POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra policejních činností

Zpravodajství z otevřených zdrojů (OSINT) v oblasti finančního a ekonomického zpravodajství – zdroje, metody, postupy a nástroje

Bakalářská práce

(Open Source Intelligence (OSINT) in the Field of Financial and Economic Intelligence – Sources, Methods, Procedures and Tools)

Bachelor thesis

VEDOUCÍ PRÁCE
Ing. Bc. Luděk MICHÁLEK, Ph.D.

AUTOR PRÁCE
Luděk Zvolánek

PRAHA
2022

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Krucemburku, dne 16. 9. 2021

Luděk Zvolánek

ANOTACE

Tato bakalářská práce se zabývá problematikou zpravodajství, především zpravodajstvím z otevřených zdrojů v oblasti ekonomického a finančního zpravodajství. Cílem práce je nastínit metody používané ve zpravodajství z otevřených zdrojů, zdroje dat a informací, vhodnou literaturu, legislativní úpravu a porovnat možnosti získávání informací v České republice se zahraničními praktikami.

KLÍČOVÁ SLOVA

OSINT, competetive intelligence, otevřené zdroje, finační a ekonomické zpravodajství

ANNOTATION

This thesis examines the field of intelligence, mainly open source intelligence in the field of economic and financial intelligence. The goal of this thesis is to illustrate methods one can employ in an open source investigation, possible sources of data and information, recommended handbooks and legislatory boundaries for such activities, and compare the possibilities of OSINT use in the Czech republic with the rest of the world.

KEYWORDS

OSINT, competetive intelligence, open sources, financial and economical intelligence

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval zejména panu doktorovi Luďku Michálkovi za jeho trpělivost s mým přístupem a velice vítanou zpětnou vazbu na mou práci. Zároveň bych rád poděkoval své rodině, která mi během tvorby této práce byla oporou, bez níž bych se nikam nedostal.

OBSAH

ÚVOD

O zpravodajství se říká, že se jedná o druhé nejstarší povolání na světě, protože zmínky o této činnosti jsou již v Bibli. Metody a zdroje pro tuto činnost se s vývojem civilizace výrazně měnily a reflektovaly politický a sociální vývoj a jeho potřeby. Jednou z disciplín zpravodajství, dovolím si říct, neprávem opomíjenou v populární kultuře, je zpravodajství z otevřených zdrojů – OSINT. Nejedná se o výdobytek moderní doby, ani posledního století, nýbrž o obor, který byl hojně využíván od dob prvních informací předaných širšímu publiku.

Pravdou je, že tento obor s rozmachem moderních technologií, především internetu, výrazně nabyl na důležitosti a užitnosti. Stal se velice podstatným a nepostradatelným nástrojem státních zpravodajských služeb, žurnalistů, především v oblasti investigativy a i jednotlivců, nadšenců. OSINT sehrál podstatnou roli při monitorování válečných konfliktů posledního desetiletí, vyšetřování například v česku známého případu „zmizení“ syna premiéra Andreje Babiše, nebo trasování pohybu rozvědčíků vojenské zpravodajské služby Ruské Federace, GRU, kteří měli být přímo zapojeni do explozí v českém muničním skladu ve Vrběticích.

O efektivitě OSINT není pochyb a v této práci se pokusíme aplikovat metodiky zpravodajství z otevřených zdrojů v oblasti finančního a ekonomického zpravodajství. Pokusím se zodpovědět, zda může být OSINT využit v poměrně restriktivním prostoru, kterým je Český právní řád, zvláště v oblasti ochrany soukromí osob. Mnohé příručky jsou vytvořeny pro americký přístup k ochraně soukromí, který pro představu umožňuje přístup široké veřejnosti k trestním evidencím jiných občanů, což je v kontinentálním právním systému nepředstavitelné. Pro práci budeme čerpat z nejrelevantnější a nejužitečnějších příruček k této činnosti, zmíníme je a metody v nich popsané budeme později aplikovat v kontextu finančního a ekonomického zpravodajství.

TEORETICKÁ ČÁST

1. ZÁKLADNÍ POJMY

Než se posuneme dále, je třeba vymezit si pojmy, se kterými se v této práci budeme často setkávat.

1.1 Zpravodajství

V českém prostředí se častěji pod termínem zpravodajství čtenáři vybaví činnost žurnalistů, nebo označení výsledků jejich práce.[1] Nicméně pro oblast, ve které se nacházíme v rámci této práce je třeba zmínit, že mluvíme o cílevědomé činnosti zpravodajských služeb, ať už státního, či jiného charakteru, která má za cíl shromažďovat data a informace, zpracovat je a na tomto základě vytvářet závěry použitelné v oblasti, která byla analyzována a pro níž jsou určeny.

1.2 Data

Obecně lze data definovat jako údaje, které jsou nějakým způsobem fyzicky zaznamenané a vyjadřují nějaký jev, nebo vlastnosti. Často se vyskytují ve formě numerické, ale mohou mít i podobu symbolů nebo písmen. Pro účel této práce se daty rozumí především předmět sběru informací, základní hodnota sloužící k následnému zpracování a tvoření informací a zpravodajských informací.

1.3 Informace

Termín „informace“ (z latinského *in-formatio*, utváření) představuje zpracovaná, strukturovaná a do určitého kontextu zasazená data. Zpracování dat v informace je jednou ze základních činností zpravodajského cyklu. Za data se například dá považovat jednotlivý nákup kávy zákazníkem kavárny, na základě několika nákupů se dá vytvořit informace o nejprodávanějším, nebo naopak nejméně prodávaném artiklu.[2]

---

[1] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 15.
[2] JONÁK, Zdeněk. Informace. KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Dostupné také z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000456&local_base=KTD.

1.4 Zpravodajská informace

Data a informace získané a zpracované zpravodajskou činností poté můžeme označovat jako „zpravodajské informace“. Je nutné zdůraznit, že vstupní hodnoty je nutné zasadit do kontextu požadavků zadavatele, neboť pouze v takové sestavě mají informace a data hodnotu zpravodajských informací. Jedná se o výsledek jedné ze základních fází zpravodajského cyklu – zpracování a tvorba zpravodajských informací. Dochází zde tedy k dosazení zjištěných skutečností do širokého pohledu a vyhodnocení zdánlivě pravděpodobného stavu.

1.5 Zpravodajský cyklus

„Zpravodajský cyklus je základním metodologickým postupem zpravodajské činnosti. Je to sled postupných, vzájemně na sebe navazujících a cyklicky se opakujících kroků, v jejichž průběhu jsou získávány a shromažďovány data a informace, zpracovány do podoby zpravodajských informací a předávány oprávněnému uživateli.“ [3] V oboru zpravodajství se jedná o velice populární koncept, široce akceptovaný a využívaný, neboť se nezdá být obyčejným konstruktem, nýbrž spíše odrazem reálných činností zpravodajských služeb. Nicméně v posledních letech je třeba také vzít na vědomí další označení tohoto konceptu, jako je například zpravodajský proces, nebo produkční proces. Literatura se zpravidla shoduje na rozdělení a pojmenování jednotlivých fází tohoto procesu, který si můžeme představit jako uzavřený kruh, který se neustále opakuje a první fáze následuje fázi poslední. Fáze jsou rozděleny následovně:

1) Řízení a plánování
2) Sběr a shromažďování informací a dat
3) Analýza/zpracování informací a dat
4) Distribuce zpravodajský informací

[3] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 130.

Výsledky jednotlivých kroků tohoto procesu jsme si představili v předchozích odstavcích, a proto není nutné je zde dále rozvádět.

1.6 Zpravodajská analýza

Termínem „zpravodajská analýza“ označujeme výše zmíněný třetí krok zpravodajského cyklu – Zpracování informací a dat. Jedná se o proces, kde jsou vstupními hodnotami data a informace, které jsou zpracovány v informace zpravodajské. Literatura tuto fázi dále dělí na dvě dílčí fáze a to sice:

1) Analýza informace
2) Integrace a tvorba zpravodajské informace

První sub-fáze spočívá ve zhodnocení informací a dat získaných ze všech dostupných zdrojů a stanovení věrohodnosti takové informace. V této fázi se taktéž stanovuje spolehlivost zdroje.

Sub-fáze „Integrace a tvorba zpravodajské informace“ oproti tomu „znamená komplexní vyhodnocení jednotlivých informací, rozpoznání nových významných faktů a jejich porovnání s jinými dostupnými informacemi v dané oblasti, syntézu všech informací a vypracování závěrů, a především vytvoření výstupní zpravodajské informace buď jako komplexního popisu daného jevu, nebo jako výhled budoucího vývoje daného jevu.“[4]

1.7 Competetive intelligence

Termín „competetive intelligence“ je do češtiny překládán jako „konkurenční zpravodajství“, autor Molnár však uvádí následující:

“Termín konkurenční zpravodajství ale nevystihuje správně podstatu competetive intelligence a tak stejně, jako je tomu i v jiných, nově vznikajících a dynamicky se rozvíjejících oblastech, potýká se čeština s problematikou správného významového překladu původních anglických pojmů. Problém je hlavně s překladem slova intelligence, které se ve spojení s pojmem competetive intelligence překládá do češtiny nepřesným výrazem „zpravodajství“, protože se v něm ztrácí pravý význam tohoto slova.“[5]

[4] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 133.
[5] MOLNÁR, Zdeněk. *Competitive intelligence, aneb, Jak získat konkurenční výhodu*. S. 33.

Často se také objevuje použití označení „Business intelligence“, dále v této práci zmíním některé zdroje, které blíže definují rozdíl a shodu mezi těmito dvěma obory.

Competetive intelligence je „proces a sestava činností spojená s vyhledáváním, zpracováváním a tvorbou informací a znalostí o konkurenčním prostředí pro zvýšení výkonnosti organizace“[6] (překl. vlastní). Cílem je na základě dat a informací předpovídat další vývoj konkurence, trhu, zákaznických preferencí, nastínit budoucí hrozby a příležitosti a připravit strategii organizace pro vypořádání se s takovou změnou. Za organizaci v kontextu termínu CI můžeme považovat jakékoliv uskupení lidí zabývající se cílevědomou a soustavnou činností. Zatímco lze bezpochyby říct, že tento obor nachází svůj původ v činnosti zpravodajských služeb, jak je známe, je třeba vyvrátit domněnky, že se jedná o činnost na pomezí, nebo dokonce za hranou zákona. Competetive intelligence čerpá pro své fungování informace výhradně z legálních, etických zdrojů, čímž se zásadně odlišuje od průmyslové špionáže.

1.8 Otevřené zdroje

Za otevřené zdroje považujeme takové zdroje, které jsou veřejně a volně přístupné. Jejich získávání je striktně legální, ačkoliv v určitých případech může být považováno za nemorální. Jednoznačně nejtypičtějším takovým zdrojem je v dnešní době informační síť – internet a veškeré její veřejnosti přístupné podmnožiny. Nesmíme opomenout ani jiná média od psaných týdeníků a jiných periodik, přes rozhlasové a televizní vysílání, k různým formám literatury. Otevřené zdroje se vyznačují tím, že jsou dostupné v obrovském množství každému, kdo je schopen je vnímat a tvoří tak hlavní vstupní hodnotu pro činnost zpravodajství z otevřených zdrojů. Díky těmto výhodám se staly nedílnou součástí činnosti zpravodajských služeb i

[6] *Technological Forecasting and Social Change: Competitive intelligence: A unified view and modular definition.* [online]. Dostupné také z: https://www.sciencedirect.com/science/article/abs/pii/S0040162521005199

investigativních žurnalistických serverů – jako nejvýraznější příklad můžeme uvést vyhlášený Bellingcat.

2. ZPRAVODAJSTVÍ

Základní definici zpravodajství jsme uvedli v první kapitole, zde si problematiku této činnosti více rozebereme a přiblížíme celkovému charakteru této práce. Nejdříve si zodpovíme otázku „kdo může být uživatelem zpravodajství?“ Obecně lze říci, že naprosto kdokoliv, jelikož existuje mnoho oborů a metod zpravodajství, na určité úrovni je může využívat kdokoliv, od jedince až po státní zpravodajské služby. Takto široké vymezení s sebou však pochopitelně přináší úskalí velké rozdílnosti výkonu zpravodajství jednotlivých subjektů, kdy například podle toho, zda se jedná o státní službu – orgán veřejné moci, či obyčejného občana, vyvstávají jisté právní otázky a rozdíly v možnostech výkonu zpravodajství. Dále je proto nezbytné si blíže rozdělit zpravodajství podle několika základních kritérií.

2.1 Členění zpravodajství

Existuje mnoho kritérií, podle nichž můžeme zpravodajství členit a pokud bychom chtěli odvést skutečně důslednou práci a vyjmenovat je všechny, pravděpodobně by to bylo neúměrné účelu této práce. Proto je níže uvedené rozdělení omezeno na ty kritéria, která považuji za podstatná a která nám umožní lépe pochopit další skutečnosti a argumenty uvedené v této práci.

2.1.1 Členění dle „veřejnosti“ zpravodajství

Veřejné, nebo také komerční či tiskové zpravodajské agentury jsou tím, co si často laik vybaví pod pojem zpravodajství. Spadají sem veřejné hromadně sdělovací prostředky jako jsou noviny, televizní a radiové zpravodajství nebo internetové portály. Cílem těchto subjektů při využití zpravodajských metod je vytvořit svůj produkt – informaci a předat ji širokému publiku, čímž mohou generovat zisk, nejčastěji peněžní. Tyto subjekty jsou zaměřeny na sběr širokého souboru informací o nesourodých oblastech a oficiálně nesledují žádný záměr ani neselektují, jakému publiku je výsledná informace prezentována. Postup a využití zpravodajského cyklu se může výrazně lišit od subjektu k subjektu. Zatímco některé subjekty mohou pouze opakovat informace převzaté z jiných zdrojů, jiné tyto informace porovnávají s dalšími

zdroji a teprve poté produkt své práce zveřejňují. Právní rámec pro výkon činnosti těmito subjekty je charakterizován tím, že „co není zákonem zakázáno, je povoleno.“[7] Pro úplnost zmíním, že tyto subjekty jsou obrovským zdrojem informací pro zpravodajství z otevřených zdrojů. Do této kategorie si dovolím mimo tradiční zpravodajské agentury zařadit také jiné fyzické či právnické osoby, které jakýmkoliv způsobem zveřejňují informace, protože tyto subjekty naplňují většinu znaků výše uvedených. Vyvstává zde otázka, zda je účelem „šíření vlastního produktu – informace“ i v případě těchto tvůrců, kdy si dovolím tvrdit, že jediný důvod, proč osoby informace zveřejňují, je aby byly zaznamenány jinými osobami a proto zde vidím jistou shodu.

Tajná zpravodajská služba je zpravidla orgánem veřejné moci, který jedná v zájmu státu. Veškerá jejich činnost směřuje k využití zpravodajských metod k podpoře rozhodování na různých úrovních státní politiky a bezpečnosti. V ČR působní několik státních zpravodajských služeb, které mají svá specifická zaměření. Oproti veřejným agenturám je zde užší výběr sběru dat a informací, který je zaměřený na otázky a oblasti relevantní pro rozhodování státu. Zároveň zde v naprosté většině nedochází ke zveřejňování výsledných zpravodajských informací mezi široké publikum, ale pouze určitému uzavřenému okruhu osob. Postupy a metody použité těmito službami bývají více rafinované a důsledné a směřují k co nejvyšší efektivitě činnosti. Nejzákladnějším rozdělením může být zpravodajství vnější a vnitřní, kdy první označuje sběr informací o zahraničních vlivech, hrozbách a aktérech, zatímco druhý obor má za cíl předcházet činnosti nepřátelských zpravodajských služeb a agentů v oblasti vnitřní bezpečnosti. Právní rámec je více restriktivní, jelikož tyto služby mohou svou činnost provádět pouze dle zásady secundum et intra legem.

2.1.2 Členění dle hierarchické úrovně

Hierarchické rozdělení pomáhá pochopit význam jednotlivých úrovní zpravodajských činností, ale nelze toto rozdělení brát jako dogma, neboť to, co může být považováno za strategické zpravodajství pro jeden subjekt,

[7] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 22.

může subjekt jiné povahy považovat za zpravodajství taktické, nebo operační. Hranice mezi těmito děleními jsou často silně rozmazané a nejednoznačné. Různé zdroje uvádějí jiné hierarchické uspořádání, než zde uvedu, kdy se často zaměňuje termín operační a taktické. Nadále v oboru competetive intelligence se termín taktické zpravodajství prakticky subsumuje pod zpravodajství operační. V této práci ale z hlediska hierarchického seřazení zpravodajství, je sestupně dělíme na:

- **Strategická úroveň** – slovník NATO s termíny a definicemi AAP-06 z roku 2019 definuje strategickou zpravodajskou informaci jako „zpravodajská informace potřebná pro tvorbu politiky, vojenské plánování a poskytnutí příznaků a varování na národní a/nebo mezinárodní úrovni.“[8] Zpravodajská činnost na strategické úrovni, jejímž výsledkem je strategická zpravodajská informace, se ovšem netýká jenom státních zpravodajských služeb a zájmů, ale na této úrovni mohou rozhodovat i další subjekty, především obchodní společnosti při competetive intelligence. Znakem této úrovně zpravodajství je relativní dlouhodobost informací a sledovaných objektů – rozhodnutí činěná na základě těchto informací mají dlouhodobý, strategický, charakter.
- **Operační úroveň** – záběr této úrovně je užší než u zpravodajství strategického a širší než u níže uvedeného taktického. Je zaměřeno na jednotlivé dílčí části většího celku, pracuje s informacemi v reálném čase a slouží k adekvátní reakci na rychle se měnící prostředí. V competetive intelligence je cílem této úrovně včasná identifikace a reakce na příležitosti, hrozby a řízení efektivity provozu.
- **Taktická úroveň** – „je zpravodajství potřebné pro plánování a vedení taktické činnosti, tedy na nejnižším organizačním stupni. Zpravidla se jedná o získávání informací za a o rychle se měnící situaci sloužící k přípravě, a především úspěšnému vedení činnosti na základním organizačním stupni velení a řízení.“[9] Jedná se tedy o nejbezprostřednější formu zpravodajské činnosti, vyznačuje se

[8] Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti*: Slovník NATO s termíny a definicemi [online].* S. 301.
[9] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 28.

krátkodobou životností získaných a zpracovaných informací, radikálně se měnícím prostředím a nutností, či příležitostí rychle reagovat.

2.1.3 Členění dle zdrojů a prostředků

Zde je třeba zmínit, že dle odborné literatury je dělení dle tohoto kritéria obsáhlejší než to, které zde je uvedeno, nicméně následující stručné shrnutí by mělo postačit pro další pochopení této práce. Dle zdrojů a prostředků proto rozděluji zpravodajskou činnost pouze na OSINT – zpravodajství z otevřených zdrojů a jiné formy zpravodajské činnosti. Jediným a nejdůležitějším odlišením mezi těmito dvěma formami je to, že OSINT čerpá informace výhradně z veřejně dostupných zdrojů, zatímco jiné formy mohou čerpat i ze zdrojů neveřejných, nebo tajných.

2.1.4 Členění dle funkce zpravodajství

Opět se nejedná o plný výčet ale pouze o vzorek potřebný a užitečný v této práci. Mezi nejpodstatnější obory dle funkce řadím:

- **Finanční zpravodajství (FININT)** – označuje získávání informací o finančních záležitostech zájmových fyzických a právnických osob, jehož účelem je pochopit jejich fungování a vytvořit si přehled o jejich záměrech a schopnostech. Termín se nejčastěji využívá v kontextu práce bezpečnostních složek a souvisejících aktivit. Jedním z hlavních účelů finančního zpravodajství je identifikovat peněžní transakce, které nesou znaky daňových úniků, praní špinavých peněz nebo dalších protiprávních činů. Tento obor je také často uplatňován při vyšetřování finančních zdrojů pro teroristické a zločinné organizace. Sběr dat je obvykle realizován státními agenturami, do jejichž kompetence finanční a ekonomické zpravodajství spadá. Taková agentura získává data často od bankovních institucí, které mají státem danou povinnost vydávat určité informace o finančních transakcích svých klientů. Data také mohou být sdílená s jinými státy na základě mezinárodních smluv o spolupráci na tomto poli. Analýza těchto dat zahrnuje přebírání obrovského množství dat o transakcích a často je v tomto procesů

využíváno automatizovaných procesů. Výsledné zpravodajské informace mohou najít využití i v jiných oborech zpravodajství.

- **Ekonomické zpravodajství (Economic Intelligence – EI)** – *„se zabývá informacemi týkajícími se výroby, obchodu zboží a služeb, pracovní síly, financí a dalších aspektů národního hospodářství a mezinárodně ekonomického systému. Z hlediska národní bezpečnosti takové informace mimo ochranu vlastního hospodářství umožňují odhadnout velikost možné vojenské hrozby ze strany potencionálního protivníka a předvídat jeho záměry.“*[10]

2.2 Zpravodajský cyklus

Obecná definice tohoto pojmu je uvedena v první kapitole této práce, zde si však problematiku detailněji rozebereme. Michálek uvádí následující: “*Jedním z charakteristických rysů zpravodajské činnosti je její cílevědomost a zaměření na plnění požadavků zadavatele. Naplnění tohoto rysu se ve zpravodajské praxi projevuje aplikací tzv. zpravodajského cyklu.*“[11] Dá se proto považovat ze nedílnou součást veškeré zpravodajské činnosti a pomůcku při jejím prvotním plánování. Někteří autoři považují zpravodajský cyklus za přežitek, nebo nevhodné zobrazení reality, například uvádí, že zpravodajský cyklus ve své zažité podobě nepočítá s možností kontra zpravodajství, tento argument je dobré mít na paměti v případě aplikace zpravodajského cyklu.

Tradičně se uvádí čtyři fáze zpravodajského cyklu, ale některé zdroje je blíže specifikují a rozdělují na pět, nebo šest fází (viz. obrázek 2). Existují také znázornění, která zobrazují překryv zpravodajského cyklu například s rozhodovacím cyklem OODA, se kterým se setkáme dále v této práci. Ve výsledku se však tyto modely, co se obsahu týče neliší, jedná se zpravidla pouze o bližší určení a rozdělení jednotlivých kroků cyklu, nebo snahu o přehlednější grafické znázornění. Literární zdroje se ovšem v některých otázkách neshodují. Například zařazení třídění a porovnání získaných informací a dat, některé zdroje subsumují pod samotný sběr, jiné spíše pod

[10] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 35.
[11] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 130.

zpracování a analýzu. Na pováženou je, použijeme-li tradiční čtyř fázový cyklus, zda se v kroku „získávání a shromažďování informací“, myslí shromažďováním pouhé skladování, nebo i jejich organizace. Považuji za logičtější při shromažďování dat, či už předtím, mít připravený systém pro organizaci, neboť to značně usnadní další orientaci a práci.

Obrázek 1: **Zpravodajský cyklus dle H. Gibson (překl. vlastní)**[12]

2.2.1 Plánování a řízení zpravodajské činnosti

„Hlavním úkolem všech zpravodajských institucí je poskytovat relevantní odpovědi na informační požadavky svých zákazníků (zřizovatelů)“[13] Při přečtení JP 2-0, příručky Ministerstva obrany USA, je tento výrok blíže specifikován rozdělením této fáze do čtyř kroků:

- *„Identifikace a určení priority zpravodajských požadavků*
- *Příprava struktury pro organizaci získaných dat*
- *Příprava metod sběru dat*

[12] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation.* S. 72.
[13] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 131.

- *Vydání pokynů a požadavků relevantním zpravodajským skupinám"*[14]

Ve fázi plánování tedy dochází ke stanovení zpravodajských požadavků. Tento základní požadavek je poté zapracován do tvorby plánu, podle kterého se bude zpravodajská činnost vykonávat a bude dále řízena. Často se například v CI zpravodajská instituce setkává s příliš obecným zadáním a s touto situací se musí vypořádat.[15] Takový přístup je problematický mimo jiné i proto, že po dokončení cyklu může být zjištěno, že zpravodajské informace jsou nedostatečné, nebo nevěcné.

V této fázi také dochází k vymezení časových, předmětných a například i finančních limitů.

Je dobré si položit otázku, kdo může zadávat úkoly zpravodajským institucím? Odpovědi se výrazně liší v závislosti na to, o jakou instituci se jedná, obecně však lze říci, že tak může učinit externí, či interní autorita. Pro představu si můžeme představit na jedné straně Bezpečnostně Informační Službu (BIS), která reprezentuje státní zpravodajskou organizaci, a na straně druhé obchodní společnost, která má zřízené oddělení pro competetive intelligence. V případě BIS bude externí autoritou například prezident republiky s vědomím vlády, u obchodní společnosti to může být ředitel, předseda, nebo vedoucí oddělení.

Pokud by však zpravodajské instituce pracovaly pouze s úkoly takto explicitně zadanými, byl by celý proces zbytečně rigidní. Prezident, nebo ředitel společnosti, by pravděpodobně nedělali nic jiného, než zadávali úkoly. V praxi se proto setkáváme s tím, že úkoly mohou vyplývat přímo ze zákona, nebo z prosté povahy zaměření instituce, Michálek toto pojmenovává jako „*nejobecnější úkoly*".[16] Dále se úkoly dělí na úkoly dlouhodobé – ty vyplývají z dlouhodobých zájmů zadavatele a zpravidla se opakují v určité lhůtě, často v době jednoho roku. Na závěr zmíníme úkoly krátkodobé, které reagují na

[14] *Joint Publication 2-0: Joint Intelligence*.
[15] MOLNÁR, Zdeněk. *Competitive intelligence, aneb, Jak získat konkurenční výhodu*. S. 46.
[16] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 131.

rychle vzniklé příležitosti a hrozby a jsou významné na hierarchicky nižších úrovních zpravodajství.

2.2.2 Získávání a shromažďování informací

V této fázi je na úvod třeba vyvodit hlavní zaměření udaných požadavků, jaké prostředky budou procesu alokovány a jaké překážky mohou vyvstat. Je také dobré zvážit případné zásady ochrany – zejména v OSINT je třeba přijmout jisté opatření, aby nedošlo k infiltraci informačních systémů zařazených v procesu. Pokud přijmeme, že struktura dat byla již připravena v předchozím kroku, můžeme začít se sběrem dat. Ten probíhá všemi dostupnými metodami a směřuje k zajištění co největšího množství alespoň zdánlivě relevantních informací a dat. Toto může mít za následek nepřehlednost získaných dat, s tímto by měla pomoci již určená architektura a organizování a se vzestupem informačních technologií může být tato úloha výrazně usnadněna automatizovanými systémy třídění a sběru.

2.2.3 Zpracování a tvorba zpravodajských informací

Je třeba zmínit, že tato fáze často nečeká na skončení fáze předchozí, ale velice často běží prakticky souběžně a navzájem se podporují. Dobrá zpětná vazba získaná zpracováním informací může pomoci při efektivnějším sběru. „Podstatou této fáze je přeměna získaných a shromážděných informací na výstupní zpravodajské informace.“[17] Ve všem získaném obsahu se hledají různé souvislosti a propojení. Mnohost zdrojů může pomoci při určování věrohodnosti a spolehlivosti jednotlivých informací. Tato fáze také zahrnuje případný překlad získaného cizojazyčného obsahu. Na základě kvalitní analýzy lze poté vytvořit výslednou zpravodajskou informaci.

2.2.4 Distribuce zpravodajských informací

S hotovými zpravodajskými informacemi je poté seznámen zadavatel, nebo jiné, relevantní, nebo určené osoby, například státní instituce, ředitel obchodní společnosti, marketingové oddělení. Ty pak na základě těchto

[17] MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. S. 133.

informací mohou jednat. Naprosto klíčovou je zpětná vazba, předané informace mohou být nedostačující, nebo málo přesné, zpětnou vazbou lze tedy celý zpravodajský cyklus uzavřít do smyčky a pracovat v dalším „kole“ efektivněji.

3. ZPRAVODAJSTVÍ Z OTEVŘENÝCH ZDROJŮ

Lidé jsou konzumenty a tvůrci informací. Psané slovo nám umožnilo uchovávat vědomosti a zprávy technologický postup nám umožnil k nim stále jednodušeji přistupovat za kratší dobu ve větším množství. Jakmile zařadíme takto získané informace do zpravodajského cyklu jako vstupní hodnotu, můžeme mluvit o zpravodajství z otevřených zdrojů, nemusí jít však o informace pouze fyzicky zaznamenané a vytěžené, ale také o mluvou předané. Disciplínu zpravodajství z otevřených zdrojů lze považovat za jednu z nejsnáze dostupnějších forem zpravodajské činnosti, a proto také nepřekvapí, že některé odhady uvádí, že zpravodajství z otevřených zdrojů má na svědomí vytvoření 80–95 % veškerých zpravodajských informací.

Za nejzásadnější výhody OSINT můžeme považovat minimální náklady na sběr a zpracování informací, bezkonkurenční objem dostupných dat, rychlost, s jakou můžeme data získávat a relativně nízké nebezpečí pro operativce, ve srovnání s jinými metodami zpravodajství. Významnou výhodou je také teoreticky neomezené geografické rozložení dostupných zdrojů. Pro jiné formy zpravodajství může být sběr informací ze vzdálených míst nákladný, nebezpečný, a to jak fyzicky, tak z právních důvodů. Například policejní orgány ČR nemohou bez dohody s jinými státy provozovat zpravodajskou činnost na území jiných států, ale využití OSINT by nemělo činit žádný problém.

Jako první nevýhodu lze uvést jako pomyslný dvojsečný meč právě objem dostupných dat, protože z tohoto důvodu je kladen obrovský nárok na řádnou organizaci dat, zpracování do přijatelné podoby a jejich analýzu, kdy některé zdroje uvádí, že právě tato část zpravodajského cyklu zabírá *50 – 80% celkového času.*[18] Zatímco zpravidla jsou k dispozici mnohé zdroje, které mohou sloužit k ověření věrohodnosti informace, často tomu také tak být nemusí a spolehlivost a věrohodnost může být, stejně jako v jiných oborech

[18] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation.* S. 71.

zpravodajství, prakticky kdekoliv na stupnici spolehlivosti. Při sběru dat také dochází k nezáměrnému sběru dat, která nebudou využitelná, nebo jsou irelevantní, což se děje především při automatizovaném sběru. Taková data lze nazývat jako „šum“, nemají pro nás žádnou hodnotu a ztěžují další postup. Některé informace, například na sociálních médiích, nebo jiných internetových zdrojích, mohou mít omezenou existenci, protože autor je může kdykoliv odstranit. Řádné dokumentování a ukládání takto získaných informací je proto naprosto klíčové (ačkoliv můžou vyvstat otázky souladu s právními nařízeními na ochranu osobních údajů). Na závěr se hodí zmínit, že zatímco OSINT obstojí i v takových situacích, kdy je jediným zdrojem zpravodajských informací, při kombinaci s dalšími zdroji a způsoby získávání informací je jeho účinnost a spolehlivost mnohonásobně vyšší.

Tato činnost je užívána ke dvěma hlavním účelům – sběr informací pro účely žurnalismu a sběr informací pro využití zpravodajskými agenturami. Nelze však podceňovat další subjekty, které aktivně a úspěšně využívají metody OSINT. Řadí se mezi ně marketingové agentury, které sběrem veřejně dostupných informací vytvářejí profily svých aktuálních nebo potenciálních zákazníků a na základě těchto profilů tvoří cílenou reklamu. Personální agentury, které pro renomované klienty získávají informace o možných uchazečích o zaměstnání. Internetoví podvodníci, kteří mohou buď cílit na široké spektrum cílů – tzv. phishing, nebo díky velkému kvantu informací získanému o jedné určité osobě nebo organizaci, mohou vytvořit velice komplexní podvod – tzv. spearphishing.

3.1 Historie zpravodajství z otevřených zdrojů

Prakticky každá osoba je konzumentem informací z otevřených zdrojů – noviny, televizní zpravodajství, sociální sítě. V dnešní datové době každý k nám proudí neuvěřitelné množství informací. S čím dal větší digitalizací a v neposlední řadě, také díky pandemii viru Covid-19 se čím dále větší část našeho života odehrává v síti – online, nejsme proto jenom příjemci informací, ale také jejich tvůrci. Dalo by se proto očekávat, že OSINT je mladá metoda, která vznikla až s popularizací internetu a sociálních sítí. Je naprosto nepochybné, že rozmach informačních technologií byl naprostou revolucí ve

všech odvětvích zpravodajských metod a činností, včetně zpravodajství z otevřených zdrojů. Zdokumentovaný počátek této metody však nalezneme v době druhé světové války. Spojené Státy Americké v této době tvořily s pomocí Britské služby MI6 svou vlastní zpravodajskou službu – Office of Strategic Services. Do této doby Americká vláda viděla zpravodajské služby, které získávaly informace o zahraničních subjektech jako nemorální, oči jim však plně otevřel až útok na Pearl Harbor. V roce 1942 proto vznikla výše zmíněná OSS, která mimo všech tradičních metod jako je špionáž atp. hojně využívala i metodu OSINT – měla pro tuto metodu zřízenou vlastní odnož organizace. Její agenti sbírali noviny ze všech regionů zájmových zemí nebo poslouchali radiové vysílání. Získávali tak například fotografie nově spuštěných bitevních lodí Třetí Říše, informace o různých stavbách atp. Tato organizace na konci války zanikla a její místo zaujala agentura CIA, která funguje dodnes, nicméně důležitost OSINT byla v CIA podceněna a zmínky o jejím užívání v době po druhé světové válce jsou zanedbatelné.

Od té doby upadl OSINT prakticky v zapomnění, pravděpodobně byl využíván, ale nebyla mu věnována dostatečná pozornost, nebo informacím z těchto zdrojů nebyla přisuzována velká hodnota. Se vzrůstající popularitou internetu metodu OSINT začaly využívat novinářské servery. Státní aktéři k ní opět začaly upírat zrak v roce 2004. Tři roky po útocích na New Yorská dvojčata, organizace „National commision on terrorist attacks upon the United States“, vydala doporučení ke vzniku služby, která by čerpala informace z otevřených zdrojů. V roce 2005 na základě tohoto doporučení vzniklo „Open Source Center“ – „Centrum pro otevřené zdroje“, které mělo za úkol zpřístupnit informace z těchto zdrojů agentům zpravodajských služeb. Centrum bylo v roce 2015 přejmenované na „Open Source Enterprise“ a inkorporováno do CIA.

Na straně využití metod zpravodajství z otevřených zdrojů v oblasti žurnalismu server Bellingcat spatřuje počátek moderního OSINT v roce 2009, kdy v Iránu po prezidentských volbách došlo ke vzniku „Íránského zeleného hnutí“, které

označovalo výsledky voleb za zfalšované.[19] Podle Bellingcatu, v prvním týdnu těchto nepokojů bylo více než 60 % veškerých příspěvků na sociální platformě Twitter právě o zmíněném protestu. Data o Iránských uživatelích také poukazují na fakt, že využívání internetu v roce 2009 stouplo na 48 %, oproti předchozím 34 % a odběr internetových dat v mobilních telefonech vyskočil na 72 % z 59 %. BBC toto označilo za obrovský rozmach „občanské žurnalistiky“. Díky těmto skutečnostem mohl svět sledovat videozáběry a nepřeberné množství dalších informací o tom, co se právě dělo v Iránu. Státní režim zareagoval drastickým omezením dostupnosti internetového připojení. Motto demonstrace a další informace však proudily dál a internet byl využíván k organizování demonstrací. Bellingcat zároveň zmiňuje, že celá tato událost – rozšířené občanské nepokoje, vděčí za svou existenci třem klíčovým faktorům:

1) obrovské množství mobilních telefonů s 3G technologií bylo v rukou nespokojených občanů,

2) tito občané využívali malé množství sociálních platforem ke sdílení obrovského množství informací a organizaci protestů,

3) zmíněná data a informace byly veřejně přístupné celému světu. Pro srovnání s dneškem – technologie se posunuly již ke standardu 5G a počet sociálních platforem se více než zdvojnásobil.

Pro srovnání v České republice v roce 2021 využívalo internet v mobilu 72% obyvatelstva ve věku od 16+.[20] Výše uvedené skutečnosti poodhalují, jak výrazným zdrojem informací pro OSINT jsou samotní uživatelé sítí, kdy může jít o jediný dostupný zdroj v případě určitých vyšetřování. V kontextu této práce ale tento argument funguje pouze velmi omezeně, neboť hlavním zdrojem

[19] A Brief History of Open Source Intelligence. Bellingcat [online]. Dostupné také z: https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/

[20] Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci - 2021: Používání mobilního telefonu a internetu na mobilním telefonu [online]. Dostupné také z: https://www.czso.cz/documents/10180/142872020/062004210304.pdf/bd5804b7-03a8-43eb-a78b-67d3b040a3f0?version=1.1

budou více, či méně oficiální data a informace, poskytnuté zpravidla státními institucemi.

3.2 Právní rámec pro práci s otevřenými zdroji

Už z podstaty zpravodajství z otevřených zdrojů je jasné, že se musí jednat o informace získané legální cestou, z legálních zdrojů. Veškerý postup v oborech rozebíraných v této práci proto musí respektovat platnou právní úpravu. Zpravodajství z otevřených zdrojů často bývá ne neprávem spojováno s aktivitami hackerů a hackerských skupin, je tomu tak, protože se jedná o nesmírně efektivní nástroj, umožňující plošný sběr informací. Nicméně sběr informací a dat je základním krokem veškeré zpravodajské činnosti, a proto se vzestupem informačních technologií byl sběr dat často neúměrně amplifikován oproti skutečným potřebám, nebo účelům nejen zpravodajských organizací. Pro příklad lze uvést skutečnost, že každý web, který uživatel na internetu navštíví o něm automaticky sbírá základní informace. Nemusí ani nutně jít o zákeřné taktiky správce webu, ale často se tak děje pouze pro usnadnění navigace, například pro zobrazení relevantnějšího obsahu, či zapamatování různých uživatelských preferencí.

Tyto pozitivní stránky sběru informací jsou však vyváženy také výraznými negativními skutečnostmi. V informační době si společnosti a organizace uvědomily hodnotu informací a jak snadno je lze nejen na internetu sbírat, za nejzávažnější příklad můžeme považovat například sociální sítě, kdy nejen jejich správci, ale při malé snaze i pouzí uživatelé mohou efektivně vytvořit profil jiných uživatelů na základě údajů, které byly na stránce vědomě a účelně zveřejněny těmito samotnými uživateli. Situace dosáhla takových rozměrů, že si kontinentální zákonodárci začali uvědomovat, že právní úprava ochrany osobních údajů je v mnoha případech zastaralá a nereflektuje masivní pokrok, který byl učiněn od přijetí těchto zákonů.

Termín „osobní údaj“ je definovaný v Obecném nařízení o ochraně osobních údajů, které je také nejvýznamnějším právním dokumentem, který tuto

problematiku upravuje, za osobní údaje považuje *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě, identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*[21]

Sběr a nakládání s osobními údaji může být a zpravidla i je považováno za zásah do soukromí osob a záruka ochrany této hodnoty je stanovena v Ústavním pořádku České republiky. Zde si uvedeme právní předpisy upravující správu, sběr a jiné nakládání s osobními údaji, které jsou platné v České republice a instituce, které mají v této oblasti působnost.

3.2.1 Právní základ a instituce

Základní institucí, do jejíž působnosti spadá dohled na ochranu osobních údajů v ČR je Úřad pro ochranu osobních údajů. Jedná se o ústřední správní úřad, který svou činnost vykonává nezávisle. Jeho vznik, ačkoliv pod jiným jménem najdeme v roce 2000. Úřad ve své současné podobě funguje od roku 2019, kdy vstoupil v platnost zákon č. 110/2019 Sb., o zpracování osobních údajů, ke kterému si uvedeme podrobnější informace později v této práci.

Tato instituce na svých webových stránkách jako právní základ pro ochranu osobních údajů úmluvu Rady Evropy č. 108 z roku 1981, která stanoví jistá pravidla pro automatizovaný sběr osobních údajů. Dále potom uvádí článek 8 Charty základních práv Evropské Unie, který stanoví následující zásady:

1. *„Každý má právo na ochranu osobních údajů, které se ho týkají.*

2. *Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.*

[21] Slovníček nejdůležitějších pojmů: Osobní údaj [online]. Úřad pro ochranu osobních údajů, 2013. Dostupné také z: https://www.uoou.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617

3. *Na dodržování těchto pravidel dohlíží nezávislý orgán.“*[22]

Stejnou otázku upravuje i článek 16 Smlouvy o fungování Evropské unie. Dalším podstatným dokumentem pro ochranu osobních údajů a soukromí osob je Listina základních práv a svobod, která je zařazena do Ústavního pořádku ČR, ta v 1. odstavci, článku 7 stanoví že „nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“[23]

Pro praxi OSINT je relevantní ještě 3. odstavec článku 10 stejného zákona, který stanoví že „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“ Ochrana soukromí je tedy jednoznačně považována za jednu z nejdůležitějších hodnot, které nachází ochranu v Ústavním zákonu, jelikož je ale Ústavní zákon vcelku stálý a neměnný, spoléhá se na dodatečnou právní úpravu, která je flexibilnější a může lépe držet krok s vývojem technologií.

3.2.2 GDPR

General Data Protection Regulation, do češtiny přeloženo jako Obecné nařízení o ochraně osobních údajů je Nařízením Evropské unie, jehož cílem je výrazné zvýšení ochrany osobních dat občanů.[24] Schválením tohoto nařízení došlo k nesmírnému rozdělení praktické činnosti OSINT v kontextu kontinentálního práva a například Amerického právního prostoru – ten je totiž značně benevolentnější při nakládání s osobními údaji, kdežto v EU, potažmo i v ČR je kladen mnohem větší důraz na soukromí osob. Zatímco v USA je možné za malý poplatek legálně získat přístup ke kompletním trestním evidencím jednotlivců, v zemích EU je takový přístup nepředstavitelný. Nařízení bylo poprvé navrhnuto na začátku roku 2012 a stalo se účinným 25. května 2018, je platné ve všech státech EU, nebo při shromažďování a

[22] *Listina základních práv Evropské unie: HLAVA II - SVOBODY: Článek 8: Ochrana osobních údajů*.
[23] ČESKO. *Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky.*

[24] Obecné nařízení o ochraně osobních údajů. *Wikipedia: the free encyclopedia* [online].

zpracovávání osobních údajů občanů členských států EU i pokud sběr a zpracování probíhá mimo území unie. Existují jisté výjimky, jako je například:

a) *„výkon činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU,*
b) *fyzickou osobou v průběhu výlučně osobních či domácích činností a v neposlední řadě příslušnými orgány za účelem prevence*
c) *vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.“*[12]

Zvláště poslední uvedená výjimka se může vztahovat na uživatelé určitých metodik, které budou popsány dále v této práci a je proto třeba ji vzít na vědomí, za takových okolností ale rozhodně není na škodu považovat některé normy uvedené v nařízení jako dobré zásady pro OSINT.

Nařízení rozeznává tři základní subjekty při nakládání s osobními údaji, kterými jsou:

a) subjekt údajů – fyzická osoba, s jejíž údaji je nakládáno
b) správce údajů – fyzická osoba, právnická osoba, orgán veřejné moci a další subjekty, které jsou držiteli údajů
c) zpracovatel osobních údajů – fyzická osoba, právnická osoba, orgán veřejné moci a další subjekty, které pro správce údajů zpracovávají tyto údaje pro správce (např. i správa databází, cloudové služby)

Nelze si nepovšimnout, že subjektem údajů může být pouze fyzická osoba, nikoliv osoba právnická, což výrazně ovlivní další charakter výkonu OSINT v oblasti finančního a ekonomického zpravodajství, neboť se zde velice často shromažďují a zpracovávají právě údaje právnických osob.

Při práci s osobními údaji, na které se vztahuje GDPR je třeba se řídit několika zásadami.

- **Zákonnost zpracování** – GDPR uvádí šest různých možností, kdy se musíme při zpracování dat pohybovat přinejmenším v jedné z nich, aby byla naplněna zákonnost zpracování osobních údajů. První možností je

situace, kdy subjekt údajů udá výslovný souhlas pro zpracování svých osobních údajů. Toto upravuje sedmý článek zmíněného nařízení. Problematická ale může být skutečnost, že subjekt údajů může udaný souhlas kdykoliv vzít zpět, čímž nám je znemožněna jakákoliv další manipulace s již získanými daty a informacemi. Druhou možností relevantní pro OSINT je situace, kdy je zpracování údajů nezbytné pro splnění právní povinnosti, která se na správce údajů vztahuje. S ohledem na charakter této práce lze zdůraznit například povinnost některých finančních institucí mít určitou úroveň znalosti svých klientů. Třetí možností je tzv. oprávněný zájem. Tato možnost přichází v úvahu za předpokladu, že zpracování osobních údajů sice není vyžadováno žádnou zákonnou povinností, nicméně ze zpracování vyplývá jednoznačná výhoda, a to za předpokladu, že tímto zpracováním nedojde k porušení zájmu ochrany soukromí subjektů údajů a nadále subjekt údajů může důvodně očekávat, že jím poskytnutá data mohou být tímto způsobem použita. V praxi pod tuto možnost spadají například případy, kdy se správce údajů snaží předejít podvodnému jednání, nebo jedná z důvodu bezpečnosti informačních systémů, nebo když existuje důvodné podezření, že může takové zpracování napomoci k objasnění nebo odhalení nezákonných aktivit, nebo jiného ohrožení veřejné bezpečnosti.[25]

- **Zodpovědnost** – při práci v OSINT je třeba přijmout naprostou zodpovědnost za zpracovávání a sběr dat a za jejich řádnou ochranu před zneužitím. Na správce, či zpracovatele je též přenesena plná zodpovědnost za prokazování zákonnosti tohoto procesu, a proto je nutné učinit dostatečná opatření k tomu, aby byla tato skutečnost snadno prokazatelná. Pro zlehčení lze uvést, že v OSINT je dobrým zvykem a často i naprostou nezbytností řádně evidovat veškerý postup

[25] *What Is Legitimate Interest Under the GDPR? [online].* Drogheda: Luke Irwin, 2022. Dostupné z: https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply

a zjištěné skutečnosti, proto by splnění takové povinnosti nemělo činit potíže.

- **Zásady zpracování osobních údajů** – článek 5 GDPR uvádí tři základní zásady, kterými jsou „zákonnost, korektnost, transparentnost". První z nich jsme již rozebrali výše. Korektností je zde míněna jistá proporcionalita, ve které je třeba zohlednit, zda objem a druh dat, která shromažďujeme jsou v rozumném poměru vůči závažnosti zkoumané skutečnosti, nebo zda jsou opodstatněny jiným způsobem. Transparentnost jsme taktéž zmínili výše, prakticky se překrývá s definicí zodpovědnosti, kdy musíme být schopni obhájit rozsah a způsob sběru a zpracování veškerých dat.
- **Minimalizace údajů** – tímto je stanovena výše uvedená povinnost neshromažďovat přebytečné údaje a získávat pouze takové, které jsou naprosto nezbytné pro účel sledovaný zpravodajskou činností.
- **Přesnost** – údaje které získáváme a zpracováváme musí být v co nejvyšší možné míře pravdivé a aktuální. Musí být učiněna veškerá možná opatření, aby nedocházelo ke sběru nespolehlivých informací a v případě že k takové situaci dojde, aby došlo co nejdříve k nápravě.
- **Omezení uložení** – nařízení velice vágně stanovuje, že „*získaná data nesmí být uložena ve formě umožňující identifikaci subjektů po dobe delší, než je nezbytně nutné pro účely, pro které jsou zpracovávány.*"[26] Zde je patrné ponechání dostatečného prostoru pro správní výklad neurčitého termínu a spoléhá se na rozumný přístup subjektů GDPR.
- **Integrita a důvěrnost** – data a informace musí být zpracovány a uloženy takovým způsobem, aby předešlo jejich zneužití. Toto může znamenat jak technické opatření, jako je například prevence před hackerským útokem, tak i úprava přístupu k datům na úrovni organizačních opatření.

Jelikož metody OSINT může používat kdokoliv od jedince, který zkoumá určitou problematiku, přes obchodní společnosti, až po orgány veřejné moci,

[26] EU. *Obecné nařízení o ochraně osobních údajů*.

je vždy třeba blíže prostudovat, jak je činnost těchto subjektů upravena danými právními předpisy. Abychom naplnili podstatu a klíčovou zásadu OSINT, musíme informace čerpat a nakládat s nimi v souladu se všemi platnými předpisy. Dále v této práci se setkáme se dvěma hlavními uživateli těchto metod – společnosti, které OSINT uplatní při realizaci konkurenčního zpravodajství a také orgány veřejné moci na poli finančního zpravodajství při odhalování a předcházení hospodářské a finanční trestné činnosti.

3.2.3 Zákon číslo 110/2019 Sb., o zpracování osobních údajů

Od roku 2000 byl v ČR platný zákon o ochraně osobních údajů, který zajišťoval zaručené právo na ochranu soukromí všech občanů a osob. Ten byl v roce 2019 nahrazen zákonem o zpracování osobních údajů, kterým se provádí výše uvedené Nařízení o ochraně osobních údajů. Upřesňuje některé termíny, určuje přestupky na úseku ochrany osobních údajů a sankce za ně. Stanoví také orgán, do jehož působnosti spadá dozor nad řádnou ochranou osobních údajů, určí mu povinnosti, pravomoci a další základní podklady.

3.3 Členění OSINT

Zpravodajské informace z otevřených zdrojů můžeme členit několika způsoby, mezi ty nejvýraznější však řadím členění dle vstupního zdroje a členění dle druhu informace.

3.3.1 Členění dle zdroje

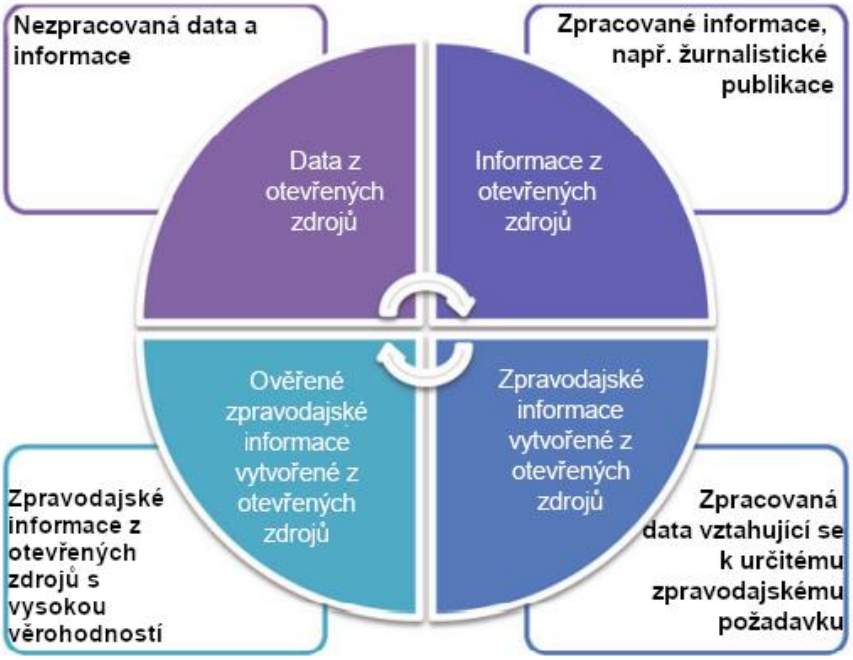
Za hlavní zdroje pro tvorbu a práci s OSINT můžeme označit televizní a radiové vysílání, tiskové zpravodajství, šedá literatura, komerční data, knihy, internetové zpravodajství nebo jakékoliv jiné formy zveřejňování informací a dat na internetu, jako například státní či nestátní databáze, blogy, akademické weby, diskusní weby a v neposlední řadě sociální sítě. Každý jmenovaný příklad má svá specifika. Například databáze umožňují získat strukturovaná data, která mají jistou vnitřní architekturu a jasný vztah, s těmito daty se pak mnohem lépe pracuje. Sociální sítě, které jsou jedním z nejpodstatnějších zdrojů v OSINT v poslední době, jsou specifické tím, že zpravidla obsahují data

a informace, které byly zveřejněny samotným subjektem údajů – lidé píšou sami o sobě, často bez jakéhokoliv filtru, zvážení toho, co je a není vhodné zveřejňovat.

3.3.2 Členění dle druhu informace

„NATO člení informace a zpravodajské informace z otevřených zdrojů do čtyř kategorií.“[27] (překl. vlastní). Tyto kategorie můžeme vidět na níže přiloženém obrázku č. 2. Vrchní dvě kategorie – data z otevřených zdrojů a informace z otevřených zdrojů, jsou jediným produktem, který lze získat pouhým sběrem a základním zpracováním informací. Tyto vstupní data a informace se dále rozlišují podle toho, zda se jedná o strukturovaná, nebo nestrukturovaná data. Za strukturovaná data můžeme považovat například výše uvedené databáze, statistiky, kdy je jasné, co jaké pole v tabulce vyjadřuje a jaký je vztah k dalším polím. Výše zmíněný pravý opak se potom vyznačuje chybějící strukturou – může jít o příspěvky na fórech, blozích, různá média – audiovizuální záznamy. Dalšími procesy, které si uvedeme později v této práci, se můžeme propracovat až k ověřeným zpravodajským informacím. Níže zobrazený vzorec kopíruje základní koncept zpravodajského cyklu, protože z něho vychází a pouze aplikací jeho jednotlivých kroků se lze posouvat dále.

[27] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation.* S. 70.



Obrázek 2: **„Postup od dat k ověřené zpravodajské informaci“** [28]

3.4 Metody získávání informací z otevřených zdrojů a hlavní nástroje

Pro vypracování této části silně spoléháme na publikaci Open Source Intelligence Investigation od kolektivu autorů zkušených v OSINT, jmenovitě především Babak Akhbar a Saskia Bayerl. Tato příručka je jedním z nejvhodnějších zdrojů pro kohokoliv, kdo se zajímá o teorii OSINT a jeho aplikaci při zpravodajské činnosti. Metody v ní popsané byly ověřeny zpravodajskou praxí v institucích jak kontinentálních, tak amerických, a proto je zde decentní míra relevance pro český právní řád. Lze se obrátit i na Příručku NATO pro OSINT[29], která je ovšem dostupná pouze ve svém znění z roku 2002 a tím pádem je silně neaktuální. Dají se zde však najít principy OSINT, které platí dodnes.

Na začátku procesu sběru dat musíme mít zodpovězené otázky první fáze zpravodajského cyklu – co je předmětem naší činnosti, jaké otázky se snažíme

[28] AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation.* S. 70.
[29] *NATO Open Source Intelligence Handbook* [online].

zodpovědět. Na základě toho lze vyvodit, jaká data budou potřeba k dalšímu postupu. Pokud se nám podaří najít data v ideální podobě, tj. připravené ke zpracování a analýze, může nám to výrazně urychlit celý proces, taková situace ale nastává zřídkakdy.

První, technicky nejméně náročnou, naopak však časově nejnáročnější metodou sběru dat je manuální sběr. Tímto je myšlena činnost jedince, či jedinců, kteří bez pomoci složitějších automatizovaných procesů vyhledávají střípky informací a dat. Přístup je využitelný při čerpání z kteréhokoliv otevřeného zdroje, nejčastěji se však čerpá z internetu. Tuto metodu může využít kdokoliv i s minimem zkušeností, vystačí si pouze se základní znalostí fungování informačních systémů a základních modifikátorů dotazů uživatelsky nenáročných vyhledávacích enginů, jako je například Google, DuckDuckGo, nebo mírně složitější Wolfram Alpha. Pomoci modifikátorů, také nazývaných operátorů, se například dá omezit zobrazovaný výčet výsledků pouze na relevantnější výsledky, obsahující například nejenom jednotlivá slova, ale také doslovné znění slovního spojení nebo formát souboru. Stejným způsobem lze zaměřit vyhledávání na určitou část webové stránky. Výhodou této metody je individuálnější přístup ke všem získaným datům, člověk a jeho uvážlivost zde funguje jako jakýsi filtr, který může pomoci při přesnějším sběru. Toto ovšem může být kontraproduktivní z důvodu lidských chyb – člověk vyhodnotí při sběru informaci jako irelevantní a vyřadí ji, ačkoliv by se toto mělo dít až ve fázi analýzy. Ve finančním a ekonomickém zpravodajství se jedná o jednu z nejpodstatnějších metod, využívají ji jak orgány činné v trestním řízení, tak jiné zpravodajské skupiny. Důvodem je především skutečnost, že například vyšetřování skutku je zaměřeno na úzký okruh osob nebo společností a data, která k nim lze metodami OSINT získat jednak nebudou nijak obsáhlá a zároveň pravděpodobně bude postačovat menší objem dat.

Ve většině případů však bude manuální sběr hrát tzv. druhé housle a bude sloužit pouze jako podpůrná metoda. Primárně se proto využívají různé druhy automatizovaných sběrů a vyhledávání dat. Pro tuto činnost existují programy a služby, které mohou využít méně zkušení uživatelé, úskalí nicméně spočívá v rigidnosti těchto programů. Zdatný uživatel se znalostí programovacích

jazyků by si pravděpodobně dokázal základní nástroj vytvořit sám a více přiléhavý jeho konkrétním potřebám. Lze proto říci, že při využití automatizovaných metod je znalost programovacích jazyků, především Python, spíše nutností než možností.

- **Web crawler** – „*Web crawler (někdy také spider) je v informatice specializovaný internetový bot, který prochází World Wide Web za účelem vytvoření obrovské databáze (web index). Navštěvuje automaticky veškeré dostupné webové stránky a tím umožní zaznamenat, která slova kde viděl. Webový vyhledávač pak na dotaz uživatele (jedno nebo více slov) může z web indexu odpovědět, na kterých stránkách jsou hledaná slova k nalezení.“*[30] Typickým příkladem je nástroj Spiderfoot, který je volně dostupný na internetu k omezenému bezplatnému použití. Jakýkoliv zpravodajec by byl nucen zaplatit nemalou částku, aby pro jeho činnost byl tento nástroj použitelný. U nástroje lze nastavit jaký typ dat má sbírat, jaké korelace má hledat a trasovat. Spiderfoot také umí nalézt případné skuliny v ochraně webu, což ho činí užitečným i pro defenzivní zpravodajství. K dispozici je také Googlebot od poskytovatele nejrozšířenejšího vyhledávacího enginu, stejně tak Bingbot, nebo Scrapy. Použití Web crawleru je tedy dobrým prvním krokem při sběru dat.
- **Jednotlivá API** – neboli Application Programming Interface *„označuje v informatice rozhraní pro programování aplikací. Jde o sbírku procedur, funkcí, tříd či protokolů určité knihovny, nebo programu, které může programátor využívat. API určuje, jakým způsobem jsou funkce knihovny volány ze zdrojového kódu programu. Funkce API jsou programové celky, které programátor používá namísto toho, aby je sám naprogramoval.“* Za API můžeme považovat například i výše zmíněné crawlery od společností Google a Microsoft. Nicméně mezi nejprominentnější API používané v OSINT se řadí rozhraní jednotlivých sociálních sítí, jmenovitě REST API od Twitteru, nebo Graph od

[30] Web crawler [online]. Web browsers introduction. Dostupné také z: https://webbrowsersintroduction.com/

Facebooku. Přístup k těmto funkcím je omezený a každý jednotlivec musí nejdříve získat přístupový klíč. Poté je dále omezen například počtem hledání, která může v API provést. Tímto způsobem se například dá získat přehledná tabulka zobrazující jaké účty sdílely zveřejňovaly stejná slova, nebo s jakými účty prováděli interakci.

- **Whois** – primitivní nástroj, který prohledá databázi domény nejvyššího řádu, kterou v ČR spravuje sdružení CZ.NIC. Tímto nástrojem můžeme zjistit na koho je jaká webová stránka registrovaná v dané databázi. U fyzických osob je odpověď jednoznačná, u osob právnických je třeba pokračovat zjišťováním skutečného majitele.
- **OSIRT** – neboli Open Source Internet Research Tool je nástroj ke kompletnímu zaznamenávání vyšetřování na internetu. Umožňuje uživateli vytvořit a kategorizovat jednotlivé případy a přistupovat na web za pomoci integrovaného prohlížeče. Ten je upraven k tomu, aby sloužil ke sběru dat a informací, tzn. automatické ukládání fotografií procházených stránek, případně videozáznamů, nebo stažení celých webových stránek. Zároveň umožňuje výstup shromážděných dat převést do běžně užívaných formátů. Při manuálním sběru informací se jedná o velice populární řešení.
- **Maltego a CaseFile** – pravděpodobně nejvyhlášenější nástroj k získávání, organizování a následné analýze dat na poli OSINT. Nástroj má jak svou placenou, tak neplacenou verzi. Jeho hlavní výhodou je možnost instalace jednotlivých modulů, které silně rozšiřují jeho funkce. Hlavní funkcí je zobrazení vazeb dle různých kritérií, například uzlů mezi webovými stránkami, osobami, profily na sociálních sítích, nebo obchodními společnostmi. Maltego v sobě obsahuje většinu již uvedených nástrojů cenných pro zpravodajství z otevřených zdrojů, nicméně jejich užití je silně omezeno v závislosti na druh uživatelského účtu, komunitní – neplacená verze obsahuje pouze základní funkce a možnost vizualizace. Placená verze je pro osoby, které neprovozují zpravodajství z otevřených zdrojů jako výdělečnou činnost prakticky nesmyslné, nicméně nástroj je nezbytný pro profesionály.

4. OSINT VE FINANČNÍM A EKONOMICKÉM ZPRAVODAJSTVÍ

V této části práce můžeme dříve uvedené praktiky a zásady konečně dát do kontextu s polem finančního a ekonomického zpravodajství. Je třeba si zde opět zodpovědět několik základních otázek. Odkud lze čerpat další informace pro rozvoj metodik a praktické využití FININT a EI? Kdo může být uživatelem těchto metod? Jaké jsou zdroje specifické pro tuto oblast v ČR a v zahraničí a na jakém právním základě jsou tyto informace poskytovány subjekty?

Hlavní příručkou pro získání podkladů k vypracování této kapitoly, k praktické části práce a k pochopení především finančního zpravodajství, mi byly weby Lexperanto[31], Certifix[32] a příručka pro rozkrývání vlastnických struktur a skutečných majitelů[33], vytvořená za podpory Evropského Úřadu pro boj proti podvodům a Transparency International.

V první kapitole práce jsme uvedli definice jak finančního, tak ekonomického zpravodajství. Zejména co se uživatelů těchto zpravodajství týče, existuje zde silný překryv, hlavní rozdíl mezi těmito dvěma oblastmi proto spatřujeme především v oblasti jejich zájmu, případně záměru jejich uživatelů. Co je tedy objektem těchto dvou zpravodajství? Finanční zpravodajství slouží především státním orgánům, včetně orgánů činných v trestním řízení, při vyšetřování trestné činnosti spojené s daňovými úniky, korupcí, financováním terorismu, organizovanou trestnou činností ve finanční oblasti, praní špinavých peněz a zneužívání dotací a veřejných zakázek. Činnost v tomto zpravodajství proto bude zpravidla směřovat k objasnění okolností těchto činů a jejich rozkrytí. Nelze však opominout také upotřebitelnost pro investigativní novináře.

Ekonomické zpravodajství pokrývá velice širokou oblast – od strategických zájmů států, přes soupeření jednotlivých obchodních společností až po prostou

[31] Lexperanto [online]. 2022. Dostupné také z: http://lexperanto.cz/
[32] Certifix [online]. TXP Association, 2022. Dostupné také z: www.certifix.eu
[33] VONDRÁČEK PH.D., LL.M., JUDr. Ondřej. Příručka pro rozkrývání vlastnických struktur a skutečných majitelů.

novinařinu. Z podstaty této práce se novinářským uplatněním ekonomického zpravodajství prakticky vůbec zajímat nebudeme.

4.1 Zákony upravující oblast FININT a EI

Nejvhodnější zdroje pro práci v oblastech finančního a ekonomického zpravodajství vznikají na základě zákonem uložené povinnosti prověřovat své subjekty, nebo evidovat jisté skutečnosti, nebo události, jako jsou transakce atp. Povinnosti vyplývají nejen ze zákonů vydaných Českou republikou, ale také vydaných Evropskou unií a v ČR ratifikovaných. Pro činnost FININT a EI stále platí všechna legislativa a zásady uvedené v kapitole o otevřeném zpravodajství, nicméně tyto zákony jsou velice specifické ve svém poli úpravy, a proto je nutné klíčové je zmínit.

4.1.1 Zákon č. 21/1992 Sb., o bankách

Důležitost tohoto zákona pro FININT spočívá v povinnosti České národní banky ověřovat pozadí žadatele o bankovní, pojišťovací, či podobnou licenci. ČNB je zde proto v pozici jak uživatele FININT, tak tvůrcem informací pro další uživatele, neboť při licenčním řízení vydává rozhodnutí, kterým musí být potvrzeno, že žadatel splnil široké množství podmínek. Mezi tyto podmínky spadá především průhledný a nezávadný původ základního kapitálu a dalších finančních zdrojů banky, důvěryhodnost osoby, které má být licence udělena, průhlednost skupiny osob s úzkým propojením s bankou. Zároveň je z takové žádosti automaticky vyloučen kdokoliv, kdo v minulosti páchal trestnou činnost s majetkovou povahou, nebo související s bankovní činností. Vzniká zde tedy státním orgánem podložený důkaz o původu kapitálu takové společnosti a o ověření spolehlivosti žadatelů.

4.1.2 Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

Tento zákon, často nazývaný jako „zákon proti praní špinavých peněz“, nebo AML – anti-money laundering, je stěžejním pro veškerou činnost orgánu

činných v trestním řízení v oblasti finanční a hospodářské kriminality. Na úvod specifikuje, kdo je „povinná osoba“, která musí evidovat údaje o svých klientech – opět se zde objevuje především povinnost mít průběžný přehled o struktuře ať už fyzických nebo právnických osob, které jsou jejími klienty, zjišťovat původ majetku těchto osob, a především ukládá uchovávat po určenou dobu a v určeném rozsahu informace. Povinnými osobami jsou zejména bankovní nebo poradenské instituce, investiční společnosti, obchodníci s nemovitostmi atp. Ačkoliv toto znamená, že jsou k dispozici podstatná data a údaje, nemůžou být považovány za otevřené zdroje, neboť přístup k nim je výrazně omezen. Jedná se proto o zdroj důležitý, ne-li klíčový pro finanční zpravodajství, ale nenaplňuje znak otevřenosti požadovaný pro jeho užití v OSINT. V tomto zákonu byla až do května roku 2021 uvedena také povinnost právnických osob evidovat své skutečné majitele, která však byla přesunuta do zákona č. 37/2021 Sb., o evidenci skutečných majitelů.

4.1.3 Zákon č. 37/2021 Sb., o evidenci skutečných majitelů

Jinak také tzv. „evidenční zákon“. Tento zákon funguje paralelně s informačním systémem veřejné správy „Evidence skutečných majitelů“, který spravuje Ministerstvo spravedlnosti. Zákon zapracovává příslušné předpisy Evropské unie[34] a upravuje vedení evidence skutečných majitelů a práva a povinnosti s tím související. Rovněž stanoví, kdo nemá povinnost evidovat skutečného majitele, což je například stát a územní samosprávný celek, společenství vlastníků jednotek nebo politické strany. V porovnání s předchozí úpravou ve výše uvedeném zákonu zde došlo ke změně definice skutečného majitele, která nyní zní: *“každá fyzická osoba, která je koncovým příjemcem nebo osobou s koncovým vlivem.“*[35] Skutečným majitelem tedy může být pouze fyzická osoba. Zákon se navíc pokusil usnadnit evidenci těchto údajů tím, že

[34] Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES.
Směrnice Evropského parlamentu a Rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU.
[35] ČESKO. Zákon č. 37/2021 Sb., o evidenci skutečných majitelů. Dostupné také z: https://www.zakonyprolidi.cz/cs/2021-37

umožnil tzv. automatický průpis skutečného majitele, který má probíhat převzetím údajů z veřejných rejstříků – obchodních atp. Za správnost takového průpisu zodpovídá subjekt těchto údajů. Oproti předchozímu zákonu je zde patrný rozdíl ve veřejnosti takto uchovaných informací – je zde výslovně uvedeno, že *„Ministerstvo umožní komukoli na svých internetových stránkách získat z evidence skutečných majitelů částečný výpis platných údajů“*[36]. Údaje, které díky tomuto systému a zákonu lze čerpat jsou taxativně vyjmenovány a jedná se především o:

- jméno, stát bydliště, rok a měsíc narození, státní občanství skutečného majitele,
- údaj o povaze postavení skutečného majitele,
- údaj o velikosti přímého nebo nepřímého podílu skutečného majitele, zakládá-li tento podíl jeho postavení,
- den, od kterého je fyzická osoba skutečným majitelem,
- den, do kterého byla fyzická osoba skutečným majitelem,
- další údaje, s jejichž uveřejněním dal skutečný majitel souhlas.

4.1.4 Další zákony

Za zmínku stojí například zákon č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů, který udává pravomoci Úřadu pro ochranu hospodářské soutěže a specifikuje jeho činnost. Za podstatnou také můžeme považovat vyhlášku č. 67/2018 Sb., o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, která stanoví rozsah a způsoby pro kontroly klientů. Nesmíme také opomenout Metodický pokyn č. 3 Finančního analytického úřadu ze dne 31. května 2021, který může sloužit jako dobrý zdroj pro vysvětlení jednotlivých termínů zákona AML. Dalším zákonem, díky kterému získáváme další podstatný otevřený zdroj pro FININT je zákon č. 563/1991 Sb., o účetnictví. Ten ukládá povinnost účetním jednotkám zveřejňovat určité části účetní uzávěrky.

[36] ČESKO. Zákon č. 37/2021 Sb., o evidenci skutečných majitelů. Dostupné také z: https://www.zakonyprolidi.cz/cs/2021-37

4.2 Uživatelé FININT a EI

Finanční zpravodajství je především doménou státních zpravodajských služeb, v České republice se mu věnuje například Bezpečnostní informační služba (BIS), která tak dělá zejména ve vztahu ke sledování organizovaného zločinu, nebo vyšetřování terorismu, v kontextu FININT se tedy jedná především o jeho financování. V tomto ohledu byl významný například případ z roku 2018, kdy pražský imám Samer Shehadeh měl organizovat výjezdy českých muslimů do Sýrie, kde měli bojovat po boku teroristických skupin. Na tuto činnost dostával značné finanční obnosy od ambasády Saudské Arábie v Praze. Sám také organizoval v české muslimské komunitě pravidelné sbírky, jejichž výnosy měly sloužit na léčbu zraněných bojovníků teroristických skupin. BIS případ řešila ve spolupráci s Národní centrálou proti organizovanému zločinu (NCOZ).

BIS působí rovněž na poli ekonomického zpravodajství.

„BIS informuje odpovědné představitele státu o rizicích směřujících proti významným ekonomickým zájmům České republiky. Smyslem je zajistit, aby adresáti informací byli včas seznámeni s riziky ohrožujícími zájmy státu v jejich působnosti, a aby měli pro svá klíčová ekonomická rozhodnutí všechny relevantní poznatky, např. o vnějších snahách tato rozhodnutí ovlivnit, o plánovaných krocích rizikových subjektů nebo o skrytých zájmech stojících v jejich pozadí.“[37]

Za významné ekonomické zájmy dále BIS označuje:

„Významným ekonomickým zájmem se rozumí zájem na funkčnosti systémů s plošným hospodářským dosahem (energetika, doprava, zdravotnictví, telekomunikace, bankovnictví, výběr daní) a na optimální správě majetku (finance, majetkové podíly, nemovitý majetek, nehmotný majetek), jehož ztráta by mohla ohrozit nebo omezit základní funkce státu. Škody na ekonomických zájmech státu vznikají skrze přímé finanční ztráty, ohrožení energetické bezpečnosti, ohrožení jiné infrastruktury s plošným hospodářským dosahem (např. doprava, telekomunikace, zdravotnictví, bankovnictví a kapitálové trhy) či ohrožení entit, jejichž poškození má nepřímý, ale doložitelný negativní hospodářský dopad na stát (životní prostředí, zdraví, podpora exportu, hospodářská soutěž, nezávislost regulačních úřadů, členství v mezinárodních organizacích apod.). Významnost ekonomického zájmu je dána nejen zabezpečením funkčnosti dané oblasti hospodářství, ale i výší případných finančních dopadů pro stát a zejména dopady na bezpečnost státu. Tyto zájmy

[37] Ekonomické zájmy státu [online]. Praha, 2022. Dostupné také z: https://www.bis.cz/ekonomicke-zajmy-statu/

jsou konkretizovány příslušnými usneseními vlády, které zadávají BIS přímé úkoly.“[38]

NCOZ spadá pod Policii České republiky a je rozdělena na několik sekcí, z nichž čtyři vykonávají činnost spadající pod definici finančního zpravodajství. Sekce korupce a závažné trestné hospodářské činnosti, sekce terorismu a extremismu, sekce organizovaného zločinu a sekce finanční kriminality, všechny tyto sekce nepochybně využívají za jeden ze zdrojů finanční zpravodajství.

Úřad pro zahraniční styky a informace (UZSI) je vnější zpravodajskou službou České republiky, která působí na poli finančního zpravodajství, ačkoliv oproti předchozím dvěma institucím spíše okrajově. UZSI se zde věnuje *„bezpečnostnímu zpravodajství o mezinárodním terorismu a jiných asymetrických bezpečnostních hrozbách, ohrožujících bezpečnostní zájmy České republiky a její mezinárodní závazky.“*[39] Daleko významnější je působení UZSI na poli ekonomického zpravodajství, zejména na strategické úrovni. Úřad informuje příslušné orgány státní správy o skutečnostech, které mohou mít vliv na ekonomický vývoj a bezpečnost České republiky.

Další skupinou, která má obrovské zastoupení na poli ekonomického zpravodajství jsou obchodní společnosti. Ty tak činí v rámci competetive intelligence, kdy jim vstupní data získána ekonomickým zpravodajstvím zodpovídají na klíčové otázky jejich podnikání. Především se jedná o mapování konkurence, analýza silných či slabých stránek, příležitostí a hrozeb, také nazývána SWOT. Ekonomické zpravodajství je zde naprostou nezbytností, ne-li jediným vhodným zdrojem informací. Společnosti jsou tímto způsobem schopny sestavit obchodní strategie a připravit se na vývoj trhu, různé trendy, lépe sestavovat své marketingové strategie nebo upravovat produkty.

[38] Ekonomické zájmy státu [online]. Praha, 2022. Dostupné také z: https://www.bis.cz/ekonomicke-zajmy-statu/
[39] Úřad pro zahraniční styky a informace: Co děláme [online]. Praha, 2022. Dostupné také z: https://www.uzsi.cz/co-delame

4.3 Zdroje FININT, EI v ČR a zahraničí

Jak lze usuzovat z kapitoly o zákonech upravujících tuto oblast, nejčastějším zdrojem budou registry veřejné správy. Informace z nich dostupné budou poměrně strohé, zato se dá předpokládat, že budou poměrně věrohodné. Nadále zde máme jistotu, že jsou informace v databázích shromážděny v souladu se zákony o ochraně soukromí osob. Mezi nejvýznamnější registry spadají například:

- **Evidence skutečných majitelů** – tento registr vždy obsahuje jméno přímého, či nepřímého majitele společnosti, může také obsahovat další údaje k této osobě, zejména datum narození, místo trvalého pobytu a bližší povahu jeho vlastnického podílu. Zároveň jsou zde uvedeny změny skutečných majitelů a data, kdy tyto změny proběhly a IČO společnosti. Vyhledávat lze dle několika základních kritérií, zejména dle názvu subjektu, jeho identifikačního čísla nebo spisové značky. Počet hledání není žádným znatelným způsobem omezený, ani neověřuje, zda hledání provádí osoba, nebo automatizovaný nástroj.
- **Obchodní rejstřík** – pravděpodobně nejobsáhlejší registr české veřejné správy pro účely finančního a ekonomického zpravodajství. Umožňuje zjistit osobní údaje všech členů statutárního orgánu společnosti a data jejich přípisu či odpisu. Zároveň zde lze dohledat informace o probíhajících, nebo minulých exekucích. Lze se zde dostat i ke sbírce listin dostupných k dané společnosti, kde nalezneme kompletní roční účetní uzávěrky, ve kterých lze nalézt nespočet dalších finančně relevantních informací.
- **Insolvenční rejstřík** – uschovává informace o dlužnících v insolvenci. Pokud jde o vyšetřování zaměřené na jednotlivce, pokud zde existuje záznam takové osoby, dá se předpokládat, že v obšírném kvantu uveřejněných dokumentů v tom to registru bude možné dohledat například trvalé a současné bydliště osoby, její telefonní číslo, příbuzné osoby, současné místo zaměstnání a další informace které mohou vést k dalším skutečnostem důležitým pro vyšetřování.

- **ARES** – neboli Administrativní registr ekonomických subjektů funguje spíše jako unifikovaný vyhledávač ve většině dalších registrů státní správy, jednou jeho užitečnou funkcí je porovnání údajů uvedených v jednotlivých registrech pro zjištění případných nesrovnalostí.

Mimo registry vytvořené státní správou lze také nalézt komerční společnosti spravující a tvořící databáze, které shromažďují finanční a ekonomické informace. Kromě toho, že sami užívají OSINT jsou také hodnotným zdrojem v tomto poli. Některé takové služby jsou nabízené zdarma, jiné mohou být zpoplatněné.

- **ASPI Bisnode** – placená služba od společnosti Wolters Kluwer, nabízí přístup k profilům firem v ČR, od jejich základních údajů, přes kontakty až po zhodnocení rizikovosti takové společnosti. Data pro tento systém vychází opět ze základních registrů státní správy a není zde proto vysoká přidaná hodnota této služby.
- **Podnikani.cz** – služba poskytovaná zdarma, stejně jaké většina služeb v tomto seznamu čerpá zejména ze státních registrů. Tato specifická služba však na rozdíl od jiných uvedených prokazatelně kontroluje i evidenci skutečných majitelů. Zároveň zahrnuje nástroj, který umožňuje vizuální zobrazení společnosti a souvisejících právnických, či fyzických osob.
- **Rejstřík firem na kurzy.cz** – vedle typicky dostupných dat ze státních registrů umožňuje přístup na výše uvedený vizualizační portál. Zároveň zde lze najít recenze zákazníků dané obchodní společnosti, nebo na internetu nalezená inzerovaná volná místa.

Jiné státy světa mají zpravidla své vlastní registry evidující srovnatelné údaje s jejich českými protějšky, dá se říct, že ve státech Evropské unie budou mít některé registry srovnatelnou podobu, protože budou vycházet z předlohy zákona proti praní špinavých peněz. Velkým krokem vpřed je iniciativa „The European Business Registry Association“, která na své webové stránce obsahuje rozcestník na veřejné registry finančního charakteru naprosté většiny zemí světa. Zároveň zaštiťuje činnost „European Business Register Network“,

který má zajišťovat mezinárodní spolupráci v otázce obchodních registrů. Do tohoto projektu je však aktivně zapojeno pouze zhruba šestnáct států. Zároveň tato instituce odkazuje na autorizované distributory informací z těchto mezinárodních registrů. Podobné databáze v USA budou benevolentnější k poskytování informací o osobách, protože se na ně nevztahuje GDPR ve stejném rozsahu, jako na subjekty působící v EU, nebo na subjekty nakládající s daty o občanech EU, registry této povahy jsou vedeny jednotlivými členskými státy USA, ne na federální úrovni. Za zahraniční, či mezinárodní zdroje však můžeme považovat především následující:

- **Opencorporates.com** – vyhledávací engine pro dotazy do obchodních rejstříků většiny států světa, včetně ČR. Tento systém se stal primárním zdrojem otevřených informací pro nespočet finančních vyšetřování a zahrnuje ho ve svém portfoliu i věhlasný nástroj Maltego.
- **Sledování kryptoměn** – jsou mezinárodním zdrojem pro FININT. Naprostá většina kryptoměn eviduje veškeré transakce veřejně v takzvaném blockchainu. K účelu sledování těchto transakcí vznikl na webu nespočet nástrojů, srozumitelných i pro naprosté laiky. Každá transakce má svůj vlastní identifikátor, stejně jako všechny účty, které s nimi obchodují. Kryptoměny poskytují prakticky naprostou anonymitu, pokud se však podaří nějakým způsobem zjistit, kdo je majitelem určitého kryptoměnového účtu, dají se jeho veškeré transakce do posledního detailu vystopovat.

PRAKTICKÁ ČÁST

5. VYUŽITÍ OSINT K SESTAVENÍ PROFILU PODNIKU

Zde se pokusíme uplatnit metodiku popsanou v této práci k sestavení kompletního profilu zájmového podniku – společnosti. Jako jediná vstupní informace bude sloužit pouze název společnosti, ze které budeme vycházet a postupně v logickém sledu získávat a organizovat další informace z výše uvedených zdrojů. Klíčové bude dodržení zpravodajského cyklu. Postup zde popsaný může v praxi sloužit k získání veškerých dostupných informací o společnosti, tedy k naprostému vyčerpání dostupných otevřených zdrojů. Informace takto získané poté mohou sloužit zejména podpůrně při další zpravodajské činnosti, čerpající z jiných způsobů získávání informací. V naší modelové situaci se jedná o středně velkou nábytkářskou společnost operující prakticky výlučně na území ČR.

Před zahájením samotného zpravodajského cyklu je vhodné si stanovit například finanční prostředky, které mohou být vynaloženy na tuto operaci. Je sice možné, že nám bohatě vystačí informace získané z neplacených zdrojů, nicméně často jsou ty nejlepší zdroje schovány za poplatky, které musíme být ochotni uhradit. Stejně tak většina nástrojů pro sběr a analýzu zdarma nabízí pouze velice „osekanou“ verzi, která nám neumožní využít její plný potenciál. V případě, že jsme součástí organizace bude také otázkou velikost týmu, který na případu bude pracovat. To může ovlivnit rychlost celého procesu. Žádoucí také může být jistá úroveň utajení získaných informací, v případě práce pro komerční společnosti bude pravděpodobně na místě tzv. dohoda o mlčenlivosti. Z cesty musí také být veškeré právní otázky. V neposlední řadě je třeba si stanovit určitý deadline, tedy čas, ve kterém by měl zpravodajský cyklus dokončit celou rotaci. To může být omezeno různými zákonnými lhůtami, vyplývajících například z GDPR, nebo požadavky zadavatele.

5.1 Určení požadavků

Prvním krokem v každém vyšetřování je určení rozsahu a obsahu informací, které je třeba získat a analyzovat. Zde si klademe za cíl:

- Zjistit velikost společnosti
- Sestavit vlastnickou strukturu společnosti
- Zjistit ekonomické ukazatele, včetně historie vývoje společnosti
- Zjistit reakce zákazníků na společnost, zejména ve smyslu zjištění uživatelských recenzí
- Zjistit nemovitosti vlastněné společností
- Zjistit historii společnosti a vlastníků

Splnění těchto požadavků může sloužit k mnoha účelům, od navazování obchodních vztahů, přes průzkum trhu až po případné vyšetřování ve finanční rovině, ať už orgány činnými v trestním řízení, nebo třeba investigativními žurnalisty.

5.2 Sběr dat a informací

Dříve než přikročíme k samotnému sběru, je vhodné mít sestavenou alespoň obecnou strukturu shromažďování a organizování dat. Struktura může mít primitivní formu, jako například členění dle zdroje informací, tj. například na informace získané ze sociálních sítí, informace získané z registrů veřejné správy. Můžeme také zvolit formu dělení dle toho, k jakému bodu zadání se získaná data vztahují. Nicméně takový přístup je spíše fikcí, neboť data nezodpovídají vždy jednoznačně pouze jeden z bodů, a pokud ano, nemusí tento vztah být zřejmý při samotném sběru, ale až při analýze. Klíčovým bodem zde tedy je mít dobře uspořádaná data dle logického systému. Jelikož zde většinu sběru budeme provádět manuálně, protože se nezaměřujeme na abstraktní subjekt, ale jednu velice specifickou společnost, dá se předem předpokládat, že objem dat a počet zdrojů nebude natolik velký, aby byla organizace složitá. Pro všechny účely je však nutné zachovávat alespoň nějakou strukturu a evidovat veškerou činnost sběru. Vhodný k tomuto je nástroj OSIRT, který většinu zmíněné činnosti udělá za nás tím, že automaticky

ukládá fotografie procházených webových stránek a informací na nich uložených, opatří je časovou známkou, takže si následně můžeme sestavit přehlednou časovou linku předchozího vyšetřování.

V OSINT se setkáváme s paradoxem, který většina jiných zpravodajských odvětví moc nezná – dostupných dat a informací je až příliš. Z tohoto důvodu je nutností dobře zhodnotit zdroje, ze kterých budeme čerpat. Informace z otevřených zdrojů mohou být cíleně klamavé, zdroje mohou být zaujaté a nepřesné, proto je dobré mít alespoň nějakou předchozí zkušenost s danými zdroji a podle toho usoudit, zda je vhodné takový zdroj využít při dalším sběru dat a informací.

Při automatizovaném sběru dat platí předchozí tvrzení dvojnásobně, nicméně kromě ohodnocení zdrojů je také třeba tyto automatizované nástroje nastavit tak, aby filtrovaly nepotřebné informace a sbíraly data, která jsou relevantní. Zde je třeba dát pozor na to, abychom omylem nezpůsobili, že některá data tímto pomyslným sítem propadnou, ačkoliv mohla být věcná a hodnotná.

Nyní můžeme přikročit ke sběru dat a informací. První a jedinou informací, kterou máme k dispozici je název obchodní společnosti, začneme tedy následovně:

5.2.1 Dotaz do obchodního rejstříku

Zadáním názvu společnosti do obchodního rejstříku získáme výpis společností s názvem odpovídajícím již známé informaci. Dle jednoznačnosti takového názvu se zde může vyskytovat větší množství firem, a proto je třeba mít alespoň představu o oblasti podnikání nebo geografické lokaci podniku. Pokud jsme schopni určit z výpisu o jakou firmu se jedná, získáváme dodatečné informace, zejména:

- Identifikační číslo
- Informace o současném a minulých sídlech společnosti
- Předmět podnikání
- Statutární orgán, jména, data narození, bydliště jeho členů a data zápisu a výmazu těchto členů z rejstříku

- Údaje o exekucích

Velice podstatnou položkou zjištěnou z tohoto zdroje je přístup ke sbírce listin společnosti. Nejvýznamnějšími takovými publikovanými dokumenty pro naše vyšetřování budou nepochybně účetní uzávěrky, při jejichž budoucí analýze můžeme zjistit, jak se společnosti daří v ekonomické rovině. Veškeré listiny je proto žádoucí stáhnout ve vhodném formátu, který umožňuje další práci s obsaženým textem, například PDF, což je zejména u starších dokumentů neproveditelné, nicméně i u novějších dokumentů je takový formát k dispozici spíše výjimečně, protože se nejčastěji jedná o naskenované dokumenty. Nahlédnutím do těchto dokumentů můžeme zjistit poměrně srozumitelnou historii společnosti, ale také dodatečné detaily k osobám v těchto listinách uvedeným. Není výjimkou například zjištění kompletních rodných čísel, či vzorů podpisů těchto osob. Lze také sestavit historii bydlišť.

5.2.2 Insolvenční rejstřík, rejstřík úpadců a komerční evidence exekucí

Z předchozího kroku bychom měli mít k dispozici dostatek osobních údajů k prověření jednotlivých osob, které jsou uvedeny v obchodním rejstříku společnosti. Varovnými ukazateli u společnosti by například mohly být osoby které byly společníky ve větším množství selhaných společností, nebo osoby které jsou v dané době v insolvenci. Co se evidencí exekucí týče, jedná se o zpoplatněné komerční služby, jednu takovou službu provozuje například portál cebia.cz, kdy jeden požadavek do systému stojí zhruba 50 Kč. V případě vážného zájmu o tento údaj se proto nejedná o výraznou finanční položku.

5.2.3 ARES a rejstřík subjektů DPH

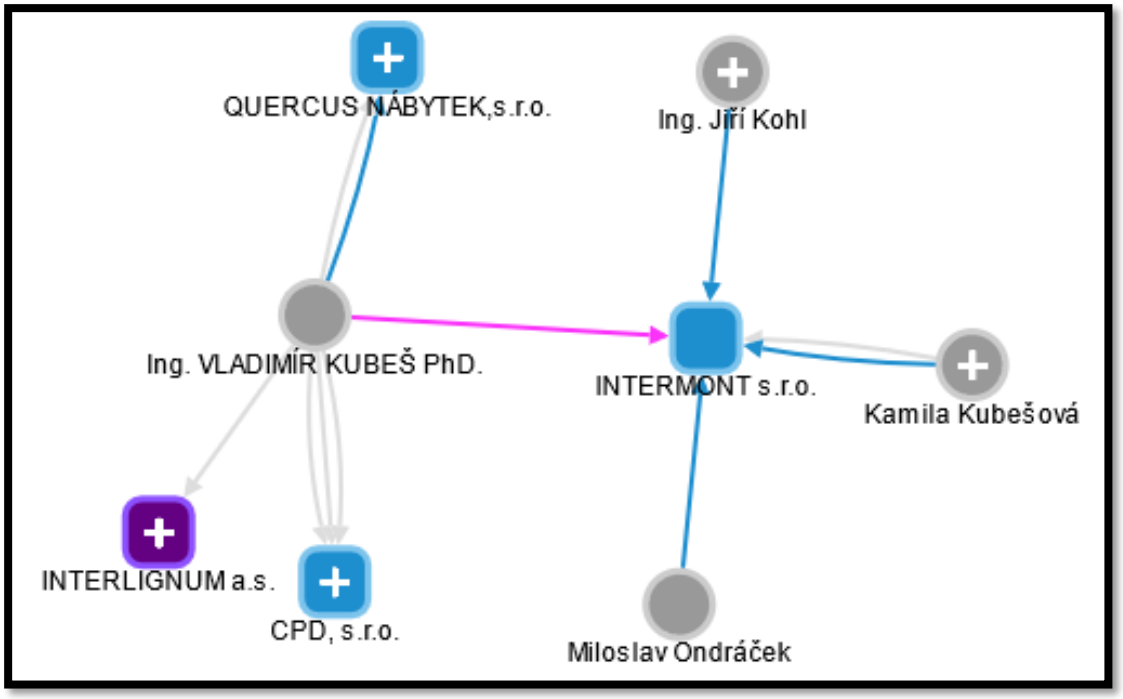
V tomto systému můžeme porovnat údaje z jednotlivých registrů veřejné správy a zjistit případné nesrovnalosti. Lze se tímto způsobem také dostat k rejstříku Ministerstva financí o subjektech DPH. Tímto způsobem lze zpravidla získat bankovní účty, které byly společnostní zveřejněny. Také zde je uveřejněn ukazatel spolehlivosti plátce.

5.2.4 Kurzy.cz a graf na podnikani.cz

Tyto webové stránky poskytují výpis z registrů veřejné správy, z důvodu neprimárnosti tohoto zdroje však je vhodnější čerpat přímo z těchto registrů, a ne z tohoto zrcadla. Oproti registrům však umí zobrazit i nabídky práce inzerované poptávanou společností, a to jak minulé, tak aktuální. Dá se proto zjistit, jací zaměstnanci firmě momentálně chybí, nebo jak chce firma rozšiřovat svoje operace. Zároveň je zde uveden údaj o počtu zaměstnanců společnosti, vyplývající z registru statistického úřadu.

Abychom zjistili vztahy osob uvedených v obchodním rejstříku a případné spojitosti s dalšími společnostmi, využijeme vizualizační nástroj na podnikani.cz. Zadáním buď jména fyzické osoby, nebo dané společnosti nám automaticky na základě údajů z registrů veřejné správy vytvoří přehlednou vizualizaci vztahu těchto osob, nebo firem. Výhodou je, že oproti jiným nástrojům, nevyžaduje velkou znalost počítačových systémů na straně vyšetřovatele, ovládání vizualizace je extrémně jednoduché a intuitivní. Tímto způsobem se dopracujeme k dalším osobám a jejich vztahům k jiným společnostem, kdy však v kterémkoliv daném časovém bodě existoval nějaký vztah s výchozí společností, nebo osobou. Nástroj také umožňuje posouvat časovou linku a postupně si tak zobrazit změny tak, jak byly v čase evidovány. Tyto informace můžeme dále sledovat, zejména pokud nás zajímají předchozí společnosti společníků, nebo jiné vazby.

Využitím těchto zdrojů jsme prakticky vyčerpali zdroje, které buď přímo zveřejňují, nebo zprostředkují povinně zveřejňované informace. Při dalším sběru informací se tedy přesuneme do volného internetu. Zde se můžeme potýkat s obrovským množstvím dostupných dat, zvláště, pokud se jedná o vysoce exponovanou společnost, nicméně dobrým pravidlem bude se zprvu věnovat takovým zdrojům, které jsou společnosti přirozeně nejblíže.



Obrázek 3: **Vizualizace vztahů ve společnosti** [40]

5.2.5 Web společnosti

Použitím základního vyhledávače, jako je například Google můžeme nalézt oficiální webové stránky společnosti. To, že by dnes společnosti neměli vlastní web je dnes spíše výjimkou, protože pro společnosti je žádoucí využít internet k marketingovým účelům. Na svůj web tak společnosti umisťují informace, které považují za žádoucí a nezbytné. Lze zde zjistit například nabídku a ceny výrobků, či služeb, informace vztahující se k fungování podniku, inzerci volných míst, kontaktní údaje společnosti, nebo pozice a jména jednotlivých pracovníků.

5.2.6 Google hledání

Samotný Google používá algoritmy k získání triviálních informací o společnosti, navíc umožňuje, aby si společnost sama založila profil na Google Mapách, čímž lze zjistit, kde se nacházejí jednotlivé provozovny, či sídlo. Ve funkci Google Street View poté můžeme díky fotografiím ulic ověřit, zda se na

[40] Podnikání.cz: Vizualizace vztahů firem [online]. ALIAWEB, 2022. Dostupné také z: www.podnikani.cz

takovém místě například nachází poutač společnosti. Lze také zjistit, jaká vozidla stojí na parkovišti společnosti. Google přikročil k cenzurování registračních značek vozidel, nicméně například nálepky na vozidlech bývají stále viditelné a lze díky nim identifikovat jednotlivá vozidla. Zvláště zajímavé mohou být dobře známé a poměrně rozšířené nálepky s diagramy dětí nebo příbuzných, které jsou často doplněný o jejich jména. Dostává se nám tak do ruky informace o rozložení rodiny majitele takového vozu, což může v korelaci s dalšími zdroji informací pomoci při dalším vyšetřování. Můžeme zde nalézt odkazy na sociální sítě společnosti, některé její produkty a uživatelské recenze. Stejně hodnotnými informacemi mohou být také výsledky z hledání systémem Google obrázky, kde mohou být umístěny například fotografie prostorů provozoven. Významné výsledky mohou vzejít nejen z hledání názvu společnosti, ale i jmen zájmových osob v těchto společnostech, například rozhovory pro různé noviny, blogy, atp.

5.2.7 Wayback Machine

V případě, že nás zajímá i historie podniku, lze využít neplacené služby, která archivuje webové stránky. Lze tak zjistit, jak se například měnila nabídka společnosti, jak reagovala na trendy dané doby, či jiné údaje. Toto může být velice významné při vyšetřování některých druhů podvodných jednání, na mysl přichází například klamavá nabídka, která se na webu společnosti objevila pouze velice krátkou dobu.

5.2.8 Sociální sítě

Většina společností se v dnešní době prezentuje nějakým způsobem na sociálních sítích, lze proto využít ruční vyhledávání, nebo například na Twitteru či Facebooku dostupné API k získání relevantních příspěvků. Opět zde platí, že na sociální sítě dávají společnosti pouze informace pro ně žádoucí, nicméně opět se zde nachází sekce, kde mohou diskutovat uživatelé, která může prozradit mnoho o náladách zákazníků.

5.2.9 Další zdroje

Zatímco jsme doposud čerpali data z uvedených zdrojů především ručně, je vhodné paralelně provádět i automatický sběr. Za vhodné nástroje se potom dá považovat především zmíněné Maltego, nebo Spiderfoot, které jsou v kvantitě a přehlednosti získaných dat bezkonkurenční a usnadňují organizaci a další manipulaci se získanými daty. Zároveň lze využít pokročilé nástroje, které jsou schopny identifikovat strukturu e-mailů ve společnosti a dát nám tak výpis těchto e-mailů.

5.3 Převod a zpracování dat a informací

Při sběru dat se nám povedlo jak manuálními metodami, tak automatizovanými nástroji získat obrovské množství informací a dat. Pokud jsme si na základě doporučení předpřipravili alespoň nějakou strukturu organizace dat, můžeme začít izolovat jednotlivá data a vkládat je do korespondujících databází či grafů. Jen zřídkakdy se nám povede získat informace ve formátu, který umožňuje je zařadit do širšího kontextu, nebo porovnat s jinými zjištěnými informacemi. Maltego a Spiderfoot však většinu této práce udělají za nás a z těchto dvou nástrojů by zpravidla měl být výstup v již přijatelném formátu pro další práci. Data jsou členěna například podle toho, o jaký druh dat se jedná – telefonní čísla, e-mailové adresy, IP adresy, dokumenty v různých formátech, jména osob.

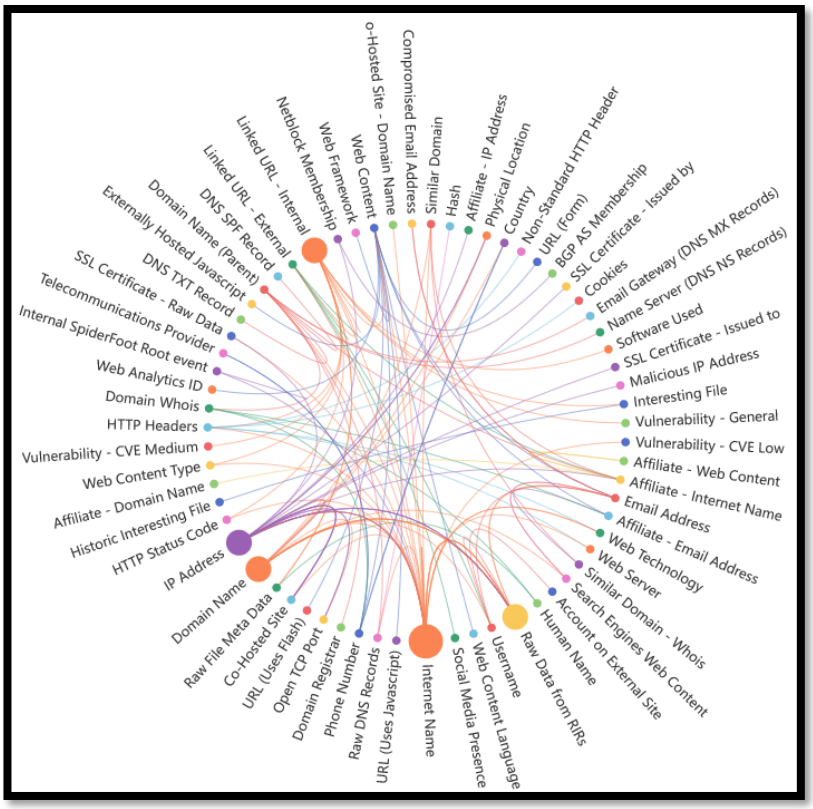
Naším cílem v této části práce tedy je z netvárné hmoty, kterou jsou veškerá získaná data utvořit alespoň relativně přehledné prostředí, ve kterém mezi sebou můžeme jednotlivé informace porovnávat. Ve všech ohledech lze doporučit, aby k tomuto účelu byly v co největší míře využívány automatické nástroje, protože v opačném případě může tato činnost zabrat až 80 % času celého cyklu.

Zde stojíme na rozcestí podle toho, jaké máme programovací schopnosti a dostupný software. Pokud máme přístup k zařízení s operačním systémem Kali Linux, které je vytvořeno specificky se zaměřením na OSINT, můžeme

využít nespočet programů a skriptů, které slouží přesně k účelu zpracování dat.

Jedním z nejužívanějších a nejužitečnějších způsobů, jak získat použitelná, strukturovaná data, je použít systém pro zpracování přirozeného jazyka. Jedná se o metodu, ve které počítačový program analyzuje vstupní text a izoluje z něj prvky, které se shodují s určitým parametrem. Nástrojů k použití této metody je nespočet, lze jmenovat například Natural Language Toolkit (NTLK).

Problematické, specificky pro náš případ může být převedení dokumentů dříve získaných z obchodního rejstříku, do formátu čitelného pro tyto nástroje. Jelikož se jedná zpravidla o oskenované dokumenty, je třeba nejdříve použít program, který dokument přečte a z obrazového formátu jej převede do formátu textového. K tomu může sloužit například Wondershare PDF Converter Pro, ale existuje i nespočet dalších alternativ.



Obrázek 4: **Chord diagram vztahů mezi entitami** [41]

[41] Spiderfoot HX: Chord diagram [online]. SM7 Software OÜ, 2022. Dostupné také z: https://www.spiderfoot.net/

5.4 Analýza dat a informací

Veškerá získaná data nyní máme v takové podobě, že s nimi můžeme nadále pracovat. V této části je tedy naším úkolem zodpovědět pomocí získaných dat na otázky položené v zadání. Nyní bychom měli mít dostupná veškerá k tomu potřebná data a informace a měla by být v přijatelném formátu, řádně kategorizovaná a případně přeložená.

Pokud jsme čerpali z dostatku zdrojů, porovnáme jednotlivé informace mezi těmito zdroji, abychom mohli určit průnik, nebo rozdíl takových informací a vyvodit z nich závěr – konstatovat objektivní fakt. Ve zdrojích, ze kterých probíhal sběr v této práci, by měly být k dispozici veškeré informace potřebné k zodpovězení zadaných otázek. Analýzou je třeba je zasadit do kontextu, zejména je třeba zjistit, zda jsou informace aktuální, zde může vzniknout potřeba zajistit i osoby se znalostí specifických problematik, například při analýze účetních informací.

Analýzou musí dojít k vyloučení informací nespolehlivých, neaktuálních, nebo značně nepřesných. K tomuto by měla napomoci mnohost zdrojů, kdy by mělo být patrné, pokud jeden ze zdrojů bude předkládat informace, které budou v konfliktu s informacemi z jiných zdrojů. V našem případě jsme čerpali informace z velké části z registrů veřejné správy, kdy prakticky není pochyb o jejich spolehlivosti, na paměti je však třeba mít, že subjekt těchto údajů – prověřovaná společnost, mohla záměrně udat informace nepravdivé, což samo může být předmětem vyšetřování. V tomto případě záleží na tom, do jaké míry správci těchto registrů ověřují udané informace.

Při analýze budeme používat stejné nástroje jako v předchozích dvou krocích – Maltego, případně OSIRT a Spiderfoot. V těchto programech jsou skvěle vizualizovány vztahy mezi jednotlivými entitami, jsou řádně kategorizovány druhy dat a informací a nabízí se nespočet možností zobrazení těchto vztahů a členění. Některé zdroje také uvádějí nástroj zvaný IBM Security i2 Analyst's Notebook, který v tomto případě však využit nebyl, protože jeho funkce se jeví jako duplicitní k amalgamaci užitých nástrojů.

Výsledkem analýzy by měla být zpravodajská informace, která by měla být ohodnocena podle své celkové spolehlivosti. V závěru vyšetřování můžeme dojít k tomu, že se nepodařilo zjistit informace vysoké kvality, což může být řešeno pouze opětovným zopakováním celého procesu, revizí metodiky sběru dat, upravením filtrů automatizovaných nástrojů, nebo pátráním po dalších možných zdrojích informací.

5.5 Distribuce a zpětná vazba

Distribuce je kulminací zpravodajského cyklu, zde je třeba doručit osobě – s největší pravděpodobností zadavateli, zjištěné zpravodajské informace. Mohou mít samozřejmě prostou textovou podobu, nebo mohou být doprovázeny různými grafickými znázorněními – grafy, fotografiemi, statistikami. Zadavatel samozřejmě mohl určit jiné osoby, nebo organizace, kterým mají být zjištěné skutečnosti distribuovány, toto je spíše otázka, která by měla být zodpovězena již v zadání. Zadavatel samozřejmě může se získanými zpravodajskými informacemi nakládat, jak sám uzná za vhodné.

Očekává se, že celý proces neprobíhal bezdůvodně, ale že na základě získaných poznatků budou zmocněné osoby reagovat. V našem případě, kdy jsme vytvořili komplexní přehled zkoumaného podniku, se dá předpokládat, že bude využit a že byl sestavován z důvodu zájmu jiného podniku o pole, ve kterém zkoumaný podnik působí. Postup popsaný v praktické části je však jakýmsi první krokem ve veškerých vyšetřováních. Je to začátek vyšetřování, který může položit základní kámen pro další způsoby získávání informací.

Po distribuci zpravodajských informací oprávněným osobám se může zpravodajský cyklus opakovat, zejména, pokud jde o soustavnější činnost nějaké organizace. Klíčová v tomto kroku je zpětná vazba, a to jak od osob, které obdržely výsledky šetření, tak od samotných vyšetřovatelů. Tímto způsob se dá rafinovat celý zpravodajský proces. Lze odstranit nesrovnalosti v získávání informací a v zaměření vyšetřování. Mohou se objevit různé nedostatky, které bude třeba doplnit. Opakovanost takového cyklu je proto klíčová pro získání širšího pohledu na šetřenou věc. V případě zkoumání

podniku, jako tomu je zde, může být žádoucí provádět takové šetření periodicky, neboť obchodní trh je prostor, kde se situace velice volatilně mění.

ZÁVĚR

Zpravodajství z otevřených zdrojů je prakticky bezedná studnice informací. Jak bylo zmíněno v průběhu této práce, dobrá disciplína při strukturování získaných dat je naprosto klíčová pro to, aby zpravodajská činnost probíhala plynule, bez zbytečných zádrhelů. Metody získávání informací pro finanční zpravodajství, kde je předpoklad, že budou využity orgány činnými v trestním řízení, budou odlišné od metod, které mohou uplatnit jiné skupiny vyšetřovatelů. Je zde zvláště důležité dbát na důslednou evidenci celého postupu, aby bylo v každém bodě prokazatelné, že informace pochází z legálního zdroje a mohou být použity v případném trestním řízení. OSINT sice nevznikl na internetu, ale komunita uživatelů internetu ho přijala za svůj nástroj a dokázala ho uplatnit způsoby, jaké byly v minulosti považovány pouze za díla science fiction. Tato skutečnost má za následek to, že spousta velice kvalitních příruček pro provádění OSINT je k dispozici zcela zdarma právě na internetu, v komunitách, které se tímto druhem zpravodajství zabývají. Kromě publikovaných příruček se mohou zájemci také přidat do různých fór, která mohou výrazně prohloubit uživatelovu znalost této metodiky.

V porovnání získávání informací pod křídly českého právního řádu, oproti řádům zahraničním je třeba říci, že vzhledem ke kontinentálnímu přístupu k ochraně osobních údajů zde je taková činnost značně těžší. Zároveň je zde však vidět jistý posun, zejména v problematice předcházení a odhalování praní špinavých peněz a související kriminality. Evropské státy přijaly zákony vycházející ze směrnice AML, kdy však právě český registr Evidence skutečných majitelů je kritizován pro nedostatečnou průhlednost této evidence.

Problematické dále může být prokazování daňových úniků, kdy společnosti z České republiky peníze ukládají v daňových rájích, které prakticky neumožňují žádný přístup k informacím o těchto společnostech. Nepodařilo se vytvořit elegantní technické řešení pro zobrazení mezinárodních vztahů společností, což by takové vyšetřování mohlo výrazně ulehčit.

Užitečnost zpravodajství z otevřených zdrojů nelze v žádném případě popřít, zejména při competetive intelligence, kdy je jasná potřeba setrvat v mezích zákona. V ostatních případech užití OSINT, například ve finančním zpravodajství, narážíme na jistou netransparentnost relevantních českých registrů. OSINT proto bude nejlépe využit v tandemu s jinými formami zpravodajské činnosti.

CONCLUSION

Open source intelligence can be considered a bottomless well of information. As we have stated many times troughout this thesis, it is key to keep in mind the importance of data structuring, when collecting data. Otherwise, the ongoing investigation can stall and take much longer. In the case of OSINT use by law enforcement and other institutions of the criminal justice system, it is imperative that those users keep a good paper trail of the collected evidence and that they are able to prove, that every step they have taken is legal and the intelligence gathered can be used in a court of law.

OSINT may have not been created by the internet community, but since it’s appearance, it has been adopted by the community and used in ways previously thought to only be possible in science fiction. This has resulted in the fact that many of the best available handbooks and guides are available for free on the internet, in communities interested in OSINT work. It i salso advised to join various OSINT forums.

If we compare the differences of OSINT use under Czech law, and then under foreign law systems, it is instantly obvious, that due to the continental approach to personal data protection, it will be much harder to conduct an investigation in Czechia, or EU, as opposed to the United States, for example. However, the EU has recently adopted anti-money laundering laws, which aim to help in combat against such practice. The law that has adopted the corresponding EU regulation into the Czech law system, is being critised for not being transparent enough.

When it comes to investigating international money laundering and other such financial criminal activities, it is problematic to prove that Czech companies are storing, or running money through tax havens, because there is no available database, that would trace and visualize relations between multiple national databases.

The efficiency of open source intelligence is undeniable, especially in competetive intelligence, where the need to remain within legal boundaries is paramount. In other cases of OSINT use, e.g. in financial intelligence, we encounter the intransparency of Czech financial databases. In such cases, OSINT is best employed in tandem with other forms of intelligence.

SEZNAM POUŽITÉ LITERATURY

1. AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). *Open Source Intelligence Investigation. From Strategy to Implementation.* Springer, 2016. ISBN 978-3-319-47671-1.
2. MICHÁLEK, Luděk. *Zpravodajství a zpravodajské služby*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 9788073804282.
3. MOLNÁR, Zdeněk. *Competitive intelligence, aneb, Jak získat konkurenční výhodu*. V Praze: Oeconomica, 2012. Odborná kniha s vědeckou redakcí. ISBN 978-80-245-1908-1.
4. VONDRÁČEK PH.D., LL.M., JUDr. Ondřej. *Příručka pro rozkrývání vlastnických struktur a skutečných majitelů.* Praha: Transparency International – Česká republika, 2017. Dostupné také z: https://www.transparency.cz/publikace-a-analyzy/prirucka-pro-rozkryvani-vlastnickych-struktur-a-skutecnych-majitelu/
5. JONÁK, Zdeněk. Informace. KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha: Národní knihovna ČR, 2003. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000456&local_base=KTD.
6. MADUREIRA, Luís. *Technological Forecasting and Social Change: Competitive intelligence: A unified view and modular definition*. 2021. ISSN 0040-1625. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0040162521005199
7. *Listina základních práv Evropské unie: HLAVA II - SVOBODY: Článek 8: Ochrana osobních údajů*. In: Evropská Unie: Úřední věstník Evropské unie, 2000, ročník 2016, C 202/395. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:12016P008
8. EU. *Obecné nařízení o ochraně osobních údajů*. In: EU: Evropský parlament, Evropská rada, 2016, ročník 2016, 2016/679/EU. Dostupné také z: https://eur-lex.europa.eu/eli/reg/2016/679/oj

9. ČESKO. Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-2
10. ČESKO. Zákon č. 37/2021 Sb., o evidenci skutečných majitelů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022. Dostupné z: https://www.zakonyprolidi.cz/cs/2021-37
11. A Brief History of Open Source Intelligence. *Bellingcat* [online]. Nizozemsko: Cameron Colquhoun, 2016 [cit. 2021-10-24]. Dostupné z: https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/
12. Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci - 2021: Používání mobilního telefonu a internetu na mobilním telefonu [online]. Praha: Český Statistický Úřad, 2021. Dostupné z: https://www.czso.cz/documents/10180/142872020/062004210304.pdf/bd5804b7-03a8-43eb-a78b-67d3b040a3f0?version=1.1
13. Slovníček nejdůležitějších pojmů: Osobní údaj [online]. Úřad pro ochranu osobních údajů, 2013. Dostupné také z: https://www.uoou.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617
14. *What Is Legitimate Interest Under the GDPR?* [online]. Drogheda: Luke Irwin, 2022. Dostupné z: https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply
15. *Slovník NATO s termíny a definicemi [online].* PRAHA: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, 2020. Dostupné také z: https://oos.army.cz/terminologicky-slovnik-aap-06
16. *Joint Publication 2-0: Joint Intelligence*. 2013. USA: US Department of Defense, 2013. Dostupné také z: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf
17. *NATO Open Source Intelligence Handbook* [online]. USA, 2001. Dostupné z: https://archive.org/details/NATOOSINTHandbookV1.2
18. Web crawler [online]. Web browsers introduction. Dostupné také z: https://webbrowsersintroduction.com/

19. Lexperanto [online]. 2022. Dostupné také z: http://lexperanto.cz/
20. Certifix [online]. TXP Association, 2022. Dostupné také z: www.certifix.eu
21. Ekonomické zájmy státu [online]. Praha, 2022. Dostupné také z: https://www.bis.cz/ekonomicke-zajmy-statu/
22. Úřad pro zahraniční styky a informace: Co děláme [online]. Praha, 2022. Dostupné také z: https://www.uzsi.cz/co-delame
23. Podnikání.cz: Vizualizace vztahů firem [online]. ALIAWEB, 2022. Dostupné také z: www.podnikani.cz
24. Spiderfoot HX: Chord diagram [online]. SM7 Software OÜ, 2022. Dostupné také z: https://www.spiderfoot.net/

SEZNAM OBRÁZKŮ