT využito například těmito způsoby:

- **Lepší přehled o situaci** - Videa, fotky a jiné informace z místa dění mohou dát mnohem lepší představu o tom, v jaké situaci ohrožení se obyvatelé nachází.
- **Geograficky cílené hodnocení rizik** - Jedná se o přehled událostí, které by mohli v blízké době ohrozit hlídanou oblast. Jedná se například o blížící se extrémní počasí nebo o teroristické hrozby.
- **Správa dezinformací** - Správa dezinformací se řeší v takových případech, aby obyvatelé neztráceli drahocenný čas nebo zdroje. Dezinformace můžou šířit v takové situaci například podvodníci za účelem zisku.[70]

Jak jsem již zmínil v podkapitole *Sociální sítě*, sociální média jsou dnes velmi cenným zdrojem informací a to platí i v případech přírodních katastrof. V Japonsku při zemětřesení hrál velkou roli SOCMINT v zjišťování informací o situaci osob, kteří tyto informace zveřejňovali na platformy Twitter a Facebook.[70] Vyšetřovatelé, po zpracování těchto informací, mohou pro jednotlivce v daných oblastí vyhodnotit závažnost situace a podle toho vytvořit například evakuační nebo záchranný plán.

2.3.5 Využití z pohledu neetické osoby

OSINT se nepoužívá jen a pouze eticky. Je to technika, která se dá jednoduše zneužít proti někomu jinému, jako tomu bylo u rappera Pop Smoke.

Útočníci za pomocí OSINTu zjistili, kde se zrovna Pop Smoke nachází na základě fotek, které byly zveřejněné na platformu Instagram. Rapper zprvu zveřejnil,

že u sebe má velký obnos peněz v hotovosti, což mohlo útočníkům dát dostatečný motiv. Další příspěvky v podobě příběhů na Instagramu zveřejňované Pop Smokem už napověděli útočníkům, kde se přibližně rapper nachází. Rapper zveřejnil fotku, kde stál před domem. To ještě nevěděl, že tato fotka bude jeho osudná, jelikož díky tomu se útočníkům odhalila přední část domu a popisné číslo. Díky těmto fotkám byli útočnici schopni určit přesný dům, ve kterém se celebrita zrovna nacházela. Další nápomocný zdroj byly fotky, které poskytovala společnost, která pronajímala tento dům. Tento zdroj pomohl útočníkům určit, jak dům vypadá uvnitř a kudy se dostat do oblasti. Dům byl z velké části prosklený, takže bylo vcelku snadné se vloupat dovnitř. Útočníci nakonec pronikli do tohoto domu a Pop Smoke byl 19.2. 2020 zastřelen.[71]

Ačkoliv útočníci nepronikli do žádného počítačového systému, využili OSINT k provedení průzkumu neboli Reconnaissance, který tvoří první fázi tzv. *Cyber Kill Chainu*. Průzkum se soustředí na pozorování běžných operací cíle, aby se získaly cenné informace, například o používaném hardwaru a softwaru a komunikačních vzorcích.[72] Získané informace pak slouží jako podklad pro následující fáze útoku a výrazně usnadňují jejich realizaci.

Cyber Kill Chain je model, který popisuje postup, respektive cestu kyberútočníka, který má za cíl proniknout do počítačového systému.[73]. Z hlediska obrany a prevence útoků je klíčové porozumět tomu, že jednotlivé fáze na sebe navazují a úspěšný průzkum výrazně zvyšuje efektivitu všech následujících kroků. Cyber Kill Chain se skládá ze sedmi kroků.

1. **Průzkum (Reconnaissance)** - Jedná se o sběr informací o individuální osobě nebo organizačním subjektu.[73] Průzkum se dále dělí na pasivní průzkum, kdy útočník nemá žádnou interakci s cílem a aktivní průzkum, kdy útočník naopak má přímou interakci s cílem, aby získal informace, které by mohli být zneužity v pozdější fázi.[74] Technika OSINT je součástí této fáze Cyber Kill Chainu a z definice spadá konkrétně do **pasivního** průzkumu.
2. **Vyzbrojení (Weaponize)** - V této fázi útočník, na základě získaných informací, vytváří škodlivý software, který je vytvořený na míru pro proniknutí do systému.[74]
3. **Doručení (Delivery)** - Nasazení kybernetické zbraně v cílovém prostředí.[73] Může se jednat o nakažené USB zařízení, škodlivé e-maily a podobné.[74]
4. **Exploit** - Exploit je fáze, kdy útočníkem vytvořená kybernetická zbraň úspěšně využije existenci zranitelnosti cílového systému.[74]
5. **Instalace (Installation)** - Jedná se o instalaci, aktualizaci a následné ovládání škodlivého softwaru, který je nainstalovaný na cílovém zařízení oběti.[73] V této fázi se útočník mimo jiné snaží vyhnout jakékoliv detekci ať už před antivirusem nebo jiným detekčním systémem.[74]

6. **Řízení a ovládání (Command and Control)** - Útočník převezme kontrolu nad cílovým zařízením a vytvoří tzv. zadní vrátka (backoor) pro uchování přístupu.[74]
7. **Opatření k dosažení cílů (Action on Objectives)** - Nyní po zřízení komunikace s cílovým zařízením, útočník využívá příkazy na základě jeho zájmů a může se jednat o nějaký hromadný útok, kdy útočník chce zaútočit na více systémů nebo chce sestavit tzv. BOTNet, a nebo cílený útok, kdy útok je mnohem obezřetnější a sofistikovanější, aby byl útočník schopen získat tajná, resp. citlivá data oběti.[73]

Během průzkumu může útočník získat citlivá nebo soukromá data a rozhodnout se je zveřejnit bez souhlasu dotčené osoby, čímž by došlo k tzv. doxingu. *Doxing* nebo také *Doxxing* či *d0xing*, je definován, jako shromažďování nebo sdílení soukromých či identifikačních údajů o konkrétní osobě online bez jejího souhlasu.[77] Získání soukromých či citlivých údajů je možné i za pomocí OSINTu. Dané soukromé údaje mohou být veřejně dostupné na webu, avšak nemusí být snadno dosažitelné, což znamená, že běžný uživatel bez použití OSINT a určitého úsilí, se k těmto datům jen tak nedostane.[75] Příkladem takových dat, by mohli být veřejně dostupné kamery, které by útočník mohl najít pomocí nástrojů, jako Shodan, kde by následně bylo možné vidět do oken bytů a útočník by pořídil snímek oběti, která se například zrovna převléká. Útočník by pak zneužíval tento snímek proti oběti ať už v rámci nějakého vyhrožování, stalkování nebo nějakého očernění dané oběti, za účelem se pomstít.[76] Ovšem mezi tyto citlivé údaje mohou patřit i informace z uniklých dat firem, uniklé vládní informace, organizační záznamy a nebo třeba informace získané přímo od oběti a to ať už úmyslně či neúmyslně.[75]

Podle Douglase by se Doxing dal kategorizovat na 3 typy a to de-anonymizace, zaměření a de-legimitizaci.

- Doxing typu de-anonymizace odhalí identitu oběti, která byla do daného okamžiku známá pod nějakým pseudonymem a nebo tato osoba známá doposud nebyla, tedy byla anonymní.[75] Toto může být typický příklad tzv. influencerů na platformě YouTube, Twitch a jím podobné, kdy vystupují pod určitým pseudonymem a zakrývají svoji tvář.
- Doxing zaměření na danou osobu odhaluje fyzickou lokalitu oběti ať už se jedná o lokalitu, jejího bydliště nebo zaměstnání.[75] Takový doxing může být součástí žertů, jako objednání Pizzy se jménem známého vraha na adresu oběti a nebo může také vést přímo k vyhledání a fyzickému napadení.[75]
- Doxing typu delegitimizace slouží k poškození reputace nebo důvěryhodnosti oběti, se snahou oběť zahanbit a ponížit.[75] S tímto typem se dnes velmi potýkají mladí jedinci v rámci kyberšikany, kdy si mezi sebou přeposílají citlivé informace o obětech.[77]

Doxing nejen že je neetický, ale porušuje také mnoho právních ustanovení. Doxing často zahrnuje zveřejňování osobních údajů, což je v rozporu s nařízením GDPR.[78] Pokud by útočník zveřejnil osobní údaje oběti, jako například telefon, e-mail nebo bydliště, dopustil by se tím nezákonného zpracování osobních údajů.

Na Doxing by se mohla vztahovat skupina trestných činů, kde dochází k neoprávněnému užití informací a to za pomocí použití Internetu, kdy v této dané souvislosti je možné uvést ustanovení zejména § 180 (Neoprávněné nakládání s osobními údaji), § 316 (Vyzvědačství), § 317 a § 318 (Ohrožení utajované informace) trestního zákoníku.[28] Pokud by se útočník dostal k soukromým fotkám a tyto fotky následně zveřejnil bez souhlasu dané osoby, je možné, aby se dotčená osoba domáhala ochrany svých práv a to v rámci občanskoprávního řízení (konkrétně by se jednalo o § 84 občanského zákoníku o ochraně soukromí).[28]

Výše jsem zmínil, že Doxing může vést ke stalkingu nebo vydírání a to i v rámci kyberšikany. Kyberšikana, podobně jako tradiční šikana, není sama o sobě považována za trestný čin ani přestupek, jelikož záleží na jednání, kterým útočník šikanoval.[28] V případě Doxingu by toto jednání mohlo mít podobu právě zmíněného vydírání, kdy by se uplatnil § 175 trestného zákoníků o Vydírání.[27] V případě stalkingu a obtěžování oběti, je možné využít ustanovení § 354 trestného zákoníku, který pojednává o Nebezpečném pronásledování.[28]

Pokud se například útočník dostane k **neodeslaným** zprávám, což je v této skutkové podstatě vyjádřeno slovem *tajemství*, a poté bude jednat za účelem způsobení škody jinému nebo získání neoprávněného prospěchu pro sebe nebo jiného, § 182 trestného zákoníku by nabyl své skutkové podstaty.[28] (viz. kapitola *Právní limity etického hackingu*)

Další kapitola se zaměřuje také na právní limity, ale tentokrát v rámci OSINTu samotného.

2.4 OSINT a jeho právní limity

Jelikož technika OSINT se využívá pro sbírání informací z veřejně dostupných zdrojů, jedná se o zcela legální činnost. Nicméně, jak bylo uvedeno v části věnované etickému hackingu, i v rámci této techniky existují určité právní a etické hranice, jako například ochrana soukromí, ochrana osobních údajů a další.[79] Tyto limity se v mnoha ohledech aplikují i na aktivity spojené s OSINT. Tato kapitola se zaměřuje na případy, kdy v rámci techniky OSINT nebo také v kontextu praktického využití nástrojů, jako je např. nástroj Puppint a jím poskytovaných funkcionalit, může dojít k porušení českých, respektive evropských práv.

Prvním právním ustanovením, který se váže k OSINT je ochrana soukromí, tedy § 84 občanského zákoníků, který stanoví, že zachytit jakýmkoli způsobem podobu

člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.[80]. Dále pak § 86 občanského zákoníku vyjmenovává zakázaná jednání v rámci ochrany soukromí, kde jedním z těchto jednání je sledování soukromého života jiného, a to včetně pořizování videozáznamu nebo audiozáznamu pozorované osoby.[28]

V případě, kdy by OSINT vyšetřovatel pravidelně monitoroval osobu v rámci svého vyšetřování a uchovával si nějaké poznámky v podobě snímků obrazovky mohlo by se jednat o stalking či kyberstalking, který je možný subsumovat pod ustanovení § 354 trestného zákoníku o nebezpečném pronásledování.[28] Je velmi úzká hranice mezi prováděním konkrétních, cílených a krátkodobých pozorování a činnostmi, které by mohly být vnímány jako zásah do soukromí.[66]

Ovšem existují jisté výjimky, kdy by svolení do zásahu soukromí vyšetřovatel nepotřeboval. Svolení k zásahu do výše uvedených práv není nutné, pokud je podobizna či zvukový nebo obrazový záznam pořízen nebo použit k ochraně práv či oprávněných zájmů jiných osob, nebo je pořízen či použit na základě zákona k úředním účelům, při veřejném vystoupení ve věci veřejného zájmu, nebo pro vědecké, umělecké účely či zpravodajství v médiích, jako je tisk, rozhlas nebo televize.[28] To znamená, že výjimky existují jen v přesně stanovených případech, například při ochraně práv, úředních činnostech nebo při zpravodajství.

Uchování jistých informací může být také pro OSINT vyšetřovatele problematické. V případě, kdy vyšetřovatel, který provádí online vyšetřování zahrnující dětskou pornografii (například v případě hledání na Dark Webu) a **vědomě** uchovává obsah pocházející z těchto stránek, může dojít k naplnění skutkové podstaty § 192 trestního zákoníku (Výroba a jiné nakládání s dětskou pornografií).[27] Přechovávání zahrnuje jakoukoli formu držení dětské pornografie, přičemž nezáleží na délce držení ani na fyzickém umístění, stačí, že je dětská pornografie v moci pachatele, například v e-mailu nebo cloudovém úložišti.[28] Existuje ovšem výjimka pro tzv. agenta čímž je příslušník Policie České republiky a nebo Generální inspekce bezpečnostních sborů, který může být použit například k odhalení trestné činnosti související se zneužíváním dětí k výrobě pornografie.[28]

Další zajímavý aspekt v této problematice je, zda data, která jsou shromažďována jsou opravdu veřejná. Za veřejné by se daly považovat i sociální sítě, jelikož k nim je volný přístup. Nicméně problém spočívá v tom, že tyto služby stojí za registrací. Ačkoli je registrace bezplatná, uživatel musí uzavřít smlouvu se sociální sítí a souhlasit s jejími podmínkami poskytování služeb.[69] Tyto podmínky samozřejmě uživatel musí dodržovat, aby platformu mohl využívat.

Touto problematikou se zabýval i samotný Ústavní soud České republiky v Nálezu ze dne 30. října 2014, sp. zn. III. ÚS 3844/13. Ten uvedl, že povaha údajů na sociálních sítí není jednoznačně veřejná či soukromá a závisí na každém uživa-

teli na tom, jakou míru soukromí na svém profilu zvolí.[81] Jestliže se orgány činné v trestném řízení rozhodnou zjišťovat z facebookového profilu informace soukromé povahy, musí dodržovat rámec stanovený zákonem a respektovat obecné principy, na nichž je založena jejich činnost, zejména šetřit ústavně zaručená práva a svobody dotčených osob.[81]

Z toho plyne, že je důležité odlišovat, zda jsou sbírané informace z veřejně dostupného profilu a nebo zda jsou chráněny nastavením soukromého profilu. Je také důležité zajistit, aby použití OSINT nástrojů nebylo v rozporu s podmínkami služeb, například při automatizovaném přístupu na Facebook či Instagram nebo při tvorbě falešných účtů, přičemž například Facebook navíc aktivně blokuje služby související s OSINT.[69]

Problém tedy nespočívá pouze ve shromažďování informací, ale také v jejich využívání, nicméně nedostatek komplexního mezinárodního právního rámce pro OSINT vytváří prostor pro nejasnosti.[82] Avšak tomu, jak by vyšetřovatel měl postupovat při OSINT vyšetřování a dodržovat právní rámec GDPR bude vysvětleno v následující kapitole.

2.4.1 GDPR

V důsledku dynamického vývoje online prostředí a technologií je nevyhnutelné, aby byly osobní údaje jednotlivců a jejich soukromí chráněny před neoprávněnou manipulací, zneužitím a použitím. Primární povinnost na zabezpečení této ochrany mají především správci a zpracovatelé osobních údajů.

V oblasti ochrany osobních údajů bylo přijato několik právních předpisů. Významným předpisem přijatým na úrovni Evropské unie je Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Toto nařízení, jinak nazývané GDPR (General Data Protection Regulation), je evropské nařízení, které reguluje, jak mohou být osobní údaje zpracovány a to včetně těch získaných z otevřených zdrojů.[83] V roce 2019 byl přijat Zákon č. 110/2019 Sb. o zpracování osobních údajů v České Republice. Tento zákon implementuje relevantní předpisy Evropské unie, doplňuje přímo použitelný předpis EU a stanovuje práva a povinnosti při zpracování osobních údajů s cílem zajistit ochranu soukromí každého jednotlivce.[84]

S rostoucím významem ochrany osobních údajů v digitálním prostředí je důležité zaměřit se i na to, jaké konkrétní aspekty GDPR by měli zohledňovat OSINT vyšetřovatelé v praxi. Block uvedl 5 klíčových aspektů GDPR pro OSINT vyšetřovatele:

- **Zodpovědnost** - Pokud kdokoliv zpracovává osobní údaje a podléhá GDPR,

měl by dodržovat GDPR a také být schopen prokázat, že tak i učinil. Nejlepší prevence je dokumentace podniknutých kroků při zpracovávání těchto údajů.

- **Právní základ pro zpracování osobních údajů** - V jádru GDPR omezuje zpracovávání osobních údajů, kdy existuje alespoň jeden ze šesti právních základů pro zpracování osobních údajů (článek 6 odstavec 1.). Pro práci s technikou OSINT jsou relevantní tři z těchto právních základů a těmi jsou souhlas, právní povinnost a oprávněný zájem.
  - **Souhlas** - Článek 7 GDPR uvádí, že subjekt údajů by měl mít svobodnou vůli k udělení souhlasu, ovšem svobodná vůle může být v tomto případě celkem zrádný pojem, jelikož například u vztahu mezi zaměstnancem a zaměstnavatelem, kdy odmítnutí souhlasu zaměstnance v případě nějaké prohlídky nebo něčeho podobného může mít důsledky na jeho zaměstnání. GDPR také uvádí, že souhlas lze kdykoli odvolat, což může být při OSINT vyšetřování vcelku problém, když daná osoba tento souhlas odvolá v průběhu vyšetřování. Z důvodu této právní povahy, se souhlasu vyšetřovatelé vyhýbají.
  - **Právní povinnost** - Právní povinnost může vzniknout v případech, kdy zákony nebo jiné právní předpisy ukládají konkrétním subjektům povinnost shromažďovat, uchovávat nebo zpracovávat osobní údaje, například za účelem prevence trestné činnosti, vyšetřování podvodů a dalších. Příkladem tohoto může být případ, kdy klient vyšetřovatele má právní povinnost identifikovat své zákazníky a zdroj jejich finančních prostředků podle předpisů proti praní špinavých peněz (zákon AML).
  - **Oprávněný zájem** - Třetím nejpoužívanějším právním základem je oprávněný zájem, který vzniká v případě, kdy jsou data získávána za účelem uplatnění svých práv. Příkladem tohoto může být jakákoliv občanskoprávní obžaloba, kde obě strany sporu mají oprávněný zájem na shromažďování osobních údajů na podporu svého případu.
- **Uplatňování klíčových zásad při zpracování osobních údajů** - Jedná se o dodržování zásad, které jsou uvedeny v článku 5 GDPR. Mezi zásady patří zákonnost, tedy aby metody shromažďovaní informací byli zákony povoleny, korektnost, která se zabývá otázkami v rámci závažnosti shromažďování osobních údajů, jejich množství apod. a transparentnost, kdy zpracovatel musí být transparentní v případě, kdy se jedná o účel a typ zpracovaných údajů. Další právní zásadou je minimalizace údajů, která pojednává o zpracování osobních údajů na takovou míru, která je potřebná k dosáhnutí cílů zpracování údajů, to znamená pouze tolik, kolik je nutné. Právní základ přesnost udává, že zpracovaná data musí být aktuální a kvalitní
- **Předvídání, chápání a dodržování práv subjektu údajů** - Dle GDPR má

subjekt údajů právo na to být informován o zpracování osobních údajů, právo k přístupu, právo na opravu, právo na vymezení zpracování údajů a právo na vymazání údajů. Ovšem podle článku 23 GDPR je možno omezit některé povinnosti správců údajů, včetně oznamovací povinnosti, Z nich jsou pro výzkum OSINT pravděpodobně nejrelevantnější:
  - Vyšetřování, prevence, odhalování nebo stíhání vůči trestnému činu
  - Ochranu subjektu údajů nebo práv a svobod jiných osob
  - Vymáhání občanskoprávních nároků nebo vyšetřování, stíhání, prevence a odhalování v rámci porušení etiky regulovaných povolání.
- **Uvědomovat si zda osoba využívající OSINT je správce nebo zpracovatel údajů** - Správce údajů je ten, kdo určuje, jaké jsou účely zpracování osobních údajů a jaké k tomu použije prostředky. Zpracovatel údajů je naopak ten, kdo zpracovává tyto osobní údaje jménem správce. Určení, zda je osoba zpracovatel nebo správce osobních údajů závisí na míře svobody, kterou daná osoba má v rámci výběru účelu a metod zpracování údajů, jelikož pokud osoba určuje účel, typy údajů a použité metody, nemůže tvrdit, že je zpracovatel, když ve skutečnosti údaje "řídí".[79] Obecné nařízení se nevztahuje na činnosti fyzických osob, při nichž jsou osobní údaje zpracovávány výhradně pro osobní nebo domácí potřebu, například při tvorbě rodinného rodokmenu určeného pouze pro osobní účely.[85]

Ochrana osobních údajů však není pouze právní otázkou, ale je nezbytné ji řešit i z pohledu vývoje softwaru. V této souvislosti je možné uvést myšlenku Hoepmana, který specifikoval osm strategií, které se dají uplatnit pro vývoj softwaru a těmi jsou: minimalizovat, schovat, oddělit, agregovat, informovat, kontrolovat, prosazovat a demonstrovat.[86] Tyto strategie by se efektivně dali využít i v rámci sběru informací a to například při minimalizaci, kdy shromažďování a zpracování osobních údajů by mělo být minimalizováno na nezbytné množství, osobní údaje by měly být chráněny před neoprávněným přístupem a zrakem nepovolaných osob, a data by měla být agregována na co nejvyšší úrovni.[66]

Dosažené výsledky prostřednictvím techniky OSINT by mohly ovlivňovat dva přístupy, které rozlišuje Nařízení GDPR v čl. 25. Tyto přístupy se nazývají Privacy by Design a Privacy by Default.

Dané přístupy byli vytvořeny, aby správce zavedl opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů, jako jsou: co nejrychlejší pseudonymizaci osobních údajů, transparentnost s ohledem na funkce, umožnění subjektům údajů monitorovat zpracování osobních údajů a umožnění správcům vytvářet a zlepšovat bezpečnostní prvky.[87] Tyto opatření je mnohdy nutné implementovat i do samotného vývoje aplikací, služeb a produktů, které v rámci své funkčnosti osobní údaje zpracovávají nebo jsou založeny na tom, aby osobní údaje zpracová-

vali a je třeba, aby zhotovitel těchto služeb, aplikací a produktů bral v potaz právo na ochranu údajů.[87]

Společnosti by standardně měli zajistit to, aby osobní údaje nebyly zpřístupněny neomezenému počtu osob a také, aby tyto údaje byly zpracovávány s co největší ochranou soukromí, jako zpracování pouze nezbytné údaje nebo krátká doba uchování.[88] Tento přístup se nazývá „Standardní ochrana údajů" nebo také Privacy by Default.

Privacy by Design je přístup, který zahrnuje integraci ochrany soukromí do návrhu produktů a služeb od jejich počátečního vývoje až po finální podobu.[66] V souvislosti s OSINT, je důležitý pro přizpůsobení návrhu OSINT nástrojů. V ideálním případě je proces technického vývoje nástrojů OSINT kombinován tak, aby zahrnoval normativní požadavky, zejména právní a aby výsledné produkty měly právně vyhovující design, byly přijatelné ve společnosti (social embedding) a zároveň dostatečně flexibilně splňovaly různé požadavky různých skupin koncových uživatelů.[86]

2.4.2 Duševní vlastnictví

Pokud se vyšetřovatel, při shromažďování veřejně dostupných dat pomocí techniky OSINT, setká s informacemi, které spadají pod práva duševního vlastnictví, může narazit na problém s jejich využitím. Práva duševního vlastnictví chrání výsledky tvůrčí činnosti člověka, například filmy, počítačové programy nebo literární díla.[28] Pro OSINT jsou nejvýznamnějšími autorská práva a práva k databázím. Mnoho informací, které jsou dostupné v rámci veřejných zdrojů, je chráněno těmito právy a nelze předpokládat, že se držitel práv vzdal svých práv jen proto, že jeho dílo je veřejnosti k dispozici zdarma nebo že chybí upozornění na autorská práva.[89]

Aby vyšetřovatel při OSINT operacích respektoval práva duševního vlastnictví, měl by dodržovat následující zásady:

- **Kopírování databází**: Databáze mohou být chráněny zvláštním právem pořizovatele databáze, a to i v případě, že jsou veřejně přístupné. Není přípustné systematicky kopírovat nebo extrahovat podstatné části takové databáze bez svolení.[90]
- **Licence**: Licenční smlouvou poskytuje poskytovatel nabyvateli oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném omezeném nebo neomezeném rozsahu a nabyvatel se zavazuje, není-li ujednáno jinak, poskytnout poskytovateli odměnu.[80] Před použitím obsahu by měl vyšetřovatel zjistit, zda je obsah licencován, případně pod jakými podmínkami.
- **Volná užití**: Při používání obsahu chráněného autorskými právy je nutno si vyžádat povolení. Avšak možné řešení může být také spolehnutí se na výjimky týkající se volného užití nebo bezúplatné zákonné licence.[91] Volné

užití je definováno, jako užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu.[28]

- **Distribuce chráněného obsahu**: Materiály chráněné autorským právem by neměly být dále rozšiřovány, zveřejňovány nebo jinak využívány mimo účel osobního použití v rámci analýzy, pokud k tomu neexistuje explicitní svolení.[28]
- **Ochranné známky**: Při zacházení s logy společností nebo jinými chráněnými prvky je třeba dbát na to, aby se zabránilo jejich porušování a aby se neuváděly v omyl nebo nenaznačovaly podporu.[91]

OSINT je také možné využít k ochraně duševního vlastnictví. Pomáhá organizacím monitorovat potenciální hrozby, odhalovat protiprávní jednání a identifikovat slabá místa, která by mohla vystavit jejich duševní vlastnictví riziku ke zneužití.[92] Organizace jsou poté díky tomu schopné detekovat společnosti, které profitují z užívání softwaru bez řádného licencování a přijmout jistá protiopatření k nápravě a zabránění dalšímu zneužívání.[93]

2.4.3 Due Diligence

Due Diligence jsou aktivity, které zkoumají společnost nebo osobu před podepsáním obchodní smlouvy, přičemž cílem je získat co nejvíce kvalitních vstupů, respektive informací, na základě kterých bude možné učinit informativní rozhodnutí.[94] Due Diligence provádějí manažeři fondů, individuální investoři, analytici akciového výzkumu, makléři, ale i společnosti, které uvažují o akvizici jiných společností.[95]

Jedná se opět o hledání informací, ovšem tentokrát z více byznysové stránky. Technika OSINT může hrát v rámci procesu Due Diligence velmi důležitou roli, jelikož OSINT může investorům usnadnit strategickou Due Diligence tím, že poskytne podklady pro posouzení navrhované transakce, ověření komerční atraktivity obchodní příležitosti a schopnosti kupujícího dosáhnout zamýšlené hodnoty.[96]

Jak bylo uvedeno v definici, Due Diligence se používá i v rámci zkoumání jisté osoby, před podepsáním obchodní smlouvy. Pokud se osoba bude ucházet o zaměstnání, zaměstnavatel může využít techniky OSINT v rámci procesu Due Diligence, prozkoumat sociální sítě, veřejně dostupné informace a další, za účelem rozhodnutí, zda osobu do svého zaměstnání přijme či nikoliv.

3 Klamavé účty

Tato kapitola se bude věnovat tzv. klamavým účtům. Klamavé účty využívají hlavně kyberzločinci, za účelem využívání slabin sociálních sítí a jedinců, kteří je využívají, k provádění nezákonných, škodlivých, zavádějících nebo diskriminačních operací.[97] Jelikož klamavý účet je jeden z mnoha způsobů, jak skrýt svoji identitu na sociální síti, popíšu nyní i ostatní typy pro upřesnění rozdílů.

- **Falešné profily (Fake profiles)** - Falešné profily vznikají ať už s dobrým úmyslem, jako toho využívají vyšetřovatelé OSINT nebo se zlým úmyslem, kdy se většinou útočníci snaží obelhat danou osobu. Mezi falešné profily patří **Sybil útoky**, při kterých útočník vytvoří velké množství pseudoanonymních profilů, dále **klamavé účty**, což jsou jednotlivé falešné profily a posledním typem jsou tzv. **sociální botnety**, přičemž botnet je soubor sociálních botů, které řídí člověk a to tzv. botmaster.[98] Tyto botnety poté komunikují s uživateli na různých sociálních sítí a poté navazují komunikaci s botmasterem.[98]
- **Krádež identity (Identity theft)** - Jedná se o krádež identity, kdy nejčastější případ bývá ukradení účtu a následně vydávání se za majitele tohoto účtu. Spadají sem **ohrožené účty**, kdy se útočník dostal do profilového účtu oběti a **unesené účty** při nichž se útočník dostal do profilového účtu a zbavil přístupu původního majitele.[98]
- **Klonování identity (Identity Cloning)** - Tento princip funguje tak, že útočník vytvoří profilový účet na základě identity někoho jiného. Útočníci se snaží dostat mezi přátele a blízké, aby zjistili co nejvíce soukromých informací o oběti. Patří sem **Single-Site klonování identity**, kdy útočník naklonuje profilový účet oběti v rámci jedné sociální sítě. Dalším je **Cross-Site klonování identity**, kde útočník naopak vytvoří klonovaný profilový účet na vícero sociálních sítích a to i na těch, kde se oběť ani neregistrovala.[98]

Klamavé účty jsou profily, které působí na sociálních sítích, blozích, fórech a jim podobných platformách s cílem obelhat ostatní nebo něco či někoho propagovat.[97] Tzv. puppetmasteři zneužívají klamavé účty i v rámci různých anket, kdy se snaží ovlivnit hlasování.[98] Jak již bylo zmíněno výše, v těchto činnostech, jako jsou ankety a jim podobné, jsou Sybil útoky efektivnější, ale existují i případy, kdy se použijí klamavé účty samotné, jako tomu bylo při čínské dezinformační kampani v době COVID-19 na platformě Twitter, kdy více než 23 000 účtů propagovalo tvrzení, že COVID-19 mohl být do Číny dovezen ze Spojených států prostřednictvím šarže humrů z Maine, která byla v listopadu 2019 dodána na trh s mořskými plody ve Wuhanu.[99]

Více klamavých účtů má výhodu a to ať už z důvodu většího zásahu nebo jako zálohu při případném odhalení nebo podobném problému. Vytváří se i tzv. skupiny

klamavých účtů, což jsou skupiny vytvořené jedním tzv. puppetmasterem, které mezi sebou komunikují a snaží se propagovat něco, jakožto skupina.[100] Podle studií je chování klamavých účtů mnohdy jiné oproti normálním účtům na fórech a nebo i sociálních sítích, jako je Facebook nebo X, jelikož se zde snaží získat co nejvíce sledujících nebo vést propagandu v rámci retweetů nebo komentářů.[97] I když se může zdát, že se tímto klamavé účty podobají botům na sociálních sítích, nejedná se o to samé. Klamavé účty jsou řízeny puppetmastery, respektive lidmi, přičemž boti jsou počítačové programy provádějící různé skripty, které mají provádět úkony, jako člověk na těchto sítích, a to za účelem spamu, propagace reklamy apod.[97]

Vytváření klamavých účtů je mnohdy běh na dlouhou trať, protože je potřeba, aby byli dostatečně věrohodní k použití.[101] Vytvořený klamavý účet by měl mít určitou historii na sociálních sítí, kde bude později působit. Čím více této historie bude mít, tím více bude klamavý účet přesvědčivý. Touto historii se má na mysli Facebookový profil s příspěvky klamavého účtu na různých výletech a zábavě, LinkedIn profil, kde se klamavý účet snaží ucházet o práci, profil na platformě X, kde se zapojuje do komunity skutečným a konzistentním způsobem.[101]

Při vytváření klamavého účtu musí puppetmaster brát v potaz spoustu faktorů, aby byl účet efektivní a přesvědčivý. Nejdříve musí vytvořit dostatečně promyšlenou historii, jako odkud pochází, jak se jmenuje, kde studoval, jakým jazykem mluví a hlavně také jakou bude mít osobnost.[102] Odtud může navázat dále na to, kde žije nyní, zda vyznává nějakou víru a jaké má politické postoje.[102] Guise Bule ve svém článku uvádí, že je efektivnější vytvářet klamavý účet ženy, jelikož v případě, kdy puppetmaster vytvoří přesvědčivý klamavý účet v podobě krásné ženy, muži (i vysoce postavení) jsou schopni se svěřit s důvěrnými informacemi se snahou získat si srdce ženy.[101]

Jake Creps uvádí ve svém článku postup vytváření klamavého účtu z pohledu OSINT vyšetřovatele a to následujícím způsobem:

- **Mít zvláštní počítač pro práci s klamavým účtem** - Jedna z nejdůležitější součástí. Pokud by vyšetřoval používal počítač, jak pro osobní účely, tak i pro správu klamavého účtu, tak ne jen, že by byl účet snadno odhalen, ale také by to odhalilo jeho identitu samotnou, čemuž se chce vyšetřovatel za každou cenu vyhnout.
- **Šifrované e-maily** - Hodí se nejen pro používání v rámci klamavých účtů, ale i OSINTu samotného. Pokud by vyšetřovatel používal gmail nebo jemu podobný e-mail, byl by stále pod dohledem daných služeb.
- **Zvláštní telefon** - Creps doporučuje používat zvláštní telefon pro vyšetřování, kvůli podobnému problému, jako s počítačem.
- **VPN** - K velké zvýšení anonymity, je dobré ke všemu používat připojení přes VPN.

- **Profily na sociálních sítích** - Jakmile jsou splněny všechny předchozí kroky, vyšetřovatel je připraven vytvářet profily na různých sociálních sítích, přidávat příspěvky a sledovat další profily, respektive postupně budovat přesvědčivé profily pro klamavý účet.[103]

Dnes je pro vyšetřovatele výhodné si vytvořit klamavý účet, jelikož při některých vyšetřování jde technika OSINT ruku v ruce s technikou HUMINT.[101] Klamavé účty jsou v rámci OSINT využíváni za účelem přístupu k informacím ze soukromých profilů.[104] Cíl tohoto klamavého účtu bývá sblížit se s daným cílem a získat od něj dostatečné, respektive potřebné informace pro dané vyšetřování.[102] Díky klamavým účtům a jejich aktivním využíváním ve vyšetřování, mohou vyšetřovatelé získat hlubší a různorodější informace oproti pasivnímu pozorování.[105] Dalším důvodem také bývá zakrytí své identity k zamezení případné odplaty od vyšetřovaného subjektu.[106]

Ovšem i klamavé účty se dají jednoduše zneužít. Příkladem toho může být takzvaný Catfishing, který je probrán v následující kapitole.

3.1 Catfishing

Catfishing je novodobý fenomén, který se používá k obelhání osoby, za účelem vybudovat online vztah pomocí falešně vytvořené identity.[107] Tento fenomén se začal objevovat a využívat přibližně od roku 2010 na základě filmového snímku *Catfish*, který pojednává o mladém fotografovi jménem Nev, který si vybudoval romantický vztah s 19 letou Megan na platformě Facebook. S Megan se setkal přes její mladší sestru Abby, která krásně malovala a on kupoval její obrázky. Ovšem Megan nebyla osobou, za kterou se po celou dobu vydávala. Nev znal Megan pouze ze zpráv a když se ji snažil konfrontovat osobně, zastihl místo toho pouze její matku Angelu, otce a sestru. Nev později zjistil, že Megan neexistuje a že její profilový Facebook byl založen na základě modelky z jiného státu. Za onu Megan se celou dobu vydávala její matka Angela. [108]

Catfisheři se často zaměřují na jedince, kteří touží po nějakém vztahu či lásce a vynaloží pro to co největší úsilí, aby vytvořili přesvědčivou osobnost.[109] Jinými slovy si tedy vytvoří klamavý účet a hledají oběti, které by byli schopni zmanipulovat. Rozdíl ovšem je, že se více chovají podle své reálné osobnosti než podle osobnosti, kterou zamýšleli pro jimi vytvořený klamavý účet a to ať už ze zvědavosti nebo kvůli osobnímu prospěchu, případně aby experimentovali s různými perspektivami.[110] Příkladem může být případ, kdy by Catfishery byli trenéři, kteří by se vydávali za přátele a společníky hráčů, aby je motivovali k lepší hře.[110]

Protože Catfisheři se zaměřují hlavně na emoce a jedince, kteří těmto emocím snadno podlehnou, často se objevují na seznamkách, jako je Tinder a jemu

podobné.[109] Ovšem důvodů, proč se na těchto platformách vydávají za někoho jiného, může být celá spousta, a to jak se záměrem uškodit, tak i bez něj. Může se jednat například o nejistotu v sami sebe, kdy si například jedinec myslí, že není dostatečně přitažlivý, tak si vytvoří falešný účet s představou toho, jak by chtěl vypadat a podobně.[109] Mohou tuto činnost dělat čistě za účelem finančního podvodu, využít oklamaného jedince k získání citlivých či jiných informací nebo za účelem, aby oklamanému jedinci jednoduše ublížili.[107]

Dalšími častými motivy jsou:

- **Pomsta** - Zde si Catfisheři vytvoří falešnou identitu za účelem ublížení oběti a to ať už psychicky, emočně nebo finančně. Často se jedná o žárlivé ex partnery nebo osoby, které byli oběti odmítnuty někdy v minulosti.
- **Kyberšikana** - Catfisher může vytvořit falešnou identitu, aby získal důvěru oběti, kterou následně obrátí kolem ní. Zde je možné si představit scénář šikany na základní škole, kdy spolužák šikanuje jiného spolužáka tak, že vytvoří falešný profil slečný, která o něj jeví zájem, ale po určitém čase oběť poníží a emočně ublíží.
- **Sociální inženýrství a extrakce důvěrných informací** - Hackeři, firemní špióni, vyděrači a jim podobné používají Catfishing v rámci získávání důvěrných informací o cíli. Aby se k těmto informacím dostali, používají sociální inženýrství.[109]

Catfishing může mít na oběti velice negativní dopad. Oběti uvádějí pocity deprese, úzkosti a paranoie spolu se silnějším prožíváním studu, hněvu a strachu.[107]

3.2 Právní limity klamavých účtů

Jak již bylo zmíněno v předešlých kapitolách, klamavé účty mohou být zneužívány i za účelem nezákonného či škodlivého jednání. V případě tvorby klamavého účtu by uživatel měl dbát na právní rámec, aby nedošlo k porušení jistých právních ustanovení, které by například mohli narušit ochranu soukromí, osobnosti a další. Tato kapitola se věnuje právním aspektům tvorby a správy klamavých účtů a zároveň navazuje na praktickou část práce. Slouží jako právní analýza zaměřená na identifikaci potenciálních rizik spojených s využíváním nástrojů, zejména nástroje Puppint a jeho funkcionality pro generování klamavých účtů.

Nejprve bude pozornost zaměřena na občanský zákoník, kde bude hrát roli zásah do soukromí a ochrany osobnosti, tedy § 81, § 84, § 85 a § 86 občanského zákoníku. Klamavý účet nemusí poškodit čistě jen osobu, ale může ovlivnit i společnost, proto bude důležitý i § 135 občanského zákoníku.

Pokud by se puppetmaster rozhodl vytvořit klamavý účet na základě existující osoby, může tím silně narušit soukromí a ochranu osobnosti jedince. V případě,

kdy by se pomocí klamavého účtu za jedince vydával a pomocí tohoto účtu šířil například kontroverzní názory, dezinformace nebo politická stanoviska, které dotyčný nikdy nevyjádřil, mohlo by tím dojít k poškození jeho vážnosti, cti, soukromí a jeho projevy osobní povahy a tedy k zásahu do jeho osobnosti ve smyslu § 81 občanského zákoníku.[80]

V případě, kdy by puppetmaster použil fotografii jedince pro klamavý účet (například pro profilový obrázek) a to bez jeho svolení, porušil by tím § 84 občanského zákoníku, který stanoví, že zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.[28] Toto právní ustanovení bylo také probráno v kapitole *OSINT a jeho právní limity*.

K fotografii se váže také § 85 občanského zákoníku, který stanoví, že rozšiřovat podobu člověka je možné jen s jeho svolením.[80] K porušení tohoto právního ustanovení může dojít v případě, kdy by puppetmaster sdílel další fotografie daného jedince v rámci svého klamavého účtu (například na profilu na sociální síti). Ovšem jak uvádí druhý odstavec, pokud jedinec svolí k zobrazení své podoby za okolností, z nichž je zřejmé, že bude šířeno, platí, že svoluje i k jeho rozmnožování a rozšiřování obvyklým způsobem, jak je mohl vzhledem k okolnostem rozumně předpokládat.[80]

Posledním právním ustanovením v rámci soukromí a ochrany osobnosti je § 86 občanského zákoníku, který vyjmenovává jednání, která jsou zakázána. Může se jednat například o sledování soukromého života jiného, včetně pořizování zvukového nebo obrazového záznamu této osoby, je zakázáno využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou nebo takové záznamy o jeho soukromém životě šířit.[80] Ve stejném rozsahu chrání občanský zákoník i soukromé písemnosti osobní povahy.[28] To znamená, že puppetmaster by tímto mohl narušit soukromí jedince například v případech, kdy využije osobní informace o osobě bez jejího souhlasu, použije fotografii, kterou pořídil v soukromém prostředí nebo třeba vystupuje za jedince a zveřejňuje soukromé detaily.

Na začátku kapitoly bylo zmíněno, že klamavý účet nemusí poškodit čistě jen osobu, ale může mít vliv i na společnost. Pokud by klamavý účet uváděl, že pracuje v určité společnosti, ale ve skutečnosti u dané společnosti nepracuje, může porušit druhý odstavec § 135 občanského zákoníku, který se týká soukromí a pověsti tím.[80] Porušení by nastalo tím, že například zveřejní v rámci svého profilu podrobnosti o interních prostorech, projektech apod. Pověst by mohla být narušena, pokud by klamavý účet například zastával kontroverzní názory, což se pak může jevit tak, že firma zaměstnává takové lidi, nebo že se s těmito postoji ztotožňuje.

Vedle možného porušení občanskoprávních ustanovení je třeba zohlednit i trestněprávní aspekty tvorby a správy klamavých účtů, zejména v případech, kdy jednání puppetmastera naplňuje znaky trestných činů, jako je neoprávněný přístup k počí-

tačovému systému, podvod nebo vydírání.

Jedním z trestněprávních rizik spojených s vytvářením a správou klamavých účtů je **krádež identity**, známá také jako identity theft. Krádež identity je útok, při kterém dochází k odcizení virtuální identity, tedy jde o jakékoliv převzetí kontroly nad touto identitou.[28] Dalším typem útoku, který byl zmíněný i v kapitole *Klamavé účty*, je klonování identity, který se do tohoto útoku také vztahuje. V těchto případech spočívá jednání útočníka v několika protiprávních krocích zároveň a to například v prolomení přístupových údajů nebo instalaci malwaru do počítačového systému oběti za účelem získání přístupu k její virtuální identitě.[28] Získané informace pak může útočník zneužít buď k útoku přímo na danou osobu, nebo k útoku na jinou osobu, při kterém vystupuje pod ukradenou identitou. Příkladem tohoto může být případ, kdy ex přítel získá, jedním ze zmíněných způsobů, přístup k virtuální identitě své ex přítelkyně, aby se ji pomstil tím, že urazí její kamarádky. Do krádeže identity spadají také botntety, kdy provádějí extrakci dat o uživatelích napadeného počítačového systému.[28].

Těmito činy dojde k naplnění následujících znaků trestných činů dle § 230 trestného zákoníku (Neoprávněný přístup k počítačovému systému a nosiči informací) a pokud útočník odcizí identitu s cílem oklamat jiného, tedy vyvolat v oběti omyl s cílem obohatit se, mohlo by takové jednání být posouzeno i dle § 209 trestného zákoníku (Podvod).[28]

Klamavý účet může být ať už v rámci Catfishingu či nikoliv, nástrojem pro kyberšikanu. Kyberšikanující osoby si často vytvářejí falešné profily v podobě klamavých účtů, aby zakryli, kdo doopravdy jsou.[102] Kyberšikana, jako taková není trestným činem, ovšem kyberšikanující osoba může svoji oběť vydírat, čímž by porušil § 175 trestného zákoníku, který pojednává o vydírání.[28]

Poslední případ se týká autorského práva, u kterého může dojít k porušení při vytvoření klamavého účtu. Puppetmaster může například vytvořit klamavý účet, který v rámci své profilové fotografie bude mít logo, které je považováno za dílo někoho jiného. Dílem se myslí buď literární, umělecké nebo vědecké dílo, které je jedinečným výsledkem tvůrčí činnosti člověka a je vyjádřeno v jakékoliv vnímatelné podobě a to i v podobě elektronické, trvalé nebo dočasně trvalé, bez ohledu na jeho rozsah, účel nebo význam.[28]

Všechny závěry a poznatky získané z analýzy právních limitů budou využity jak v praktické části, tak i při formulaci dokumentace README k nástroji.

4 OSINT nástroj

Následující kapitoly popisují návrh, tvorbu a využití nástroje s názvem Puppint.

Puppint je nástroj vytvořený za účelem sjednocení různých nástrojů pro OSINT analýzu a jednoduchou generaci klamavého účtu pomocí umělé inteligence Gemini. Vzhledem k tomu, že většina OSINT nástrojů je určena pro použití mimo EU, byl celý nástroj přizpůsoben českému prostředí.

Původní zadání práce určovalo vytvoření nástroje pro využití jak v rámci Evropské unie, tak specificky pro Českou republiku. Avšak v průběhu práce jsem došel k závěru, že rozdíly mezi prostředím EU a ČR se od sebe zásadně neliší, přičemž ve většině případů by se jednalo o změnu lokalizace a úpravu jistých vstupních parametrů. Po konzultaci s vedoucím práce jsem se rozhodl plně orientovat na použití nástroje tak, aby byl nástroj efektivní k použití v českém prostředí.

V případě, že by nástroj měl být rozšířen pro evropské prostředí, bylo by zapotřebí přeložit vstupní parametry pro umělou inteligenci Gemini, parametry spouštějícího skriptu `puppint.py` a také přeložit přední část webu.

Součástí nástroje jsou také seznamy českých jmen, příjmení a měst. Některé z těchto seznamů (např. seznam křestních jmen) využívá i umělá inteligence pro dosažení přesnějších výsledků. Seznamy se v nástroji nachází v případě, kdy by umělá inteligence nebyla funkční. Pro rozšíření by bylo nutné přidat jména, příjmení a města, které by odpovídali evropskému prostředí, do jednotlivých existujících seznamů.

4.1 Návrh

Pro tvorbu nástroje byl vybrán Django framework pro Python. Framework Django se tradičně využívá pro tvorbu webových aplikací, mezi které patří populární služby, jako YouTube, Instagram, Spotify a další. Důvodem je přehlednost pro uživatele a jednoduchá implementace.

Následující podkapitoly popisují jednotlivé funkcionality nástroje Puppint.

4.2 PUPPINT

4.2.1 IPstack

IPstack je aplikace sloužící k získání geolokačních dat na základě veřejné IP adresy. Pomocí API lze získat informace o zemi, regionu, městě, souřadnicích daného místa a dalších.

4.2.2 Hunter

Hunter je nástroj, který vyhledává e-mailové adresy, které jsou přiřazené jednotlivým doménám či organizacím. Nástroj také kontroluje, zda jsou jednotlivé e-mailové adresy stále validní.

4.2.3 Shodan

Nástroj Shodan slouží k shromažďování informací o zařízeních připojených k internetu. Shodan oproti indexování webových stránek, jako to dělá Google, indexuje otevřené služby, porty a metadata z odpovědí jednotlivých síťových protokolů z těchto zařízení.

4.2.4 Google Reverse Image Search a Google Dorking

Nástroj Google Reverse Image Search slouží k hledání referencí na uživatelem vložený obrázek. Google Dorking pak provádí konkrétní vyhledávání na základě uživatelem vložných dotazů. API pro tyto služby poskytuje web `serpapi.com`.

4.2.5 Generace klamavého účtu

Ke generaci klamavého účtu je použit seznam jmen, umělá inteligence Gemini a služba Mail.tm pro vytvoření emailové adresy.

Umělá inteligence Gemini od společnosti Google byla vybrána z důvodu poskytování API bez jakýchkoliv poplatků. V nástroji generuje: příjmení, město, adresu a biografii. Nástroj umožňuje také stažení informací o klamavém účtu ve formátu JSON, případně i úpravu jednotlivých informací.

Služba Mail.tm umožňuje vytvořit bezplatně dočasnou jednorázovou anonymní emailovou adresu. Tato služba také poskytuje API, díky kterému můžeme vše vytvořit uvnitř nástroje.

V rámci vytváření klamavého účtu byla zvažována také generace profilového obrázku pomocí umělé inteligence. Většina poskytovatelů této služby však generování obrázků zpoplatňuje. Implementace této funkcionality je nicméně možná, pokud budou k dispozici odpovídající finanční prostředky.

4.2.6 FullHunt

V průběhu vývoje nástroje byl také implementován nástroj FullHunt, který byl později odstraněn. FullHunt je platforma, která společnostem umožňuje průběžně odhalovat, monitorovat a zabezpečovat vnější útočnou plochu a prostředky směřující k internetu, tedy jinými slovy poskytuje analýzu domén a subdomén, umožňuje

zjištění známých zranitelností (CVE). V pozdější fázi vývoje nástroje Puppint se však objevily problémy s rozhraním FullHunt API. Odpovědi z API byly objemné a přenos dat byl často přerušen, což vedlo k neúplnému doručení výsledků. Z tohoto důvodu jsem se rozhodl tento nástroj z finální verze práce vynechat.

4.3 Tvorba nástroje

Po vytvoření Django projektu, bylo zapotřebí vytvořit funkce, které umožní zasílání požadavků a přijímání odpovědí jednotlivých API. Tyto funkce byly nadefinovány ve skriptech `hunter.py, ipstack.py, reverse.py, dorking.py, shodan_api.py` a `tempmail.py`, které odpovídají jednotlivým službám.

Aby jednotlivé API fungovaly, potřebují tzv. API klíče. Řešením bylo přidání souboru `api.env`, do kterého uživatel vloží své API klíče pro jednotlivé služby, aby s nimi funkce mohly pracovat.

Pro generaci klamavého účtu byl vytvořen skript `sockpuppet.py`. Jako první je náhodně vybráno křestní jméno ze seznamu `filtered_worldist_names.txt`. Seznam jmen byl použit z důvodu častého opakování stejných křestních jmen, které generovala umělá inteligence. Dále se náhodně vygeneruje číslo v rozmezí 18 a 45 let, které bude představovat věk. Příjmení, město, ulice a biografie je generována umělou inteligencí.

Posledním prvkem, který je potřeba vytvořit, je emailová adresa. Pro správné vytvoření emailové adresy, byl pro tuto funkci vytvořen skript `tempmail.py`.

Pro zobrazení veškerého obsahu byly potřeba vytvořit tzv. templates neboli šablony v podobě souborů HTML. V rámci templatů, byl pro přívětivější vzhled využit framework Bootstrap 5. Templaty byly navrženy tak, aby byly pro uživatele přehledné.

4.4 Návrhy na zlepšení

Nástroj *Puppint* byl navržen s ohledem na jeho další rozšiřitelnost. Tato podkapitola se zaměřuje na návrhy, jak by bylo možné nástroj dále rozšířit.

Jedním z nedostatků nástroje je absence možnosti generace profilového obrázku pro vytvořený klamavý účet. Tento prvek by bylo možné doplnit využitím generativní umělé inteligence, která umožňuje tvorbu realistických portrétů na základě zadaného textového popisu. Většina těchto služeb je však dostupná pouze ve formě placených API, což v rámci této práce představovalo omezení. V budoucnu by bylo vhodné integrovat tuto funkcionalitu, pokud budou dostupné odpovídající finanční prostředky nebo bezplatné alternativy.

Po vygenerování klamavého účtu by bylo uživatelsky přívětivější, kdyby bylo možné účet ihned upravit, bez nutnosti přecházet do záložky administrace. Toto by bylo možné pomocí přidání JavaScriptu, který by tuto dynamickou úpravu umožňoval.

Image Reverse Search je již v nástroji zakomponován, avšak v rámci funkčnosti vrací URL adresy, které jsou s poskytnutým obrázkem vázané. Existuje ovšem nástroj TinEye, který je daleko přesnější. Je důležité zdůraznit, že pro implementaci TinEye API je zapotřebí finančních prostředků.

API klíče jsou načítány ze souboru `api.env`, do kterého je uživatel povinen zadat klíče jednotlivých služeb, aby aplikace fungovala správně. Praktickým vylepšením by však bylo umožnit zadání těchto klíčů přímo v rozhraní aplikace.

5 Právní rámec a limity legálního použití nástroje Puppint

5.1 Úvod

Tato kapitola slouží k vymezení právního rámce pro užití nástroje Puppint, který byl vytvořen v rámci bakalářské práce. V nástroji jsou implementovány služby OSINT a generace klamavého účtu pro účely vzdělání, testování a etického užití.

5.2 Legální rámec využití

Získávání informací

Nástroj slouží k získávání veřejně dostupných informací a vytváření klamavých účtů. Přístup k informacím z neveřejných nebo chráněných částí služeb (např. pomocí klamavých účtů), může být považováno za porušení práva.

§ 230 trestního zákoníku stanoví, že kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

- Uživatel může porušit toto právní ustanovení v případě, že pomocí nástroje získá neoprávněný přístup k počítači nebo jeho části.

§ 231 trestního zákoníku pojednává o opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Tedy toto právní ustanovení poruší ten, kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává například počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části.

- Toto právní ustanovení může uživatel porušit v případě, že pomocí nástroje vyhledá a získá například heslo k počítačovému systému a uchová toto heslo pro budoucí použití nebo v případě, že se toto heslo rozhodne sdílet.

§ 232 trestního zákoníku pojednává o neoprávněném zásahu do počítačového systému nebo nosiče informací z nedbalosti, přičemž toto právní ustanovení stanoví, že kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté.

- V případě, že by uživatel byl fyzická či právnická osoba, která vykonává zaměstnání, povolání, postavení nebo funkci, nebo má jiné povinnosti mu uložené

podle zákona nebo smluvně převzaté, může toto právní ustanovení porušit.

Ochrana soukromí

Uživatel je odpovědný za užívání nástroje tak, aby dodržoval principy ochrany soukromí podle § 84 a § 86 občanského zákoníku.

§ 84 občanského zákoníku stanoví, že zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.

- Toto právní ustanovení může uživatel porušit v případě, že si uloží nebo analyzuje profilovou fotografii reálné osoby z veřejné sociální sítě bez jejího vědomí a souhlasu, aby ji použil pro vytvoření klamavého účtu.

§ 85 občanského zákoníků, který stanoví, že rozšiřovat podobu člověka je možné jen s jeho svolením.

- Právní ustanovení bude porušeno v případě, že uživatel použije fotografii reálné osoby k vytvoření falešného profilu a šíří ji v rámci OSINT vyšetřování nebo klamavých interakcí online, čímž šíří její podobu bez souhlasu.

§ 86 občanského zákoníků poté vyjmenovává zakázaná jednání v rámci ochrany soukromí. Stanoví, že nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit.

- V případě, že uživatel pomocí nástroje Puppint zjišťuje, kde se konkrétní osoba pohybuje (např. na základě metadat nebo IP adresy) a tato data ukládá nebo šíří bez jejího souhlasu, poruší tím toto právní ustanovení.

Uživatel by se také měl vyhnout jakémukoliv pronásledování, jelikož může dojít k naplnění skutkové podstaty § 354 trestního zákoníku, který pojednává o nebezpečném pronásledování.

Podvod

§ 209 trestného zákoníku, který pojednává od podvodu může nabýt své skutkové podstaty v případě, že uživatel odcizí identitu s cílem oklamat jiného, tedy uvést jinou osobu v omyl s cílem se obohatit.

- Uživatel poruší právní ustanovení tak, že vytvoří falešnou identitu s cílem vylákat od jiné osoby informace, služby nebo přístup k uzavřeným systémům,

což naplňuje znaky podvodného jednání.

Osobní údaje

Uživatel je také povinen se řídit Nařízením (EU) 2016/679 (GDPR) a českým zákonem č. 110/2019 Sb. o zpracování osobních údajů.

- Toto nařízení musí uživatel dodržovat, jelikož může zpracovávat osobní údaje získané přes nástroj Puppint (např. jména, e-maily, IP adresy, fotografie) bez právního základu (souhlasu, oprávněného zájmu, plnění smlouvy apod.), a porušil by tím GDPR i český zákon o zpracování osobních údajů.

Vyloučení odpovědnosti

Autor tohoto nástroje ani Vysoké učení technické v Brně nenese žádnou odpovědnost za jakékoliv škody způsobené jeho používáním. Uživatel je plně zodpovědný za způsob používání nástroje a je také zodpovědný za způsob, jakým nakládá se zpracovanými daty.

Závěr

Tato práce se zaměřila na zkoumání právních a etických limitů spojených s využíváním techniky OSINT a vytvářením klamavých účtů v rámci etického hackingu.

V teoretické části byl popsán etický hacking, činnosti etického hackingu a jakým způsobem ho ovlivňují české zákony. Následně byla vysvětlena a analyzována technika OSINT, její využití v různých scénářích, právní aspekty vyplývající z legislativy České republiky a Evropské unie, a také etické otázky související s jejich aplikací. V neposlední řadě se práce zaměřila na klamavé účty. Byly vysvětleny rozdíly mezi klamavými účty, boty a dalším jím podobné. Dále bylo popsáno využití klamavých účtů v rámci OSINTu a Catfishingu a v neposlední řadě byly popsány jejich právní limity v rámci jejich vytváření a využívání.

V rámci praktické části byl navržen a implementován nástroj Puppint, který unifikuje určité nástroje OSINT a umožňuje automatizovanou tvorbu klamavých účtů pomocí umělé inteligence. Nástroj je přizpůsoben použití v českém prostředí a v práci je rovněž specifikován jeho právní rámec pro legální využití.

Z provedené analýzy vyplynulo, že využívání OSINT představuje zásadní přínos pro oblast kybernetické bezpečnosti, především v rámci prevence a odhalování hrozeb. Zároveň však podléhá významným právním omezením, která vyžadují důkladnou znalost legislativy, například GDPR a striktní dodržování pravidel ochrany osobních údajů. Podobně je tomu i u vytváření a využívání klamavých účtů, které mohou být cenným nástrojem, avšak jejich použití je podmíněno dodržováním přísných etických a právních pravidel. Respektování těchto mantinelů je nezbytné, aby nedošlo k překročení hranic etického hackingu.

Závěrem lze konstatovat, že legální využívání OSINT a klamavých účtů je možné pouze za předpokladu striktního dodržování právního rámce a pečlivého zvážení etických aspektů každé konkrétní situace.

Literatura

[1] TUDOR, Steve, 2019. Chapter 1) Hackers: The Practical Beginner's Guide to Learn How To Hack With Kali Linux in One Day Step-by-Step (#2020 Updated Version | Effective Computer Programming). In: TUDOR, Steve. Hacking with Kali LinuxThe Practical Beginner's Guide to Learn How To Hack With Kali Linux in One Day Step-by-Step. S. 3. ISBN 9781703885675.

[2] What Is Hacking? | IBM, 2024. Online. Dostupné z: https://www.ibm.com/topics/cyber-hacking. [cit. 2024-12-10].

[3] What is Ethical Hacking? | IBM, 2023. Online. 20. 10. 2023. Dostupné z: https://www.ibm.com/topics/ethical-hacking. [cit. 2024-12-10].

[4] CHNG, Samuel; LU, Han Yu; KUMAR, Ayush a YAU, David, 2022. Hacker types, motivations and strategies: A comprehensive framework: A comprehensive framework. Computers in Human Behavior Reports. Vol. 5, s. 100167. ISSN 24519588. Dostupné z: https://doi.org/10.1016/j.chbr.2022.100167.

[5] FARSOLE, Ajinkya A; KASHIKAR, Amruta G a ZUNZUNWALA, Apurva, 2010. Ethical Hacking. International Journal of Computer Applications. Vol. 1, no. 10, s. 14-20.

[6] DETECTIFY, Fredrik Nordberg Almroth, 2023. What you need to know about the mindset and motivation of ethical hackers. Online. VentureBeat. 27.5. 2023. Dostupné z: https://venturebeat.com/security/what-you-need-to-know-about-the-mindset-and-motivation-of-ethical-hackers/. [cit. 2024-12-10].

[7] Deciphering the Hacker Mindset: Personalities, Motivations, and Moral Landscapes - Blue Goat Cyber: Personalities, Motivations, and Moral Landscapes - Blue Goat Cyber, 2024. Online. Blue Goat Cyber. 9.1. 2024. Dostupné z: https://bluegoatcyber.com/blog/deciphering-the-hacker-mindset-personalities-motivations-and-moral-landscapes/. [cit. 2024-12-10].

[8] NOORDEGRAAF, Judith E. a WEULEN KRANENBARG, Marleen, 2023. Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. Criminology & Public Policy. Vol. 22, no. 4, s. 803-824. Dostupné z: https://doi.org/10.1111/1745-9133.12650.

[9] CELESTIN, Mbonigaba a VANITHA, N, 2015. ETHICAL HACKING DEMYSTIFIED: HOW 'GOOD' HACKERS KEEP US SAFE: HOW 'GOOD'

HACKERS KEEP US SAFE. International Journal of Multidisciplinary Research and Modern Education (IJMRME). Vol. 1, no. 1, s. 721-725. ISSN 2454 - 6119.

[10] CAVUSOGLU, Hasan, Huseyin CAVUSOGLU a Srinivasan RAGHUNATHAN. EMERGING ISSUES IN RESPONSIBLE VULNERABILITY DISCLOSURE.

[11] WALSHE, Thomas a Andrew SIMPSON. An Empirical Study of Bug Bounty Programs. London, ON, Canada: IEEE, 2020. ISBN 978-1-72816-280-5. DOI: 10.1109/IBF50092.2020.9034828

[12] 12 Practical Benefits of Bug Bounty Programs | Nordic Defender | #1 Nordic Crowd-Powered MSSP, 2023. Online. Dostupné z: https://nordicdefender.com/blog/benefits-of-bug-bounty-programs. [cit. 2024-12-10].

[13] PRIVATE VS PUBLIC BUG BOUNTY PROGRAM, 2023. Online. BugBase. Dostupné z: https://bugbase.ai/blog/private-vs-public-bug-bounty-program. [cit. 2024-12-10].

[14] MAURUSHAT, Alana, 2019. Ethical Hacking. Erscheinungsort nicht ermittelbar: University of Ottawa Press / Les Presses de l'Université d'Ottawa. ISBN 978-0-7766-2791-5.

[15] What is Penetration Testing? | IBM, 2023. Online. IBM. Dostupné z: https://www.ibm.com/topics/penetration-testing. [cit. 2024-12-10].

[16] DENIS, Matthew; ZENA, Carlos a HAYAJNEH, Thaier, 2016. Penetration testing: Concepts, attack methods, and defense strategies: Concepts, attack methods, and defense strategies. In: 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, s. 1-6. ISBN 978-1-4673-8490-2. Dostupné z: https://doi.org/10.1109/LISAT.2016.7494156.

[17] MBA, Jason Firch. What Are The Different Types Of Penetration Testing? Online. PurpleSec. Dostupné z: https://purplesec.us/learn/types-penetration-testing/. [cit. 2025-04-22].

[18] White Papers 2023 Physical Penetration Testing. Online. ISACA. Dostupné z: https://www.isaca.org/resources/white-papers/2023/physical-penetration-testing. [cit. 2025-04-22].

[19] DEFENSE, Ministry of. A Guide to Red Teaming. The Development, Concepts and Doctrine Centre. Vol. 2010.

[20] TEICHMANN, Fabian, 2023. Teichmann a Boticiu - 2023 - An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming. International Cybersecurity Law Review. S. 391.

[21] What is Red Teaming? | IBM, 2024. Online. IBM. Dostupné z: https://www.ibm.com/think/topics/red-teaming. [cit. 2024-12-10].

[22] What is Red Teaming? | CrowdStrike. Online. CrowdStrike. Dostupné z: https://www.crowdstrike.com/en-us/cybersecurity-101/advisory-services/red-teaming/. [cit. 2024-12-10].

[23] REHBERGER, Johann, 2020. Cybersecurity attacks - red team strategies: a practical guide to building a penetration testing program having homefield advantage. 2020. Birmingham: Packt Publishing. ISBN 978-1-83882-886-8.

[24] VOSTOUPAL, Jakub et al. The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond. Computer Law & Security Review. 2024, roč. 53, s. 105988. ISSN 2212-473X. DOI: 10.1016/j.clsr.2024.105988

[25] YOUNG, Louis, 2025. Rules of Engagement in Penetration Testing: A Comprehensive Guide. Online. VaultMatrix.com. Dostupné z: https://www.vaultmatrix.com/rules-of-engagement-in-penetration-testing-a-comprehensive-guide/. [cit. 2025-03-30].

[26] Etický hacking a právo, 2024. Online. GDPR. Dostupné z: https://www.gdpr.cz/eticky-hacking-a-pravo. [cit. 2024-12-10].

[27] Zákon č. 40/2009 Sb.: Zákon trestní zákoník, 2009. Online. In: Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40?citace=1. [cit. 2024-12-11].

[28] KOLOUCH, Jan, 2016. CyberCrime. CZ.NIC ;. Praha : CZ.NIC, z.s.p.o. ISBN 978-80-88168-15-7.

[29] What Is OSINT (Open-Source Intelligence)? | IBM, 2024. Online. IBM. Dostupné z: https://www.ibm.com/topics/osint. [cit. 2024-12-10].

[30] SCHENO, Richard. Open-Source Intelligence by Law Enforcement: The Impacts.

[31] What Is Raccoon Infostealer Malware?, 2021. Online. BlackBerry. Dostupné z: https://blogs.blackberry.com/en/2021/09/threat-thursday-raccoon-infostealer. [cit. 2024-12-10].

[32] BLOGS.BLACKBERRY.COM, 2022. How a hacker who stole data of millions of people was tracked & arrested because his girlfriend uploaded this pic on Instagram. Online. Security Newspaper. Dostupné z: https://www.securitynewspaper.com/2022/11/04/how-a-hacker-who-stole-data-of-millions-of-people-was-tracked-arrested-because-his-girlfriend-uploaded-this-pic-on-instagram/. [cit. 2024-12-10].

[33] BLOCK, Ludo, 2024. The long history of OSINT. Journal of Intelligence History. Vol. 23, no. 2, s. 95-109. Dostupné z: https://doi.org/10.1080/16161262.2023.2224091.

[34] TEAM, IMSL Web, 2023. The Historical Use of OSINT Through The Centuries | IMSL. Online. IMSL. Intelligent Management Support Services. Dostupné z: https://www.intelmsl.com/osint-history/. [cit. 2024-12-10].

[35] What is Intelligence? Online. Office of the Director of National Intelligence. Dostupné z: https://www.dni.gov/index.php/what-we-do/what-is-intelligence. [cit. 2025-04-23].

[36] Understanding the Different Types of Intelligence Collection Disciplines, 2022. Online. Maltego. Dostupné z: https://www.maltego.com/blog/understanding-the-different-types-of-intelligence-collection-disciplines/. [cit. 2024-12-10].

[37] NARASIMHAN, Pranesh Kumar; BHOSALE, Chinmay; PERVEZ, Muhammad Hasban; NAQVI, Najiba Zainab; ECEVIT, Mert Ilhan et al., 2023. Open-source Intelligence (OSINT) investigation in Facebook. Electronic Imaging. Vol. 35, no. 3, s. 357-1-357-12. ISSN 2470-1173. Dostupné z: https://doi.org/10.2352/EI.2023.35.3.MOBMU-357.

[38] GROCE, Andrea. LibGuides: Intelligence Studies: Types of Intelligence Collection: Intelligence Studies: Types of Intelligence Collection. Online. Dostupné z: https://usnwc.libguides.com/c.php?g=494120&p=3381426. [cit. 2024-12-10].

[39] A Guide to Measurement and Signature Intelligence (MASINT), 2023. Online. Grey Dynamics. Dostupné z: https://greydynamics.com/a-guide-to-measurement-and-signature-intelligence-masint/. [cit. 2024-12-10].

[40] MASINT by Office of the Director of National Intelligence, 2021. Office of the Director of National Intelligence. Dostupné také z: https://www.dni.gov/files/ODNI/documents/21-113_MASINT_Primer___2022.pdf.

[41] LAYTON, Robert a WATTERS, Paul A., 2016. Automating open source intelligence: algorithms for OSINT: algorithms for OSINT. Amsterdam Boston: Elsevier/Syngress. ISBN 978-0-12-802916-9.

[42] MALTEGO. Maltego FAQ. Online. Maltego. Dostupné z: https://www.maltego.com/maltego-faq/. [cit. 2025-04-24].

[43] What is Google Dorking/Hacking | Techniques & Examples | Imperva. Online. Learning Center. Dostupné z: https://www.imperva.com/learn/application-security/google-dorking-hacking/. [cit. 2024-12-10].

[44] How does reverse image search work? Online. PimEyes. Dostupné z: https://pimeyes.com/en/blog/how-does-reverse-image-search-work?utm_source=open%20graph&utm_medium=social&utm_campaign=open_graph. [cit. 2025-04-02].

[45] TCM Security, Inc. Online. Dostupné z: https://academy.tcm-sec.com. [cit. 2024-12-10].

[46] SHODAN. What is Shodan? - Shodan Help Center. Online. Shodan. Dostupné z: https://help.shodan.io/the-basics/what-is-shodan. [cit. 2025-04-24].

[47] What is Hunter? Online. Hunter Help Center. Dostupné z: https://help.hunter.io/en/articles/11048031-what-is-hunter. [cit. 2025-05-30].

[48] POLITE, Taylor, 2025. A Step-by-Step Guide to Email Penetration Testing. Online. Nenalezený vydavatel. Dostupné z: https://gibraltarsolutions.com/blog/a-step-by-step-guide-to-email-penetration-testing/. [cit. 2025-05-30].

[49] Most used social networks 2025, by number of users, 2025. Online. Statista. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. [cit. 2025-06-02].

[50] Instagram. Online. Centrum nápovědy pro Instagram. Dostupné z: https://help.instagram.com/424737657584573/?helpref=related_articles. [cit. 2025-04-02].

[51] Které kategorie informací jsou dostupné v nastavení Facebooku | Centrum nápovědy pro Facebook. Online. Dostupné z: https://www.facebook.com/help/930396167085762?cms_id=930396167085762. [cit. 2024-12-10].

[52] RANDOM TOOLS, 12.5. What is Facebook ID and how it is used ? Online. Random Tools. Dostupné z: https://randomtools.io/blog/facebook-id-used/. [cit. 2024-11-06].

[53] New user FAQ. Online. X Help Center. Dostupné z: https://help.x.com/en/resources/new-user-faq. [cit. 2025-04-02].

[54] Twintproject/twint, 2024. Online. TWINT Project. Dostupné z: https://github.com/twintproject/twint. [cit. 2025-05-08].

[55] Telegram. Online. Telegram. Dostupné z: https://telegram.org/. [cit. 2025-03-30].

[56] OSINT INDUSTRIES TEAM, 2025. OSINT on Telegram: Find Phone Numbers, Emails and User Details. Online. OSINT Industries. Dostupné z: https://www.osint.industries/post/osint-on-telegram-find-phone-numbers-emails-and-user-details. [cit. 2025-03-30].

[57] TIDY, Joe, 2024. Telegram: 'The dark web in your pocket'. Online. BBC. 2024-08-31. Dostupné z: https://www.bbc.com/news/articles/cdey4prn3e1o. [cit. 2025-03-30].

[58] AKASAKA, Yuzuka. Telegram and OSINT Investigations: An Essential Platform in 2023. Online. Security Boulevard. Dostupné z: https://securityboulevard.com/2023/05/telegram-and-osint-investigations-an-essential-platform-in-2023/. [cit. 2025-03-30].

[59] Reddit. Online. Buffer: All-you-need social media toolkit for small businesses. Dostupné z: https://buffer.com/social-media-terms/reddit. [cit. 2025-04-02].

[60] Help LinkedIn Help. Online. LinkedIn. Dostupné z: https://www.linkedin.com/help/linkedin/answer/a548441. [cit. 2025-04-02].

[61] DISK0NN3CT, 2024. Dchrastil/ScrapedIn. Online. Dostupné z: https://github.com/dchrastil/ScrapedIn. [cit. 2025-05-08].

[62] FINKLEA, Kristin, 2017. Dark Web. Congressional Research Service. S. 1-6.

[63] How to Collect OSINT on the Dark Web, 2023. Online. Dostupné z: https://liferaftlabs.com/blog/how-to-collect-osint-on-the-dark-web. [cit. 2024-12-10].

[64] The Dark Web Browser: What Is Tor, Is it Safe, and How Do You Use It?: What Is Tor, Is it Safe, and How Do You Use It?, 2024. Online. The Dark

Web Browser: What Is Tor, Is it Safe, and How Do You Use It? Dostupné z: https://www.avast.com/c-tor-dark-web-browser. [cit. 2024-12-10].

[65] RAJAMÄKI, Jyri, 2022. OSINT on the Dark Web: Child Abuse Material Investigations: Child Abuse Material Investigations. Information & Security: An International Journal. Vol. 53, s. 21-32. Dostupné z: https://doi.org/10.11610/isij.5302.

[66] Open Source Intelligence Investigation: From Strategy to Implementation: From Strategy to Implementation, 2016. Cham: Springer International Publishing. ISBN 978-3-319-47670-4. Dostupné také z: https://link.springer.com/10.1007/978-3-319-47671-1.

[67] GOKHALE, C. a OLUGBARA, O. O., 2020. Dark Web Traffic Analysis of Cybersecurity Threats Through South African Internet Protocol Address Space. Online. SN Computer Science. Vol. 1, no. 5, s. 273. Dostupné z: https://doi.org/10.1007/s42979-020-00292-y. [cit. 2025-05-08].

[68] HEAD, Department of Journalism and Mass Communication, 2020. Communication & Journalism Research. Head, Department of Journalism and Mass Communication. Roč. 9, č. 1. ISSN 2348-5663. Dostupné také z: https://cjrjournal.in/Uploads/Files/CJR%202020%20JUNE.pdf#page=74.

[69] BÖHM, Isabelle a LOLAGAR, Samuel, 2021. Open source intelligence: Introduction, legal, and ethical considerations: Introduction, legal, and ethical considerations. Online. International Cybersecurity Law Review. Vol. 2, no. 2, s. 317-337. Dostupné z: https://doi.org/10.1365/s43439-021-00042-7. [cit. 2025-05-09].

[70] MANSOOR, Nazneen; SCHWARZ, Klaus a CREUTZBURG, Reiner, 2023. Importance of OSINT/SOCMINT for modern disaster management evaluation - Australia, Haiti, Japan. Online. Electronic Imaging. Vol. 35, no. 3, s. 354-1-354-14. ISSN 2470-1173. Dostupné z: https://doi.org/10.2352/EI.2023.35.3.MOBMU-354. [cit. 2025-05-09].

[71] MENTOR, The Cyber, 2022. Deadly Social Media: The Final Hours of Pop Smoke: The Final Hours of Pop Smoke. Online. Dostupné z: https://www.youtube.com/watch?v=xIWqvJXKLjg. [cit. 2025-05-09].

[72] ZHAO, Letao, 2024. Navigating the Cyber Kill Chain: A modern approach to pentesting: A modern approach to pentesting. Online. Applied and Computational Engineering. Vol. 38, no. 1, s. 170-175. Dostupné z: https://doi.org/10.54254/2755-2721/38/20230549. [cit. 2025-05-13].

[73] SABU, Thampi a THAMPI, Sabu, 2015. Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings. 536. Cham: Springer International Publishing. ISBN 978-3-319-22914-0. Dostupné také z: https://link.springer.com/10.1007/978-3-319-22915-7.

[74] AHMED, Yussuf; ASYHARI, A.Taufiq a ARAFATUR RAHMAN, Md, 2021. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. Online. Computers, Materials & Continua. Vol. 67, no. 2, s. 2497-2513. ISSN 1546-2226. Dostupné z: https://doi.org/10.32604/cmc.2021.014223. [cit. 2025-05-09].

[75] DOUGLAS, David M., 2016. Doxing: a conceptual analysis: a conceptual analysis. Online. Ethics and Information Technology. Vol. 18, no. 3, s. 199-210. Dostupné z: https://doi.org/10.1007/s10676-016-9406-0. [cit. 2025-05-09].

[76] CHEUNG, Anne, 2021. Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon: When Personal Data Become a Weapon. In: The Emerald International Handbook of Technology-Facilitated Violence and Abuse. Emerald Publishing Limited, s. 577-594. ISBN 978-1-83982-849-2. Dostupné z: https://doi.org/10.1108/978-1-83982-848-520211041.

[77] CHEN, Mengtong; CHEUNG, Anne Shann Yue a CHAN, Ko Ling, 2019. Doxing: What Adolescents Look for and Their Intentions: What Adolescents Look for and Their Intentions. Online. International Journal of Environmental Research and Public Health. Vol. 16, no. 2, s. 218. ISSN 1660-4601. Dostupné z: https://doi.org/10.3390/ijerph16020218. [cit. 2025-05-09].

[78] ČESKO. Fragment #f6448798 zákona č. 110/2019 Sb., o zpracování osobních údajů - znění od 24. 4. 2019. In: *Zákony pro lidi.cz* [online]. © AION CS 2010–2024 [cit. 17. 11. 2024]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110/zneni-20190424#f6448798

[79] GDPR essentials for OSINT research – Blockint, 2021. Online. BLOCKINT. Dostupné z: https://www.blockint.nl/methods/gdpr-essentials-for-osint-research/. [cit. 2024-12-10].

[80] Zákon č. 89/2012 Sb.: Zákon občanský zákoník, 2012. Online. In: Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89. [cit. 2025-03-26].

[81] Nález Ústavního soudu ze dne 30. října 2014, sp. zn. III. ÚS 3844/13 (téma Facebook). Online. NALUS: Vyhledávání rozhodnutí Ústavního soudu České republiky. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=3-3844-13_1. [cit. 2025-04-28].

[82] OSINT vs The Law, 2023. Online. LinkedIn. Dostupné z: https://www.linkedin.com/pulse/osint-vs-law-maciej-j%C4%99drak-cqlff. [cit. 2024-12-10].

[83] Co je GDPR - Ochrana osobních údajů. Online. Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx. [cit. 2024-12-10].

[84] ČESKO. Fragment #f6448800 zákona č. 110/2019 Sb., o zpracování osobních údajů - znění od 24. 4. 2019. In: *Zákony pro lidi.cz* [online]. © AION CS 2010–2024 [cit. 23. 11. 2024]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110/zneni-20190424#f6448800

[85] S.R.O., Simplo. Základní příručka k ochraně údajů. Online. Úřad pro ochranu osobních údajů. Dostupné z: https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju. [cit. 2024-12-10].

[86] KOOPS, Bert-Jaap; HOEPMAN, Jaap-Henk a LEENES, Ronald, 2013. Open-source intelligence and privacy by design. Online. Computer Law & Security Review. Vol. 29, no. 6, s. 676-688. ISSN 02673649. Dostupné z: https://doi.org/10.1016/j.clsr.2013.09.005. [cit. 2025-05-09].

[87] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), 2016. In: .

[88] COMMISSION, European. What does data protection 'by design' and 'by default' mean? Online. European Commission. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. [cit. 2025-03-26].

[89] CUIJPERS, Colette, 2013. Legal aspects of open source intelligence – Results of the VIRTUOSO project. Online. Computer Law & Security Review. Roč. 29, č. 6, s. 642-653. ISSN 2212-473X. Dostupné z: https://doi.org/https://doi.org/10.1016/j.clsr.2013.09.002. [cit. 2025-05-09].

[90] Zákon č. 121/2000 Sb.: Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), 2000. Online. In: Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121. [cit. 2025-04-26].

[91] OSINT Meaning & open source intelligence techniques. Online. True People Check. Dostupné z: https://truepeoplecheck.com/osint-open-source-investigations/. [cit. 2025-04-26].

[92] CYBERLY. How does OSINT help organisations protect intellectual property? Online. Cyberly. Dostupné z: https://www.cyberly.org/en/how-does-osint-help-organisations-protect-intellectual-property/index.html. [cit. 2025-04-13].

[93] Using OSINT for License Compliance: Uncovering Companies Profiting from Unauthorized Software Use. Online. Nenalezený vydavatel. Dostupné z: https://www.linkedin.com/pulse/using-osint-license-compliance-uncovering-companies-from-knowles-pwuge. [cit. 2025-04-13].

[94] Co je to Due diligence? Online. CzechWealth. Dostupné z: https://www.czechwealth.cz/slovnik-pojmu/due-dilligence. [cit. 2024-12-10].

[95] Due Diligence: Types and How to Perform: Types and How to Perform, 2024. Online. Investopedia. Dostupné z: https://www.investopedia.com/terms/d/duediligence.asp. [cit. 2024-12-10].

[96] HAILE, Issayas M, 2020. Data Analytics in Financial Institutions: How Text Analytics Can Help in Risk Management: How Text Analytics Can Help in Risk Management. Disertace. Colorado: Colorado Technical University.

[97] WANI, Mudasir Ahmad; JABIN, Suraiya; YAZDANI, Ghulam a AHMADD, Nehaluddin, 2018. Sneak into Devil's Colony- A study of Fake Profiles in Online Social Networks and the Cyber Law. Online. ArXiv. Dostupné z: https://doi.org/10.48550/arXiv.1803.08810. [cit. 2025-05-09].

[98] ALHARBI, Ahmed; DONG, Hai; YI, Xun; TARI, Zahir a KHALIL, Ibrahim, 2021. Social Media Identity Deception Detection: A Survey: A Survey. Online. ArXiv. Dostupné z: https://doi.org/10.48550/arXiv.2103.04673. [cit. 2025-05-09].

[99] China is pushing a new Covid origin theory: Maine lobsters: Maine lobsters, 2021. Online. NBC News. 2021-10-22. Dostupné z:

https://www.nbcnews.com/news/china-linked-disinformation-campaign-blames-covid-maine-lobsters-rcna3236. [cit. 2025-04-27].

[100] KUMAR, Srijan; CHENG, Justin; LESKOVEC, Jure a SUBRAHMANIAN, V. S., 2017. An Army of Me: Sockpuppets in Online Discussion Communities: Sockpuppets in Online Discussion Communities. Online. An Army of Me: Sockpuppets in Online Discussion Communities. S. 857-866. Dostupné z: https://doi.org/10.1145/3038912.3052677. [cit. 2025-05-09].

[101] The Art Of The Sock, 2018. Online. Secjuice. Dostupné z: https://www.secjuice.com/the-art-of-the-sock-osint-humint/. [cit. 2024-12-10].

[102] THE UTILIZATION OF SOCK PUPPETS IN CYBER INTELLIGENCE OPERATION, 2014. Online, Stěžejní projekt. New York: Utica College. Dostupné z: https://www.proquest.com/docview/1646872181?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses. [cit. 2025-05-09].

[103] Creating an Effective Sock Puppet for OSINT Investigations – Introduction – Jake Creps, 2021. Online. JakeCreps. Dostupné z: https://web.archive.org/web/20210125191016/https://jakecreps.com/2018/11/02/sock-puppets/. [cit. 2024-12-10].

[104] SLATER, Ana P, 2023. Social Media Intelligence (SOCMINT) Investigative Framework as a Human Trafficking Deterrent Tool. Diplomová práce. Department of Computer and Information Technology West Lafayette, Indiana: Faculty of Purdue University.

[105] Creating and Utilizing Sock Puppets for OSINT, 2023. Online. Dostupné z: https://marcelhauri.ch/blog/creating-and-utilizing-sock-puppets-for-osint/. [cit. 2024-12-10].

[106] A peek behind the curtain: How are sock puppet accounts used in OSINT?: How are sock puppet accounts used in OSINT?, 2024. Online. WeLiveSecurity. Dostupné z: https://www.welivesecurity.com/en/cybersecurity/peek-curtain-sock-puppet-accounts-osint/. [cit. 2024-12-10].

[107] LAUDER, Cassandra a MARCH, Evita, 2023. Catching the catfish: Exploring gender and the Dark Tetrad of personality as predictors of catfishing perpetration: Exploring gender and the Dark Tetrad of personality as predictors of catfishing perpetration. Online. Computers in

Human Behavior. Vol. 140, s. 107599. ISSN 07475632. Dostupné z: https://doi.org/10.1016/j.chb.2022.107599. [cit. 2025-05-09].

[108] VICTORIA H., Williams, 2020. Catfishing and Online Identity Management. Disertace. California: Alliant International University.

[109] What is Catfishing | Catfishing Signs & How to Protect Yourself. Online. Malwarebytes. Dostupné z: https://www.malwarebytes.com/cybersecurity/basics/catfishing. [cit. 2024-12-10].

[110] ARFINI, Selene; PARANDERA, Lorenzo Botta; GAZZANIGA, Camilla; MAGGIONI, Nicolo a TACCHINO, Alessandro, 2020. Personal Identity and Online Communities. University of Pavia. S. 1193-1198.