

Prikupljanje i analiza digitalnih otisaka primjenom programskog alata Maltego

Bišćan, Antonio

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:119:557934>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-11-30**



Repository / Repozitorij:

[Faculty of Transport and Traffic Sciences -
Institutional Repository](#)



**SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI**

Antonio Bišćan

**PRIKUPLJANJE I ANALIZA DIGITALNIH
OTISAKA PRIMJENOM PROGRAMSKOG
ALATA MALTEGO**

DIPLOMSKI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 6. lipnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6972

Pristupnik: **Antonio Bišćan (0135242538)**
Studij: **Promet**
Smjer: **Informacijsko-komunikacijski promet**

Zadatak: **Prikupljanje i analiza digitalnih otisaka primjenom programskog alata Maltego**

Opis zadatka:

Diplomskim radom potrebno je analizirati dosadašnja istraživanja u području prikupljanja javno dostupnih podataka. Uz navedeno potrebno je definirati scenarije prikupljanja javnost dostupnih podataka te iste prikupiti i analizirati korištenjem programskog alata Maltego. Temeljem provedenog istraživanja potrebno je prikazati dostupnost podataka i ukazati na važnost brige "digitalne higijene" korisnika.

Mentor:

Predsjednik povjerenstva za
diplomski ispit:

dr. sc. Ivan Cvitić

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

**PRIKUPLJANJE I ANALIZA DIGITALNIH OTISAKA
PRIMJENOM PROGRAMSKOG ALATA MALTEGO**

**COLLECTION AND ANALYSIS OF DIGITAL
FOOTPRINTS USING THE MALTEGO SOFTWARE
TOOL**

Mentor: dr. sc. Ivan Cvitić

Student: Antonio Bišćan
JMBAG: 0135242538

Zagreb, kolovoz 2022.

PRIKUPLJANJE I ANALIZA DIGITALNIH OTISAKA PRIMJENOM PROGRAMSKOG ALATA MALTEGO

SAŽETAK

Korištenje OSINT-a može biti odličan način za pronalaženje podataka o ljudima i organizacijama. Dosadašnja istraživanja u području prikupljanja OSINT-a pokazala su da je moguće prikupiti veliku količinu podataka iz različitih online izvora. Osim toga, istraživanje je također pokazalo da je važno voditi računa o „digitalnoj higijeni“ i biti svjestan dostupnosti podataka. Također su prikazani scenariji istraživanja osobe od interesa koji su provedeni primjenom programskog alata Maltego koji se koristi za prikupljanje i analizu javno dostupnih podataka. Ti se podaci mogu koristiti za praćenje kretanja pojedinaca, njihove aktivnosti na društvenim mrežama i njihove interakcije s vladinim i privatnim organizacijama. Analizirajući te podatke, istraživači mogu identificirati obrasce ponašanja koji mogu ukazivati na potencijalnu sigurnosnu prijetnju.

KLJUČNE RIJEČI: javno dostupni podaci; digitalna higijena; Maltego;

SUMMARY

Using OSINT can be a great way to find information about people and organizations. Previous research in the field of OSINT collection has shown that it is possible to collect a large amount of data from various online sources. In addition, the research also showed that it is important to take care of "digital hygiene" and be aware of the availability of data. Also presented are scenarios of research on persons of interest, which were carried out using the software tool Maltego, which is used to collect and analyze publicly available data. This data can be used to track individuals' movements, their social media activity, and their interactions with government and private organizations. By analyzing this data, researchers can identify patterns of behavior that may indicate a potential security threat.

KEY WORDS: publicly available data; digital hygiene; Maltego;

Sadržaj

1. UVOD	1
2. PREGLED DOSADAŠNJIH ISTRAŽIVANJA	3
2.1. Prednosti i nedostaci OSINT-a	4
2.2. OSINT analiza	7
2.3. Integracija OSINT-a u kibernetičkome napadu	8
2.4. Izazovi i budući trendovi OSINT-a	11
2.4.1. Automatizacija prikupljanja podataka	11
2.4.2. Poboljšanje procesa analize podataka	11
2.4.3. Integracija podataka iz više otvorenih izvora	11
2.4.4. Lažne vijesti	12
2.4.5. Interoperabilnost OSINT-a	12
2.4.6. Svijest o privatnosti, etičkim i pravnim razmatranjima	13
2.4.7. Sprječavanje zloupotrebe OSINT-a	13
3. DIGITALNI OTISCI NA JAVNOJ KOMUNIKACIJSKOJ MREŽI	15
3.1. Sigurnosne prijetnje digitalnog otiska	16
3.2. Upravljanje kriznim situacijama pomoću digitalnog otiska	19
4. METODOLOGIJA PROVEDBE ISTRAŽIVANJA	22
4.1. Osnovni pojmovi	22
4.2. Primjena tehnika mrežnog praćenja	25
4.3. Scenarij istraživanja osobe od interesa	27
5. ANALIZA DIGITALNIH OTISAKA PRIMJENOM PROGRAMSKOG ALAT MALTEGO	30
5.1. Sučelje programskog alata Maltego	30
5.2. Provođenje postupka analize osobe od interesa	35
6. REGULATORNI OKVIR PRIKUPLJANJA I ANALIZE OSINT PODATAKA	43
6.1 Pravo na poštivanje privatnog života i pravo na zaštitu osobnih podataka	43
6.2. Poštivanje privatnog i obiteljskog života	43
6.3. Europska konvencija o ljudskim pravima	44
6.4. Konvencija Vijeća Europe	44
6.5. Zakon o zaštiti podataka Europske unije	45
6.6. Osobni podaci	47

6.7. Obrada podataka	50
6.8. Korisnici osobnih podataka	51
7. ZAKLJUČAK	55
Literatura	56
Popis kratica	60
Popis slika	61
Popis tablica	62

1. UVOD

Razvojem tehnologije dolazi do sve većeg broja korištenja mobilnih terminalnih uređaja, a samim time razvoja društvenih mreža preko kojih dolazi do masivnog dijeljenja podataka. Ti podaci mogu uključivati informacije o lokaciji, pretplatama, osobnim mišljenjima, te mnogim drugim informacijama koje pojedinac ostavlja kroz poruke, objave na društvenim mrežama, videozapise i fotografije. Analizom digitalnih tragova prikupljenih sa interneta može se dobiti dobar dojam o interesima, ponašanju i samom identitetu osobe koja ih generira. To je od posebnog značaja za prikupljanje digitalnih dokaza koje se mogu upotrijebiti unutar kaznenog postupka. Digitalne tragove ponekad može biti teško pronaći, ali i međusobno povezati sa istom osobom jer ona može koristiti različite autentifikacijske podatke ili jer su određeni setovi podataka o korisniku zaštićeni GDPR-om. Podaci koji se mogu prikupiti kroz običnu pretragu po internet pretraživaču nazivaju se OSINT (engl. *Open Source Intelligence*) podaci.

Kako bi se pristupilo analizi OSINT podataka potrebno je uočavati povezanosti određenih entiteta zbog kompleksnosti i složenosti podataka. Čovjeku ne samo da je teško uočiti tu povezanost već bi mu trebalo jako puno vremena da poveže podatke, radi čega su proizvedeni razni programski alati. Za potrebe istraživanja OSINT podataka u okviru ovog diplomskog rada koristit će se programski alat Maltego. Ovaj alat ima ugrađenu funkcionalnost pretraživanja internet prostora i analize prikupljenih podataka, a razlikuje se od ostalih alata po tome što njegova analiza podataka može identificirati nepoznate odnose između njih.

Svrha istraživanja u okviru diplomskog rada je prikaz postojanja OSINT podataka i njihove dostupnosti. Prikazati gdje se oni mogu nalaziti te na koje sve načine se dolazi do digitalnih dokaza. Rezultati istraživanja će također povećati svjesnost korisnika o važnosti adekvatnog upravljanja digitalnim otiskom na internetu.

Cilj istraživanja u okviru diplomskog rada je provesti analizu digitalnih otisaka i prikazati mogućnosti alata Maltego kao što su dohvaćanje OSINT podataka i njihovo međusobno povezivanje.

Rad se sastoji od 7 poglavlja:

1. Uvod
2. Pregled dosadašnjih istraživanja
3. Digitalni otisci na javnoj komunikacijskoj mreži
4. Metodologija provedbe istraživanja
5. Analiza digitalnih otisaka primjenom programskog alat Maltego
6. Regulatorni okvir prikupljanja i analize OSINT podataka
7. Zaključak

U drugom poglavlju opisuje se analiza OSINT-a, njegove prednosti i nedostaci u provedbi analize, otvoreni izazovi i budući trendovi.

Trećim poglavljem pobliže je opisano što je digitalni otisak, koje su njegove sigurnosne prijetnje na društvenim mrežama i kako upravljati kriznim situacijama pomoću digitalnog otiska.

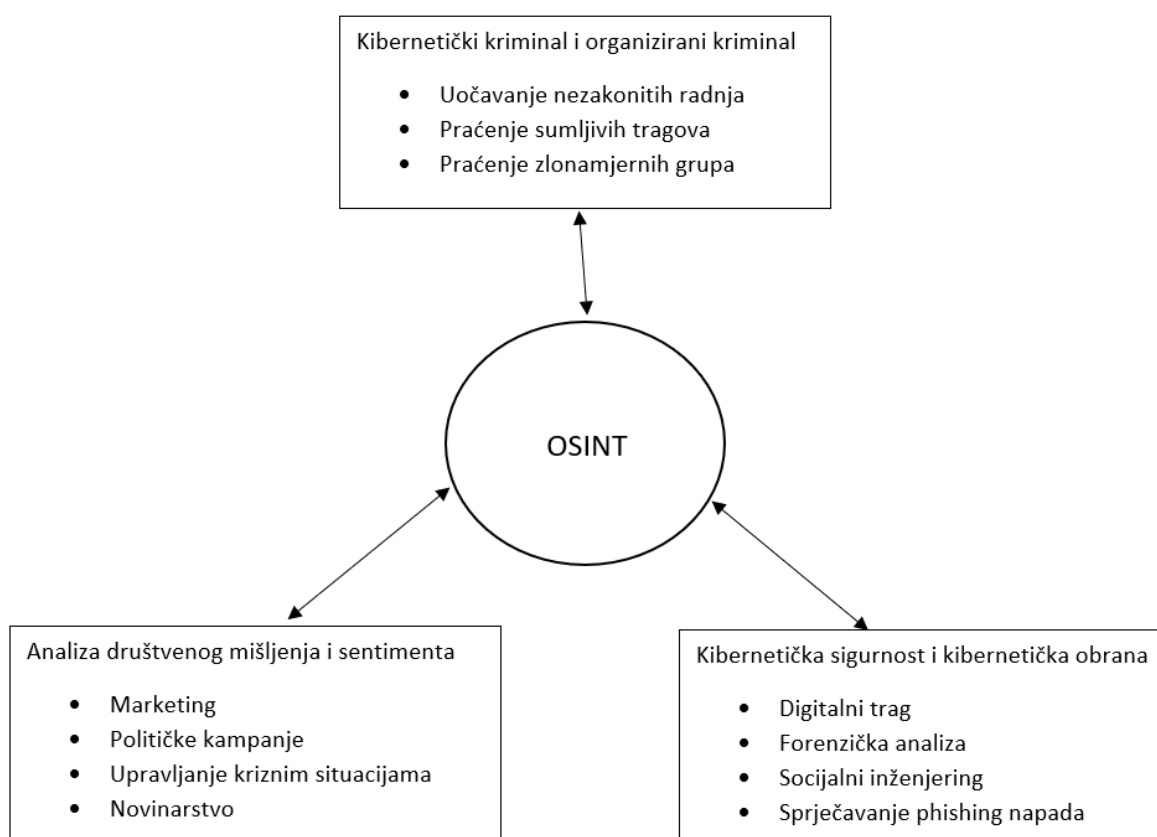
U četvrtom poglavlju se opisani opći pojmovi digitalne forenzike zbog uvođenja čitatelja u područje digitalnog istraživanja. Također su opisane primjene tehnika mrežnog praćenja kako bi se dobio što bolji uvid o subjektu koji se istražuje.

U petom poglavlju izvršeno je pretraživanje internetskog prostora, dohvaćanja podataka, te analiza podataka u svrhu korelacije nepoznatih odnosa između njih. Također se opisuju opcije i mogućnosti programskog alata Maltego.

U šestom poglavlju su navedeni pravni okviri prikupljanja i analize OSINT podataka. Također obrađena je terminologija povezana sa zaštitom podataka i propisi europskog zakonodavstva o zaštiti podataka.

2. PREGLED DOSADAŠNJIH ISTRAŽIVANJA

Javno dostupni podaci (engl. *Open Source Intelligence* - OSINT) sastoje se od prikupljanja, obrade i korelacije javnih informacija iz otvorenih izvora podataka kao što su mediji, društvene mreže, forumi i blogovi, javni državni podaci, publikacije ili komercijalni podaci. S obzirom na neke ulazne podatke, uz primjenu naprednih tehnika prikupljanja i analize, OSINT kontinuirano proširuje znanje o određenom subjektu. Na taj način pronađene informacije ponovno pokreću proces prikupljanja kako bi prikupile što veći broj informacija o subjektu [1]. OSINT koriste vlade i obavještajne službe za provođenje istraga i borbi protiv kibernetičkog kriminala. Također primjenjuju se i druge istraživačke svrhe, a mogu raspodijeliti na tri glavna slučaja primjene koji su prikazani na slici 1:



Slika 1. Prikaz glavnih područja primjene OSINT-a [1]

a) Analiza društvenog mišljenja i sentimenta

Uz procvat online društvenih mreža, moguće je prikupljati interakcije korisnika, poruke, interese. Dokazi prikupljeni na društvenim mrežama su dalekosežni i široko korisni [2]. Takvo prikupljanje i analiza mogli bi se primijeniti na marketing, političke kampanje ili upravljanje segmentima katastrofalnih događaja.

b) Kibernetički kriminal i organizirani kriminal

Javno dostupni podaci kontinuirano se analiziraju i uspoređuju OSINT procesima kako bi se kriminalne namjere uočile u ranoj fazi. Uzimajući u obzir obrasce zlonamjernih napadača i odnose među kaznenim djelima. OSINT ima mogućnosti pružiti sigurnosnim snagama priliku za brzo otkrivanje nezakonitih radnja [3]. S tim ciljem bilo bi moguće pratiti djelovanje terorističkih organizacija, koje su sve aktivnije na internetu.

c) Kibernetička sigurnost i kibernetička obrana

Informacijsko i komunikacijske sustave kontinuirano napadaju kriminalci s ciljem ometanja dostupnosti pruženih usluga. Istraživanje stoga postaje ključno za obranu tih sustava od zlonamjernih napadača, konkretno suočavanjem s izazovima koji su još uvijek novi u području kibernetičke sigurnosti. U tom smislu, istraživanja služi za preventivnu zaštitu organizacija i tvrtki. Konkretno, tehnike rudarenja podataka mogu pomoći vršeci analizu svakodnevnih napada, povezujući ih i podržavajući procese donošenja odluka za učinkovitu obranu, ali i za brzu reakciju [4].

OSINT se može primijeniti i na druge kontekste. Konkretno, moguće je izvući relevantne informacije izvođenjem napada društvenim inženjeringom. Loše motivirani subjekti iskorištavaju javno dostupne podatke objavljene na internetu kako bi stvorili zamke za hvatanje mete. Štoviše, moguće je izvršiti automatsku procjenu istinitosti javno dostupnih podataka s ciljem otkrivanja lažnih vijesti [5].

Ipak, korištenje javnih dostupnih podataka ima i kompromitirajuća pitanja. S jedne strane, Opća uredba Europske unije o zaštiti podataka (engl. *General Data Protection Regulation* - GDPR) ograničava obradu osobnih podataka koji se odnose na pojedince u zoni Europske unije [6]. S druge strane, postoji jaka etička komponenta koja je povezana s privatnošću korisnika. Posebno, profiliranje ljudi koje može otkriti osobne detalje kao što su njihove političke sklonosti, seksualna orijentacija ili vjerska uvjerenja. Osim toga, iskorištavanje tako velike količine informacija može dovesti do zlouporabe, što dovesti do internetskog zlostavljanja, internetskog ogovaranja ili kibernetičke agresije [7].

Sa stajališta kibernetičke sigurnosti, OSINT predstavlja vrijedan alat za poboljšanje mehanizama zaštite od kibernetičkih napada. Korištenje OSINT-a koristi se kako bi se spriječili napadi i omogućilo strateško predviđanje. Ne uključuje samo prikupljanje informacija, već i modele strojnog učenja za izvođenje analize raspoloženja [8].

2.1. Prednosti i nedostaci OSINT-a

Područja primjene OSINT-a su brojna, a rješenja koja se razvijaju iz godine u godinu su bolja. S tehničke točke gledišta, kao što se može vidjeti u tablici 1., OSINT je izložen nizu prednosti, ali mora se nositi i s nekim ograničenjima, koja su detaljno opisana u nastavku.

Tablica 1. Prikaz prednosti i nedostataka OSINT-a [9]

Prednosti	Nedostaci
Velika količina dostupnih informacija	Složenost upravljanja podacima
Veliki računalni kapacitet	Nestrukturirane informacije
Big data i strojno učenje	Dezinformacije

Komplementarne vrste podataka

Fleksibilna svrha i široki opseg

Pouzdanost izvora podataka

Snažna etička i pravna razmatranja

a) Velika količina dostupnih informacija

Trenutno postoji velika količina vrijednih javno dostupnih podataka koje treba analizirati, korelirati i povezati. To uključuje društvene mreže, javne vladine dokumente, izvješća, online multimedijски sadržaj, novine, pa čak i *Deep Web-a*. Zapravo, *Deep Web* sadrži više informacija od običnog preglednika odnosno internet pretraživača poznatog većini korisnika [9]. Kako bi se moglo pristupiti tim mrežama, potrebno je koristiti posebne alate budući da njihov sadržaj nije indeksiran od strane tradicionalnih tražilica. *Deep Web* nudi anonimnost i privatnost korisnicima koji ga koriste. To omogućuje kriminalcima da koriste mrežu za pretraživanje i objavljivanje u nelegitimne svrhe prekrivajući svoj identitet. Stoga je *Deep Web* idealan izvor za primjenu OSINT-a i borbu protiv kibernetičkog kriminala, organiziranog kriminala ili kibernetičkih prijetnji [10].

b) Veliki računalni kapacitet

Napredak u računalnoj arhitekturi, procesorima i grafičkim procesorskim jedinicama omogućuju izvođenje intenzivnih operacije u smislu prikupljanja, obrade, analize i skladištenja podataka [11]. Zahvaljujući ovoj značajki, moguće je primijeniti OSINT na miješanje velikog broja skupova podataka, odnosa i obrazaca iz različitih vrsta otvorenih izvora, uz primjenu naprednih tehnika obrade i analize.

c) *Big data* i strojno učenje

Analiza podataka i tehnika rudarenja podataka, kao i algoritama strojnog učenja, koji mogu automatizirati i učiniti procese istraživanja i donošenja odluka inteligentnijima i učinkovitijima. Omogućuje uočavanje složenih korelacija koje su ljudima nepredvidive. Ova točka je ključna u budućim aktivnostima OSINT-a, jer označuje razliku između istraživanja koji su vođeni ljudskim djelovanjem i istraživanja koji su vođeni umjetnom inteligencijom. Uključivanjem tih tehnika, vladine protuobavještajne agencije mogu iskoristiti takvu paradigmu za daljnje poboljšanje kvalitete upravljana informacija [12].

d) Komplementarne vrste podataka

Struktura sustava dovoljno je otvorena da uključuje podatke koji zapravo nisu dobiveni iz otvorenih izvora. Ova činjenica znači da OSINT može biti još učinkovitiji ako postoji mogućnost dodavanja vanjskih dijelova informacija koji bi nadopunili istragu [13]. Naprimjer, agencije za provođenje zakona mogu iskoristiti suradnju građana za unos OSINT pretraživanja, obavještajne službe mogu iskoristiti povjerljive informacije o kibernetičkim kriminalcima ili incidentima kako bi obogatile OSINT istragu.

e) Fleksibilna svrha i široki opseg

Zbog fleksibilnosti OSINT-a, istrage se mogu proširiti i mogu prikupiti dijelove informacija diljem mrežnog prostora. Mogu se koristiti za ekonomske, psihološke, strateške, novinarske i sigurnosne aspekte [13]. Posebno se mogu istaknuti prednosti u području kriminala i kibernetičke sigurnosti, gdje bi OSINT mogao pratiti sumnjive osobe ili opasne skupine i proučavati zabrinjavajuće trendove u društvu.

f) Složenost upravljanja podacima

Količina podataka je velika te je stoga teško učinkovito i djelotvorno postupati. Za OSINT je korisno uzeti u obzir što je moguće više informacija, ali također imati napredne tehnike i značajna sredstva kako bi se osigurala visoka kvaliteta prikupljanja, obrade i analize [14].

g) Nestrukturirane informacije

Javno dostupni podaci na internetu sami po sebi su masovno neorganizirani. To znači da su podaci prikupljeni OSINT-om toliko heterogeni da ih je teško klasificirati, povezati i ispitati kako bi se izdvojili relevantni odnosi [15]. U tom smislu, OSINT zahtijeva mehanizme kao što su rudarenje podataka ili analitika teksta za homogeniziranje nestrukturiranih informacija kako bi ih se kasnije moglo iskoristiti.

h) Dezinformacije

Društvene mreže i mediji preplavljeni su subjektivnim mišljenjima i lažnim vijestima. Iz tog razloga, postojanje netočnih informacija mora se uzeti u obzir pri implementaciji OSINT mehanizama. OSINT aktivnosti moraju se baviti pouzdanim informacijama i slijediti pouzdane linije istraživanja kako bi se osigurali pozitivni i uvjerljivi rezultati [16].

i) Pouzdanost izvora podataka

Vjerodostojnost i autoritet podataka su ključni za uspješnu OSINT istragu [17]. U idealnom slučaju, prikupljeni podaci trebaju potjecati iz pregledanih i pouzdanih izvora. U praksi OSINT također koegzistira sa subjektivnim ili neautoritativnim izvorima, poput sadržaja društvenih mreža ili manipuliranih medija [17]. Iako je ova vrsta izvora sklonija dezinformacijama, tu se zapravo može izvući više znanja za istraživanje ljudi, grupa ili tvrtki. Ako vjerodostojnost otvorenih izvora informacija doista predstavlja ograničenje, to postaje još veći izazov s obzirom na moguću dvosmislenost upita korisnika za dohvaćanje željenih informacija [17].

j) Snažna etička i pravna razmatranja

S razvojem OSINT-a pojavljuju se brojne brige o privatnosti, poštovanju i osobnom integritetu [18]. S jedne strane, iako je javno dostupan, OSINT ima mogućnost otkriti podatke koje nisu eksplicitno objavljene na *webu*. Neotkriveni rezultati trebaju poštovati privatnost korisnika i ne otkrivati intimne i osobne probleme [6]. U tom smislu, aspekti poput seksualne orijentacije, vjerskih uvjerenja, političke sklonosti ili kompromitirajućeg ponašanja mogu se isčitati s interneta. S druge strane, opseg pretraga temeljenih na OSINT-u trebao bi biti, po

definiciji, ograničen na otvorene izvore podataka. Ni pod kojim uvjetima se kontrole pristupa ili metode provjere autentičnosti ne smiju zaobići u svrhu izvlačenja znanja.

2.2. OSINT analiza

OSINT kao i svaka druga vrsta obavještanja, ima dobro definiranu i preciznu metodologiju. Prvo, u fazi prikupljanja, javno dostupni podaci se dohvaćaju iz relevantnih otvorenih izvora. Konkretno, internet je odličan izvor zbog količine postojećeg materijala i lake dostupnosti. Proces prikupljanja je posebno važan jer se od ove faze nadalje pokreće cijeli proces generiranja obavještajnih podataka. Zatim se u fazi analize sakupljeni podaci obrađuju kako bi se dobile vrijedne i razumljive informacije. Podaci sami po sebi nisu korisni, pa ih je potrebno interpretirati kako bi se dobile prve činjenice proizašle iz dubinske analize. Nadalje, u procesu ekstrakcije znanja, informacije koje su prethodno pročišćene, uzimaju se kao ulaz za sofisticiranije algoritme zaključivanja. Zahvaljujući računalnim naprecima sadašnjeg doba, moguće je detektirati obrasce, profilirati ponašanja, predvidjeti vrijednosti ili korelirati događaje. Drugi i treći korak obuhvaćaju tehnologije koje su široko korištene i poznate u kontekstu rudarenja podataka.

Kontinuirane iteracije kroz različite OSINT tehnike treba analizirati i razumjeti kako bi se stvorile vrijedne informacije. Osim toga, sve je veći broj aplikacija, u ovom kontekstu poznatih kao OSINT usluge, koje olakšavaju okupljanje na internetu, a postoji sve veća količina tehnika analize [19], a u nastavku se ističu postupci koji su primjenjivi:

- Leksička analiza podrazumijeva neobrađene podatke koje je potrebno ispitati kako bi se izdvojili entiteti i odnosi iz teksta. Bitno je primijeniti procese prevodenja na jezik korišten u OSINT istraživanju i filtrirati šum koji ne dodaje vrijednost iz rečenica [20].
- Semantička analiza objašnjava značenje riječi iz velike količine podataka. U svrhu razumijevanja podataka, koriste se algoritmi obrade prirodnog jezika [21]. Osim toga, tehnike analize osjećaja dopuštaju kontekstualizaciju subjektivnih postova ili mišljenja kako bi se klasificirao emocionalni status autora .
- Geoprostorna analiza obuhvaća prikupljene podatke s društvenih mreža, događaja, senzora i IP adresa temeljene na lokaciji. U tom smislu, korištenje karata ili grafikona olakšava predstavljanje i razumijevanje podataka [22], kao i izdvajanje smislenih veza između incidenata ili osobe.
- Analiza društvenih medija odnosi se na značajke koje donose moderni društveni mediji, a omogućuju istraživačima da provedu dubinsku analizu korisnika [22]. U takvom scenariju, analiza društvenih podataka omogućuju stvaranje mreže kontakata, interakcija i mjesta događaja.

Rezultati pokretanja gore navedenih tehnika smatraju se izlaznim informacijama i kategoriziraju se u tri glavne skupine:

- Osobni podaci spajaju podatke o identitetu osobe koji se uglavnom dobivaju iz pravog imena, adrese elektroničke pošte, korisničkog imena, društvenih mreža i pretraživača.
- Organizacijske informacije formiraju timove. U osnovi se prikupljaju putem društvenih mreža, tražilica, lokacija, naziva domene i tehnika IP adresa.

- Informacije o mreži pokrivaju tehničke podatke o sustavima i komunikacijskim topologijama što se obično postiže tehnikama lokacije, naziva domene i IP adrese.

Ova tri bloka informacija mogu se proširiti s više elemenata. Štoviše, jedna istraga može imati različite vrste izlaznih informacija koje se međusobno nadopunjuju. Međutim, ekstrakcija obavještajnih podataka tih nalaza zapravo vodi do onoga što će omogućiti prepoznavanje mete. U tu svrhu prikupljanje znanja kao obrade rezultata analize izlaznih informacija koristeći rudarenje podataka u nastavku su spomenute neke tehnike:

- Korelacija koja se odnosi na detekciju odnosa između ljudi, događaja ili dijelova podataka općenito [24]. Povezane značajke posebno su vrijedne za otkrivanje neeksplicitnih asocijacija koje postoje u skupu podataka.
- Klasifikacija se odnosi na podatke koji se mogu podijeliti u skupine prema unaprijed definiranim kategorijama. Ova tehnika dopušta organiziranje velikih količina informacija za učinkovitije izvlačenje znanja [23].
- Otkrivanje izvanrednih vrijednosti postupak je analiziranja skupa podataka i otkrivanja anomalije u njemu. Ova tehnika posebno je zanimljiva za promatranje malignih uzročnika, čije se ponašanje ili djelovanje razlikuje od opće populacije [23].
- Grupiranje je tehnika koja dodjeljuje dijelove podataka u klastere, a ima mogućnost uzeti u obzir veliku količinu uvjeta. Ova tehnika pomaže pri otkrivanju različitih načina ponašanja na mreži, razne vrste online profila ili kategoriziranje oblika napada na pojedince, organizacije ili infrastrukture bez prethodnog znanja o postojanju te različitosti [23].
- Regresija je tehnika kojoj je glavni cilj predvidjeti numeričke vrijednosti ili činjenice [24]. Naprimjer, linearna regresija vraća vrijednost koja se odnosi na linearnu funkciju, neuronska mreža je struktura koja preslikava složene kombinacije ulaza u izlaz ili dubinsko učenje koje se sastoji od nekoliko slojeva koji se kombiniraju i izvode operacije s ulazom.
- Praćenje uzoraka je tehnika koja za razliku od otkrivanja anomalija, prepoznaje uzorke za otkrivanje pravilnosti u podacima [24].

Zapravo, svaka tehnika umjetne inteligencije prikladna je za ekstrakciju znanja otvorenih podataka. Ove inteligentne tehnike omogućuju zaključivanje apstraktnih, složenih pitanja o meti koja nisu eksplicitno objavljena na internetu. Međutim, proces se uglavnom odnosi na istraživanje i razvoj procesa izvlačenja znanja za identifikaciju, profiliranje ili praćenje kriminalaca, prepoznavanje i istraživanje zlonamjernih organizacija ili otkrivanje i pripisivanje kibernetičkih incidenata [24]. Izvučeno znanje o osobi, tvrtki ili organizaciji može biti posebno osjetljivo i njegova manipulacija neizravno dovodi do etičkih i pravnih problema.

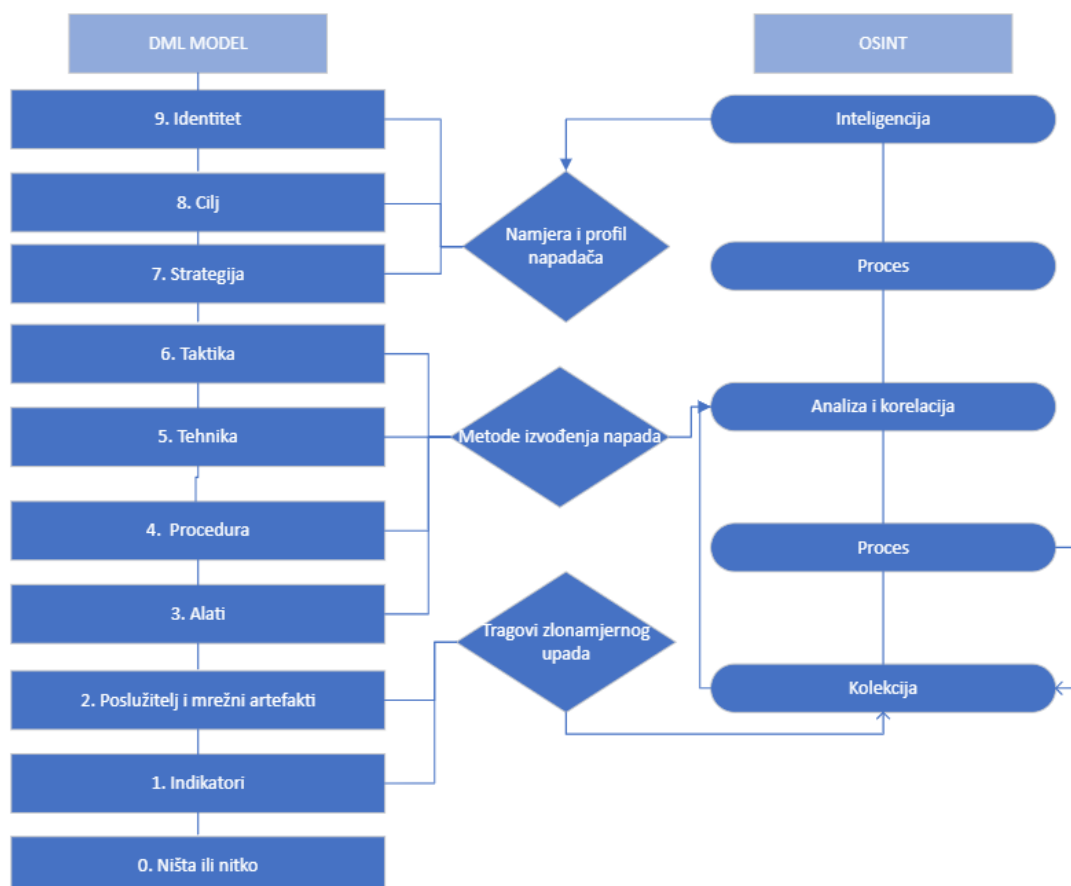
2.3. Integracija OSINT-a u kibernetičkome napadu

Implementacija mehanizama detekcije i odgovora na kibernetičke incidente danas je obveza. Tvrtke i organizacije koje su sve više izložene na internetu ulažu u kibernetičku sigurnost kako bi zaštitile svoju imovinu od kriminalaca. Stoga je iznimno važno učinkovito upravljati prijetnjama i incidentima protiv informacijskih sustava. Kibernetička obrana nije samo implementacija tehničkih rješenja kao što su vatrozidi, sustavi za otkrivanje upada, sustavi

za sprječavanje upada, upravljanje sigurnosnim informacijama i događajima ili antivirusi za izbjegavanje poznatih prijetnji, već i ugradnja kibernetičku inteligenciju za izdvajanje i analizu tragova. Zapravo, kontinuirani ciklus izvlačenja i dijeljenja dokaza, odnosa i posljedica incidenata poznat je kao obavještajni podaci o prijetnjama. On nadopunjuje tradicionalne obrambene mehanizme s ažuriranim informacijama i značajno poboljšava zaštitu infrastrukture, upravljanje opasnostima i učinkovitost odgovora [25].

Štoviše, informacije koje se obično koriste za forenziku i istrage samo su tehničke prirode. Međutim, tragovi koje kibernetički napad ostavi sadrže vrijedne informacije o društvenim mrežama, forumima, medijima, tehničkim i vladinim dokumentima i drugim digitalnim javnim izvorima [25]. U svrhu poboljšavanja kibernetičke sigurnosti potrebno se fokusirati na predlaganje obrambenih poboljšanja pri suočavanju s prijetnjama. OSINT je izvor znanja koji može podržati istragu kibernetičkog napada do najsitnijih detalja zlonamjerne akcije sve do korijena problema [25]. Konkretno, OSINT bi omogućio da se razumije motivacija kibernetičkog napada, pogodi postupak analize i u konačnici izvrši profil počinitelja.

Predložena metodologija i model za definiranje zrelosti otkrivanja incidenta organizacije ilustrirana je na slici 2., koja je ključna za izvlačenje dokaza od izvršenog kibernetičkog napada stoga je predložena modificirana verzija distribucije razine upravljanja (engl. *Data manipulation language - DML*) modela [26].



Slika 2. DML model otkrivanja incidenta [26]

DML model na hijerarhijski način predstavlja različite razine apstrakcije u detekciji kibernetičkih napada. Tvrtka koja ne ulaže u kibernetičku sigurnost s vremenom postaje ranjiva na potencijalne napade. Naprotiv, organizacija koja je tehnički vješta u kibernetičkoj obrani može interpretirati složenije činjenice odnosno popeti se na višu razinu apstrakcije.

Dok se niže razine mogu lako pokriti, izazov leži u dosezanju viših slojeva. U tu svrhu prikazana je primjena OSINT-a koji se nadopunjuje najosnovnijim dokazima kako bi se došlo do konkretnih činjenica:

- a) Prva pretpostavka je da moguće pokriti razine DML-1 i DML-2. Nulti sloj sastoji se od jednostavnih detalja poput niza u modificiranoj datoteci, vrijednosti memorijske ćelije ili bajta koji se prenosi kroz mrežu, a koji sami po sebi imaju vrlo nisku vrijednost, ali zajedno čine sljedeću razinu. Sloj poslužitelja i mrežnih artefakata izgrađen je na pokazateljima opaženim tijekom ili nakon kibernetičkog napada kao što su IP adrese, nazivi domena, zapisnici, transakcije i detalji o manipulaciji datotekama [26]. Stoga je izdvajanje tih tragova početna točka OSINT procesa.
- b) Zatim slijede razine DML-3 do razine DML-6. Treća razina alati, sastoji se od otkrivanja prijenosa, prisutnosti i funkcionalnosti alata koje koristi napadač. Sljedeća razina procedura je pokrivena ako se zapamte stanja odnosno koraci koji su izvedeni tijekom incidenta. Tehnika pete razine opisuje kako je napadač specifično izveo različite faze napada. Posljednja razina navedena u ovom dijelu je taktika koja uzima u obzir spomenute razine i izvodi analizu niza aktivnosti u vremenu i kontekstu [26].

U ovom slučaju informacije otkrivaju detalje o izvršenju kibernetičkog napada. Takvi podaci uvelike obogaćuju fazu analize OSINT ciklusa. Obrasci izvedeni iz ovih podataka, kao i korelacija s drugim već pohranjenim slučajevima, omogućuje inteligentniju i sveobuhvatniju analizu. Zapravo, ove zaključke treba integrirati zajedno s rezultatima koji su dobiveni u fazi prikupljanja. Na taj se način istraživanje kroz mrežu pročišćava kako bi se došlo prema konačnom cilju.

- c) Dok kontinuirani proces prikupljanja i analize OSINT-a stvara vrijedne informacije na koje se primjenjuju tehnike izvlačenja znanja. Znanje ekstrahirano OSINT-om od razine DML-1 do DML-6 omogućuje dosezanje najviše razine. Sedma razina, strategija, odnosi se na opis visoke razine planiranog kibernetičkoga napada. Osmo razina, ciljevi, specifični su ciljevi napadača i izražavaju stvarnu motivaciju akcije. Na vrhu se nalazi razina identiteta, koja je u biti ime osobe, organizacije ili čak zemlje koja je odgovorna za zlonamjerne radnje [26]. Budući da je izuzetno teško pronaći te detaljne informacije, povezanost s drugim kibernetičkim napadima i sličnost s drugim događajima mogu poduprijeti relativnu atribuciju [27]. Odnosno, dovršetak istrage trenutnog slučaja dodatnim informacijama o drugim incidentima koje je prouzročio isti akter dovodi do identifikacije kibernetičkog napadača.

Ova OSINT aplikacija predstavlja inovativnu proces djelovanja u borbi protiv kibernetičkih prijetnji. Izazov leži u implementaciji učinkovitih mehanizama prikupljanja i postupaka inteligentne analize za izdvajanje detalja visoke razine koji se ne mogu izravno

izdvojiti iz zlonamjernih radnji. Takvi detalji su najsloženiji dijelovi informacija za postizanje, jer imaju vrlo visok stupanj apstrakcije. Zato je potrebno potražiti otvorene izvore za bilo kakav odnos ili obrazac s kojim bi se otkrilo više o kontekstu i izvorima incidenta. OSINT je ključni dio koji nedostaje u opremi za profiliranje kibernetičkih napadača i za poboljšanje otkrivanja sofisticiranih napada [27].

2.4. Izazovi i budući trendovi OSINT-a

Do danas su razvijene brojne tehnike i alati. Međutim, postoje neke praznine i ograničenja u području javno dostupnih podataka kako bi se moglo nastaviti istraživati i iskorištavati ponuđene prilike. Potrebno je napraviti sofisticiranija rješenja primjenjiva na nekontrolirane scenarije stvarnog svijeta.

2.4.1. Automatizacija prikupljanja podataka

Što je veća količina prikupljenih informacija, veća je vjerojatnost stvaranja zaključaka i odnosa. Međutim, količina javnih podataka koja je danas dostupna je ogromna i ne može se prikupljati na ručni način [28]. Iako su OSINT tehnike i alati već veliki korak, većina njih još uvijek uvelike ovisi o krajnjem korisniku. Trenutne tehnike velikih podataka koje se ističu su pretraživanje interneta kao potencijalne paradigme za automatizaciju i poboljšanje OSINT istraživanja velikih količina otvorenih podataka [28]. Važan aspekt procesa sakupljanja je proširenje potrage i poboljšanje analize. Rezultati dobiveni pretragama trebali bi poslužiti kao podloga za sljedeće krugove prikupljanja.

2.4.2. Poboljšanje procesa analize podataka

Tumačenje prikupljenih otvorenih podataka ključna je točka u OSINT postupku. Izdvajanje rezultata, uspostavljanje odnosa između odvojenih dijelova informacija ili izvođenje zaključaka koji nisu eksplicitno izloženi povećava kvalitetu rezultata. Međutim, OSINT analiza danas ne implementira inteligentne mehanizme. Postojeći alati ograničeni su na bacanje svih pronađenih informacija i njihovih eksplicitnih odnosa [29]. Proces analize trebao bi uključivati semantičku analizu, proučavanje obrazaca, korelaciju s drugim događajima, pojavama ili skupovima podataka. Moderne tehnike rudarenja podataka kao što su analiza društvenih mreža i strojno učenje su dizajnirane za rješavanje ovakve vrste izazova [29].

U idealnom slučaju, OSINT bi u budućnosti trebao krajnjem korisniku moći pružiti konkretnu informaciju koju traži kao i vratiti uvjerljive odgovore u istragama. Izvorno pretraživanje također bi imalo ne samo izravne zaključke, već i neizravne, a ne eksplicitne odnose.

2.4.3. Integracija podataka iz više otvorenih izvora

OSINT aktivnosti se trebaju povezati sa što više izvora kako bi se pokrio što širi spektar. Nije dobra ideja fokusirati istraživanje na jednu društvenu mrežu. U tom smislu, uspjeh leži u kombiniranju izvora podataka kako bi se dobili najbolji mogući rezultati. To znači da sustav mora normalizirati dostupne informacije koje su obično nestrukturirane, kako bi izvršio učinkovitu analizu i korelaciju. Kao rezultat toga važno je odbaciti stavke koje se ponavljaju.

S druge strane, poželjno je uključiti različite vrste podataka. Osim podataka izvučenih s Interneta, *Deep Web*a, OSINT bi tijekom rada također trebao uzeti u obzir informacije

prikupljene na terenu, s društvenim inženjeringom ili u suradnji s građanima [30]. Svaka informacija koja je zanimljiva istrazi mora se iskoristiti kako bi se postigla sljedeća prekretnica u potrazi. Dodatno, nužna je implementacija procesa otkrivanja istine za one slučajeve kada su informacije iz različitih izvora proturječne [30].

2.4.4. Lažne vijesti

Zbog velike količine podataka koji su javno dostupni, OSINT proces mora imati mogućnost razlikovanja relevantnosti svake informacije, odbacujući podatke koji ne doprinose kvaliteti istrage [31]. Istraživač se ne može usredotočiti na istraživanje pojedinosti cijele *web* stranice, čitanja vijesti na više stranica ili analizu složenog vladinog dokumenta. OSINT istraživanje bi trebalo izdvojiti ključne riječi koje zapravo daju vrijednost i otkrivaju znanje o meti. Informacija koja zanima provoditelja istrage možda neće biti eksplicitno izražena, a izazov je izdvojiti bit izvora podataka koji se proučava.

U isto vrijeme, precizni izdvojeni pojmovi služe kao središnje točke za stvaranje novih puteva istraživanja. Nadalje, ključno je otkriti dezinformacije koje bi pokvarile rezultate. Internet je po prirodi subjektivan i za većinu sadržaja nema jamstva da je pouzdan i služben. Provoditelji OSINT istrage trebaju utvrditi je li sve veće oslanjanje na javno dostupne podatke još uvijek u kombinaciji s validacijom izvora, što predstavlja primarni zahtjev i prioritet [31]. Te neistinite informacije mogu preokrenuti istragu i dovesti do pogrešnih rezultata. Ovaj problem je prisutan u istraživanjima u stvarnom životu. Izvori podataka u kojima se pronalaze vrijednije informacije o osumnjičenicima bit će istaknuti na forumima i društvenim mrežama. Na tim stranicama, istraživač se mora baviti mišljenjima, subjektivnim objavama i osobnim preferencijama čija je istinitost upitna [32]. Profiliranje osoba koje u stvarnosti ne predstavljaju prijetnju mogu izazvati diskriminatorne i nepravedne stavove koji mogu utjecati na potencijalne žrtve.

2.4.5. Interoperabilnost OSINT-a

Jedan od glavnih nedostataka mnogih postojećih OSINT izvora je taj što funkcioniraju samo za određene zemlje, smanjujući njihovu sposobnost profiliranja na ograničenu skupinu ljudi koji pripadaju određenoj nacionalnosti. Međutim, OSINT bi trebao biti univerzalna tehnika za trenutno obilaženje svih kutaka Zemlje bez razlikovanja zona kibernetičkog prostora. Stoga je interoperabilnost poželjno svojstvo koje treba uzeti u obzir u dizajnu OSINT-a jer povećava, ne samo opseg pretraživanja, već i njegovu upotrebu od strane krajnjih korisnika. OSINT tijekom rada trebao bi kombinirati točke informacija diljem svijeta i korelirati distribuirane izvore podataka. Zapravo, iako se odnos između zona pretraživanja može napraviti ručno, pravi izazov leži u OSINT aplikacijama koje implementiraju te skokove [31].

Generička i fleksibilna implementacija posebno je korisna za nomadske ciljeve kojima je mobilnost dio svakodnevnog života. Ako je subjekt od interesa osoba koja je proživjela faze svog života u nekoliko zemalja, ili tvrtke sa sjedištem na nekoliko kontinenata, ili čak kriminalci koji mijenjaju svoju lokaciju kako bi ih bilo teže progoniti [31]. U tim slučajevima, statična pretraga u određenoj zemlji ostavila bi mnogo informacija ne prikupljenih i puno tragova neanaliziranih.

2.4.6. Svijest o privatnosti, etičkim i pravnim razmatranjima

S etičkog gledišta, OSINT mora poštivati privatnost korisnika kako ne bi narušio privatni život, kao i privatnost obitelji, prijatelja i suradnika. Činjenica da je informacija javno dostupna, ne znači da nije i osjetljiva. Razotkrivanje političkih misli na određenim mjestima može imati kobne posljedice. Priopćavanje seksualne orijentacije može biti potencijalno opasno po život u određenim zemljama. Poznavanje vjerskih uvjerenja može dovesti do kaznenih presuda na određenim teritorijima. Stoga se s javno dostupnim podacima mora pažljivo postupati, u legitimne svrhe i u interesu društva.

S pravnog stajališta, OSINT bi se trebao koristiti na temelju zakona i poštujući politiku zaštite podataka. Dolaskom GDPR-a promijenila se regulativa koja se tiče osobnih podataka [33]. U tom smislu osobni podaci obuhvaćaju sve informacije koje se mogu odnositi na bilo kojeg građanina. Ne smiju se objaviti prikupljeni osobni podaci, čak ni ako su objavljeni na *webu*. Osim toga, korisnik koji primjenjuje OSINT ne može pasti u pogrešku pokušaja oponašanja cilja kako bi pronašao više informacija. Također barijere provjere autentičnosti ne mogu se probiti kako bi se pristupilo informacijama koje se traže. Štoviše, različite informacije, koje su zajedno prikupljene mogu dovesti do identifikacije pojedinca, a mogu predstavljati osobne podatke, čak i ako su informacije šifrirane ili anonimizirane [6]. Moguće rješenje za rješavanje takvog izazova je prilagodba dizajna OSINT alata sa ugrađenim ograničenjima [33].

OSINT je po definiciji potpuno legalan zbog javne prirode izvora podataka koje koristi. Ipak, istražitelji ne smiju objaviti prikupljene osobne podatke, čak ni ako su objavljeni na *webu*. Korištenje OSINT-a treba biti ograničeno na legalne aktivnosti i svrhe koje nisu zlonamjerne. OSINT načelno ne krši ljudsku slobodu i prava, stoga su njegove prethodno navedene tehnike i usluge u toj mjeri legalne [33]. Zahvaljujući OSINT-u, novinari mogu pružiti ažurne, objektivne i kvalitetne vijesti. Menadžeri ljudskih potencijala mogu bolje upoznati kandidate za svoj posao. Državna tijela mogu istraživati kriminalne i terorističke skupine. Tvrtka može revidirati svoju izloženost kibernetičkim prijetnjama u inozemstvu. Međutim, takva otvorenost prema korištenju OSINT tehnika za određene kategorije treba uvijek biti ispravno opravdana [33].

S druge strane, OSINT krajnji korisnik mogao bi biti delinkvent koji pokušava počiniti zločin. Zlonamjerni haker bi mogao profilirati metu kako bi povećao vjerojatnost uspjeha. Lopov bi mogao analizirati članove obitelji kako bi krao od kuće u najboljem trenutku. Iznuđivač bi mogao objaviti privatne i osobne podatke žrtve ako otkupnina nije plaćena. U svakom slučaju, najmoćniji alati trebali bi biti dostupni samo obavještajnim agencijama.

2.4.7. Sprječavanje zloupotrebe OSINT-a

Mogućnosti OSINT paradigme prilično su široke. OSINT je moguće iskoristiti za potrebe kibernetičke sigurnosti i kiberobrane, istražujući tako napadače i terorističke skupine [34]. Unatoč tome, iskorištavanje javno dostupnih podataka podložno je zloporabama. To jest, loše motivirani akteri mogu iskoristiti ogromnu količinu informacija kako bi počinili kibernetičku agresiju, kao što su internetsko zlostavljanje i kibernetičko ogovaranje [34]. Nažalost, te su pojave sve više i zabrinjavajuće učestalije na *webu*, a žrtve dovode do tjeskobe, usamljenosti, depresije, pa čak i do samoubojstva u najgorem slučaju [7]. Konkretno,

kibernetičko ogovaranje izvodi skupina ljudi koji putem digitalnih uređaja daje subjektivne komentare o nekome tko nije prisutan. Ovo kibernetičko ponašanje utječe na društvenu skupinu u kojoj se pojavljuje i može ometati međuvršnjački odnosi, nanoseći štetu žrtvi [34]. U tom je smislu važno kontrolirati da se OSINT tehnike i servisi koriste na ispravan način, a da se pritom ne štete pravima i slobodama drugih [34]. Konkretnije, moglo bi se razmišljati o davanju različitih privilegija na temelju kategorije krajnjeg korisnika, čime bi se izbjeglo odobravanje potpunog pristupa cijelom spektru informacija. Naprimjer, zaposlenici mogu imati pristup osnovnim informacijama kako bi unaprijedili svoje zadatke, dok vladine i policijske snage mogu istraživati otvorenije podatke [34]. U tom smislu, zlouporaba OSINT-a vjerojatno će se ispravno otkriti pomoću alata temeljenih na OSINT-u.

3. DIGITALNI OTISCI NA JAVNOJ KOMUNIKACIJSKOJ MREŽI

Digitalni otisak se odnosi na trag podataka koji se ostavlja tijekom korištenja interneta. To uključuje *web* stranice koje se posjećuju, elektronička pošta koja se šalje i informacije koje se šalju online. Digitalni otisak može se koristiti za praćenje online aktivnosti i uređaja korisnika. Korisnici interneta aktivno ili pasivno stvaraju svoj digitalni trag na internetu [35]. Aktivni digitalni otisak je mjesto gdje je korisnik namjerno podijelio informacije o sebi. Naprimjer, objavljivanjem ili sudjelovanjem na društvenim mrežama ili online forumima. Ako je korisnik prijavljen na *web* mjesto putem registriranog korisničkog imena ili profila, sve objave koje objavi dio su njegovog aktivnog digitalnog otiska. Ostale aktivnosti koje pridonose aktivnom digitalnom otisku uključuju ispunjavanje online obrasca ili pristanak na prihvaćanje kolačića u pregledniku. Pasivni digitalni otisak stvara se kada se prikupljaju informacije o korisniku, a da on nije svjestan da se to događa. Naprimjer, to se događa kada internetska mjesta prikupljaju informacije o tome koliko su puta korisnici posjetili određenu stranicu. Ovo je skriveni proces za koji korisnici možda ne znaju da se odvija. Drugi primjeri pasivnog otiska uključuju mjesta društvenih mreža i oglašivače koji koriste korisnikove lajkove, dijeljenja i komentare kako bi profilirali i ciljali korisnika određenim sadržajem. Neki od načina na koje korisnici ostavljaju svoj digitalni otisak uključuju [35]:

- kupnja s *web* stranica e-trgovine,
- prijavljivanje za kupone ili kreiranje računa,
- preuzimanje i korištenje aplikacija za kupnju,
- korištenje aplikacije za mobilno bankarstvo,
- kupnja ili prodaja dionica,
- pretplata na financijske publikacije i blogove,
- otvaranje računa kreditne kartice,
- korištenje društvenih medija na računalu ili uređajima,
- prijava na druge *web* stranice pomoću vjerodajnica društvenih medija,
- povezivanje s prijateljima i kontaktima,
- dijeljenje informacija, podataka i fotografija ,
- pridruživanje stranici ili aplikaciji za upoznavanje,
- pretplata na internetski izvor vijesti i
- pregledavanje članaka u aplikaciji za vijesti.

Ponekad nije uvijek očito da korisnik ostavlja digitalni trag. Naprimjer, internetska mjesta mogu pratiti korisnikovu aktivnost instaliranjem kolačića na uređaj, a aplikacije mogu usporediti podatke, a da za to korisnik ne zna. Nakon što se organizaciji dopusti pristup podacima, ona bi mogla prodati ili podijeliti korisnikove podatke s trećim stranama. Također potrebno je voditi brigu o dijeljenju osobnih podataka na društvenim mrežama iz kojih napadači mogu otkriti lokaciju i ostale važne osobne podatke korisnika.

3.1. Sigurnosne prijetnje digitalnog otiska

Društvene mreže više nisu samo za održavanje kontakta s prijateljima. Potrošači, tvrtke i organizacije također su primijetili prednosti koje društvene mreže nude današnjem društvu. Uobičajeni razlog zašto korisnici aktivno sudjeluju na društvenim mrežama je da bi ostali u kontaktu sa starim prijateljima, a da pritom zadrže svoje trenutne odnose [36]. Korisnici dobivaju priliku kreirati profile koji ih prikazuju u najboljem svjetlu i na taj način ih prihvaćaju njihovi vršnjaci. Informacije koje se nalaze u profilima mogu biti vrlo općenite, kao što su ime, omiljene knjige i vrste glazbe. Profili također mogu sadržavati više osobnih podataka, kao što su politička stajališta, seksualna orijentacija i vjerska uvjerenja. U početku su članovi društvenih medija koristili internetska mjesta za komunikaciju i širenje informacija drugima, ali trenutno su te stranice dodale i potrošačku komponentu svojoj bazi [36].

Iznimno rijetko da tvrtka nema barem jednu društvenu mrežu pomoću kojih oglašava proizvod. Ne samo da su tvrtke otkrile besplatno oglašavanje, već mogu objavljivati proizvode u svakom dijelu svijeta. Osoblje u prodaji i marketingu shvatilo je potencijalne društvene stranice za njihove tvrtke te su proučile, razvrstale društvene mreže prema namjeni i maksimizirali taj potencijal kako bi prodali svoju robu [36]. Društvene mreže se mogu kategorizirati u nekoliko namjena prikazanih u tablici 2:

Tablica 2. Kategorizacije društvenih mreža prema namjeni [36]

MREŽA	NAMJENA
<i>LINKEDIN, VISIBLE PATH</i>	Poslovno-profesionalna društvena mreža
<i>DOGSTER, CARE2</i>	Upoznavanje stranih osoba na temelju zajedničkih interesa
<i>LAST.FM, YOUTUBE</i>	Razmjena podataka i medija između korisnika

Određena kategorija društvenih mreža s posebnom namjenom sadrži podatke korisnika s kojima raspolaže. Ti podaci su vidljivi na profilu osobe, ukoliko je ta osoba odlučila podijeliti sve podatke s drugima oni će biti vidljivi. Dok postoje podaci koji nisu vidljivi svim korisnicima, a isti su zanimljivi zlonamjernim napadačima koji imaju različite motive za zlonamjerni napad.

Zlonamjerni napadi događaju se sve češće na društvenim mrežama, većinom zbog nepažnje korisnika i sigurnosnih propusta za vrijeme korištenja internetskog preglednika. Također nepovoljna je okolnost što starije verzije društvenih mreža dozvoljavaju postavljanje komentara u obliku programskog jezika za izradu internetskih stranica (engl. *Hyper Text Markup Language* - HTML) koda. Na ovakav način, zlonamjerni napadač može unijeti maliciozni kod koji se korisnicima čini kao normalna poveznica na multimedijske sadržaje [36].



Slika 3. Prikaz zlonamjernog koda pomoću DDoS napada [36]

Primjerice, na slici 3. je prikazan kod kojeg je pokraj teksta niz točki. Napadačeva je namjera zapravo izvesti napad uskraćivanjem usluge (engl. *Distributed denial of service attack - DDoS*) na određeni poslužitelj. Na slici 4. je prikazan zlonamjerni kod kojeg je napadač unio u polje za unos komentara.

```
"Awesome music"





```

Slika 4. Prikaz određivanja veličine slike u HTML kodu i poveznice na slike određene u HTML kodu [36]

Iz slike 4. vidljivo je da je napadač odredio veličinu slike, visine 1 piksela i širine 1 piksela. Na ovakav način zlonamjerni napadači iskorištavaju propust na društvenoj mreži kako bi oštetili poslužitelja.

Pojavom društvenim mreža došlo je i do pojave sigurnosnih incidenata, počevši od brojnih *phishing* napada pa sve do napada virusima i crvima. *Phishing* napad često se koristi za krađu korisničkih podataka, uključujući vjerodajnica za prijavu i brojeva kreditnih kartica. Događa se kada napadač, maskirajući se kao povjerljivi entitet, navede žrtvu da otvori elektroničku poštu ili tekstualnu poruku. Primatelj zatim klikne na zlonamjernu vezu, što može dovesti do instalacije zlonamjernog softvera, zamrzavanja sustava kao dijela napada ili otkrivanja osjetljivih informacija. Napadi ovakve vrste dogodili su se na *Facebook*, *Twitter* i *LinkedIn* mreži. Zbog učestali i velikog broja prijatnji društvenim mrežama moguće ih je podijeliti u četiri skupine [37]:

- prijatnje privatnosti,
- prijatnje mrežama i podacima,
- prijatnje identitetu i
- društvene prijatnje.

a) Prijetnje privatnosti

Prijetnja privatnosti znači bilo koju prijetnju ili niz povezanih prijetnji nezakonitim korištenjem ili otkrivanjem javnosti osobnih identifikacijskih nejavnih informacija koje su protupravno prisvojene od osiguranika u svrhu traženja novca, uključujući virtualnu, digitalnu i elektroničku valutu, vrijednosne papire ili druge vrijednosna imovina osiguranika. Prikupljanje digitalnih zapisa o korisnicima odnosi se na korisničke profile sa stranica društvenih mreža, stvarajući digitalne zapise o korisnicima bez njihovih pristanka. Neki od rizika prikupljanja digitalnih zapisa je uzrokovanje štete ugledu korisnika, ucjena korisnika i otkrivanje povjerljivih podataka o korisniku. Prikupljanje sporednih podataka odnose se na podatke koje korisnik društvene mreže svojevremeno otkriva, te koje je korisnik posjetio. Rizici prikupljanja sporednih podataka su zlouporaba sporednih podataka za ciljano oglašavanje i prodaja prikupljenih podataka drugim tvrtkama. Prepoznavanje lica korisnika se odnosi kada korisnik objavi fotografiju, gdje postavljene fotografije mogu direktno ili indirektno omogućiti identifikaciju korisnika. Otkrivanje podataka pomoću fotografija je tehnologija koja omogućuje prepoznavanje svojstava fotografije, uspoređujući zadanu fotografiju s drugima u bazi fotografija [37]. Na temelju okoline iz fotografije moguće je locirati točnu lokaciju korisnika. Povezivanje podacima i oznakama u fotografijama opisuje korisnika koji se označio na zajedničkim fotografijama. Moguće je označiti ime i prezime pojedinca, staviti poveznicu na korisnički profil pojedinca. Fotografije također sadržavaju podatke o uređaju i vremenu kada su snimljene, a rizici povezivanja podataka i oznaka mogu dovesti do nenamjernog otkrivanja povjerljivih podataka i otkrivanja podataka o korisniku. I zadnja od prijetnja privatnosti je nemogućnost potpunog brisanja korisničkog računa gdje korisnik koji žele obrisati svoj korisnički račun na društvenoj mreži će se otkriti da nije moguće ukloniti sve podatke vezane uz korisnički profil. Deaktivacijom profila, korisnik uklanja svoj profil sa društvene mreže, dok osobni podaci ostaju pohranjeni [37].

b) Prijetnje mrežama i podacima

Najčešće prijetnje mrežama i podacima su: napadi zlonamjnim *softverom*, krađa lozinka i krađa podataka. Naprimjer neželjene poruke se odnose na slanje poruka koje sadržavaju poveznice na internetske stranice putem kojih se želi prodati određeni proizvod. Rizici neželjenih poruka su preopterećenje mreže, gubitak povjerenja korisnika i preusmjerenje na zlonamjerne ili stranice neprimjerenog sadržaja. Napadi virusa i crva mogu ugroziti korisnički račun, može se izvršiti DDoS napad, izvršiti krađa lozinki i povjerljivih podataka i otkriti adresu elektroničke pošte i ostalih podataka o korisniku. Dok alati grupiranje profila više društvenih mreža dozvoljavaju korisnicima da dodavanjem novih podataka ažuriraju korisničke profile na više društvenih mreža istovremeno. U alat je potrebno unijeti korisnička imena i lozinke računa kojima se želi pristupiti, a korištenje ovakvih alata povećava opasnost otkrivanja povjerljivih podataka o korisničkim računima [37].

c) Prijetnje identitetu

Prijetnje identitetu korisnika društvenih mreža smatraju se jednom od najgorih mrežnih prijetnji. Mogu se podijeliti na *phishing* napade, otkrivanje podataka, te kreiranje lažnih korisničkih profila. *Phishing* napadi se mogu izvesti kada korisnik putem poruke ili komentara

na vlastitom profilu gdje zaprima poveznicu koja ga vodi na zlonamjernu internetsku stranicu koju kontrolira napadač. Takve zlonamjerne internetske stranice su najčešće identične kopije *web* stranica društvenih mreža, banaka, te drugih servisa koji bi napadaču mogli koristiti. Od korisnika se najčešće zahtjeva unos korisničkog imena i lozinke odabranog servisa. Dok se otkrivanje podataka može odnositi na svjesno dijeljenje podataka do kojih prijatelji na društvenim mreža mogu doći. Primjer je prihvaćanje zahtjeva za prijateljstvo od nepoznatog pojedinca, te ukoliko je zahtjev odobren, vrlo lako se mogu pronaći osobni podaci kao što su mjesto stanovanja i e-mail adresa [37].

d) Društvene prijetnje

Glavne društvene prijetnje su prijete koje svakoj osobi u procesu digitalizacije stvaraju ovisnost o internetu, degradaciju ličnosti, pad mentalnog zdravlja, pa čak i porast nezaposlenosti u društvu. Također društvene prijetnje mogu se razvrstati u uhođenja, kibernetička nasilja i industrijsku špijunažu. Uhođenje uključuje prijeteće ponašanje u kojem izvršitelj zahtjeva fizički ili virtualni kontakt s osobom koju uhodi. Kibernetičko nasilje je termin kojim se opisuje besciljno i ponavljano nanošenje štete drugom pojedincu pomoću tehnologije, najčešće pomoću mobilnih telefona ili putem interneta. Najčešće se radi o izmijenjenim multimedijским sadržajima kojima je cilj poniziti pojedinca. Što se tiče industrijske špijunaže napadači na prijevaru pokušavaju od zaposlenika neke tvrtke dobiti povjerljive podatke. Gdje objava bilo kakvih povjerljivih informacija može naštetiti organizaciji. Rizici industrijske špijunaže je gubitak intelektualnog vlasništva, napad na računalnu infrastrukturu, ucjena zaposlenika i pristup materijalnoj imovini pojedinca ili tvrtke [37].

3.2. Upravljanje kriznim situacijama pomoću digitalnog otiska

Višestruke promjene diljem svijeta u posljednjim desetljećima dovele su do značajnih promjena u obavještajnoj paradigmi. Globalizacija i informacijska revolucija povećale su složenost trenutnog sigurnosnog okruženja. Također, politički sporovi, oružani sukobi, tehnološki incidenti ili prirodne katastrofe pridonijeli su nastanku političkih, vojnih ili humanitarnih kriza [36]. U tom kontekstu, korištenje najnovijih tehnologija za prikupljanje i analizu javno dostupnih podataka u stvarnom vremenu za stvaranje obavještajnih proizvoda otvorenog koda, a širenje tih proizvoda donositeljima odluka uključenim u upravljanje krizama može spriječiti eskalaciju situacije, pa čak i izbjeći neželjene učinke. Predlošci za podršku odlučivanju koji se uspješno primjenjuju u predvidljivim konvencionalnim situacijama, temeljeni na propisima, ne rade tako dobro u slučaju nekonvencionalnih, nepredvidivih situacija. Složenost trenutnih kriza naglašava potrebu za razvojem računalnih alata za rano upozoravanje kako bi se donositeljima odluka pomoglo u donošenju proaktivnih odluka.

Alat za praćenje društvenih medija omogućuje prikupljanje i obradu informacija iz otvorenih izvora u svrhu dobivanja OSINT-a [36]. Kombinacija najsuvremenijih inteligentnih tehnologija, kao što su indeksiranje internetskog preglednika i rudarenje podataka ključni je element za podršku donositeljima odluka da predvide razvoj krize i poduzmu preventivne mjere za izbjegavanje eskalacije krize. Unatoč učestalosti uporabi pojma krize, trenutno ne postoji jednoglasno prihvaćena definicija. Teškoća formuliranja jedinstvene definicije krize proizlazi

kako iz njezine složenosti, tako i iz mnoštva pristupa različitim subjektata kao što su donositelji političkih odluka, vojnih ili nevojnih organizacija, civilnog društva uključenih u njezino rješavanje. U biti, kriza može biti političke, vojne ili humanitarne prirode i može biti uzrokovane političkim sporovima ili oružanim sukobima, tehnološkim incidentima ili prirodnim katastrofama. Kako ne postoji međunarodno prihvaćena definicija, kriza je složena situacija koja se percipira kao prijetnja vrijednostima, interesima ili ciljeva uključenih entiteta, što često zahtijeva intervencije gotovo u stvarnom vremenu kako bi se smanjile ometajuće interakcije među njima. Pod situacijom se razumijeva svaki spor, problem ili stanje u kojem se nalazi subjekt [36]. Bilo to kada se država, nacija ili drugi nedržavni entitet nađe se u nekom trenutku, ekonomski, politički ili društveno, i u kojem donositelji odluka mogu intervenirati kroz izmjene i poboljšanja. Situacija je složena ako ju je teško definirati ili ako uzrokuje nepredvidive promjene koje dovode do narušavanja postojećeg poretka. Posljednjih godina tehnološka revolucija pridonijela je povećanju kompleksnosti prostora u kojem se događaju aktualne krize. Prije svega, čimbenik koji povećava složenost prostora u kojem se događaju trenutne krize je zbog raširene upotrebe tehnologija od strane osoba i organizacija, posebno platformi društvenih medija i radikalizacije, a sve u svrhu dezinformiranja.

Također, informatička revolucija očituje se u procesu upravljanja krizama. Prijelaz iz mira u nepovjerenje, a potom u sukob ili oružani sukob, moguće je detektirati pomnim definiranjem i praćenjem određenih pokazatelja uz korištenje odgovarajućih informatičkih alata [36]. Ti bi pokazatelji trebali oblikovati ključne karakteristike krize kako bi se procijenio rizik od pojave pokretačkih čimbenika koji bi zaključili situaciju.

Prema otvorenim izvorima u posljednjih deset godina virtualni prostor je pretvoren u najveći otvoreni izvor podataka na svijetu. Otvoreni izvori u *web* prostoru su i prilika i izazov za OSINT produkciju. Mogućnosti proizlaze iz mogućnosti pristupa javnim podacima koje generiraju različiti subjekti na internetu, posebno podacima sa stranica društvenih medija kao što su *YouTube*, *Facebook*, *Twitter* i *TikTok* koji mogu pružiti povratnu informaciju o pojavi čimbenika okidača. Izazovi korištenja otvorenih izvora sastoje se od karakteristika velikih podataka koje ti podaci imaju: obujam, raznolikost, brzina i istinitost. Volumen karakterizira veličinu podataka. Dimenzije podataka otvorenog koda mjere se u terabajtima. Raznolikost se odnosi na heterogenu strukturu skupa podataka. Napredne tehnologije omogućuju prikupljanje različitih vrsta struktura podataka, a to su strukturirane podatke, polustrukturirane podatke i nestrukturirane podatke. Trenutno strukturirani podaci čine samo pet posto ukupnih podataka [6]. Brzina se odnosi na brzinu kojom se podaci otvorenog koda generiraju i analiziraju. Povećani broj digitalnih uređaja doveo je do neviđene stope stvaranja podataka i potaknuo razvoj tehnika analize u stvarnom vremenu. Stoga podaci prikupljeni iz otvorenih izvora zahtijevaju inovativne oblike obrade koji omogućuju bolji uvid u krizu i podržavaju pravovremeno donošenje odluka.

Sustav za praćenje društvenih medija u stvarnom vremenu kao OSINT platforma za rano upozoravanje u kriznim situacijama. Podrazumijeva pružanje pravovremenih informacija, koje omogućuju donositeljima odluka da detaljno analiziraju podatke i po potrebi postavе interventne mjere kako bi se izbjegle ili umanjile neželjene posljedice i pripremile se za učinkovit odgovor. Ovi sustavi mogu prikupljati, pohranjivati, analizirati i širiti informacije u

svrhu razumijevanja i mapiranja opasnosti. Kao praćenja i predviđanja nadolazećih događaja, obrade i širenja razumljivih upozorenja političkim vlastima i stanovništvu, te poduzimanja odgovarajućih i pravovremenih radnji kao odgovor na upozorenja [7].

4. METODOLOGIJA PROVEDBE ISTRAŽIVANJA

Digitalna forenzika je relativno nova znanost koja postaje sve važnija kako kriminalci koji su upućeni u tehnologiju koriste računala i uređaje u svojim nezakonitim aktivnostima. Dokazana kompetencija u digitalnoj forenzici zahtijeva raznoliko znanje i skup vještina koji uključuje dubinsko razumijevanje računalnog hardvera i softvera, računalnih mreža, forenzičke znanosti, primjenjivih lokalnih, državnih i nacionalnih zakona, kao i sposobnost komuniciranja u verbalnom i pisanom obliku.

4.1. Osnovni pojmovi

Zbog sveprisutnosti digitalnih medija i njihove upotrebe u kriminalnim aktivnostima, provedbi zakona, poslovanju i industriji, zajednica forenzičkih znanosti postala je sve svjesnija važnosti digitalne forenzike i činjenice da se njome treba baviti kao strukom i znanošću s obzirom na njegovu važnost u mnogim sudskim predmetima. Ključno je da oni uključeni u obnavljanje, ispitivanje i očuvanje digitalnih dokaza imaju potrebnu obuku i obrazovanje kako bi se učinkovito nosili s rastućom količinom dokaza s kojima će se susresti. Neki od bitnijih pojmova za provedbu istraživanja su [38]:

- digitalni forenzičar
- prikupljanje potencijalnih dokaza
- identifikacija dokaza
- analiza dokaza
- redoslijed operacija forenzičke istrage.

a) Digitalni forenzičar

Postoji niz pozicija poslova za koje netko s iskustvom u digitalnoj forenzici može biti kompetentan. Najčešća pozicija je pozicija ispitivača digitalne forenzike. Iako se stvarna titula digitalnog forenzičara najvjerojatnije može pronaći u policiji. Dok zaposlenici u privatnom sektoru obavljaju te iste zadatke pod različitim imenima, kao i konzultanti. Jedna od najvažnijih kvaliteta forenzičara je sposobnost pisanja detaljnog izvješća o korištenim postupcima i nalazima ispitivanja na tehnički i ne tehnički način kako bi mogli točno posvjedočiti o nalazima na sudu pred porotom.

Postoji pet ključnih kompetencija povezanih s određivanjem kompetencija u digitalnoj forenzici. Te su kompetencije podijeljene prema primarnim zadacima s kojima se ispitivač susreće, a ti opći zadaci uključuju [38]:

- sposobnost identificiranja i prijenosa medija koji mogu sadržavati dokaze.
- sposobnost stvaranja forenzički ispravne kopije medija i njezine provjere, kao i pregleda medija bez mijenjanja njegovog sadržaja.
- s obzirom na različite kriterije, sposobnost povrata dokaza koji zadovoljavaju kriterije.
- sposobnost donošenja tumačenja i zaključaka u vezi s pronađenim dokazima.
- sposobnost učinkovitog i točnog svjedočenja na sudu.

Posao ispitivača digitalne forenzike zahtijeva različita znanja i vještine. Kompetentan ispitivač mora biti u stanju pokazati tehničko razumijevanje različitih vrsta računalnog hardvera, računalnih mreža, operativnih sustava, datotečnih sustava i raznih vrsta aplikacijskog softvera. Kao i razumijevanje lokalnih, državnih zakona koji mogu doći u obzir tijekom istrage kriminala povezanog s računalom.

b) Prikupljanje potencijalnih dokaza

Od ključne je važnosti da ispitivači mogu identificirati sve digitalne uređaje koji mogu pohraniti potencijalne dokaze. Ovaj popis uključuje unutarnje računalne tvrde diskove, vanjske tvrde diskove, *flash* memorijske kartice, mobilne telefone, diskete, bežične mrežne pristupne točke, igraće konzole itd. Nakon identificiranja medija, ispitivač mora biti u mogućnosti stvoriti „forenzički“ zvučnu kopiju medija bez mijenjanja sadržaja medija [38]. Ispitivač mora moći demonstrirati ove postupke na mjestu zločina izravno, preko mreže i u laboratoriju ako je medij zaplijenjen. Ključno je da ispitivač ne prekrši važeće zakone tijekom procesa oporavka medija. Ispitivač mora pokazati poznavanje naloga, suglasnosti, naloga za otkrivanje i sudskih poziva. Ovo je ključno jer svi zakoni, bilo namjerno ili nenamjerno, koje je prekršio ispitivač mogu dovesti do izuzimanja dokaza od strane suca, što bi dovelo do odbacivanja predmeta.

Ispitivač će možda morati otvoriti računalo kako bi imao izravan pristup tvrdom disku, kako bi utvrdio koliko je pogona instalirano i utvrdio jesu li neki dokazi skriveni unutar računala. Ispitivač mora razumjeti kako prepoznati specifične postavke računala, kao što su serijski brojevi, postavke kratko spojnika na tvrdom disku, identifikatori mrežne kartice itd [38]. Ispitivač mora razumjeti kako ispitati sadržaj medija na scene kako bi se utvrdilo ima li na mediju ikakvih dokaza, što se često naziva pregledom na licu mjesta.

c) Identifikacija dokaza

Svrha forenzičkog ispitivanja je identificirati potencijalne dokaze koji se nalaze na digitalnom mediju. S obzirom na raznolikost digitalnih dokaza, kompetentan ispitivač mora razumjeti tehnologije i primjene. Gdje su informacije pohranjene, u kojem su formatu pohranjene i svi posebni postupci koji bi mogli biti potrebni za oporavak informacija [38]. Ispitivači moraju pokazati razumijevanje više verzija svake vrste aplikacije. Ispitivači bi trebali razumjeti različite vrste posebnih datoteka koje se mogu nalaziti na medijima, uključujući kako ih identificirati i prevesti ako je potrebno. Ove posebne datoteke uključuju zlonamjerni softver, datoteke prikrivene enkripcijom, steganografiju i programe za sigurno brisanje.

Ispitivači moraju biti upoznati s nizom alata, uključujući komercijalne kao i softverske alate otvorenog koda. Uobičajeni zadaci ispitivanja za oporavak dokaza uključuju stvaranje digitalnih otisaka prstiju datoteka za provjeru autentičnosti ili osiguranje integriteta podataka, traženje datoteka pomoću različitih kriterija uključujući ključne riječi, datumske i vremenske oznake, te razumijevanje koncepta vlasništva podataka i povijesti.

Ispitivači moraju razumjeti razliku između logičke i fizičke analize digitalnih medija, kao i pokazati koje se vrste informacija mogu prikupiti iz svake od njih. Podaci na logičkoj razini pregledavaju podatke sa stajališta datotečnog sustava i uključuju sve datoteke koje su

trenutno dodijeljene i praćene od strane datotečnog sustava [38]. Podaci na fizičkoj razini gledaju medij za pohranu kao jednu veliku datoteku i uključuju dodijeljene datoteke, kao i izbrisane datoteke.

d) Analiza dokaza

Konačni skup znanja i vještina uključuje razumijevanje zakona i postupaka, istražnih i tehničkih analitičkih praksi. Ključno je da ispitivač ima široku istraživačku svijest o okolnostima koje okružuju slučaj jer to može diktirati vrste dokaza koji su važni za predmet. Također je važno da ispitivač razumije što ne zna o predmetu i da zna kamo otići kako bi prikupio informacije koje mogu pomoći u identificiranju i povratu dokaza. Također moraju biti u stanju donositi zaključke na temelju dokaza koje pronađu. Ispitivači moraju biti u stanju identificirati izvore elektroničke pošte, trenutnih poruka i drugih komunikacija. Slučajevi mogu zahtijevati postavljanje događaja na vremensku traku i objašnjenje ispitivača kako operacijski i datotečni sustavi dodjeljuju datumske i vremenske oznake [38]. Ispitivači moraju unutar razumnih granica biti u mogućnosti pripisati digitalne artefakte određenom korisniku, lokaciji ili događaju.

Digitalni dokazi prikazuju različite razine volatilnosti. Naprimjer, računalna memorija čijem se sadržaju može izravno pristupiti (engl. *Random Access Memory* – RAM) će nestati nakon što se računalo isključi, a također će biti izgubljene sve informacije vezane uz mrežu. Vraćanje nepostojanih dokaza je moguće, međutim čin vraćanja dokaza će u većini slučajeva promijeniti sadržaj dokaza, a to se posebno odnosi na RAM [38].

e) Redoslijed operacija forenzičke istrage

Istražitelji slučaja i digitalnog mjesta zločina trebali bi razgovarati o rezultatima prikupljanja obavještajnih podataka i razviti strategije za postupanje ne samo s vjerojatnim scenarijem nego i opcijama ako se okruženje promijeni ili se utvrdi da nije očekivano. Potrebno je pažljivo odvagati pitanja kao što su vrijeme pretrage i ljudstvo ponašanje. Vrlo je važno da istražitelji slučaja i digitalnog mjesta zločina imaju zajedničko razumijevanje ciljeva potrage, prioriteta i tko će biti odgovoran za donošenje odluka na mjestu zločina. Cilj faze planiranja je razvoj „Operativnog naloga“ koji se koristi za informiranje sudionika procesa, dodjeljivanje odgovornosti i upravljanje mjestom događaja. Mnoge agencije za provedbu zakona imaju standardizirane obrasce. Ako standardizirani format ne postoji, istražitelj bi trebao razmotriti njegovo razvijanje [38].

Tijekom forenzičke istrage potrebno je obratiti pažnju na nekoliko stvari.. Zaštititi fizičko mjesto događaja, tražiti dokaze, ispitati subjekte i svjedoke, a cijeli proces dokumentirati. Uz uključivanje digitalnih istražitelja, važno je odrediti specifične odgovornosti za svakog sudionika u istrazi i gdje se uklapaju u obradu mjesta događaja.

Nakon što su obavještajni podaci prikupljeni i planiranje završeno, važno je prikupiti ljude i opremu potrebnu za istragu. Ovisno o složenosti planirane istrage, istražitelj može zatrebati dodatno osoblje za pomoć u procesu istrage. Uz to, jedan od najvrjednijih resursa koje istražitelj može donijeti na mjesto događaja je adresar s kontakt podacima tehničkih stručnjaka

[38]. Ako planirana istraga ima određene probleme, bilo bi mudro potražiti stručnjake za to područje koji će se staviti na raspolaganje tijekom istrage. Potreba za specijaliziranom opremom i alatima jedan je od aspekata koji digitalna mjesta istrage izdvajaju od ostalih istraga.

4.2.Primjena tehnika mrežnog praćenja

Koncept potpune online anonimnosti izuzetno je teško postići uz korištenje skupa alata i taktika za prikriivanje bilo kakvog traga koji mogu prekriti identitet ili čak vrstu hardvera i veze koja se koristiti za pristup internetu jer zahtijeva ozbiljne tehničke vještine. Slučajevi vezani uz nacionalnu sigurnost ili inozemnu špijunažu zahtijevaju razinu anonimnosti i obično ih vode sigurnosne agencije koje dobro znaju kako prikriti svoje aktivnosti. Ali u svrhu provođenja redovitih aktivnosti prikupljanja OSINT-a, potrebno je postati anonimn do odgovarajuće razine kako subjekt ne bi otkrio da se pokušavaju izvući informacije o njemu. Kako bi se saznalo što više podataka o subjektu, postoje nekoliko mrežnih praćenja, a to su [39]:

- praćenje IP adrese
- praćenje kolačića
- praćenje oznake entiteta
- praćenje tražilice
- praćenje društvenih mreža.

a) Praćenje IP adrese

Računalni uređaj ne može pristupiti internetu bez adrese internetskog protokola (engl. *Internet protocol* - IP). Ona je jedinstveni identifikator koji identificira bilo koji uređaj sposoban za internet kada se spaja na IP mrežu. Dva uređaja ne mogu posjedovati istu IP adresu na istoj IP mreži, zbog čega je IP adresa prvi izbor za mrežne tragače kada prate korisnike na mreži. Kada se korisnik povezuje na internet, svaki put koristiti istu IP adresu, tj. statičku IP adresu [39].

Statička IP adresa je adresa koju dodjeljuje pružatelj internetskih usluga i ne mijenja se tijekom vremena. Statičke adrese obično koriste tvrtke, javne organizacije i tvrtke koje nude telekomunikacijske usluge pojedincima i privatnom sektoru. Dok dinamičku IP adresu dinamički dodjeljuje pružatelj internetskih usluga kad god se korisnik spoji na internet. Koristi protokol za dinamički poslužiteljsku konfiguraciju protokola (engl. *Dynamic Host Configuration Protocol* - DHCP) kako bi dodijelio novu IP adresu svaki put kada se računalni uređaj ili usmjerivač ponovno pokrene.

Također potrebno je imati na umu da se IP adresa može sakriti kada se poveže na mrežu i to korištenjem različitih tehnika kao što su virtualna privatna mreža (engl. *Virtual Private Network* – VPN) i mreže anonimnosti poput mreže (engl. *The Onion Router* – TOR). Korisnik također može sjediti iza usmjerivača gdje se dijeli jedna javna IP adresa za sve računalne uređaje koji pripadaju istoj mreži [39]. Iz tih razloga se ne može smatrati da je IP adresa sama po sebi dovoljna da se razlikuju pojedinačni korisnici na internetu, ali i dalje ostaje prvi izbor za praćenje ljudi na mreži.

b) Praćenje kolačića

Kolačići su najčešća tehnika za praćenje korisnika na mreži, kolačić je mala tekstualna datoteka stvorena kada korisnik posjeti određenu internetsku stranicu. Standardne informacije sadržane unutar nje uključuju jedinstveni broj koji razlikuje uređaj klijenta, datum isteka i naziv internet stranice kolačića. Kolačić se koristi za razlikovanje klijentskog uređaja kada se ponovno vrati na istu internetsku stranicu. Internetske stranice koriste kolačiće uglavnom u dvije svrhe:

- pohranjivanje vjerodajnica za prijavu i
- praćenje ponašanja korisnika na mreži [39].

Kolačić je jednostavna tekstualna datoteka koja se koristi za praćenje posjeta korisnika internet stranici koja ga je postavila. Kolačići bez datuma isteka automatski se brišu kada se preglednik zatvori. Postoje uglavnom dvije vrste kolačića s obzirom na njihov vijek trajanja:

- sesijski i
- trajni kolačići [39].

Sesijski kolačić pohranjuje se u privremenu memoriju i briše se kada korisnik zatvori preglednik, ova vrsta kolačića nema datum isteka i ne pohranjuje nikakve informacije o korisničkom klijentskom uređaju. Obično se koristi za održavanje sadržaja košarice za kupnju na internet stranicama e-trgovine.

Trajni kolačić može izazvati zabrinutost za privatnost korisnika. Polovica sadržaja kolačića prve strane pripada stranici koja se posjećuje, a polovica treće strane pripada partnerima, uslugama ili oglašivačima koji rade na stranici [39]. Kolačići treće strane koriste se za praćenje aktivnosti i prepoznavanje čestih i ponovnih posjetitelja, za optimizaciju oglašavanja ili za poboljšanje korisničkog iskustva prilagođavanjem sadržaja ili ponuda na temelju povijesti tog kolačića.

c) Praćenje oznake entiteta

Oznaka entiteta su još jedan način praćenja korisnika bez korištenja kolačića, pohrane ili IP adresa. Oznaka entiteta dio je mehanizma protokola za prijenos hiperteksta koji omogućuje provjeru valjanosti predmemorije *weba* i namijenjen je kontroli koliko dugo je određena datoteka pohranjena u predmemoriju na strani klijenta [39].

Oznake entiteta pomažu internet pregledniku da izbjegne učitavanje istih internet resursa dvaput, kao kada korisnik posjeti internet stranicu koja u pozadini svira glazbu koja se mijenja prema lokalnom vremenu korisnika. Prilikom prvog posjeta, internet poslužitelj će poslati oznaku entiteta zajedno sa audio datotekom klijentskom pregledniku, koji će preuzeti audio datoteku i spremiti je u predmemoriju. Kada korisnik ponovno posjeti istu internetsku stranicu, internet poslužitelj će obavijestiti klijentski preglednik da se audio datoteka nije promijenila [39]. Kao rezultat toga, preglednik će koristiti lokalnu kopiju u predmemoriji, štedeći propusnost i ubrzavajući vrijeme učitavanja. Ako je oznaka entiteta drugačija, preglednik klijenta preuzima novu verziju audio datoteke. Oznake entiteta se mogu iskoristiti za praćenje

korisnika na sličan način kao trajni kolačići, a poslužitelj za praćenje može neprestano slati oznake entiteta klijentskom pregledniku, iako se sadržaj ne mijenja na poslužitelju. Tako poslužitelj za praćenje može održavati sesiju s klijentskim strojem koja traje neograničeno dugo [39].

d) Praćenje tražilice

Tipične tražilice kao što su *Google*, *Yahoo!* i *Bing* poznato je da prate pretraživanja svojih korisnika kako bi ih ciljali prilagođenim oglasima i prilagodili vraćene rezultate pretraživanja. Naprimjer, većina korisnika *Google* tražilice posjeduje *Gmail* račun kada korisnik provodi online pretraživanja koristeći *Google* dok je prijavljen na *Gmail* račun, online aktivnost korisnika bit će zabilježena i povezana s njegovim *Gmail* račun.

Čak i ako se korisnik nije prijavio na *Gmail* račun, *Google* i dalje može povezati povijest pregledavanja korisnika s njegovim ili njezinim stvarnim identitetom koristeći bilo koju od prethodno spomenutih tehnika praćenja [39]. Mjesta za društveno umrežavanje kao što su *Facebook* i *Twitter* mogu pratiti online korisnike na različitim internetskim stranicama iako ti korisnici trenutno nisu prijavljeni na svoje povezane račune.

4.3. Scenarij istraživanja osobe od interesa

OSINT istraživanja usmjerena su isključivo na podatke koji su javno dostupni. Postoje mnoge nijanse u području OSINT-a, uključujući vrstu podataka koji se mogu prikupiti i vrstu platformi koje se mogu koristiti za dobivanje podataka. Također, važno je razumjeti da OSINT uključuje sve platforma društvenih mreža. Mjesta za društveno umrežavanje, poput *Facebooka* i *LinkedIna*, čine samo jedan dio platformi koje se mogu koristiti za prikupljanje podataka. Informacije se mogu pronaći na stranicama kao što je *Instagram*, forumima kao što je *Reddit*, stranicama za razmjenu slika kao što je *Pinterest*, stranicama za dijeljenje videa kao što je *YouTube*, platformama za objavu blogova kao što je *Twitter*, platformama za društvene igre kao što je *Xbox Live* i ostalim društvenim mreža. Nadalje, postoje tri vrste informacija koje se mogu prikupiti s platformi društvenih mreža. Ove informacije mogu se podijeliti u tri kategorije:

a) Informacije o profilu

Statične informacije o određenom korisniku koje mogu vidjeti oni koji pristupaju profilu. To može uključivati radno mjesto korisnika, sadašnje i bivše poslodavce, vještine i podatke za kontakt [40].

b) Interakcije

Korisnici na platformi društvenih medija mogu komunicirati s platformom ili drugim korisnicima na mnogo načina. Ovi oblici interakcije uključuju objavljivanje, komentiranje, odgovaranje na tuđi sadržaj i reagiranje na postojeći sadržaj [40].

c) Metapodaci

Podaci koji se nalaze na platformama društvenih mreža nisu ograničene na tekst i slike. Također može uključivati kontekstualne informacije o navedenim dijelovima sadržaja.

Metapodaci mogu uključivati lokaciju označenu u objavi, vrijeme kada je objava objavljena ili čak vrstu uređaja korištenog za snimanje fotografije. Ono što se može pronaći na društvenim mrežama uvelike ovisi o pojedincu ili subjektu koji se istražuje i o samoj platformi. Neki, kao što je *LinkedIn*, po svojoj zamisli imaju korisničku bazu koja želi biti pronađena i želi koristiti svoj profil za prikazivanje svog profesionalnog iskustva. Drugi, poput *Twittera*, imaju profile koji mogu biti manje informativni, ali mogu pružiti više konteksta u sadržaju objava objavljenih na računima [40].

Prvi korak istrage subjekta na društvenim mrežama je pronalazak korisničkog računa subjekta istrage. To se može učiniti identifikacijom najmanje pet točaka pomoću kojih se mogu povezati korisnički računi i ostali podaci na društvenim mrežama, a tih pet točaka su:

a) Ime

Ime osobe je dobra polazna točka jer će često vratiti *Facebook*, *Myspace* ili *LinkedIn* račun. Međutim, to je također prvi osobni identifikator koji će ljudi izbjegavati koristiti ili otkriti ako ne žele da ih se pronađe [40].

b) Elektronička adresa i broj telefona

Ovo su sjajne početne točke jer se obično dijele samo između računara, a time i pojedinaца koji su na neki način povezani. Dakle, ako dva računara na različitim platformama dijele isti telefonski broj ili adresu elektroničke pošte, to znači da postoji veza između njih. Problem s tim točkama podataka je taj što ih obično nije lako pretraživati i ne prikazuju se na profilu osobe od interesa [40].

c) Korisničko ime

Često se ponavlja i koristi se na različitim platformama društvenih mreža. Prednost ovih podataka je u tome što ih je iznimno lako pretraživati. Bilo koja platforma društvenih mreža koja ima korisnička imena omogućuje pretragu korisnika, budući da je to često temeljni koncept platforme [40].

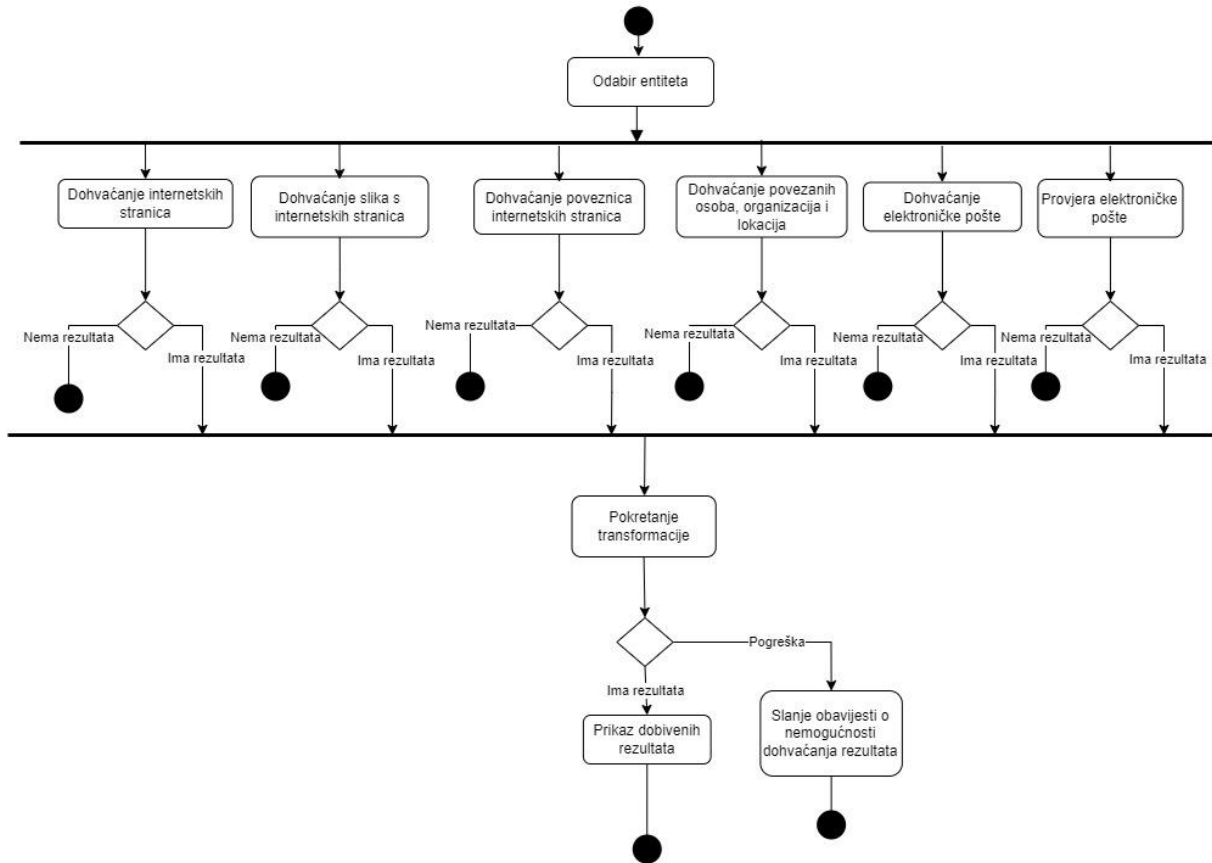
d) Profilne slike

Profilne slike spadaju u istu kategoriju kao i korisničko ime, što znači da bi obrnuto pretraživanje slike od slike pronađene na profilu moglo dovesti do računara kojim upravlja ista osoba [40]. Međutim, također se može dogoditi da dvije različite osobe imaju istu sliku profila. Pretraživanje računara sa slikom kao polaznom točkom je mnogo teže jer se potrebno osloniti na tražilice obrnutih slika, što obično nije značajka koju podržavaju platforme društvenih mreža.

e) Adresa

Adresa je najteži početni pojam za istraživanje. Rijetko će netko otkriti svoju fizičku adresu na društvenim mrežama. Veća je vjerojatnost da će platforme koje skupljaju online informacije kao što je *Pipl* omogućiti istražitelju da se okrene prema toj vrsti informacija [40].

S obzirom na gore spomenute točke za pronalazak računa na društvenim mrežama, potrebno je i definirati scenarij analize digitalnog otisaka primjenom programskog alat Maltego gdje će se pristupiti istraživanju osobe od interesa. Kako bi se preglednije mogli pratiti koraci istraživanja izrađen je dijagram aktivnosti koji je prikazan na slici 5.



Slika 5. Dijagram aktivnosti scenarija istraživanja osobe od interesa

Programski alat Maltego i dodaci programu pružit će transformacije za povlačenje većine podataka dostupnih na profilu izravno u grafikon. To će uštedjeti puno vremena jer bi puno vremena oduzelo kada bi istražitelj sam morao pregledati i prikupiti javno dostupne podatke. Međutim, transformacije dostupne u Maltegu možda neće moći dohvatiti sve podatke dostupne na platformi. Ukoliko se želi dublje pregledati profil, potrebno ga je pogledati na samoj platformi društvenih mreža, iz aplikacije ili iz internetskog preglednika.

5. ANALIZA DIGITALNIH OTISAKA PRIMJENOM PROGRAMSKOG ALAT MALTEGO

Kada je riječ o online pretraživanju informacija kao što su zapisi naziva domena, internet stranice i zapisi elektroničke pošte. Jedan od alata koji može prikazati tražene informacije u grafičkom smislu kojega je lako razumjeti je Maltego. Maltego je alat koji omogućuje prikupljanje informacija na smislen način. Može potražiti nazive domena, mrežne blok adrese povezane s njima i razmjene pošte (engl. *Email exchange* - MX) zapise. Sa samo nekoliko klikova mišem može identificirati ključne odnose između objekata umetnutih u prikaze grafa. Prednost Maltega je to što može demonstrirati složenost i ozbiljnost pojedinačnih podataka. Također može locirati, prikupiti i vizualizirati te podatke. A nekoliko ključnih točaka gdje se programski alat može koristiti [41]:

- može se koristiti za fazu prikupljanja informacija u svim poslovima povezanim sa sigurnošću.
- pomaže u procesu razmišljanja vizualno pokazujući međusobno povezane veze između pretraženih stavki.
- pruža mnogo snažnije pretraživanje, dajući pametnije rezultate.

5.1. Sučelje programskog alata Maltego

Trenutno postoje tri verzije programskog alata Maltego klijenta, a to su Maltego CE, Maltego Classic i Maltego XL. Sve tri verzije Maltego-a imaju pristup biblioteci standardnih transformacija za otkrivanje podataka iz raznih javnih izvora koji se obično koriste u online istraživanju i digitalnoj forenzici [20]. Za potrebe ovog diplomskog rada koristiti će se Maltego CE koji je dostupan besplatno nakon brze online registracije. Maltego CE sadrži većinu istih značajki kao i komercijalna verzija, ali ima neka ograničenja. Glavno ograničenje verzije zajednice je da se aplikacija ne može koristiti u komercijalne svrhe, a postoji i ograničenje maksimalnog broja jedinica koje se mogu vratiti iz jedne transformacije. Maltego se može koristiti za određivanje odnosa između sljedećih stavaka:

- čovjeka,
- imena,
- e-mail adrese,
- grupe ljudi,
- društvene mreže,
- tvrtke,
- internetske stranice.

Također Maltego se koristi za određivanje odnosa internetske infrastrukture kao što su [42]:

- domene,
- mrežni blok,
- IP adrese,
- veze,

- dokumenti i datoteke.

Veze između ovih podataka pronalaze se korištenjem tehnika OSINT-a, postavljanjem upita izvorima kao što su sustavi domenskih imena (engl. *Domain Name System* – DNS), tražilice, društvene mreže i ekstrakcija metapodataka. Za analizu će se koristiti Maltego CE, koji nudi sljedeće značajke [42]:

- analiza poveznica do 10.000,00 objekata u jednom dijagramu,
- moguće je vratiti do 12 jedinica po izvršenoj transformaciji,
- čvor zbirke koji automatski grupira entitete sa zajedničkim karakteristikama i pronalazi tražene ključne odnose
- mogućnost dijeljenja grafikona u stvarnom vremenu i s više analitičara u jednoj sesiji,
- opcije za izvoz grafike kao što su popisi entiteta,
- opcije za uvoz grafike kao što su formati tablica.

Te se informacije zatim prikazuju u grafikonu temeljenom na čvoru. Takav vizualni prikaz najprikladniji je za analizu veza. Gdje se stvarni odnosi između ljudi, internetskih stranica, domena i drugih objekata mogu lakše analizirati.

Koncept Maltego-a sastoji se od kombinacije entiteta, transformacija i strojeva. Entiteti su stvarni objekti, poput osobe, DNS zapisa, telefonskog broja i adrese elektroničke pošte. Entitet je vizualno predstavljen kao čvor na grafikonu. Međutim, moguće je kreirati i vlastite entitete.

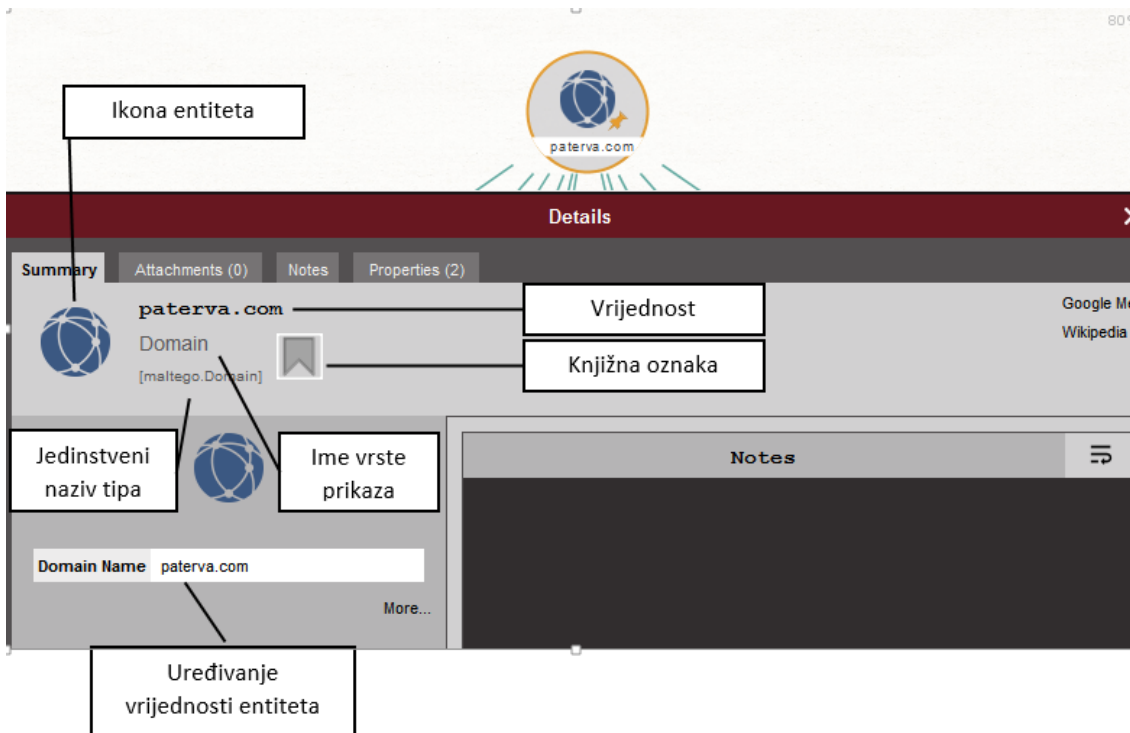
Transformacije predstavljaju odnose između entiteta. To se postiže postavljanjem upita izvoru podataka i vraćanjem rezultata kao novog entiteta na grafikone. Izvori podataka su mjesta kao što su DNS poslužitelji, tražilice, društvene mreže, informacije, vlastite baze podataka itd. Dok strojevi sastavljaju transformacije pomoću skripte za inteligentnu automatizaciju zadataka. Zatim se pokreću potpuno samostalno ili čekaju na unaprijed definiranim točkama za interakciju s korisnikom [42].

Entiteti u Maltego-u koriste se za predstavljanje različitih vrsta informacija. Na dijagramu su predstavljeni kao čvorovi. Svi entiteti dostupni u Maltego-u nalaze se u paleti entiteta koja se standardno nalazi na lijevoj strani grafikona. Entiteti su u paleti podijeljeni u grupe, a glavne kategorije su Infrastruktura i Osobno.

Postoje tri aspekta entiteta [42]:

- tip koji je vrsta informacija koje predstavljaju entitet,
- vrijednost je polje primarnih informacija entiteta,
- svojstva koje predstavlja polje s dodatnim informacijama za entitet.

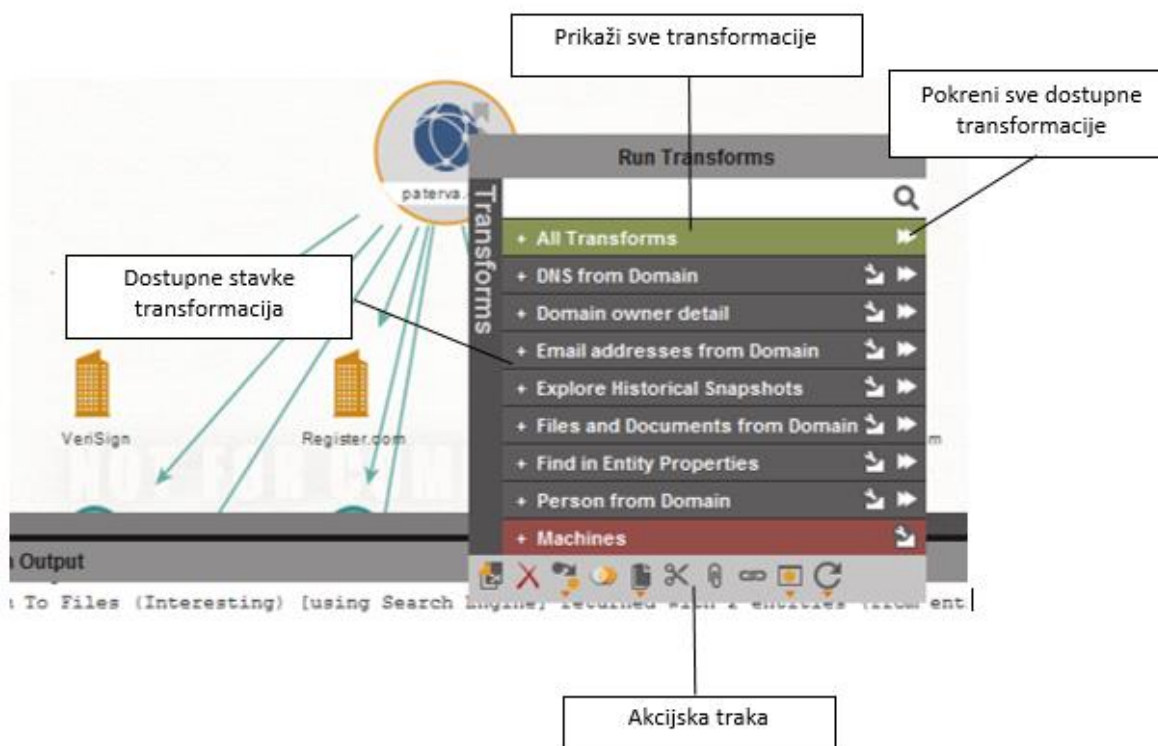
Kartica *Summary* prva se pojavljuje kada se otvori prozor detalji entiteta. Kartica sadrži sažetak svih entiteta koji se detaljnije mogu pronaći u karticama u prozoru Entitet koji je predložen od strane programskog alata Maltego, a slika 6. prikazuje sažetak entiteta domene.



Slika 6. Stranica sažetka entiteta domene

Kontekstni izbornik omogućuje izvođenje transformacije za odabrane objekte u dijagramu. Desnim klikom na entitet ili grupu entiteta prikazuje se kontekstni izbornik. Kontekstualni izbornik podijeljen je na tri različite razine, najvišu razinu, razinu postavljanja i razinu transformacije [42].

Najviša razina kontekstnog izbornika navodi različite stavke čvorišta transformacije koje su instalirane. Ako Maltego ima instaliran samo jedan unos za *Transform Hub*, kontekstni izbornik će se otvoriti na postavljenoj razini. Dok se razina postavljanja koristi za grupiranje transformacija u kategorije koje obavljaju slične zadatke i se često izvode zajedno. Razina transformacije kontekstnog izbornika mjesto je s kojeg se izvršavaju transformacije [42]. Ako se lijevom tipkom miša klikne na jednu transformaciju, ona će se izvršiti. Prikaz pokretanja transformacija prikazano je na slici 7. Klikom na ikonu konfiguracije u retku za transformaciju otvara se upravitelj transformacija. *Transform Manager* prikazuje više informacija o transformaciji i omogućuje konfiguriranje postavki. Klikom na simbol zvjezdice u liniji transformacije dodaje se u favorite, koji su uvijek navedeni na vrhu kontekstnog izbornika kao zasebna kategorija, bez obzira na kojoj se razini kontekstnog izbornika nalazi.



Slika 7. Dostupni skupovi entiteta domene

Transformacije su operacije koje se izvršavaju nad informacijama koje se pretražuju odnosno entitetima preslikavajući ih u nove entitete koji su korisniji za dobivanje nekih ključnih informacija kao što su IP adrese, lokacije, brojevi telefona itd. Svaki entitet koji se nalazi u alatu Maltego posjeduje vlastiti set transformacija koji se izvršavaju na poslužitelju. Ovo je popis entiteta i bitnijih transformacija [43]:

- **Internet Autonomous System (AS)**

- a) *ASNumberToNetblocks_Robtex* - transformacija pokazuje koje su rute locirane unutar AS broja pregledavanja poslužitelja *RobTex*.

- **Domain Name System**

- a) *DNSNameToDomain_DNS* - izvlačenje svih imena domena iz DNS imena
- b) *DNSNameTOIPAddress_DNS* - pretvara DNS ime na IP adresu pomoću DNS protokola,
- c) *DNSNameTOWebsite_QueryPorts* - transformacija određuje je li DNS ime *web* sjedišta te ukoliko se radi o *web* sjedištu provjerava ima li aktivne HTTP priključke.

- **Internet Domene**

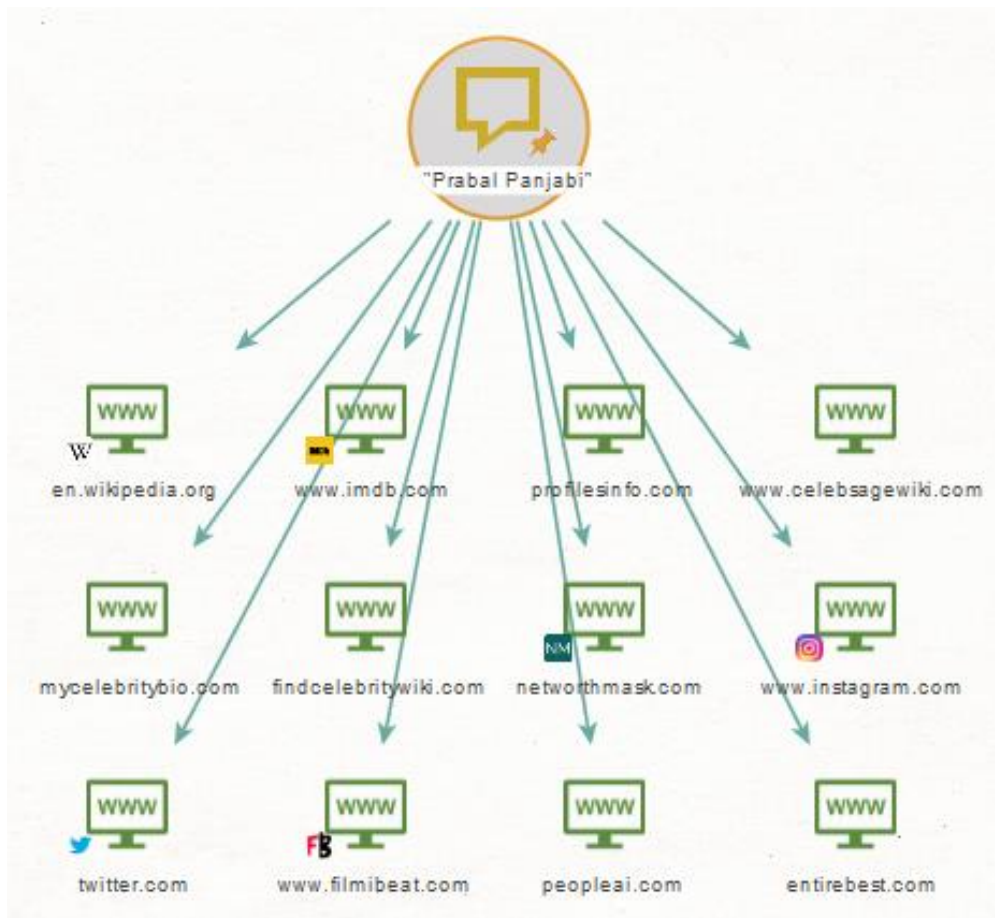
- a) *DomainToMXrecord_DNS* - pronalazi MX zapise za domenu,
- b) *DomainToNSrecord_DNS* - pronalazi NS (engl. *name server*) zapise za domenu,
- c) *DomainToDNSName_DNSBrute* - pokušava otkriti različita zajednička DNS imena unutar domene
- d) *DomainToEmailAddress_PGP* - transformacija kontaktira javni PGP (engl. *Pretty Good Privacy*) poslužitelj i vraća adresu elektroničke pošte koja sadrži danu domenu,

- e) *DomainToEntities Whois NER* - transformacija koja dohvaća informacije tko je prisutan na domeni te potom obrađuje entitete koristeći NER (engl. *Named Entity Recognition*).
- f) *Search Engine* - transformacija pretražuje lokaciju za zanimljivim dokumentima kao što su dokumenti *Microsoft Word* i *Excel* na *web* stranicama unutar domene.
- g) *DomainToPerson PGP* - kontaktira javni PGP poslužitelj i vraća entitet osobe koja je locirana na danoj domeni.
- h) *DomainToPhone Whois* - pretražuje domenu i nalazi telefonske brojeve korisnika na domeni.
- i) *DomainToWebsite DNS* - provjerava postoji li *web* stranica na domeni.
- **IPv4 (engl. *Internet Protocol version 4*) adrese**
 - a) *IPAddressToDNSName [SharedIP, SharedMX, SharedNS]* - skupina transformacija koja provjerava nasuprotnu provjeru nad IP adresama tako da pregledava *ServerSniff*, *Robtex*, *DNS*, *MX* i *NS* zapise.
 - b) *IPAddressToEmailAddress Whois*- transformacija nalazi informacije o IP adresi, zatim pretražuje adresu elektroničke pošte.
 - c) *IPAddressToNetblock NS4block* - transformacija kontaktira *Robtex* usluge i određuje ima li ikakvih *DNS* blokova koji su mu priključeni preko određene IP adrese.
 - d) *IPAddressToPhone Whois* - dohvaća telefonski broj povezan s IP adresom.
 - e) *Search Engine* - pretražuje Internet i prikazuje gdje se sve nalazi tražena IP adresa.
- **DNS zapis imena poslužitelja**
 - a) *NSrecordToDomain DNS* - dohvaća sve domene s *DNS* liste,
 - b) *NSrecordToDomain SharedNS* - dohvaća *NS* zapise pregledavajući *ServerSniff* i *RobTex* usluge. Kao nusproizvod dobivaju se netblokovi⁸ za koje je *NS* primarni poslužitelj,
 - c) *NSrecordToIPAddress_DNS* - *NS* zapis pretvara u IP adresu koristeći *DNS* protokol.
- **Website**
 - a) *WebsiteToEmailAddress Mirror* - transformacija koristi skriptu za izvlačenje adresa elektroničke pošte.
- **Email**
 - a) *EmailAddressToDomain DNS* - uklanja dio ispred znaka „@“ za danu adresu,
 - b) *EmailAddressToEmailAddress SignedPGP* - kontaktira javni PGP poslužitelj i vraća adrese elektroničke pošte potpisnika za danu adresu,
 - c) *EmailAddressToPerson Same PGP* - pretražuje javni PGP poslužitelj i vraća ime osobe za danu adresu,
 - d) *Search Engine* - pretražuje gdje se na Internetu pojavljuje tražena adresa elektroničke pošte,
 - e) *EmailAddressToEmailAddress* - provjerava postojanje adrese elektroničke pošte.
- **Person**
 - a) *PersonToEmailAddress SamePGP* - vraća adresu elektroničke pošte povezanu s osobom ukoliko postoji.
- **Phone Number**
 - a) *Search Engine* – pretražuje telefonski broj i vraća adresu elektroničke pošte povezanu s tim brojem.

5.2. Provođenje postupka analize osobe od interesa

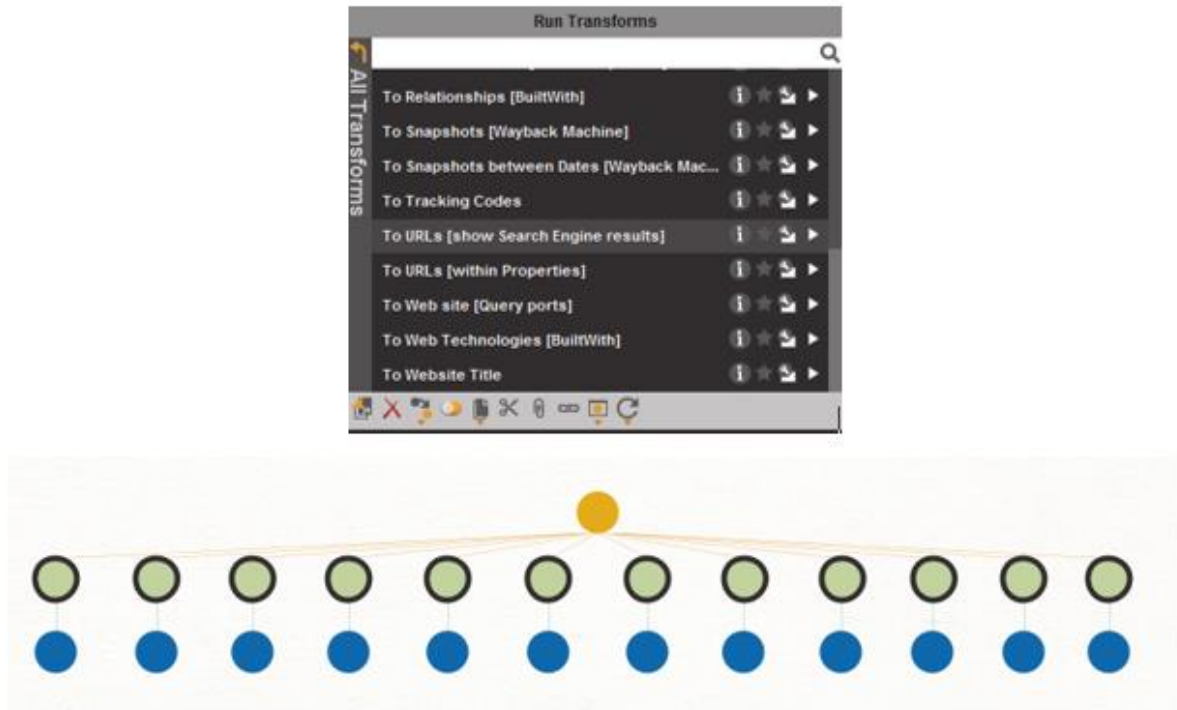
Uz programski alat Maltego, istražitelji mogu brzo i jednostavno povezati naizgled različite tragove i izgraditi sveobuhvatnu kartu digitalnog otiska ciljne osobe. Maltego je savršen alat za brzu analizu digitalne prisutnosti osobe od interesa koji je integriran s nizom OSINT-a, socijalne inteligencije i izvora podataka o identitetu.

U postupku analize provest će se istraga osobe od interesa na temelju imena „Prabal Panjabi“. Gdje će se pokušati pronaći svi *online* podaci osobe koristeći programski alat Maltego. Na slici 8. prikazan je entitet „Prabal Panjabi“ gdje je provedena transformacija koja će pretražiti zadani pojam i prikazati stranice na kojima se pojam pojavljuje.



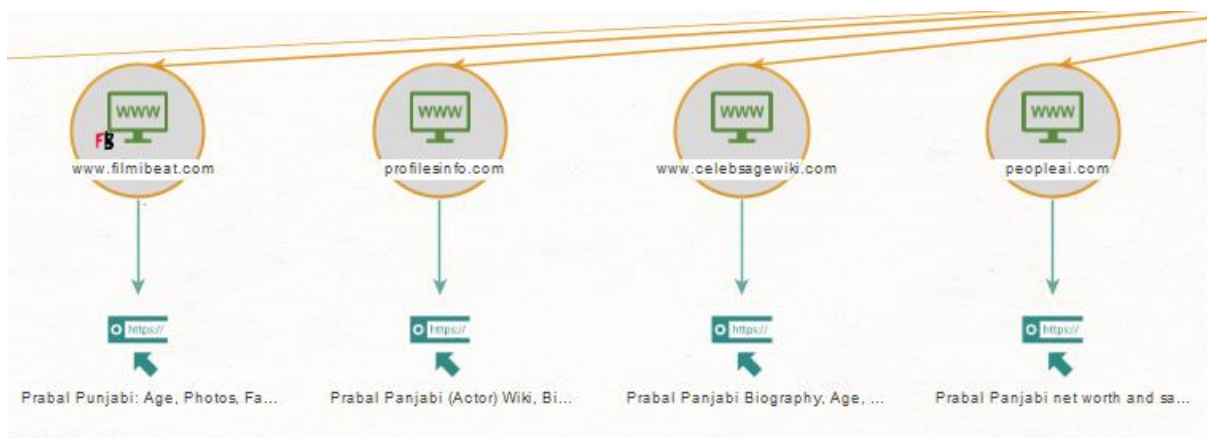
Slika 8. Transformacija To Website koja je izvedena nad definiranim entitetom

Transformacija *To Website* postavlja upit tražilici *Bing*, koja vraća sve internetske stranice koje spominju citirani pojam za pretraživanje. Pokretanje transformacije vratilo je 12 internetskih stranica, uključujući profile društvenih medija ili javne stranice kao što su Instagram, Wikipedia i baza podataka filmova (engl. *Internet movie database* – IMDB). Zatim se pokreće transformacija koja je vidljiva na slici 9. za URL-ove pomoću tražilice nad dobivenim entitetima internetskih mjesta kako bi se pronašli povezani URL-ovi.



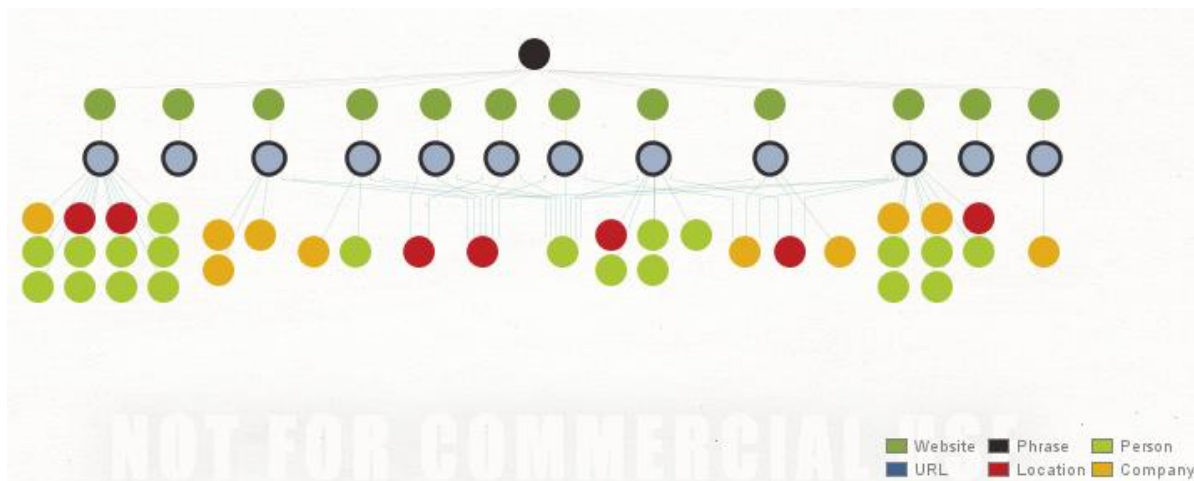
Slika 9. Dobiveni rezultati URL-ova za prethodne entitete internetskih mjesta

Iz rezultata koji su dobiveni na slici 9. i slici 10. može se primijetiti da je osoba od interesa za koju se provodi istraga glumac koji je povezan s nekoliko internetskih stranica.



Slika 10. Prikaz pojedinih entiteta vraćenih iz internetskih stranica

Zatim nakon dobivenih URL-ova internetskih stranica, pokreće se transformacija *IBM Watson*, koja će izdvojiti entitete poput organizacija, lokacija, adresa elektroničke pošte, ljudi i slika koje se nalaze na internetskim stranicama. Prikaz podataka koji se dobiju iz provedene transformacije vidljiv je slici 11., a na donjoj desnoj strani prikazana je legenda grafa kako bi se istraživač mogao bolje snaći u dobivenim rezultatima.



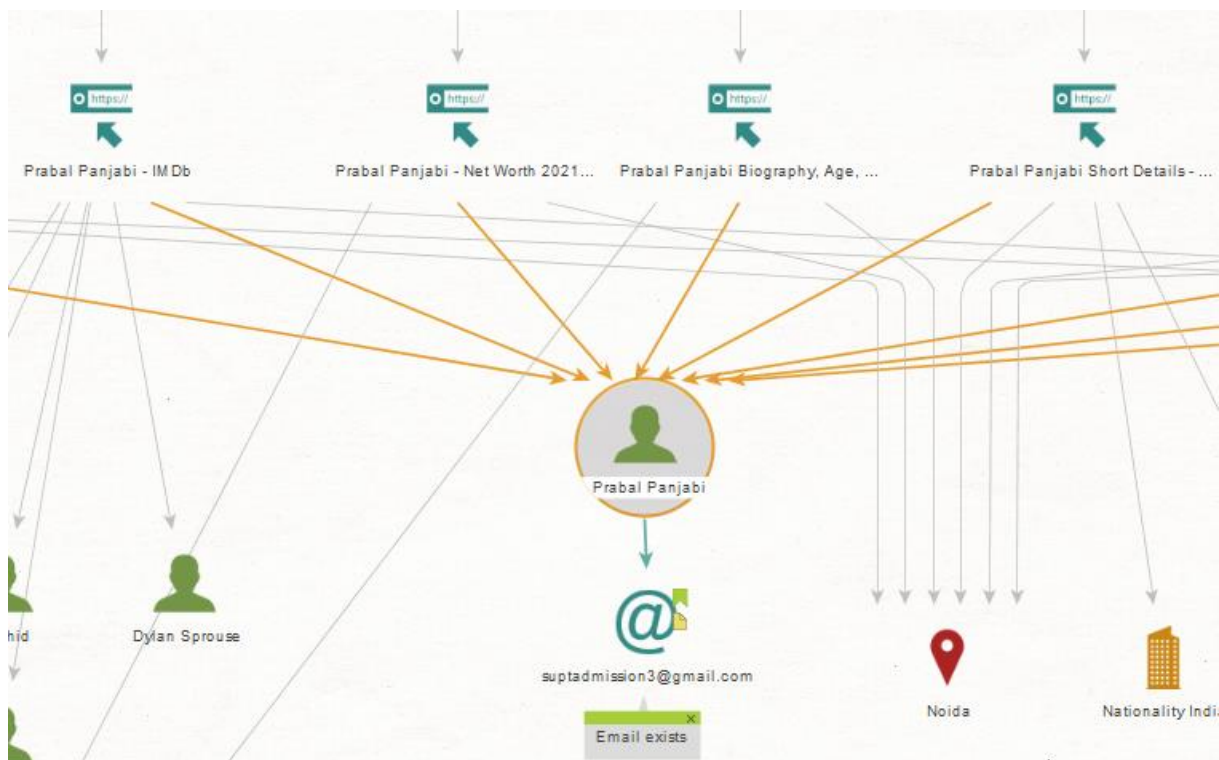
Slika 11. Prikaz dobivenih rezultata nakon transformacije IBM Watson

Nakon dobivenih rezultata putem transformacije *IBM Watson*, pokrenuta je transformacija *To Images* koja dohvaća sve slike iz dobivenog URL-a. Pojedini rezultati pretraživanja mogu se vidjeti na slici 12.



Slika 12. Rezultat transformacije To Images

Iz ovih rezultata transformacije došlo se do nekoliko zanimljivih otkrića. Naprimjer, osoba je povezana s tvrtkom *Bollywood* i Indijskim časopisem *Filmibeat*. Također osoba je povezana s nekoliko umjetnika koji se mogu vidjeti na slici 12. Transformacije su također vratile brojne slike koje mogu pomoći da se identificira osoba od interesa.



Slika 13. Prikaz entiteta koji povezuje sve internetske stranice

Najzanimljiviji rezultat koji je dobiven jest da entitet „Prabal Panjabi“ osoba povezana sa svim izvorima internetskih stranica, a isto je moguće vidjeti na slici 13. Također može se vidjeti da je provedena transformacija *To EmailAddress*, koja je dohvatila potencijalnu elektroničku adresu „Prabal Panjabi“. Uz nekoliko transformacija na grafikonu su dobiveni podaci koje je potrebno filtrirati i logičkim zaključivanjem pridružiti. Programski alat Maltego uvelike smanjuje vrijeme pretraživanja podataka, odlično povezuje dobivene rezultate i prikazuje mapu rezultata koji se mogu prilagoditi ovisno o želji istraživača.

Nakon prevedenog istraživanja potrebno je obratiti pozornost na dostupnost podataka o osobi o interesa, ali i drugim korisnicima interneta. Uz samo nekoliko transformacija moguće je doći do željenih podataka. Stoga je važno održavati „digitalnu higijenu“ na društvenim mrežama, ali i na svim internetskim mjestima na kojima korisnik dijeli svoje podatke. Postoje dvije vrste podataka koje se mogu pronaći na društvenim mrežama [44]:

- Podaci koje korisnik želi podijeliti
- Podaci koje je korisnik zaboravio sakriti zbog nedostatka brige za svoju privatnost.

Iako koncept „digitalne higijene“ postoji otkako su se računala mogla međusobno povezivati. Naravno, ono što čini dobru digitalnu higijenu razvija se baš kao i tehnologija koja se koristi za povezivanje terminalnih uređaja. Prakticiranje dobre „digitalne higijene“ uključuje redovito ažuriranje i čišćenje elektroničkih uređaja, korištenje lozinki koje slijede sigurnosne protokole, organiziranje datoteka pohranjenih na uređaju, optimiziranje postavki i još mnogo toga. To je način da digitalni uređaji koje koristi organizacija ne postanu žrtve kibernetičkog

kriminala. Ukoliko se uvelike želi smanjiti šanse za sigurnosnu prijetnju ili drugu digitalnu katastrofu potrebno je koristiti neke od sljedećih preporuka:

- Korištenje jake lozinke

Kako računala postaju brža, svladavanje jednostavnih lozinki postaje lakše. U idealnom slučaju, koristit će se dvofaktorska provjera autentičnosti, ali to ne negira potrebu za jakom lozinkom [44].

- Korištenje upravitelja lozinki

Jedan od glavnih razloga zašto ljudi koriste lozinke koje je lako probiti je taj što ih je također lako zapamtiti. Upravitelji lozinki olakšavaju pohranjivanje lozinki na siguran način tako da ih se ne mora pamtit svaki put kada se želite prijaviti na *web* mjesto [44].

- Antivirusni programi

Antivirusni programi mogu skenirati poznate prijetnje i zaštititi uređaje. Obavezno je redovito ažuriranje aplikacije kako bi bili u tijeku s prijetnjama koje se pojavljuju [44].

- Ažuriranje operativnog sustava

Ažuriranje operativnih sustava važno je za uklanjanje grešaka i dobivanje pristupa poboljšanim značajkama i funkcionalnostima. No osim toga, važno je jer svako ažuriranje poboljša sigurnosne prijetnje koje su otkrivene [44].

- Sigurnosne kopije datoteka









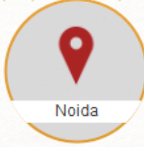
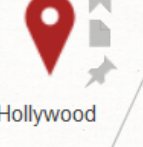
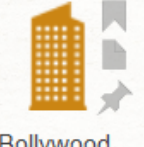




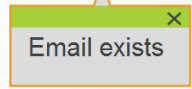
Postoji više prijetnji podacima. *Ransomware* može preuzeti kontrolu nad datotekama, prirodne katastrofe mogu uništiti opremu, tvrdi diskovi mogu otkazati. U svakom slučaju, gubitak pristupa datotekama u najboljem je slučaju smetnja, a u najgorem slučaju katastrofa. Čuvanje višestrukih sigurnosnih kopija vaših datoteka važna je zaštita od takve katastrofe [44].

- Korištenje sigurnih preglednika

Većina popularnih preglednika ima ugrađenu funkciju koja će upozoriti korisnika kada pristupi nepoželjnoj internetskoj stranici. Oni se često pojavljuju kada je sigurnosni certifikat istekao i ne može se jamčiti sigurnost stranice [44].

Nakon definiranih preporuka o važnosti „digitalne higijene“, prikazan je sistematički pregled dobivenih rezultata na temelju provedenog istraživanja osobe od interesa. U tablici 3. moguće je vidjeti dobivene rezultate nakon svake provedene transformacije.

Tablica 3. Prikaz dobivenih rezultata istraživanja

Provedene transformacije	Aktivnosti	Relevantni podaci istraživanja osobe od interesa
<i>To Website</i>	Dohvaćanje internetskih stranica	 www.imdb.com  www.filmibeat.com  en.wikipedia.org  www.veethi.com
<i>To URLs</i>	Dohvaćanje URL-ova	 Prabal Panjabi - IMDb  Prabal Panjabi - Wikipedia  Prabal Punjabi: Age, Photos, Fa...  Prabal Panjabi - Profile, Biogr...
<i>IBM Watson</i>	Dohvaćanje organizacija, lokacija i povezanih osoba	 Noida  Hollywood  Bollywood  Nationality Indian
<i>To Images</i>	Dohvaćanje slika	 /www.filmibeat.com/img/1  https://www.tvguide.com/a/img/r...
<i>To EmailAddress</i>	Dohvaćanje potencijale elektroničke adrese	 suptadmission3@gmail.com
<i>Verify email address exist</i>	Provjera elektroničke adrese	 Email exists

Kako bi se detaljnije prikazali rezultati istraživanja, u tablici 4. vidljivo je prvih 10 najbitnijih rezultata istraživanja osobe od interesa prema broju povezanih dolaznih linkova.

Tablica 4. Rezultati istraživanja osobe od interesa prema broju dolaznih linkova

Rangiranje rezultata	Tip	Relevantni rezultati istraživanja	Broj dolaznih linkovi
1	Osoba	Prabal Panjabi	8
2	Lokacija	Noida	6
3	Lokacija	Mujhse Fraaandship Karoge	3
4	Organizacija	Disney	3
5	Lokacija	India	2
6	Slika	https://secure.gravatar.com/avatar/11e2f2a43d0c781ed13267312ddf69cd?s=80&d=mm&r=g	1
7	Organizacija	Roku	1
8	E-mail adresa	suptadmission3@gmail.com	1
9	Organizacija	Wikimedia Foundation	1
10	Slika	https://entirebest.com/wp-content/uploads/2021/12/alun-armstrong-2.jpg	1

U tablici 5. prikazani su entiteti koji su na kraju istraživanja bili povezani s maksimalnim brojem linkova. S obzirom da je dobiveno 96 entitea i 112 linkova, izvojeni su samo bitniji podaci za pronalazak pouzdanih podataka o osobi od interesa.

Tablica 5. Prikaz prvih deset rezultata koji su pružili maksimalan broj linkova

Rangiranje rezultata	Tip	Entiteti	Maksimalan broj linkova
1	URL	Prabal Punjabi: Age, Photos, Family, Bio...	25
2	URL	Prabal Panjabi - Profile, Biography and ...	13
3	Entitet	"Prabal Panjabi"	12
4	URL	Prabal Panjabi - Wikipedia	11
5	URL	Prabal Panjabi Biography - EntireBest	9
6	Osoba	Prabal Panjabi	9
7	URL	Prabal Panjabi List of Movies and TV Sho...	8
8	URL	Prabal Panjabi - IMDb	8
9	URL	Prabal Panjabi Net Worth, Measurements, ...	6
10	Lokacija	Noida	6

Nakon dobivenih rezultata moguće je provesti daljnu istragu pomoću dodatka *Pipl*. *Pipl* prikuplja, unakrsno referencira i povezuje informacije o online identitetu iz nebrojenih neovisnih izvora. *Pipl* transformacije u Maltegu povezuju podatke na temelju imena, adrese elektroničke pošte, telefonskog broja unutar svoje baze podataka kako bi pronašao

odgovarajuće profile osoba. Oni se vraćaju u Maltego graf kao entiteti osoba. Od entiteta *Pipl* osobe može se dodatno pretraživati baza podataka kako bi se otkrile druge osobne informacije kao što su povijest karijere, povezane osobe, hobiji itd.

6. REGULATORNI OKVIR PRIKUPLJANJA I ANALIZE OSINT PODATAKA

Brzina tehnološkog razvoja i način na koji se osobni podaci obrađuju utječu na svakog čovjeka. Pravni okviri Europske unije i Vijeća Europe koji štite zaštitu privatnosti i osobnih podataka štite pojedince od zlonamjernih prijatelja. Reforme zaštite podataka koje provode Europska unija i Vijeće Europe su opsežne i ponekad složene, sa širokim rasponom prednosti i utjecaja na pojedince i poduzeća. Najznačajniji pravni dokumenti koji su uvedeni su pravo na poštivanje privatnog života i pravo na zaštitu osobnih podataka, Opća deklaracija o ljudskim pravima, Članak 12. poštivanje privatnog i obiteljskog života, Europska konvencija o ljudskim pravima, Konvencija Vijeća Europe 108 i Zakon o zaštiti podataka Europske unije [45].

6.1 Pravo na poštivanje privatnog života i pravo na zaštitu osobnih podataka

Pravo na poštivanje privatnog života i pravo na zaštitu osobnih podataka, iako su usko povezana, radi se o različitim pravima. Pravo na privatnost koje se u europskom pravu naziva pravom na poštivanje privatnog života. Pojavilo se u međunarodnom pravu ljudskih prava u Općoj deklaraciji o ljudskim pravima (engl. *Universal Declaration of Human Rights* - UDHR), usvojenoj 1948.godine, kao jedno od temeljnih zaštićenih ljudskih prava. Ubrzo nakon usvajanja UDHR-a, Europa je također potvrdila ovo pravo u Europskoj konvenciji o ljudskim pravima (engl. *European Convention on Human Rights* - ECHR), u ugovoru koji je pravno obvezujući za svoje ugovorne stranke i koji je sastavljen 1950.godine. ECHR predviđa da svatko ima pravo na poštivanje njegova privatnog i obiteljskog života, doma i dopisivanja. Zabranjeno je miješanje u to pravo od strane tijela javne vlasti, osim ako je miješanje u skladu sa zakonom, u svrhu ostvarivanja važnih i legitimnih javnih interesa i nužno za demokratsko društvo [45].

Poštivanje privatnog života i pravo na zaštitu osobnih podataka prava razlikuju se po svojoj formulaciji i opsegu. Pravo na poštivanje privatnog života sastoji se od opće zabrane miješanja, podložno kriterijima javnog interesa koji mogu opravdati miješanje u određenim slučajevima. Zaštita osobnih podataka smatra se modernim i aktivnim pravom, kojim se uspostavlja sustav provjera i ravnoteže kako bi se zaštitili pojedinci kada god se njihovi osobni podaci obrađuju [45]. Obrada mora biti u skladu s bitnim sastavnicama zaštite osobnih podataka, a to su neovisni nadzor i poštivanje prava ispitanika.

6.2. Poštivanje privatnog i obiteljskog života

Okvir Ujedinjenih naroda ne prepoznaje zaštitu osobnih podataka kao temeljno pravo, iako je pravo na privatnost dugo utemeljeno temeljno pravo u međunarodnom pravnom poretku. Članak 12. UDHR-a o poštivanju privatnog i obiteljskog života prvi puta označava da je jedan međunarodni instrument propisao pravo pojedinca na zaštitu njegove privatne sfere od uplitanja drugih, osobito države. Iako je neobvezujuća deklaracija, UDHR ima značajan status temeljnog instrumenta međunarodnog prava ljudskih prava i utjecala je na razvoj drugih instrumenata ljudskih prava u Europi [45].

Međunarodni pakt o građanskim i političkim pravima (engl. *International Covenant on Civil and Political Rights* - ICCPR) stupio je na snagu 1976. godine. Proglašava da nitko ne smije biti izvrnut proizvoljnom ili nezakonitom miješanju u njegovu privatnost niti nezakonitim napadima na njegovu čast i ugled. ICCPR je međunarodni ugovor koji obvezuje 169 stranaka na poštivanje i osiguravanje ostvarivanja građanskih prava pojedinaca, uključujući privatnost [45].

6.3. Europska konvencija o ljudskim pravima

Vijeće Europe osnovano je nakon Drugog svjetskog rata kako bi okupilo europske države radi promicanja vladavine prava, demokracije, ljudskih prava i društvenog razvoja. U tu svrhu usvojila je ECHR 1950. godine, koja je stupila na snagu 1953. godine. Ugovorne stranke imaju međunarodnu obvezu poštivanja ECHR-a. Sve države članice Vijeća Europe su uključile ili primijenile ECHR u svoje nacionalne zakone, što od njih zahtijeva da djeluju u skladu s odredbama konvencije. Ugovorne stranke moraju poštivati prava navedena u konvenciji pri obavljanju bilo koje aktivnosti ili ovlasti. To uključuje aktivnosti koje se poduzimaju za nacionalnu sigurnost. Značajne presude ECHR-a uključivale su aktivnosti države u osjetljivim područjima zakona i prakse nacionalne sigurnosti [45]. Sud nije oklijevao potvrditi da aktivnosti nadzora predstavljaju miješanje u poštivanje privatnog života.

ECHR je ispitao mnoge situacije koje uključuju pitanja zaštite podataka. To uključuje presretanje komunikacija, različite oblike nadzora od strane privatnog i javnog sektora, te zaštitu od pohrane osobnih podataka od strane javnih tijela. Poštivanje privatnog života nije apsolutno pravo, budući da bi ostvarivanje prava na privatnost moglo ugroziti druga prava, poput slobode izražavanja i pristupa informacijama i obrnuto. Stoga Sud nastoji pronaći ravnotežu između različitih prava o kojima je riječ. Članak 8. ECHR-a ne samo da obvezuje države da se suzdrže od bilo kakvih radnji koje bi mogle povrijediti ovo konvencijsko pravo, već da su u određenim okolnostima također pod pozitivnim obvezama da aktivno osiguraju učinkovito poštovanje privatnog i obiteljskog života [45].

6.4. Konvencija Vijeća Europe

S pojavom informacijske tehnologije u 1960-ima, postojala je sve veća potreba za detaljnijim pravilima za zaštitu pojedinaca zaštitom njihovih osobnih podataka. Do sredine 1970-ih, Odbor ministara Vijeća Europe usvojio je razne rezolucije o zaštiti osobnih podataka, pozivajući se na članak 8. ECHR-a. Godine 1981., Konvencija o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka (Konvencija 108) bila je otvorena za potpis. Konvencija 108 je jedino pravno obvezujući međunarodni instrument u području zaštite podataka. Konvencija 108 odnosi se na svu obradu podataka koju provode privatni i javni sektor, uključujući obradu podataka od strane pravosuđa i tijela za provođenje zakona. Štiti pojedince od zlouporaba koje mogu pratiti obradu osobnih podataka, a u isto vrijeme nastoji regulirati prekogranične protoke osobnih podataka. Što se tiče obrade osobnih podataka, načela utvrđena u konvenciji posebno se odnose na pošteno i zakonito prikupljanje i automatsku obradu podataka. To znači da se podaci ne smiju koristiti u svrhe koje nisu u skladu s tim svrhama i da se ne smiju čuvati dulje nego što je potrebno [45]. Osim pružanja jamstava o obradi osobnih podataka i obveza sigurnosti podataka, zabranjuje obradu „osjetljivih“ podataka kao što su politika, rasa, zdravlje, vjera, spol osobe ili kriminalni dosje.

Konvencija 108 također jamči pravo pojedinca da zna da su informacije pohranjene o njemu ili njoj, ali da ima i pravo na njihov ispravak. Ograničenja prava utvrđenih konvencijom moguća su samo kada su u pitanju važniji interesi, poput državne sigurnosti ili obrane [45]. Osim toga, konvencija osigurava slobodan protok osobnih podataka između svojih ugovornih strana i nameće određena ograničenja protoka prema državama u kojima pravni propisi ne pružaju jednaku zaštitu.

Sve države članice Europske unije ratificirale su Konvenciju 108, a 1999. godine predloženi su amandmani na Konvenciju 108 kako bi se Europskoj uniji omogućilo da postane stranka, ali nikada nisu stupili na snagu. Dok je 2001. godine usvojen dodatni protokol uz Konvenciju 108. Njime su uvedene odredbe o prekograničnom protoku podataka prema državama koje nisu stranke, takozvanim trećim zemljama, te o obveznoj uspostavi nacionalnih nadzornih tijela za zaštitu podataka. Potencijal Konvencije kao univerzalnog standarda, zajedno s njezinim otvorenim karakterom, služi kao osnova za promicanje zaštite podataka na globalnoj razini. Do danas je 51 država potpisnica Konvencije 108. One uključuju sve države članice Vijeća Europe. Urugvaj je prva neeuropska zemlja koja je pristupila u kolovozu 2013. godine zatim Mauricijus, Senegal i Tunis, koji su pristupili 2016. i 2017. godine [45].

6.5. Zakon o zaštiti podataka Europske unije

Pravo Europske unije sastoji se od primarnog i sekundarnog prava. Ugovori, odnosno Ugovor o Europskoj uniji i Ugovor o funkcioniranju Europske unije ratificirale su sve države članice Europske unije, a oni čine „primarno pravo Europske unije“. Uredbe, direktive i odluke Europske unije usvojile su institucije Europske unije koje su dobile ovlasti sukladno ugovorima, a oni čine „sekundarno pravo Europske unije“ [45]. Zakon o zaštiti podataka Europske unije sastoji se od:

- Zaštita podataka u primarnom pravu Europske unije
- Opće uredbe o zaštiti podataka
- Zaštite podataka u provedbi zakona
- Direktive o privatnosti i elektroničkim komunikacijama
- Uredbe o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane institucija i tijela Zajednice o slobodnom kretanju takvih podataka

a) Zaštita podataka u primarnom pravu Europske unije

Izvorni ugovori Europskih zajednica nisu sadržavali nikakve reference na ljudska prava niti njihovu zaštitu, budući da je Europska ekonomska zajednica u početku bila zamišljena kao regionalna organizacija usmjerena na gospodarsku integraciju i uspostavu zajedničkog tržišta. Temeljno načelo na kojem se temelji stvaranje i razvoj Europskih zajednica je načelo dodjele. Prema tom načelu, Europska unija djeluje samo u granicama nadležnosti koje su joj dodijelile države članice [45]. Za razliku od Vijeća Europe, ugovori Europske unije ne uključuju izričitu nadležnost kada su u pitanju temeljna prava.

Kako pred Sud Europske unije dolaze slučajevi u kojima se navodi kršenje ljudskih prava, a kako bi osigurala zaštitu pojedinaca, unijela su se temeljna prava u takozvana opća

načela europskog prava. Prema sudu pravde Europske unije (engl. *Court of Justice of the European Union* - CJEU), opća načela odražavaju sadržaj zaštite ljudskih prava koji se nalazi u nacionalnim ustavima i ugovorima o ljudskim pravima, posebno u ECHR-u [45].

b) Opća uredba o zaštiti podataka

Od 1995. godine do svibnja 2018. godine glavni pravni instrument Europske unije o zaštiti podataka bila je Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. godine o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka. Zakoni su proizašli iz potrebe da se usklade kako bi se osigurala visoka razina zaštite i slobodan protok osobnih podataka među različitim državama članicama [45]. Slobodno kretanje robe, kapitala, usluga i ljudi unutar unutarnjeg tržišta zahtijeva slobodan protok podataka, koji se ne može ostvariti ako se države članice ne mogu osloniti na jedinstvenu visoku razinu zaštite podataka.

Direktiva o zaštiti podataka odražava načela zaštite podataka koja su već sadržana u nacionalnim zakonima i Konvenciji 108. Konkretno, uvođenje neovisnog nadzora u direktivu kao instrumenta za poboljšanje usklađenosti s pravilima o zaštiti podataka pokazalo se važnim doprinosom za učinkovito funkcioniranje europskog prava o zaštiti podataka [45]. Direktivom o zaštiti podataka uspostavljen je detaljan i sveobuhvatan sustav zaštite podataka u Euroskoj uniji. Međutim, u skladu s pravnim sustavom Europske unije, direktive se ne primjenjuju izravno i moraju se prenijeti u nacionalne zakone država članica. Države članice neizbježno imaju diskrecijsku slobodu u prenošenju odredba Direktive. Iako Direktiva treba osigurati potpunu harmonizaciju u praksi je različito implementirana u državama članicama. To je rezultiralo uspostavljanjem različitih pravila o zaštiti podataka diljem Europske unije s definicijama i pravilima koja se različito tumače u nacionalnim zakonima. Razine provedbe i ozbiljnosti sankcija također su se razlikovale među državama članicama koje su se kasnije usklađivale radi boljeg funkcioniranja cjelokupnog sustava [45].

c) Zaštita podataka u provedbi zakona

Stavljena Direktiva o zaštiti podataka pružila je sveobuhvatan režim zaštite podataka. Taj je režim dodatno poboljšan donošenjem Opće uredbe o zaštiti podataka. Iako sveobuhvatna, područje primjene Direktive o zaštiti podataka je ograničeno na aktivnosti koje potpadaju pod unutarnje tržište i na aktivnosti javnih tijela za provedbu zakona. Stoga je potrebno donošenje posebnih instrumenata kako bi se postigla potrebna jasnoća i ravnoteža između zaštite podataka i drugih legitimnih interesa. To je slučaj s pravilima koja uređuju obradu osobnih podataka od strane tijela za provođenje zakona [45].

Dok Opća uredba o zaštiti podataka utvrđuje opća pravila za zaštitu pojedinaca u vezi s obradom njihovih osobnih podataka i kako bi se osiguralo slobodno kretanje takvih podataka unutar Europske unije, direktiva utvrđuje posebna pravila za zaštitu podataka u područjima pravosuđa suradnja u kaznenim stvarima i policijskim suradnjama. Ako nadležno tijelo obrađuje osobne podatke u svrhu prevencije, istrage, otkrivanja ili progona kaznenih djela, primjenjivat će se Direktiva 2016/680. Ako nadležna tijela obrađuju osobne podatke u druge svrhe osim gore navedenih, primjenjivat će se opći režim prema Općoj uredbi o zaštiti podataka

[45]. Osim toga, Direktiva nastoji postići ravnotežu između prava pojedinaca i legitimnih ciljeva obrade podataka povezanih sa sigurnošću.

d) Direktiva o privatnosti i elektroničkim komunikacijama

S razvojem interneta, fiksne i mobilne telefonije važno je osigurati poštivanje prava korisnika na privatnost i povjerljivost. Direktiva 2002/58/EC35 o obradi osobnih podataka i zaštiti privatnosti u elektroničkim komunikacijama (Direktiva o privatnosti i elektroničkim komunikacijama) utvrđuje pravila o sigurnosti osobnih podataka u tim mrežama, obavijest o povredi osobnih podataka i povjerljivosti komunikacije [45].

U pogledu sigurnosti, operateri elektroničkih komunikacijskih usluga moraju, između ostalog, osigurati da pristup osobnim podacima bude ograničen samo na ovlaštene osobe i poduzeti mjere za sprječavanje uništenja, gubitka ili slučajnog oštećenja osobnih podataka. Gdje postoji rizik od narušavanja sigurnosti javne komunikacijske mreže, operateri moraju obavijestiti pretplatnike o tome riziku. Ako, unatoč provedenim sigurnosnim mjerama dođe do narušavanja sigurnosti, operateri moraju obavijestiti nadležno nacionalno tijelo kojem je povjerena provedba osobnih podataka. Od operatera se ponekad zahtijeva da također obavijeste pojedince o povredama osobnih podataka, naime ako postoji vjerojatnost da će povreda negativno utjecati na njihove osobne podatke ili privatnost. Povjerljivost komunikacije zahtijeva da se slušanje, prisluškivanje, pohranjivanje ili bilo koja vrsta nadzora ili presretanja komunikacija u načelu zabrani. Direktiva također zabranjuje neželjenu komunikaciju koja se često naziva „*spam*“, osim ako korisnici nisu dali svoj pristanak na računalima i uređajima [45]. Ove temeljne obveze jasno pokazuju da je povjerljivost komunikacije značajno povezana sa zaštitom prava na poštovanje privatnog života.

e) Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane institucija i tijela Zajednice o slobodnom kretanju takvih podataka

S obzirom da se Direktiva o zaštiti podataka mogla primjenjivati samo na države članice Europske unije, bio je potreban dodatni pravni instrument za uspostavljanje zaštite podataka za obradu osobnih podataka od strane institucija i tijela Europske unije. Uredba br. 45/2001 o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane institucija i tijela Zajednice o slobodnom kretanju takvih podataka [43]. Uredba br. 45/2001 usko slijedi načela općeg režima zaštite podataka Europske unije i primjenjuje ta načela na obradu podataka koju provode ustanove i tijela u vršenju svojih funkcija. Osim toga, uspostavljeno je neovisno nadzorno tijelo, Europski nadzornik za zaštitu podataka (engl. *European Data Protection Supervisor* - EDPS) za praćenje primjene njegovih odredbi. EDPS ima nadzorne ovlasti i dužnost nadzirati obradu osobnih podataka u institucijama i tijelima Europske unije, te saslušati i istražiti pritužbe u vezi s kršenjima pravila o zaštiti podataka [45]. Također pruža savjete institucijama i tijelima Europske unije o svim pitanjima koja se tiču zaštite osobnih podataka u rasponu od prijedloga novog zakonodavstva do izrade internih pravila vezanih za obradu podataka.

6.6. Osobni podaci

Prema pravu Europske unije kao i prema zakonu Vijeća Europe osobni podaci definirani su kao informacije koje se odnose na identificiranu fizičku osobu ili fizičku osobu koja se može

identificirati. Odnosi se na informacije o osobi čiji je identitet jasan ili se može utvrditi iz dodatnih informacija. Kako bi se utvrdilo je li osobu moguće identificirati, voditelj obrade ili druga osoba mora uzeti u obzir sva razumna sredstva koja će se koristiti za izravnu ili neizravnu identifikaciju pojedinca [45]. Ako se podaci o takvoj osobi obrađuju, ta se osoba naziva „ispitanik“. Kako bi se razumio koncept osobnih podataka, opisano je nekoliko glavnih pojmova:

- Ispitanik
- Anonimizacija
- Pseudonimizacija
- Ovjera
- Kategorije osobnih podataka

a) Ispitanik

Prema pravu Europske unije fizičke osobe jedini su korisnici pravila o zaštiti podataka. GDPR definira osobne podatke kao bilo koju informaciju koja se odnosi na fizičku osobu koja se može identificirati [45].

Pravo Vijeća Europe, osobito Konvencije 108 koja se odnosi na zaštitu pojedinaca u vezi s obradom njihovih osobnih podataka. Označavaju sve informacije koje se odnose na identificiranu osobu ili osobu koju je moguće identificirati. Ova fizička osoba ili pojedinac, kako je navedeno u GDPR-u i Konvenciji 108 poznata je kao subjekt podataka [45].

Pravne osobe također imaju određenu zaštitu. Postoji sudska praksa ECHR-a koja donosi presude o zahtjevima pravnih osoba u kojima se navodi kršenje njihovog prava na zaštitu od uporabe podataka prema članku 8. ECHR. Koja pokriva pravo na poštivanje privatnog i obiteljskog života, kao i pravo na dom i korespondenciju [45]. Sud stoga može ispitivati slučajeve, ali se ne smije doticati privatnog života.

Prema Moderniziranoj konvenciji 108, zaštita podataka odnosi se prvenstveno na zaštitu fizičkih osoba. Dok Zakon o zaštiti podataka Europske unije ne pokriva obradu podataka koji se tiču pravnih osoba, a posebno ne odnose se na poduzeća osnovana kao pravne osobe, uključujući naziv i oblik pravne osobe i njihove podatke za kontakt [45]. Direktiva o e-privatnosti štiti povjerljivost komunikacije i legitimne interese pravnih osoba u pogledu povećanja kapaciteta za automatiziranu pohranu i obradu podataka koji se odnose na pretplatnike i korisnike.

b) Anonimizacija

Prema načelu ograničenja pohrane sadržanom u GDPR-u i Konvenciji 108, podaci se moraju čuvati u obliku koji dopušta identifikaciju ispitanika ne dulje nego što je potrebno za svrhe za koje se osobni podaci obrađuju. Podaci bi morali biti izbrisani ili anonimizirani ako bi ih voditelj obrade želio pohraniti nakon što više nisu potrebni i više ne služe svojoj početnoj svrsi.

Proces anonimiziranja podataka znači da se svi identifikacijski elementi eliminiraju iz skupa osobnih podataka tako da subjekta podataka više nije moguće identificirati. Kako bi se pronašlo optimalno rješenje u određenoj situaciji, potrebno je odlučiti o odgovarajućem postupku anonimizacije od slučaja do slučaja. Bez obzira na korištenu tehniku, identifikacija se mora nepovratno spriječiti. Kako bi podaci bili anonimizirani u informacijama ne smije biti ostavljen nijedan element koji bi ulaganjem razumnog napora mogao poslužiti za ponovnu identifikaciju osobe. Rizik ponovne identifikacije može se procijeniti uzimajući u obzir vrijeme, trud, potrebne resurse, konteksta njihove upotrebe, dostupnih tehnologija za ponovnu identifikaciju i povezanih troškova. Kada su podaci uspješno anonimizirani, više nisu osobni podaci i više se ne primjenjuju zakoni o zaštiti podataka [45].

GDPR predviđa da osoba ili organizacija koja kontrolira obradu osobnih podataka ne može biti obvezna održavati, prikupiti ili obraditi dodatne informacije za identifikaciju nositelja podataka [45]. Međutim, ovo pravilo ima značajan izuzetak jer kada god nositelj podataka u svrhu ostvarivanja prava na pristup, ispravak, brisanje, ograničenje obrade i prenosivosti podataka, pruži dodatne informacije voditelju obrade koje omogućuju njegovu ili njezinu identifikaciju, tada oni podaci koji su prethodno bili anonimizirani ponovno postaju osobni podaci.

c) Pseudonimizacija

Osobni podaci sadrže atribute kao što su ime, datum rođenja, spol, adresa ili druge elemente koji mogu dovesti do identifikacije. Proces pseudonimizacije osobnih podataka znači da se ti atributi zamjenjuju pseudonimom [45].

Zakon Europske unije definira „pseudonimizaciju“ kao obradu osobnih podataka na takav način da se osobni podaci više ne mogu pripisati određenom subjektu podataka bez upotrebe dodatnih informacija. Pod uvjetom da se te dodatne informacije čuvaju odvojeno i podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne pripisuju identificiranoj fizičkoj osobi ili osobi koju je moguće identificirati. Za razliku od anonimiziranih podataka, pseudonimizirani podaci su i dalje osobni podaci i stoga podliježu zakonodavstvu o zaštiti podataka [45].

GDPR prepoznaje različite upotrebe pseudonimizacije kao prikladnu tehničku mjeru za poboljšanje zaštite podataka, a posebno se spominje zbog dizajna i sigurnosti obrade podataka. To je također prikladna zaštitna mjera koja se može koristiti za obradu osobnih podataka u druge svrhe od onih za koje su izvorno prikupljeni.

Pseudonimizacija se izričito ne spominje u pravnoj definiciji Konvencije 108. Međutim, izvješće s objašnjenjima modernizirane konvencije 108 jasno navodi da: „uporaba pseudonima ili bilo kojeg digitalnog identifikatora/digitalni identitet ne dovodi do anonimizacije podataka budući da se nositelj podataka i dalje može identificirati ili individualizirati“. Jedan od načina pseudonimizacije podataka je enkripcija podataka. Nakon što su podaci pseudonimizirani, veza s identitetom postoji u obliku pseudonima plus ključa za dešifriranje [45]. Bez takvog ključa teško je identificirati pseudonimizirane podatke. Međutim, za one koji imaju pravo koristiti

ključ za dešifriranje, ponovna identifikacija je lako moguća. Posebno se mora čuvati od korištenja ključeva za šifriranje od strane neovlaštenih osoba.

d) Ovjera

Ovo je postupak kojim osoba može dokazati da posjeduje određeni identitet ili da je ovlaštena činiti određene stvari, kao što je ulazak u sigurnosno područje ili podizanje novca s bankovnog računa. Autentifikacija se može postići usporedbom biometrijskih podataka, kao što su fotografija ili otisci prstiju u putovnici s podacima osobe koja se predstavlja. Pseudonimizacija se izričito ne spominje u pravnoj definiciji Konvencije 108. Međutim, izvješće s objašnjenjima konvencije 108 jasno navodi da uporaba pseudonima ili bilo kojeg digitalnog identifikatora ili traženjem informacija koje bi trebale biti poznate samo osobi s određenim identitetom kao što je osobni identifikacijski broj ili lozinka. Također zahtijevanjem predočenja određenog tokena koji bi trebao biti isključivo u posjedu osobe s ovlaštenjem, poput posebne kartice s čipom ili ključa bankovnog sefa. Osim lozinki ili čip kartica, elektronički potpisi ponekad zajedno s lozinkom instrumenta su posebno dizajnirani za identifikaciju i autentifikaciju osobe [45].

e) Kategorije osobnih podataka

Prema pravu Europske unije, kao i prema zakonu Vijeća Europe, postoje posebne kategorije osobnih podataka koji po svojoj prirodi mogu predstavljati rizik za ispitanike kada se obrađuju te im je potrebna pojačana zaštita. Takvi podaci podliježu načelu zabrane i postoji ograničen broj uvjeta pod kojima je takva obrada zakonita. U okviru Konvencije 108, Članka 6. i GDPR-a, Članka 9., sljedeće kategorije se smatraju osjetljivim podacima:

- osobni podaci koji otkrivaju rasno ili etničko podrijetlo.
- osobni podaci koji otkrivaju politička mišljenja, vjerska ili druga uvjerenja, uključujući filozofska uvjerenja.
- osobni podaci koji otkrivaju članstvo u sindikatu.
- genetski podaci i biometrijski podaci koji se obrađuju u svrhu identifikacije osoba.
- osobni podaci koji se tiču zdravlja, spolnog života ili seksualne orijentacije [45].

Konvencija 108 uključuje osobne podatke koji se odnose na kaznena djela, kaznene postupke i osude na popis posebnih kategorija osobnih podataka. GDPR propisuje da se obrada takvih podataka može provoditi samo pod kontrolom službenih tijela ili kada je obrada odobrena zakonom Unije ili države članice koji predviđa odgovarajuće zaštitne mjere za prava i slobode ispitanika. Sveobuhvatni registri koji sadrže informacije o kaznenim presudama mogu se voditi samo pod kontrolom određenih službenih tijela [45].

6.7. Obrada podataka

Koncept obrade osobnih podataka je sveobuhvatan i prema pravu Europske unije i prema pravu Vijeća Europe podrazumijeva se kao obrada osobnih podataka koja označava bilo koju radnju kao što je prikupljanje, snimanje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, konzultacija, uporaba, otkrivanje prijenosom, širenje ili na drugi način

stavljanje na raspolaganje, usklađivanje ili kombinacija, ograničavanje, brisanje ili uništavanje osobnih podataka [45]. Postoje dvije vrste obrade podataka:

- Automatizirana obrada podataka
- Neautomatizirana obrada podataka

a) Automatizirana obrada podataka

Zaštita podataka prema Konvenciji 108 i GDPR-u u potpunosti se odnosi na automatiziranu obradu podataka. Prema pravu Europske unije automatizirana obrada podataka odnosi se na operacije koje se izvode nad osobnim podacima u cijelosti ili djelomično [45]. U praktičnom smislu, to znači da svaka obrada osobnih podataka putem automatiziranih sredstava uz pomoć osobnog računala, mobilnog uređaja ili usmjerivača obuhvaćena je pravilima o zaštiti podataka Europske unije i Vijeća Europe.

f) Neautomatizirana obrada podataka

Ručna obrada podataka također zahtijeva zaštitu podataka. Zaštita podataka prema pravu Europske unije ni na koji način nije ograničena na automatiziranu obradu podataka. Sukladno tome, prema pravu Europske unije, zaštita podataka odnosi se na obradu osobnih podataka u ručnom arhivskom sustavu odnosno posebno strukturiranoj papirnoj datoteci. Strukturirani arhivski sustav je onaj koji kategorizira skup osobnih podataka, čineći ih dostupnima prema određenim kriterijima. Naprimjer, ako poslodavac vodi papirni dosje pod nazivom „dopust zaposlenika“, koji sadrži sve pojedinosti o osoblju koje je uzelo dopust u prošloj godini i poredan je abecednim redom. Dosje će predstavljati ručni sustav arhiviranja podložan pravila zaštite podataka. Razlog za ovo proširenje zaštite podataka je sljedeći:

- papirne datoteke mogu biti strukturirane na način koji omogućava brzo pronalaženje informacija.
- pohranjivanje osobnih podataka u strukturirane papirne datoteke olakšava zaobilazanje zakonskih ograničenja za automatiziranu obradu podataka [45].

Prema pravu Vijeća Europe, definicija automatske obrade priznaje da se između automatiziranih operacija mogu zahtijevati neke faze ručne upotrebe osobnih podataka. Članak 2. Konvencije 108 navodi da ako se ne koristi automatizirana obrada, obrada podataka znači radnju ili skup radnji koje se izvode nad osobnim podacima unutar strukturiranog skupa takvih podataka koji su dostupni ili dohvatljivi prema specifičnim kriterijima [45].

6.8. Korisnici osobnih podataka

Svatko tko određuje sredstva i svrhe obrade osobnih podataka drugih je kontrolor prema zakonu o zaštiti podataka. Ako više osoba zajedno donese ovu odluku, one mogu biti „zajednički kontrolori“. Dok je izvršitelj obrade fizička ili pravna osoba koja obrađuje osobne podatke u ime kontrolora [45].

Najvažniji zadatak voditelja obrade ili izvršitelja obrade je zakonska odgovornost za poštivanje odgovarajućih obveza prema zakonu o zaštiti podataka. U privatnom sektoru to je

obično fizička ili pravna osoba. U javnom sektoru to je obično osoba s autoritetom. Postoji značajna razlika između voditelja obrade i izvršitelja obrade podataka. Prvi je fizička ili pravna osoba koja određuje svrhe i sredstva obrade, dok je drugi fizička ili pravna osoba koja obrađuje podatke u ime kontrolora. U načelu, voditelj obrade je taj koji mora vršiti nadzor nad obradom i koji za to ima odgovornost. Međutim, s reformom pravila o zaštiti podataka, izvršitelji obrade sada imaju obvezu pridržavati se mnogih zahtjeva koji se odnose na voditelje obrade [45]. Naprimjer, prema GDPR-u izvršitelji obrade moraju voditi evidenciju svih kategorija aktivnosti obrade kako bi dokazali usklađenost sa svojim obvezama prema uredbi. Izvršitelji obrade također moraju provesti odgovarajuće tehničke i organizacijske mjere kako bi se osigurala sigurnost obrade i imenovalo službenika za zaštitu podataka u određenim situacijama.

Prema definiciji voditelja obrade fizičke osobe, pravne osobe ili bilo koja druga tijela mogu biti voditelj obrade. Međutim, kako bi se pojedincima pružio stabilniji subjekt za ostvarivanje njihovih prava, treba dati prednost kontroloru tvrtke, a ne određenoj osobi unutar tvrtke [43]. Naprimjer, tvrtka koja prodaje medicinske potrepštine liječnicima, kontrolor je sastavljanja i održavanja popisa distribucije svih liječničkih djelatnika na određenom području, a ne voditelj prodaje koji zapravo koristi i održava popis.

Fizičke osobe mogu biti kontrolori prema pravu Europske unije. Međutim, kada se obrađuju podaci o drugima u vezi s osobnom ili kućanskom aktivnošću. Privatne osobe ne spadaju pod pravila GDPR-a i Konvencije 108 i ne smatraju se voditeljima obrade. Pojedinaac koji vodi svoju korespondenciju, osobni dnevnik u koji upisuje incidente s prijateljima i kolegama te zdravstveni kartoni članova obitelji, mogu biti izuzeti od pravila o zaštiti podataka, jer te aktivnosti mogu biti isključivo osobne ili samo kućne aktivnosti. GDPR nadalje precizira da osobne aktivnosti ili aktivnosti u kućanstvu također mogu uključivati rad na društvenim mrežama i online aktivnosti kada se poduzimaju u kontekstu takvih aktivnosti [45].

Pristup građana internetu i mogućnost korištenja platformi za e-trgovinu, društvenih mreža i stranica za blogove za dijeljenje osobnih podataka o sebi i drugim pojedincima sve više otežava odvajanje osobne od neosobne obrade. Aktivnosti koje imaju profesionalne ili komercijalne aspekte ne mogu potpasti pod izuzeće kućanstva. Stoga, kada opseg i učestalost obrade podataka sugerira profesionalnu aktivnost ili aktivnost s punim radnim vremenom, privatna osoba može se smatrati voditeljem obrade.

Sudska praksa prema Direktivi o zaštiti podataka utvrdila je da će se zakon o zaštiti podataka primjenjivati kada privatna osoba tijekom korištenja interneta objavi podatke o drugima na javnoj internetskoj stranici. Sud još nije presudio o sličnim činjenicama u skladu s GDPR-om, koji pruža više smjernica o temama koje bi se mogle smatrati izvan opsega zakonodavstva o zaštiti podataka pod „iznimkom kućanstva”, kao što je upotreba društvenih medija u osobne svrhe [45].

a) Voditelj obrade

Prema pravu Europske unije voditelj obrade definiran je kao netko tko sam ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka. Odluka voditelja obrade utvrđuje zašto i kako će se podaci obrađivati. Prema pravu Vijeća Europe i Konvencije 108 voditelja

obrade se definira kao fizičku ili pravnu osobu, javno tijelo, službu, agenciju ili bilo koje drugo tijelo koje, samo ili zajedno s drugima, ima ovlast donošenja odluka u vezi s obradom podataka [45]. Takva moć odlučivanja tiče se svrhe i sredstava obrada kao i kategorije podataka koji se obrađuju.

f) Zajednička kontrola

Kada dva ili više voditelja obrade zajednički određuju svrhu i sredstva obrade, smatraju se zajedničkim voditeljima obrade. To znači da zajedno odlučuju obrađivati podatke u zajedničku svrhu. Zajednički nadzor može imati različite oblike i sudjelovanje različitih voditelja nadzora u kontrolnim aktivnostima može biti nejednako. Takva fleksibilnost omogućuje rješavanje složenije stvarnosti obrade podataka. Zajednički voditelji obrade stoga moraju konkretnim sporazumom utvrditi njihove pojedinačne odgovornosti za poštivanje obveza iz propisa [45]. Zajednički nadzor dovodi do zajedničke odgovornosti za aktivnost obrade. U okviru prava Europske unije to znači da se svaki voditelj obrade ili izvršitelj obrade može se smatrati potpuno odgovornim za cjelokupnu štetu prouzročenu obradom pod zajedničkim nadzorom.

g) Izvršitelj obrade

Izvršitelj obrade je netko tko obrađuje osobne podatke u ime voditelja obrade. Aktivnosti koje su povjerene izvršitelju obrade mogu biti ograničene na vrlo specifičan zadatak ili kontekst, te mogu biti prilično općenite i sveobuhvatne. Izvršitelji obrade, osim što obrađuju podatke za druge, također će sami biti voditelji obrade podataka u odnosu na obradu koju obavljaju za vlastite potrebe [45].

h) Odnos voditelja i izvršitelja obrade

Voditelj obrade je definiran kao onaj koji određuje svrhe i sredstva obrade. GDPR jasno navodi da izvršitelj obrade smije obrađivati osobne podatke samo prema uputama voditelja obrade, osim ako to od izvršitelja obrade zahtijeva zakon Europske unije ili države članice. Ugovor između voditelja obrade i izvršitelja obrade bitan je element njihovog odnosa.

Ako je ovlaštenje za određivanje načina obrade delegirano izvršitelju obrade, voditelj obrade mora unatoč tome moći provoditi odgovarajući stupanj kontrole nad odlukama izvršitelja obrade u vezi sa sredstvima obrade. Sveukupna odgovornost i dalje leži na voditelju obrade, koji mora nadzirati izvršitelje obrade kako bi osigurao da su njihove odluke u skladu sa zakonom o zaštiti podataka i njegovim vlastitim uputama [45].

Mogu postojati i problemi oko podjele odgovornosti kada je voditelj obrade malo poduzeće, a izvršitelj obrade velika korporativna tvrtka koja ima moć diktirati uvjete svojih usluga. U takvim okolnostima, smatra se da se standard odgovornosti ne smije snižavati na temelju ekonomske neravnoteže.

Radi jasnoće i transparentnosti, pojedinosti o odnosu između voditelja obrade i izvršitelja obrade moraju biti zabilježene u pisanom ugovoru. Kontakt mora uključivati predmet, prirodu, svrhu i trajanje obrade, vrstu osobnih podataka i kategorije ispitanika [45].

Također se trebaju propisati obveze i prava voditelja obrade i izvršitelja obrade. Nepostojanje takvog ugovora predstavlja kršenje obveze voditelja obrade da dostavi pisanu dokumentaciju o međusobnim odgovornostima i može dovesti do sankcija. Kada je šteta uzrokovana djelovanjem izvana ili nepoštivanjem zakonitih uputa voditelja obrade. Ne može se smatrati odgovornim samo voditelj obrade, već i izvršitelj obrade. Izvršitelj obrade mora voditi evidenciju o svim kategorijama aktivnosti obrade provodi u ime voditelja obrade. Ti se zapisi moraju staviti na raspolaganje nadzornom tijelu na njegov zahtjev, jer i voditelj obrade i izvršitelj obrade moraju surađivati s tim tijelom u obavljanju njegovih zadataka. Voditelji obrade i izvršitelji obrade također imaju mogućnost pridržavanja odobrenog kodeksa ponašanja kako bi dokazali svoju usklađenost sa zahtjevima GDPR-a [45].

7. ZAKLJUČAK

Kao rezultat kontinuiranog tehnološkog rasta i razvoja, javlja se potreba za brzim i specifičnim prikupljanjem informacija, a to povećava i potrebu za OSINT-om. Korištenjem OSINT-a moguće je dobiti važne podatke u vrlo kratkom vremenskom periodu, što je moguće samo dubokom analizom koja se provodi nad podacima koji su dohvaćeni iz novina, časopisa, društvenih mrežama, blogova i ostalih javno dostupnih izvora. Analizom OSINT-a prikupljanju se podaci o određenom korisniku ili slučaju kako bi se utvrdilo tko su oni, koje su njihove namjere ili što se dogodilo, a sve u svrhu otkrivanja i sprječavanja prijevара. Postoje mnogi alati za prikupljanje i analizu javno dostupnih podataka, a jedan od poznatijih je programski alat Maltego koji je obrađen u ovom dijelu diplomskog rada.

Tijekom analize odabrana je osoba od interesa nad kojom se provela OSINT istraga. Nakon samo nekoliko minuta transformacija u programskom alatu Maltego moglo se doći do određenih zaključaka o osobi. Moglo se zaključiti da je profesionalni glumac iz Indije koji je bio na raznim lokacijama i povezan je s drugim poznatim osobama. Također se otkrila subjektova elektronička pošta i nekoliko njegovih slika. Svi dobiveni podaci kasnije se mogu koristiti u provedbi zakona, upravljanju rizicima i prijevarama, povećaju kibernetičke sigurnosti i različitim vojnim operacijama. Nakon analize uspješno se prikazalo kako doći do velike količine povezanih podataka o osobi od interesa i prikazano je da korisnik ne pokazuje brigu o „digitalnoj higijeni“.

Pojam „digitalne higijene“ korisnici često zaborave, a jedno je od bitnih čimbenika zaštite od kibernetičkog kriminala i prikupljanja OSINT-a. Cilj „digitalne higijene“ je čuvanje osjetljivih podataka i zaštita od krađe ili napada. Ukoliko se rade sigurnosne kopije podataka, šifriranje osjetljivih podataka, učestalo mijenjaju lozinke i ne objavljuju osobni podaci. Uvelike se mogu spriječiti kibernetički napadi na korisnika ili organizaciju. Jedan od koraka zaštite digitalne higijene je postavljanje oznake sa javne na privatnu. Tada URL adresa dokumenta na koji oznaka upućuje neće više biti dostupna. U tom slučaju digitalni istražitelji ne mogu dohvatiti podatke korisnika. Također, potrebno je pripaziti i na zakona ograničenja analiziranja, prikupljanja i spremanja podatka o osobi o interesa.

Unatoč svim prednosti OSINT-a postoji nekoliko nedostataka. Zbog prirode OSINT-a filtriranje korisnih podataka može biti prilično naporno. Bez primjene specijaliziranih alata učinkovitost provedbe OSINT analize drastično opada zbog velikih količina podataka koje je potrebno obraditi. Bez podrške umjetne inteligencije, OSINT zahtijeva puno ljudskog unosa za provjeru prikupljenih podataka. Izvore podataka je potrebno pomno ispitati jer se u suprotnom mogu analizirati lažni ili beskorisni podaci.

OSINT će u budućnosti biti suočen s velikim izazovima uzrokovanim golemim količinama nestrukturiranih podataka, jer će za njihovo prikupljanje i pravilno sortiranje biti potreban sve veći razvoj sofisticiranih programa. Također dezinformacije, privatnost i zakonitost samo su neki od aspekata koji će biti istaknuti u budućnosti OSINT-a. Kako tehnologija napreduje, tako će se razvijati i načini na koje se mogu prikupljati i koristiti podaci. Važno je biti svjestan implikacija ovih promjena i osigurati da se OSINT koristi na odgovoran i etičan način.

Literatura

- [1] H. J. Williams and I. Blum, „Defining second generation open source intelligence (OSINT) for the defense enterprise“, Santa Monica, USA: RAND Corp. 2018.
- [2] A. Powell and C. Haynes, „Social media data in digital forensics investigations“, Switzerland: Springer, 2020.
- [3] H. L. Larsen, J. M. Blanco, R. P. Pastor, and R. R. Yager, Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime. Cham, Switzerland: Springer, 2017.
- [4] J. Jang-Jaccard, S. Nepal, „A survey of emerging threats in cybersecurity“ J. Comput. Syst. Sci., 2014., vol. 80(5), pp. 973–99.
- [5] L. Ball, G. Ewan, N. Coull, „Undermining: Social engineering using open source intelligence gathering“ in Proc. Int. Conf. Knowl. Discovery Inf. Retr., 2012, pp. 275-280.
- [6] J. Simola, „Privacy issues and critical infrastructure protection,“ in Emerging Cyber Threats and Cognitive Vulnerabilities, Academic, 2020, pp. 197-226.
- [7] L. R. Betts, K. A. Spenser, „Developing the cyber victimization experiences and cyberbullying behaviors scales,“ J. Genet. Psychol., 2017., vol. 178(3), pp. 147-164.
- [8] M. J. Hernandez, C. C. Pinzon, D. O. Diaz, J. C. C. García, R. A. Pinto, „Open source intelligence (OSINT) in a colombian context and sentiment analysys,“ Technol. Sociedad, 2018., vol. 15(2), pp. 195-214.
- [9] M. K. Bergman, „White Paper: The deep *Web*: Surfacing hidden value,“ J. Electron. Publishing, 2001., vol. 7(1).
- [11] A. Gandomi, M. Haider, „Beyond the hype: Big data concepts, methods, and analytics,“ Int. J. Inf. Manage., 2015., vol. 35(2), pp. 137-144
- [10] M. Schafer, M. Fuchs, M. Strohmeier, M. Engel, M. Liechti, V. Lenders, „BlackWidow: Monitoring the dark *Web* for cyber security information,“ 11th Int. Conf. Cyber Conflict (CyCon), Tallinn, 2019, pp. 1-21.
- [12] A. Barnea, „Big data and counterintelligence in western countries,“ Int. J. Intell. Counter Intell., 2019 vol. 32(3), pp. 433-447.
- [13] T. Day, H. Gibson, S. Ramwell, „Open Source Intelligence Investigation,“, Open Source Intelligence Investigation. Cham, Switzerland: Springer, 2016, pp. 133-152.
- [14] C. S. Fleisher, „Using open source data in developing competitive and marketing intelligence,“ Eur. J. Marketing, 2008., vol. 42(7/8), pp. 852-866.
- [15] G. Bello-Orgaz, J. J. Jung, D. Camacho, „Social big data: Recent achievements and new challenges,“ Inf. Fusion, 2016., vol. 28, pp. 45-59.

- [16] F. G. Marmol, M. G. Perez, G. M. Perez, „Reporting offensive content in social networks: Toward a reputation-based assessment approach,“ *IEEE Internet Comput.*, 2014., vol. 18(2), pp. 32-40.
- [17] G. R. Weir, „The limitations of automating osint: Understanding the question, not the answer,“, *Automating Open Source Intelligence*, Boston, USA, Syngress, 2016, pp. 159-169.
- [18] H. Bean, „Is open source intelligence an ethical issue?“, *Research in Social Problems and Public Policy*, Bingley, U.K., Emerald Group Publishing Limited, 2011, pp. 385-402.
- [19] B. Liu, L. Zhang, „A survey of opinion mining and sentiment analysis,“, *Mining Text Data*. Boston, MA, USA, Springer, 2012, pp. 415-463.
- [20] P. Ranade, S. Mittal, A. Joshi, K. Joshi, „Using deep neural networks to translate multi-lingual threat intelligence“, *IEEE Int. Conf. Intell. Secur. Inform.*, 2018, pp. 238-243.
- [21] S. Noubours, A. Pritzkau, U. Schade, „NLP as an essential ingredient of effective OSINT frameworks,“, Bingley, *Proc. Mil. Commun. Inf. Syst. Conf.*, 2013, pp. 1-7.
- [22] S. Stieglitz, M. Mirbabaie, B. Ross, C. Neuberger, „Social media analytics and Challenges in topic discovery, data collection, and data preparation,“ *Int. J. Inf. Manage.*, 2018., vol. 39, pp. 156-168.
- [23] I. Deliu, C. Leichter, K. Franke, „Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks,“, *Proc. IEEE Int. Conf. Big Data (Big Data)*, 2017., pp. 3648-3656.
- [24] R. Layton, C. Perez, B. Birregah, P. Watters, M. Lemercier, „Indirect information linkage for OSINT through authorship analysis of aliases,“, *Trends and Applications in Knowledge Discovery and Data Mining*, Berlin, Germany, Springer, 2013, pp. 36-46.
- [25] C. Sauerwein, I. Pekaric, M. Felderer, R. Breu, „An analysis and classification of public information security data sources used in research and practice,“ *Comput. Secur.*, 2019., vol. 82, pp. 140-155.
- [26] S. Bromander, A. Josang, and M. Eian, „Semantic cyberthreat modelling,“, *Proc. 11th Conf. Semantic Technol. Intell., Defense, Secur.*, Fairfax, USA, 2016., pp. 74-78.
- [27] R. Layton, „Relative cyberattack attribution,“, *Automating Open Source Intelligence: Algorithms for OSINT*, Boston, MA, USA, Syngress, 2016, pp. 37-60.
- [28] R. S. Portnoff, S. Afroz, G. Durrett, J. K. Kummerfeld, T. Berg-Kirkpatrick, D. McCoy, K. Levchenko, V. Paxson, „Tools for automated analysis of cybercriminal markets,“, *Proc. 26th Int. Conf. World Wide Web*, 2017, pp. 657-666.
- [29] I. H. Witten, E. Frank, M. A. Hall, C. J. Pal, *Data Mining: Practical Machine Learning Tools and Techniques*. San Mateo, USA, Morgan Kaufmann, 2017.

- [30] X. Yin, J. Han, P. Yu, „Truth discovery with multiple conflicting information providers on the *Web*“, IEEE Trans. Knowl. Data Eng., 2008., vol. 20(6), pp. 796-808.
- [31] B. H. Miller, „Open source intelligence (OSINT): An oxymoron?“ Int. J. Intell. Counter Intell., 2018., vol. 31 (4), pp. 702-719.
- [32] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, M. Whitty, „Automatically dismantling online dating fraud“, IEEE Trans. Inf. Forensics Security, 2020., vol. 15, pp. 1128-1137.
- [33] J. Rajamaki, J. Simola, „How to apply privacy by design in osint and big data analytics?“, Proc. Eur. Conf. Inf. Warfare Secur., Coimbra, Portugal, 2019, pp. 364-371.
- [34] P. Mitzias, I. Kompatsiaris, E. Kontopoulos, J. Staite, T. Day, G. Kalpakis, T. Tsikrika, H. Gibson, S. Vrochidis, B. Akhgar, „Deploying semantic *Web* technologies for information fusion of terrorism-related content and threat detection on the *Web*“, Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Companion, 2019, pp. 193-199.
- [35] KASPERSKY. Preuzeto sa: <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint> (Pristupljeno: srpanj 2022. godine)
- [36] Elena SUSNEA, „A REAL-TIME SOCIAL MEDIA MONITORING SYSTEM AS AN OPEN SOURCE INTELLIGENCE (OSINT) PLATFORM FOR EARLY WARNING IN CRISIS SITUATIONS“, International conference knowledge-based organization, 2018, vol.24 (2), pp. 427-431
- [37] HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA. Preuzeto sa: <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-08-273.pdf> (Pristupljeno: srpanj 2022. godine)
- [38] John J. Barbara, „Handbook of digital and multimedia forensic evidence“, Totowa, New Jersey, Humana, 2008.
- [39] SECJUICE. Preuzeto sa: <https://www.secjuice.com/tracking-osint-hunters/> (Pristupljeno: kolovoz 2022. godine)
- [40] MALTEGO. Preuzeto sa: <https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/#socmint-vs-osint> (Pristupljeno: kolovoz 2022. godine)
- [41] Dale Liu, Cisco Router and Switch Forensics. Investigating and Analyzing Malicious Network Activity, Syngress, Burlington, MA, 2009.
- [42] Schwarz Klaus, Creutzburg Reiner, Design of Professional Laboratory Exercises for Effective State of the Art OSINT Investigation Tools, Electronic Imaging, 2021., vol 43(1).
- [43] CENTAR INFORMACIJSKE SIGURNOSTI. Preuzeto sa: <https://www.cis.hr/files/dokumenti/CIS-DOC-2012-05-048.pdf>, (Pristupljeno: kolovoz 2022. godine)

[44] ArcStone. Preuzeto sa:<https://www.arcstone.com/blog/digital-higiene#:~:text=Good%20digital%20higiene%20keeps%20your,attacks%2C%20and%20other%20online%20crimes>. (Pristupljeno: kolovoz 2022. godine)

[45] European Union Agency for Fundamental Rights, Council of Europe - Handbook on European data protection law (GDPR), Luxembourg, Council of Europe, 2018.

Popis kratica

OSINT	(Open Source Intelligence) javno dostupni podaci
GDPR	(General Data Protection Regulation) Opća uredba Europske unije o zaštiti podataka
DML	(Data Manipulation Language) distribucija razine upravljanja
HTML	(Hyper Text Markup Language) programski jezik za izradu internetskih stranica
DDos	(Distributed denial of service attack) napad uskraćivanjem usluge
RAM	(Random Access Memory) računalna memorija čijem se sadržaju može izvatno pristupiti
IP	(Internet Protocol) jedinstveni broj koji se dodjeljuje svakom uređaju
DHCP	(Dynamic Host Configuration Protocol) dinamička poslužiteljska konfiguracija protokola
VPN	(Virtual Private Network) virtulana privatna mreža
TOR	(The Onion Router) anonimni internetski pretraživač
UDHR	(Universal Declaration of Human Rights) Opća deklaracija o ljudskim pravima
ECHR	(European Convention on Human Rights) Europska konvencija o ljudskim pravima
ICCPR	(International Covenant on Civil and Political Rights) Međunarodni pakt o građanskim i političkim pravima
Konvencija 108	Konvencija o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka
CJEU	(Court of Justice of the European Union) Sud pravde Europske unije
EDPS	(European Data Protection Supervisor) Europski nadzornik za zaštitu podataka

Popis slika

Slika 1. Prikaz glavnih područja primjene OSINT-a [1].....	3
Slika 2.DML model otkrivanja incidenta [26]	9
Slika 3.Prikaz zlonamjernog koda pomoću DDos napada [36]	17
Slika 4.Prikaz određivanja veličine slike u HTML kodu i poveznice na slike određene u HTML kodu[36]	17
Slika 5. Dijagram aktivnosti scenarija istraživanja osobe od interesa	29
Slika 7. Stranica sažetka entiteta domene	32
Slika 8. Dostupni skupovi entiteta domene	33
Slika 9. Transformacija To Website koja je izvedena nad definiranim entitetom	35
Slika 10. Dobiveni rezultati URL-ova za prethodne entitete internetskih mjesta	36
Slika 11. Prikaz pojedinih entiteta vraćenih iz internetskih stranica.....	36
Slika 12. Prikaz dobivenih rezultata nakon transformacije IBM Watson	37
Slika 13. Rezultat transformacije To Images	37
Slika 14. Prikaz entiteta koji povezuje sve internetske stranice.....	38

Popis tablica

Tablica 1. Prikaz prednosti i nedostataka OSINT-a [9]	4
Tablica 2. Kategorizacije društvenih mreža prema namjeni [36]	16
Tablica 3. Prikaz dobivenih rezultata istraživanja	40
Tablica 4. Rezultati istraživanja osobe od interesa prema broju dolaznih linkova	41
Tablica 5. Prikaz prvih deset rezultata koji su pružili maksimalan broj linkova	41

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI


Izjavljujem i svojim potpisom potvrđujem da je _____ diplomski rad _____
(vrsta rada)

isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom __ Prikupljanje i analiza digitalnih otisaka primjenom programskog alata Maltego __, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

U Zagrebu, 09.09.2022.godine

Student/ica:

ANTONIO BIŠČAN 
(ime i prezime, potpis)