Upotreba sadržaja objavljenog na društvenim mrežama u obavještajne svrhe: akteri i ciljevi

Noršić, Karlo

Sveučilište u Zagrebu

Fakultet političkih znanosti

Diplomski studij politologije

Upotreba sadržaja objavljenog na društvenim mrežama u obavještajne svrhe: akteri i ciljevi

DIPLOMSKI RAD

Mentor: dr. sc. Robert Mikac, izv. prof.

Student: Karlo Noršić

Zagreb,

2023.

Izjavljujem da sam diplomski rad „Upotreba sadržaja objavljenog na društvenim mrežama u obavještajne svrhe: akteri i ciljevi“, koji sam predao na ocjenu mentoru dr. sc. Robertu Mikcu, izv. prof., napisao samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obveza na ovom ili nekom drugom učilištu te da na temelju njega nisam stekao ECTS-bodove.

Nadalje, izjavljujem da sam u radu poštivao etička pravila znanstvenog i akademskog rada, a posebno članke 16.–19. Etičkog kodeksa Sveučilišta u Zagrebu.

_____

Sadržaj

1. Uvod

Razvoj tehnologije, medija, društvenih mreža i interneta povećao je broj osoba koje se koriste internetom u privatne svrhe (prije svega koriste se društvenim mrežama). Pametni mobiteli, laka i jeftina dostupnost interneta te aplikacije koje pružaju brzo i jednostavno postavljanje sadržaja omogućuju ljudima objavljivanje privatnog sadržaja u većem obujmu. Lako dostupne informacije i podaci zanimljivi su svima: državi, civilnom društvu, ne-državnim akterima (NGO-s) i financijskom sektoru, kao i nekima drugima. U središtu istraživanja bit će prvonavedeni. Na temelju karakteristika ta četiri aktera mogu se podijeliti u dvije skupine: državni akteri (država) i ne-državni akteri (civilno društvo, NGO-s i financijski sektor).

Aktere vode različiti motivi zbog čega ih javno dostupni podaci zanimaju. Kako su društvene mreže svakodnevica većini ljudi, bitno je shvatiti tko se, kako i zašto koristi objavljenim. Stoga korisnici mreža postaju sve važniji i vrjedniji obavještajni izvor. Porast korisnika interneta i društvenih mreža te njihova sklonost objavljivanja potencijalno inkriminirajućeg sadržaja (može inkriminirati njih same ili nekog drugog) uzrok je većeg korištenja podataka dobivenih iz javno dostupnih izvora. Najbolji su primjeri nedavni sukobi u Siriji i Ukrajini. Država i drugi akteri dobivaju veliku količinu informacija (fotografije, videosnimke, položaj) na temelju sve učestalijeg korištenja sadržaja društvenih mreža. Kako bi što prije izvukli korist iz objavljenoga sadržaja, države, njihove institucije i drugi akteri brzo reagiraju. Korisnici društvenih mreža nisu svjesni ili su nedovoljno svjesni da se njihov objavljeni sadržaj koristi u obavještajne, ali i druge svrhe, poput personaliziranih reklama, krađe osobnih podataka i sl. Moguće posljedice takvog korištenja podataka su: sve veća zloupotreba podataka, razvijanje ilegalnih i invazivnih metoda prikupljanja podataka te povećanje moći tvrtki, vlasnica velikih društvenih mreža (poput Facebooka, Twittera i sl.).

Za prikupljanje i obrađivanje javno dostupnih podataka državne institucije i privatne tvrtke koriste se OSINT (engl. *Open-source intelligence*, hrv. obavještajne informacije iz otvorenih izvora) alatima. OSINT prikuplja razne vrste informacija i izvora koji su općenito dostupni, uključujući informacije dobivene iz medija (novine, radio, televizija, itd.), profesionalnih i akademskih zapisa (radovi, konferencije, strukovna udruženja, itd.) i javnih podataka (vladina izvješća, demografija, saslušanja, govori, itd.) (Pastor-Galindo i ostali, 2020: 10282). Jedna od prednosti OSINT-a je njegova dostupnost. Ipak, sama količina dostupnih informacija može otežati saznanje o tome koje su informacije vrijedne (Best, 2011: 62). OSINT može prikupljati

podatke i raditi pomoću izvora koji nisu nužno objavljeni na internetu (*offline* izvori) poput znanstvenih časopisa, knjiga, televizije, radija, ali najveći dio podataka prikuplja na internetu. (Hassan i Hijazi, 2018: 5). Nadalje, WEBINT ili *Web intelligence* je naziv za vrstu OSINT-a koji se sastoji isključivo od izvora prikupljenih pomoću interneta (Chauhan i Panda, 2015: 26). Razvojem interneta i pojavom velikih društvenih mreža (Facebook, YouTube, MySpace i sl.) nastaje SOCMINT (engl. *Social Media Intelligence*) kao potkategorija WEBINT-a. SOCMINT predstavlja proces identifikacije, utvrđivanja valjanosti, prikupljanja te analiziranja podataka i informacija s društvenih mreža. S ciljem razvoja proizvoda za nacionalnu sigurnost koriste se nametljivim i nenametljivim metodama (Ivan i ostali, 2015: 506). Veza između sadržaja koji se objavljuje i OSINT alata pokazuje da je s većom količinom sadržaja on važniji te se češće upotrebljava. Zbog toga dolazi do daljnjeg razvijanja OSINT alata koji postaje sofisticiraniji i učinkovitiji. Akteri koji ga rabe sve se više oslanjaju na takve dobivene informacije (Pastor-Galindo i ostali, 2020: 10302).

Zbog načina prikupljanja navedenih podataka i količine njihove dostupnosti raste broj privatnih tvrtki koje se bave prikupljanjem, analizom i upotrebom podataka objavljenih na društvenim mrežama. Države i obavještajne agencije prvi put imaju suparništvo, ali i partnerstvo, u prikupljanju podataka, a da to nije druga obavještajna agencija (Denécé, 2014: 36). Privatni sektor zbog načina funkcioniranja, u ovom slučaju, ima prednost naspram obavještajnih agencija. Tvrtke, kako bi opstale i ostvarile profit, prije svega moraju biti učinkovite, ekonomične i prilagodljive. S druge strane, država ima velike tehnološke, financijske i organizacijske izazove (Ahmet, 2020: 185-186). Stoga se privatiziraju određeni poslovi i aktivnosti unutar sigurnosnog sektora (Chesterman, 2008: 1056). Rastuća snaga privatnog sektora djelomično se temelji na njihovom visokom stupnju operativne fleksibilnosti, minimalnoj potrebi za pristajanjem na političke izbore, višoj razini učinkovitosti i često boljem omjeru povrata ulaganja, u usporedbi s državnim institucijama. Konkretno, jedan od čimbenika koji pokreće privatizaciju i suradnju s privatnim sektorom je poboljšanje učinkovitosti države. Kako bi postigle taj cilj, obavještajne agencije sve češće ugovaraju konzultante iz privatnog sektora za izvršavanje pojedinih poslova koje oni mogu učinkovitije obavljati (Ahmet, 2020: 191).

1.1. Problem istraživanja

Istraživački je problem sve veće korištenje podataka, koje korisnici objavljuju na društvenim mrežama, u obavještajne svrhe od različitih aktera koji imaju različite motive i ciljeve njihove

upotrebe. Ovo je problem vrijedan pažnje zbog nekoliko razloga: povećanje suradnje na polju prikupljanja i obrade *open-source* podataka između države i ne-državnih aktera (primarno privatnih izvođača), opasnosti koje prijete objavljivanjem sadržaja, razvoja intruzivnih načina prikupljanja osobnih podataka korisnika društvenih mreža, povećanje utjecaja i moći tvrtki u čijem su vlasništvu društvene mreže, mogućnost korištenja sadržaja u kriminalne svrhe različitih aktera zlih namjera, povećanje uporabe OSINT discipline i razvijanje OSINT alata.

1.2. Predmet istraživanja

Predmet su istraživanja akteri koji koriste javno dostupne podatke društvenih mreža. U radu će se prvenstveno razlikovati po svojim karakteristikama, načinu i svrsi djelovanja prema kojima će biti podijeljeni u dvije skupine: državni i ne-državni akteri. Objekt istraživanja su građani odnosno korisnici društvenih mreža. Građani su objekt istraživanja, zato što objavljuju potencijalno korisne podatke za razne aktere (prije svega fotografije i položaj). Ulaskom u informacijsko doba sredinom 20. stoljeća i ekspanzijom korištenja interneta prikupljanje i analiziranje javno dostupnih podataka počinje biti neizostavan dio obavještajnog djelovanja.

1.3. Cilj istraživanja

Cilj je istraživanja prikazati tko se sve koristi podacima s društvenih mreža. Objasniti koji su im motivi i ciljevi korištenja, kako razni akteri prikupljaju i rabe podatke te protumačiti na koji se način korisnici i objavljeni sadržaj upotrebljavaju u obavještajne svrhe.

1.4. Hipoteza i istraživačka pitanja

Hipoteza ovog rada je: porastom korištenja društvenih mreža i sklonošću njihovih korisnika objavljivanju sve više privatnih podataka različiti akteri češće upotrebljavaju te podatke u obavještajne svrhe te se u velikoj mjeri krši privatnost korisnika društvenih mreža.

Istraživačka pitanja diplomskog rada su:

1. Kako se koristi internet, prvenstveno društvene mreže, u svrhu prikupljanja obavještajnih podataka i zašto su korisnici sve više skloni objavljivati privatne podatke?
2. Tko se, kako i zašto koristi podatcima objavljenim na društvenim mrežama?

3. Može li se upotreba podataka objavljenih na društvenim mrežama koji se koriste u obavještajne svrhe okarakterizirati kao kršenje ljudskih prava i privatnosti?

1.5. Teorijsko-metodološki okvir istraživanja

Teorijski okvir ovog diplomskog rada sastoji se od realističke teorije međunarodnih odnosa, općih koncepata međunarodne sigurnosti, teorije privatnosti i teorije ljudskih prava. Prikazat će se različitim teorijama privatnosti i ljudskih prava može li se upotreba podataka objavljenih na društvenim mrežama u obavještajne svrhe okarakterizirati kao kršenje ljudskih prava i privatnosti.

Teorijski dio rada objašnjava zbog čega se različiti akteri sve više koriste podacima koji se objavljuju na društvenim mrežama. Koristit će se teorije međunarodnih odnosa (najviše realizam), odnosno povezat će se razlozi korištenja tih podataka s teorijama međunarodnih odnosa (motivacija aktera za korištenjem takvih podataka). Liberalne teorije inzistiraju na važnosti slobode naroda i same države zagovarajući pravo na samoodređenje, tj. uvjerenja da svaki narod ima pravo odlučivati o sebi i da nije legitimno da bilo tko drugi odlučuje o temeljnim pitanjima njegove egzistencije umjesto njega (Jović, 2014: 30). Za liberale država je korisna samo ako podupire proces oslobođenja čovjeka i ne postavlja prepreke slobodi (Jović, 2014: 37). Zbog univerzalnosti pojma slobode, za liberale, ratovi nikad nisu opravdani osim antiimperijalističke i antiokupacijske borbe za slobodu. Rat je opravdan kada je obramben i separatistički. No, liberali misle da je najbolje mirno rješavanje problema, sporazumom i uvjeravanjem (Jović, 2014: 33). Realisti vjeruju da je sukob neizbježan i vječan pa je rat uobičajen i svojstven čovječanstvu. Za realiste politika je primarno borba za moć i vlast, a liberali ju gledaju kao međuovisnost i suradnju između zemalja (Morgenthau, 2005: 5). Realisti će se između kaotične i slabe demokratske države te funkcionalne, ali nedemokratske države prije odlučiti za ovu koja je nedemokratska, ali funkcionalna (Jović, 2013: 18).

Nadalje, objasnit će se razlog nastanka društvenih mreža i motivacija korisnika za objavljivanjem sve više privatnog sadržaja. Prikazat će se argumenti zbog kojih korisnici smatraju da se njihovi podaci zloupotrebljavaju. S druge strane, govorit će se o različitim akterima i njihovoj uporabi podataka za vlastite ciljeve, smatrajući to njihovim legitimnim pravom. Pitanje krše li se ljudska prava navedenim korištenjima objasnit će se i odgovoriti stavljajući ga u kontekst različitih teorija privatnosti. Teorija *The Restricted Access/Limited Control* (hrv. ograničen pristup/ograničena kontrola) definira privatnost u smislu zaštite od

upada i prikupljanja informacija od drugih (u situacijama ili zonama ograničenoga pristupa), a ne kao kontrola nad informacijama (Tavani, 2007: 11). Ova teorija privatnosti propisuje niz radnji zaštitite određene vrste osobnih informacija koje, vjerojatno, imaju i privatne i javne karakteristike (Tavani, 2007: 18).

Društvene mreže mogu biti dvojne prirode: javne su prirode, ali se često osjećaju privatnima (Rønn i Søe, 2019: 363). Informacije objavljene na društvenim mrežama nalaze u 'sivoj zoni' između javnog i privatnog (Rønn i Søe, 2019: 363). Stoga dolazi do sigurnosne dileme, odnosno pitanja moralnosti i granica privatnosti.

Istraživački dio rada usredotočit će se na kvalitativnu metodu istraživanja tj. dubinsko razumijevanje korištenja javnih podataka četiri navedena aktera. Svako korištenje dobivenih podataka pojedinog aktera detaljnije će se opisati različitim primjerima (npr. korištenje podataka nezavisnog novinskog portala *Bellingcat,* afera *Cambridge Analytica,* sukob u Ukrajini i sl.). Nadalje, koristit će se kvantitativna metoda istraživanja u kojoj će se brojčano prikazati količina korištenja podataka dobivenih na društvenim mrežama (npr. statistički podaci koji prikazuju globalnu potražnju za tvrtkama koje se bave OSINT-om).

1.6. Pregled literature i ključni pojmovi

Prijevod engleske literature na hrvatski jezik relativno je težak jer neki pojmovi na engleskome imaju više značenja. Riječ *intelligence* u engleskom jeziku (u domeni sigurnosno-obavještajnog nazivlja) opisuje se s nekoliko različitih pojmova: naziv organizacija i sustava koji se bave prikupljanjem i obradom podataka i informacija; završni pisani uradak koji se dostavlja korisnicima obavještajnih informacija; naziv ciklusa/procesa od planiranja i prikupljanja do obrade i dostave obavještajnog uratka (Leško, 2019: 9).

U većini suvremenih rasprava obavještajna se djelatnost shvaća kao proces prikupljanja, analiziranja i korištenja informacija (Scott i Jackson, 2010: 141). Mnogi promatrači skloni su razumjeti obavještajne podatke prvenstveno kao alat stvaranja vanjske i obrambene politike. Pojedini se usredotočuju na njegovu ulogu u domaćoj sigurnosti, a drugi se usmjeravaju na ulogu koju su obavještajne službe igrale kao mehanizmi državnog ugnjetavanja (Scott i Jackson, 2010: 141).

Obavještajni ciklus obuhvaća planiranje i usmjeravanje obavještajnog ciklusa, prikupljanje informacija i provođenje istraživanja, obradu i pohranjivanje informacija, obavještajnu analizu

informacija i širenje (diseminacija) obavještajnih podataka (Bartes, 2013: 286). Sirovi podaci prikupljaju se iz javnih izvora (OSINT), posredstvom ljudskih izvora (HUMINT, engl. *human intelligence*), mjerama prisluškivanja i praćenja različitih komunikacijskih, radarskih, satelitskih i drugih elektroničkih signala (SIGINT, engl. *signals intelligence*) te njihovih potkategorija. Izvori podataka razni su izvori elektromagnetskih signala komunikacijske prirode (COMINT, engl. *communications intelligence*) ili nekomunikacijske prirode (ELINT, engl. *electronic intelligence*) (Leško, 2019: 10). Također, prikupljaju se obradom drugih obilježja objekata (MASINT, engl. *measurement and signatures intelligence*) i obradom slikovnih informacija (IMINT, engl. *imagery intelligence*) (Leško, 2019: 10).

Sirovi podatak ili informacija nije obavještajni podatak. Kako bi se pretvorila u obavještajni podatak, sirova informacija mora proći obradu i analizu (Phythian, 2013: 21). Obrada je predanalitička faza u kojoj se neobrađene informacije filtriraju i pripremaju nizom tehnika (poput dešifriranja, prijevoda jezika, redukcije podataka i sl.) za analizu (Phythian, 2013: 21). U fazi analize organizirane se informacije pretvaraju u obavještajni podatak (Phythian, 2013: 21). Dakle, obavještajni je ciklus promjena sirovih podataka u obavještajni podatak.

Kako bi se preciznije definirala dimenzija prikupljanja podataka, Bartlett, Miller i Omand skovali su termin *Social Media Intelligence* (SOCMINT), koji se odnosi na obavještajne podatke dobivene na društvenim mrežama (Bartlett i ostali, 2012: 802). SOCMINT je relativno novi pojam. To je interdisciplinarni koncept koji je nedavno dobio jasnu i općeprihvaćenu definiciju svih stručnjaka u tom području (Ivan i ostali, 2015: 506).

Svaka društvena mreža ima svoje uvjete korištenja koji daju određena prava vlasnicima, ali i korisnicima. Privatnost informacija i objavljenog sadržaja u postavkama neke društvene mreže pitanje je zaštite od nelegitimnog pristupa i korištenja osobnih podataka. Zaštita informacijske privatnosti često se definira kao ograničenje pristupa osobnim podacima ili kontrola protoka osobnih podataka (Rønn i Søe, 2019: 365). Ograničenje pristupa ili kontrole provodi se upotrebom informiranog pristanka. Korisnik mora odobriti pristanak kako bi drugi pristupili njegovim osobnim podacima i svemu što objavljuje na određenoj društvenoj mreži (Rønn i Søe, 2019: 363). Korisnici daju određenoj društvenoj mreži pristanak[1] i tako tvrtkama omogućuju pristup i korištenje njihovih osobnih podataka dostupnih na njoj (Rønn i Søe, 2019: 363).

Holtzman u svojoj knjizi *Privacy Lost: How Technology Is Endangering Your Privacy* definira sedam načina kršenja privatnosti na internetu: upadanje (engl. *intrusion*), latencija (engl.

[1] Putem prihvaćanja odredbi i uvjeta korištenja te mreže.

latency), obmana (engl. *deception*), profiliranje (engl. *profiling*), krađa identiteta (engl. *identity theft*), curenje podataka (engl. *outing*) i izgubljeno dostojanstvo (engl. *lost dignity*) (Holtzman, 2006).

Feldman i Haber u radu govore o opasnosti upadanja društva u tzv. *always on* (hrv. uvijek uključeno) doba. Odnosno mogućnosti neprestanog praćenja pojedinaca raznim uređajima, poput televizora, pametnih telefona, nosivih uređaja i sl. (Feldman i Haber, 2020: 199). Feldman i Haber smatraju da trenutni sektorski regulatorni pristup, koji štiti privatnost reguliranjem prikupljanja ili korištenja informacija samo u unaprijed definiranim industrijama, uvelike ugrožava privatnost pojedinaca. S druge strane, strogi propisi privatnosti mogli bi umanjiti korisnost podataka što je ključno za tehnološki razvoj i inovacije (Feldman i Haber, 2020: 199). Oni predlažu tehnološko rješenje. Oslanjajući se na metodu diferencijalne privatnosti, predlažu dodavanje „šuma“, odnosno smetnje podacima koje procjenjuju osjetljivima (Feldman i Haber, 2020: 234).

Edwards i Urquhart smatraju da prikupljanje podataka na društvenih mreža nije dovoljno dobro uređeno i da se krši privatnost korisnika. Govoreći o problemu privatnosti na društvenim mrežama, tvrde da je nadrealno očekivati da pojedini korisnik implicitno odustane od svih očekivanja privatnosti kada se pridruži nekoj platformi zbog uvjeta i odredbi koje nije pročitao, razumio i nije mogao promijeniti (Edwards i Urquhart, 2016: 308-309). U svome se radu bave policijskim nadzorom društvenih mreža. On je samo dio šire rasprave o tome tko ima pravo prisvajati i profitirati od digitalnih tragova koje korisnici ostavljaju. Ističu zakonske i etičke mjere zaštite koje bi korisnike društvenih mreža trebale štititi (Edwards i Urquhart, 2016: 309).

1.7. Očekivani rezultati istraživanja

Očekivani je rezultat istraživanja dokazivanje na temelju odrađenih analiza, sve veće korištenje objavljenih sadržaja građana na društvenim mrežama u obavještajne svrhe i dokazivanje važnosti OSINT alata u obavještajnoj djelatnosti. Također, očekuje se prikaz povećanja ekonomske i političke moći tvrtki u čijem su vlasništvu društvene mreže. Prikazivanje dubinskog razumijevanja korištenja takvih podataka različitih aktera trebao bi predočiti motive koji ih pokreću i ciljeve koje žele postići.

2. Korištenje interneta i društvenih mreža

Cilj je ovog poglavlja pokazati kako se koristi internet, tko su njegovi korisnici te zašto oni postaju važan i vrijedan izvor obavještajnih podataka. Ovo poglavlje odgovorit će na prvo istraživačko pitanje: „Kako se koristi internet, prvenstveno društvene mreže, u svrhu prikupljanja obavještajnih podataka i zašto su korisnici sve više skloni objavljivati privatne podatke?“

Internet je relativno nova tehnologija. Općenito nove tehnologije šire i izražavaju slobodu te decentraliziraju monopol nad postavljanjem agende oblikovanjem stvarnosti i moći (Benes, 2013: 27). One pokreću događaje, olakšavaju mobilizaciju društva, promatraju, štite, pa čak u nekim slučajevima, mogu donijeti i slobodu (Benes, 2013: 27). Sve do pojave interneta i aplikacija za komunikaciju i razmjenu informacija obavještajne informacije dobivene iz javno dostupnih podataka smatrane su niskom vrijednošću kao obavještajna disciplina (Dokman i Ivanjko, 2019: 195). Neprihvaćanje stvarne vrijednosti obavještajnih podataka otvorenog izvora uglavnom se podudaralo s apriornim stavom da obavještajni proizvod može doći isključivo iz tajnih izvora informacija. Rad s javno dostupnim podacima smatrao se manje vrijednim i manje zanimljivim za obavještajnu djelatnost i njihove korisnike (Dokman i Ivanjko, 2019: 195). Stoga je bitno shvatiti važnost interneta, koji je postao integralan dio života modernog društva, ali i razloge korisnika društvenih mreža koji objavljuju privatan sadržaj na bespućima interneta dostupnog svima. Shvatiti i objasniti motive koji pokreću korisnike društvenih mreža ključno je u pronalasku odgovora na istraživačko pitanje i, posljedično, za dokazivanje ili nedokazivanje hipoteze.

Prema različitim istraživanjima 2023. godine u svijetu je bilo 5,16 milijardi korisnika interneta, što je 64,4 % svjetske populacije. Od tog ukupnog broja, 4,76 milijardi, odnosno 59,4 % svjetske populacije bili su korisnici društvenih mreža (The Digital Study, 2023. i Statista, 2023.). Može se zaključiti kako je internet temeljni stup modernog informacijskog društva jer povezuje milijarde ljudi diljem svijeta. Web 2.0 odnosi se na drugu generaciju interneta koja naglašava sadržaj koji stvaraju korisnici, njihovu interakciju i društveno umrežavanje (O'Reilly, 2004: 24-25). On predstavlja pomak od statične, jednosmjerne komunikacije prema dinamičnoj, interaktivnoj komunikaciji. Stranice društvenih mreža (SNS, engl. *Social media network*) definiraju se kao usluge temeljene na internetu koje pojedincima omogućuju: stvaranje javnog ili polujavnog profila unutar ograničenog sustava, artikuliranje popisa drugih korisnika s kojima dijele vezu te pregledavanje njihovih popisa veza i onih koje su napravili drugi unutar sustava

(Boyd i Elison, 2007: 211). Društvene mreže važne su jer korisnicima omogućuju komunikaciju s velikim brojem korisnika određene mreže, a poruke, videozapisi, fotografije i slično, na internetu dostupne su u sekundama.

Sparck Jones (2003.) donosi niz tehnoloških svojstva koji se odnose na podatke o pojedincima:

1. Trajnost – jednom snimljena informacija rijetko nestaje.
2. Volumen – pohrana informacija je jeftina, stoga velike količine skupova informacija mogu postojati neograničeno.
3. Nevidljivost – čak i ako su prikupljene informacije dostupne osobi, ona ih možda neće moći protumačiti zbog nerazumljivog kodiranja.
4. Neutralnost – informacije se mogu apsorbirati bez obzira na njihove metapodatke, tj. ne postoje razlike između intimnih, osjetljivih informacija i neosjetljivih informacija.
5. Dostupnost – postoji niz alata za pristup informacijama pa prikupljene informacije može pročitati neznan broj ljudi. Lakoća kojom se informacije mogu kopirati, prenijeti integrirane i elektronski umnožiti dodatno povećava dostupnost.
6. Sastavljanje – postoje mnogi učinkoviti alati za traženje, sastavljanje i reorganizaciju informacija iz puno odvojenih izvora.
7. Udaljenost – prikupljene informacije obično su, i fizički i logički, udaljene od korisnika na koje se odnose. Tim informacijama mogu pristupiti i koristiti se osobe koje korisnik ne poznaje (Jones, 2003: 3-7).

Svako od ovih navedenih svojstava utječe na privatnost korisnika interneta i društvenih mreža.

Može se zaključiti da ljudi objavljuju privatni sadržaj na društvenim mrežama iz različitih razloga: povezivanje s drugima, dijeljenje iskustava, pokazivanje kreativnosti, izgradnja osobnoga brenda i traženje društvene potvrde. Društveni mediji pružili su platformu za dijeljenje osobnih života korisnika sa svojom *online* zajednicom. Posljedično, dolazi do revolucionarizacije načina na koji ljudi komuniciraju i povezuju se jedni s drugima. Međutim, važno je upamtiti da sadržaj koji ljudi dijele na društvenim mrežama može imati pozitivne i negativne posljedice. Ključno je koristiti se društvenim mrežama odgovorno. Odgovornost se prije svega odnosi na očuvanje svoje privatnosti.

2.1. Što pokreće korisnike na objavu privatnog sadržaja?

Postoje različite teorije koje govore o motivima i pokretačima objavljivanja privatnog sadržaja. Ovaj će se rad usredotočiti na teoriju korištenja i gratifikacije, teoriju upravljanja komunikacijskom privatnošću[2] te korištenje dviju osnovnih društvenih potreba pojedinaca: potreba za pripadanjem i potreba za samopredstavljanjem. Shvaćanjem razloga ponašanja pojedinaca mogu se razviti učinkovite strategije promicanja pozitivne upotrebe društvenih medija i ublažavanje njihovih negativnih učinaka na pojedince i društvo. Također, doprinijet će boljem razumijevanju motivacije korisnika oko provođenja puno vremena na društvenim mrežama na kojima dijele, prosljeđuju i šire privatne, ali i druge sadržaje.

Teorija korištenja i gratifikacije često se koristi tijekom proučavanja korištenja masovnih medija poput novina, interneta, radija, televizije i sl. Prema Ruggieru teorija pretpostavlja da se pojedinci koriste medijima kako bi zadovoljili svoje specifične potrebe i želje. Izbor medija, pozornost i interpretacija pod utjecajem su psihološkog sastava pojedinca koji ovisi o njegovom društvenom okruženju i individualnim motivima (Ruggiero, 2000: 28-29). Elementi kao što su tjelesno zdravlje, mobilnost, zadovoljstvo životom, međuljudska interakcija, društvena aktivnost i ekonomska sigurnost sadržavaju više informacija od puke demografije u objašnjavanju međuljudskih potreba i motiva (Bondad-Brown i ostali, 2012: 473). Dakle, osnovna premisa teorije korištenja i gratifikacije traženje je medija koji ispunjavaju potrebe pojedinca i vode do konačnog zadovoljstva (Lariscy i ostali, 2011: 751). Teorija, također, pruža metodologiju prema kojoj se korisničke sklonosti i zadovoljstvo mogu usporediti na društvenim mrežama (Quan-Haase, 2012: 3).

Istraživanje Whiting i Williamsa iz 2013. godine bavi se razlozima ljudskog korištenja društvenim mrežama. U istraživanju su identificirali deset načina teorije korištenja i gratifikacije pri korištenju društvenih medija: društvena interakcija (88 %), traženje informacija (80 %), provođenje vremena (76 %), zabava (64 %), opuštanje (60 %), komunikacijska korisnost (56 %), izražavanje mišljenja (56 %), pogodnost (52 %), dijeljenje informacija (40 %) te nadzor i promatranje drugih (20 %) (Whiting i Williams, 2013: 368).

Sheldon i Bryant (2016.) istražuju zbog čega se studenti koriste društvenom mrežom Instagram. Zaključuju da studenti prije svega upotrebljavaju Instagram kako bi vidjeli što im rade prijatelji, obitelj, kolege u svakodnevnom životu koji objavljuju na Instagramu, odnosno kako bi bili u

[2] CPM, engl. *Communication privacy management theory*.

toku zbivanja (Sheldon i Bryant, 2016: 96). Također, jaki motivi koji su pokretali studente bili su: osjećaj pripadanja, dokumentiranje vlastitog života objavljivanjem fotografija i videozapisa, kreativnost tijekom korištenja Instagrama (fotografiranje, *photoshop* i sl.) (Sheldon i Bryant, 2016: 96). Istraživanje je pokazalo da različite psihološke i društvene okolnosti (zadovoljstvo životom, društvena aktivnost, narcizam) mogu pojačati određene tendencije ponašanja (motivi za korištenjem Instagramom) koje u konačnici pokreću drukčije ishode ponašanja (broj sati provedenih na stranici, uređivanje fotografija, korištenje *hashtagova*) (Sheldon i Bryant, 2016: 96).

Alhabash i Ma (2017.) proveli su istraživanje među studentskom populacijom o motivima upotrebe društvenih mreža (Facebook, Twitter, Instagram i Snapchat). Autori su otkrili kako se motivi za korištenje ovih platformi razlikuju ovisno o spolu i rasi/etničkoj pripadnosti. Na primjer, studentice su se češće koristile Instagramom za samoizražavanje i inspiraciju. Studenti su se nerijetko služili Twitterom za izgradnju osobnoga brenda (Alhabash i Ma, 2017: 6). Hispanoamerički i afroamerički studenti češće su upotrebljavali Snapchat za privatnu komunikaciju od bijelih i azijskih studenata (Alhabash i Ma, 2017: 8). Sudionici su izjavili da se jednako koriste svima četirima platformama za razmjenu informacija. Motivira ih, prije svega, zabava i praktičnost (Alhabash i Ma, 2017: 7). Ovo je istraživanje pokazalo da svaka društvena mreža služi jedinstvenoj svrsi i ispunjava različite potrebe korisnika. Kao takve društvene se mreže ne mogu smatrati međusobno zamjenjivima ili identičnima.

Sve većom ulogom društvenih medija u modernom društvu, teorija zadovoljstva i gratifikacije čini se obećavajućom. Pruža teorijski okvira za ispitivanje prihvaćanja pojedinih društvenih medija u različitim segmentima stanovništva i zadovoljstva pojedinaca korištenjem različitih društvenih medija (Quan-Haase, 2012: 3).

Potreba za pripadanjem i potreba za samopredstavljanjem jedne su od važnijih društvenih potreba pojedinca. Potreba za pripadanjem temeljni je poticaj za stvaranje i održavanje međuljudskih odnosa. Ljudska bića imaju prirodni nagon za stvaranjem i održavanjem barem minimalne količine trajnih, pozitivnih i značajnih međuljudskih odnosa (Baumeister i Leary, 1995: 497). Teorija samopredstavljanja govori da je samopredstavljanja vođeno željom za upravljanjem dojmovima koji drugi imaju o nama, ali i vladanjem osjećaja u sebi – kako se zamišljamo i razmišljamo o sebi (Leary i Kowalski, 1990: 34). Ljudi imaju prirodnu želju da ih drugi vole i prihvate, zato samopredstavljanje može biti jedan od način za postizanje tog cilja. Predstavljajući drugima poželjan imidž, pojedinci mogu povećati svoje izglede kod njih.

Demografski i kulturološki čimbenici doprinose potrebi za pripadanjem, a neuroticizam, narcisoidnost, sramežljivost, samopoštovanje i vlastita vrijednost pridonose potrebi za samopredstavljanjem (Hoffman i Nadkarni, 2012: 1).

Cilj istraživanja koje su proveli Ellison, Steinfield i Lampe (2007.) bio je doznati zbog čega se ljudi služe Facebookom, ispitujući motivaciju korisnika i koristi koje imaju od platforme. U studiji je identificirana jedna od primarnih motivacija za korištenje Facebooka, a to je društvena povezanost. Korisnici su izjavili da upotrebljavaju Facebook kako bi ostali u kontaktu s prijateljima i obitelji, stekli nove prijatelje i ponovno se povezali sa starim poznanicima, što im je platforma omogućila na jednostavan način (Ellison, Steinfield i Lampe, 2007: 1162). Među prvotnom motivacijom je i samoizražavanje. Korisnici su izjavili kako se služe platformom za izražavanje, dijeljenje vlastitog mišljenja i uvjerenja te pokazivanje identiteta (Ellison, Steinfield i Lampe, 2007: 1162).

Seidman u svom istraživanju iz 2012. istražuje odnos između osobina pojedinaca i motiva korištenja društvene mreže Facebook. Tvrdi da pojedinačne osobine utječu na uporabu platformi društvenih medija, njihove motive i ponašanje (Seidman, 2012: 403). Koristeći model pet faktora (otvorenost, savjesnost, susretljivost, ekstrovertiranost i neuroticizam), kako bi prikazao vezu između potrebe za pripadnošću i samopredstavljanjem, Seidman zaključuje da su osobine susretljivosti i neurotičnosti najbolji pokazatelji pripadnosti (Seidman, 2012: 405-406). Neurotične osobe često imaju socijalne poteškoće, stoga pomoću društvenih mreža, poput Facebooka, zadovoljavaju potrebu za pripadnošću, koja nije dovoljno ispunjena izvan mreže (Seidman, 2012: 406). Visoki neuroticizam i niska savjesnost bili su najbolji prediktori samopredstavljanja (Seidman: 2012: 406). Savjesni pojedinci oprezni su u svojemu samopredstavljanju na Facebooku, a neurotični pojedinci mogu se koristiti Facebookom kao sigurnim mjestom za predstavljanje sebe, uključujući skrivene i idealne aspekte sebe (Seidman, 2012: 406).

Otkrivanje privatnih informacija na društvenim mrežama jedno je od važnijih pitanja u današnjim raspravama o upravljanju informacijama. Teorija upravljanja komunikacijskom privatnošću predstavlja mapu. Pretpostavlja da su privatna otkrivanja dijalektička. Ljudi donose odluke o otkrivanju ili prikrivanju na temelju kriterija i uvjeta koje doživljavaju kao istaknute. Pojedinci vjeruju da imaju pravo posjedovati i uređivati pristup svojim privatnim podacima (Petronio, 2002: 2). Dakle, teorija objašnjava kako ljudi donose odluke o otkrivanju ili skrivanju osobnih podataka raznim kriterijima kao što su individualne karakteristike, kontekst, motivacija

i korist-rizik (Petronio, 2002: 3-4). One utječu na određivanje granice korisnika između privatnih i javnih informacija. Rastući fenomen društvenih mreža, koje od korisnika zahtijevaju otkrivanje osobnih podataka, razotkriva ograničenja prethodnih studija koje su se usredotočile samo na dobrovoljno otkrivanje korisnika. Zbog toga su u svojoj studiji Cheng, Li i Teng (2020.) definirali dva načina ponašanja korisnika pri otkrivanju privatnih informacija: dobrovoljno dijeljenje i obvezno pružanje (Cheng, Li i Teng, 2020: 2). Ovo je istraživanje proučavalo utjecaj različitih čimbenika na spremnost otkrivanja privatnih informacija. Rezultati pokazuju da percipirane koristi imaju jači utjecaj na spremnost korisnika na otkrivanje privatnih informacija te su glavni pokretači otkrivanja informacija. Korisnici koji su oprezniji u otkrivanju osobnih podataka manje su voljni otkriti privatne podatke na internetu. Percipirane koristi imaju veći utjecaj na dobrovoljno dijeljenje nego na obvezno (Cheng, Li i Teng, 2020: 13). Poboljšanje kvalitete usluga društvenih mreža i zadovoljavanje potreba korisnika olakšava im dobrovoljno dijeljenje privatnih informacija (Cheng, Li i Teng, 2020: 13). Budući da su rizici koje korisnici percipiraju veći u obveznom pružanju, društvene bi mreže trebale pokušati izbjeći prikupljanje velikih količina osjetljivih informacija pri registraciji. Umjesto toga trebale bi od korisnika zahtijevati samo davanje ograničenih informacija (Cheng, Li i Teng, 2020: 13). Dobrovoljno dijeljenje može stvoriti kulturu dijeljenja gdje se privatne informacije smatraju svojevrsnom valutom za društvenu potvrdu. Nasuprot tome, obvezno pružanje informacija može stvoriti kulturu nadzora u kojoj se pojedinci osjećaju prisiljenima na otkrivanje osobnih podataka i sumnjaju u motive društvenih mreža.

Dakle, teorija korištenja i gratifikacije, teorija upravljanja komunikacijskom privatnošću te potreba za pripadanjem i potreba za samopredstavljanjem prikazali su duboke psihološke motive korištenja društvenih mreža i suvremeno okruženje koje utječe na svakodnevni život pojedinaca. Sve navedeno ima za posljedicu veće objavljivanje privatnih podataka i korištenje društvenih mreža čime korisnici postaju vrlo važan i vrijedan izvor obavještajnih podataka.

Internet je pravi primjer demokracije. On daje jednak pristup korištenju ili stvaranju otvorenih izvora (osim cenzuriranih ili ograničenih od antidemokratskih režima) bez obzira na osobni status ili hijerarhiju (Benes, 2013: 26). Nadalje, on podržava slobodno tržište, pomaže provođenju zakona u borbi protiv kriminala i špijunaže te ima pasivni, ali i aktivni, utjecaj na državnu moć (Benes, 2013: 26). Ostaje dojam da je internet, prije svega društvene mreže i njihovo korištenje, neizostavan dio modernoga načina života. Korištenje društvenih mreža postalo je neizbježan dio svakodnevne rutine. Proliferacija društvenih mreža i povećanje njihovog korištenja ima svoje pozitivne i negativne strane. Pružanje povezivanja, komunikacije,

zabave, poslovnih prilika, dijeljenja informacija i inovacija svakako su pozitivne strane. No, postoje i negativna stajališta, poput nepovoljnog utjecaja na mentalno zdravlje i privatnost, širenja dezinformacija, *cyberbullying*-a i ovisnosti o društvenim mrežama. Iako postoji zabrinutost zbog negativnih učinaka, dobrobiti nadmašuju nedostatke. Budući da su postali ključan alat za komunikaciju i povezivanje, malo je vjerojatno da će društveni mediji uskoro prestati postojati.

Ovo je poglavlje prikazalo važnost i veličinu društvenih mreža te motive i unutarnje pokretače pojedinčevog korištenja društvenih mreža danas. Zaključno, razumijevanje vrijednosti društvenih medija bitno je jer se promijenio način komuniciranja, međusobnog djelovanja i upotrebe informacija. Utjecaj društvenih mreža može se prepoznati u nizu domena, od osobnih odnosa do poslovanja i politike. Razumijevanje vrijednosti društvenih medija pomoći će shvatiti korištenje podataka objavljenih na njima u obavještajne svrhe.

3. Korisnici društvenih mreža: motivi i ciljevi

Ovo poglavlje odgovara na drugo istraživačko pitanje: „Tko se, kako i zašto koristi podacima objavljenima na društvenim mrežama?“. Odgovor će dati važna saznanja o tome tko eksploatira društvene mreže, na koji način to radi te koji su mu ciljevi. Shvaćanjem toga dobit će se slika današnjeg problema objavljivanja privatnog sadržaja na društvenim mrežama.

Već spomenuto, razlikovat će se dvije skupine aktera koji koriste podatke objavljene na društvenim mrežama u obavještajne svrhe: državni akteri (država) i ne-državni akteri (civilno društvo, NGO-s i financijski sektor). Državne aktere od interesa, za ovo istraživanje, koji se koriste podacima možemo podijeliti na vojsku, obavještajnu zajednicu i policiju. U ne-državne aktere, prema istoj osnovi, ubrajamo civilno društvo, financijski sektor, istraživačko novinarstvo, terorističke i kriminalne organizacije.

Internet i društvene mreže danas su na jedan način izazov nacionalnoj sigurnosti, zato što omogućuju brzo i jeftino povezivanje između aktera koji imaju maliciozne namjere (poput terorista, kriminalaca i sl.). Negativni učinci za nacionalnu sigurnost mogu nastati kada se država, ali i ne-državni akteri, koriste društvenim medijima. Posebice kada se društvenim mrežama koriste osobe koje imaju doticaja s osjetljivim sigurnosnim informacijama koje rabe u ilegalne svrhe (npr. diplomatski predstavnici, zaposlenici obavještajnih službi i sl.) (Musladin, 2012: 72). Bitno je definirati razliku između podatka i informacije. Podatak nudi činjenicu, a ne interpretaciju ili kontekst pojavnosti te opisuje samo dio onoga što se događa (Čavalić, 2016: 496-497). Informacija je obrađeni podatak koji daje odgovore na pitanja „tko“, „što“, „gdje“ i „kada“ (Chen i ostali, 2008: 13). Iz velikih količina javno dostupnih podataka samo pojedini mogu postati vrijedne i iskoristive informacije za određene korisnike ili aktere. Oni postaju informacije pomoću OSINT metode. OSINT alatima nije problem dostupnost podataka, nego im izazov predstavlja korištenje odgovarajuće metodologije za izdvajanje odgovarajućih podataka, njihovo čišćenje, obradu i kombiniranje sa što više mogućih resursa. Ključna sastavnica pretvaranja podataka dobivenih iz otvorenog izvora u korisne obavještajne informacije događa se tijekom etape analize i tumačenja (Gibson i ostali, 2016: 95).

Prema NATO-u informacije i obavještajni podaci otvorenih izvora dijele se u četiri kategorije: podaci otvorenog izvora (sirove informacije i podaci), informacije otvorenog izvora (obrađene informacije, npr. sadržaj u novinama), obavještajni podaci otvorenog izvora (OSINT) (kompilirani podaci koji se odnose na određeni upit) i potvrđeni obavještajni podaci otvorenog

izvora (OSINT koji ima visok stupanj sigurnosti u svoju istinitost) (Gibson, 2016: 70 prema NATO, 2001.). Dakle, bitno je izraditi OSINT proces pretraživanja koji će imati strukturu i niz dosljednih i sustavnih procesa pretraživanja. Općenito se proces korištenja OSINT metode sastoji od pet koraka: identificiranje izvora, prikupljanje podataka, obrada podataka, analiza i izvještavanje (Yong-Woon i ostali, 2022: 3-4). Osnovno OSINT istraživanje, unutar konteksta interneta, nastoji identificirati *online* otisak korisnika i tako izvući korisne podatke (Ramwell i ostali, 2016: 198). Otisak korisnika neizbježan je nusproizvod svakog *online* posjeta (Ramwell i ostali, 2016: 198). Nakon što je pojedinac sudjelovao *online,* sporazumno ili na neki drugi način, sposobnost uklanjanja ili brisanja digitalnog otiska postaje iznimno težak zadatak (Ramwell i ostali, 2016: 198). To dokazuju pojedine društvene mreže. Kada netko izbriše svoj profil, i dalje je moguće pristupiti pojedinim informacijama, fotografijama i sl.

Realizam je teorija međunarodnih odnosa. Prikazuje da su međunarodni odnosi vođeni težnjom za moći i sigurnošću te da države djeluju u vlastitom interesu kako bi zaštitile nacionalnu sigurnost i unaprijedile svoju moć u globalnom sustavu (Donnelly, 2000: 9-11). U tom se kontekstu korištenje podataka objavljenih na društvenim mrežama u obavještajne svrhe može promatrati kao sredstvo kojim države mogu prikupiti informacije o postupcima i namjerama drugih država. Predviđanjem i sprječavanjem potencijalnih prijetnji mogu zaštititi vlastitu sigurnost. Nadalje, realizam naglašava ograničenja politike koja nameće ljudska priroda i nepostojanje međunarodne vlade. Međunarodni odnosi postaju sfera moći i interesa (Donnelly, 2000: 9). Zbog toga se države moraju osloniti na vlastite resurse i sposobnosti kako bi zaštitile svoju sigurnost i unaprijedile svoje interese (Waltz, 2010: 92). Motiv preživljavanja osnova je za djelovanje u svijetu u kojem stanje sigurnosti nije osigurano i garantirano (Waltz, 2010: 92). Prema realistima sigurnost nije nikada zajamčena jer takva sigurnost može nastati samo uspostavom globalne vlasti koja bi bila dovoljno moćna da nameće zakone i kažnjava prekršitelje, što je malo vjerojatno (Jolić, 2011: 120). Dakle, nesigurnost (strah izazvan spojem anarhije i mogućnosti premoći jedne države nad drugima) trajno je obilježje međunarodnih odnosa (Rathbun, 2007: 533). U takvim je okolnostima za države racionalno činiti isto što rade pojedinci u prirodnom stanju, odnosno što je više moguće povećati vlastitu moć kako bi osigurale opstanak (Jolić, 2011: 120). Korištenje podataka objavljenih na društvenim mrežama u obavještajne svrhe u skladu je sa stajalištem realista. Države se koriste vlastitim resursima i stručnostima za prikupljanje, analizu i interpretaciju podataka kako bi imale uvid u postupke i namjere drugih država. Time štite same sebe i šire svoju moć. Danas većina država u svojoj

strategiji nacionalne sigurnosti ima barem jedan dio koji prikuplja javno dostupne podatke i brine o sigurnosti na internetu, a sve više novaca ulažu u kibernetičke sektore.

3.1. Korištenje podataka državnih aktera u obavještajne svrhe

Tijekom posljednjeg desetljeća *open-source* metoda prikupljanja podataka postala je sve važnija i učestalija. Jedan od razloga, koji je potaknuo povećanje, događaji su tijekom Arapskog proljeća kada su društveni mediji prvi put korišteni na prosvjedima. Kasnije su ih rabili medijski aktivisti i naoružane skupine koje su sudjelovale u sukobima proizašlim iz tih prosvjeda (Higgins, 2016: 189). Tijekom toga razdoblja pojedinci i organizacije počeli su istraživati načine prikupljanja i obrade ogromne količine informacija iz tih zemalja (Higgins, 2016: 189). Već rečeno, iz velikog bazena javno dostupnih informacija samo neke mogu postati obavještajni podaci. Kriteriji koji se koriste za procjenu obavještajnih podataka, tako i OSINT-a, su točnost, pouzdanost, pravovremenost i stjecanje konkurentske prednosti (Benes, 2013: 25).

Agencije za provođenje zakona

Kako bi se učinkovito bavile svim vrstama suvremenih sigurnosnih prijetnji, agencije za provođenje zakona (u prvom redu policija) koriste se sve više obavještajnim podacima koje prikupljaju iz javno dostupnih informacija (Staniforth, 2016: 22). Neumoljiva potraga policijskih službenika za obavještajnim podacima, radi sigurnosti zajednice, korištenjem informacija dobivenih iz otvorenih izvora, proizvela je najbrže rastuću policijsku disciplinu 21. stoljeća, a to je OSINT (Staniforth, 2016: 22). Budući da izričito cilja na informacije koje su vidljive gotovo svakom društvenom akteru, OSINT se suprotstavlja konvencionalnom razumijevanju sigurnosno-obavještajnih podataka (Trottier, 2015: 531). Policijski službenici shvaćaju da je neophodno da se njihovi napori oslanjaju na obavještajne podatke ako žele imati utjecaj na borbu protiv suvremenog kriminala (Staniforth, 2016: 23). Ovo predstavlja disciplinu poznatu kao *intelligence-led policing* (hrv. policijski rad vođen obavještajnim podacima, u daljnjem tekstu ILP) koja se definira kao:

„[…] poslovni model i upravljačka filozofija gdje su analiza podataka i obavještajni podaci o kriminalu ključni za objektivan okvir donošenja odluka koji olakšava smanjenje kriminala i problema, ometanje i prevenciju kroz strateško upravljanje i učinkovite strategije provedbe usmjerene na ozbiljne prijestupnike." (Ratcliffe, 2008: 6).

Policijsko prikupljanje OSINT-a obično se postiže praćenjem, rudarenjem podataka i istraživanjem (Staniforth, 2016: 26). Informacije se, također, mogu dobiti od izvora koji naplaćuju svoje usluge. Iako su vrijedni, treba biti oprezan jer istražitelj može razotkriti svoje djelovanje ili namjeru i tako ugroziti istragu (Ramwell i ostali, 2016: 198). Istražitelj treba uzeti u obzir da osoba pod istragom možda nije svjesna svoje *online* prisutnosti. Njegova se fotografija može pojaviti na mrežnoj stranici društvenih medija s označenim imenom na njoj, a sve je učinjeno bez njegovog znanja (Ramwell i ostali, 2016: 198). Nakon što je pojedinac sudjelovao *online,* sposobnost brisanja digitalnog otiska postaje težak zadatak. S obzirom na to da je istražitelj prošao ispravnu obuku, ima stalnu praksu i rabi ažurirane alate, obično može pronaći korisnikov *online* otisak (Ramwell i ostali, 2016: 199).

Korištenje informacija dobivenih s društvenih mreža, odnosno otvorenog izvora, ima pozitivan i velik utjecaj na modernu policijsku djelatnost. Pomoću tih informacija provode se uhićenja za ozbiljne kriminalne aktivnosti. Podrijetlo, uspoređivanje, tumačenje, analiza i primjena obavještajnih podataka otvorenog izvora postalo je vrlo aktualno i relevantno područje policijskog rada (Sampson, 2016: 295). Zaključno, zadaća i strategija policije nije provođenje nadzora i kontrole zabranama i cenzurama, već poticanje cirkulacije i vidljivosti sadržaja objavljenog na društvenim mrežama, kako bi sebi olakšala posao.

Vojska, obavještajne službe i OSINT

Svaka država posjeduje i održava određene obavještajne službe za prikupljanje i analizu informacija kako bi zajamčila sigurnost svoje zemlje (Ziółkowska, 2018: 66). Sve su radnje tajne i podupiru odluke državnih tijela. Iz sigurnosnih razloga načini na koje se radnje, strukture i učinci provode ograničeni su u njihovoj javnoj dostupnosti (Ziółkowska, 2018: 66). Terorizam, *proxy* ratovi, lijevi i desni ekstremizam, protivničko provođenje obuke, raspoređivanje snaga, sponzoriranje nedržavnih aktera nekoliko je primjera suvremenih ugroza koje je moguće pratiti i analizirati javno dostupnim izvorima (Haridas, 2015: 74).

Neke od glavnih metoda prikupljanja podataka otvorenog izvora vezanih uz vojsku su: otkrivanje i analiza vojne infrastrukture, otkrivanje i analiza premještanja vojnih snaga, uključujući procjenu potencijala protivnika, praćenje tekućih vojnih operacija, uključujući procjenu ratnih žrtava, geolociranje trupa na bojnom polju (Lakomy, 2022: 301). Ove su metode

spoj GEOINT-a[3] i IMINT-a[4], a najkorisnija aplikacija je Google Maps (Lakomy, 2022: 301). Podaci o sumnjivoj osobi ili skupinama mogu se tražiti pomoću alata za velike podatke (engl. *Big Data Tools*) na društvenim mrežama, stranicama za kupovinu i zabavnim stranicama. Na temelju prikupljenih podataka poduzimaju se daljnje radnje (Haridas, 2015: 74). Analitika velikih podataka definira se kao način obrade podataka koji su preveliki da bi se mogli ručno obraditi (Hammond-Errey, 2022: 3). Ona omogućuje milijunima informacija da se objedine i analiziraju (Hammond-Errey, 2022: 3). Analitika velikih podataka pruža dodatnu vrijednost metodama prikupljanja podataka i praćenja sumnjivih osoba, poput praćenja društvenih medija, rudarenja informacija i analize dokumenata (Haridas, 2015: 75).

Obavještajne se službe sve više koriste OSINT-om. Pristupajući ogromnoj količini sadržaja, koji se kontinuirano ažurira, mogu pratiti ciljane pojedince bez stavljanja sebe i svojih zaposlenika u neposrednu opasnost tijekom prikupljanja informacija, što bi bilo u slučaju korištenja ljudske inteligencije (Putter i Henrico, 2022: 27). Obavještajne službe upotrebljavaju OSINT i internet općenito kao protuobavještajni alat. Na primjer, mogućnost manipuliranja sadržajem na internetu u stvarnom vremenu kao dio obmane (Putter i Henrico, 2022: 28). OSINT analitički alati pružaju okvire za tehnike rudarenja podataka za analizu podataka, vizualizaciju uzoraka i nude analitičke modele za prepoznavanje i reagiranje na identificiranje uzoraka (Tabatabaei i Wells, 2016: 221). Takvi su analitički alati softverski proizvodi. Oni pružaju prediktivne i preskriptivne analitičke aplikacije od kojih se pojedine izvode na velikim računalnim platformama otvorenog koda (Tabatabaei i Wells, 2016: 221). Iz perspektive nacionalne sigurnosti, rješenja temeljena na OSINT-u trebala bi poboljšati sposobnosti sigurnosnih službi. Pružajući pristup djelotvornijim obavještajnim podacima, mogu podržati postojeće aktivnosti donošenja odluka, dodjele zadataka i koordinacije između različitih agencija (Akhgar, 2016: 7).

Incident koji se dogodio 2013. uporabom kemijskog oružja u ratu u Siriji, gdje su Sjedinjene Američke Države objavile tisuće videozapisa kako bi potkrijepile tvrdnje o napadu na Istočnu Ghoutu, primjer je kako države sve više koriste sadržaj objavljen na društvenim mrežama u obavještajne svrhe (Saugmann, 2019: 350). Još jedan dobar primjer državnoga prisvajanja fotografija građana je korištenje fotografija civila Ukrajinske države. Njima su dokazali da su

[3] engl. *Geospatial intelligence*.
[4] engl. *Imagery Intelligence*.

'mali zeleni' među separatističkim borcima u istočnoj Ukrajini i na Krimu zapravo ruski vojnici (Saugmann, 2019: 350).

U slučaju državnih aktera nije samo važno prikupljati podatke o sumnjivim osobama i neprijateljima već i educirati zaposlenike o vlastitoj zaštiti i čuvanju povjerljivih podataka. Svrhovito i zakonito praćenje, analiziranje i vizualiziranje javnih izvora podataka trebalo bi se smatrati obveznim zahtjevima svake strategije nacionalne sigurnosti (Akhgar, 2016: 9). Zaključno, OSINT je postao integralan dio nacionalne sigurnosti te ga državne službe sve više upotrebljavaju za prikupljanje informacija i analizu podataka. Konkretan primjer u Hrvatskoj je odluka Vlade 2022. o osnivanju Centra izvrsnosti za prikupljanje, obradu i analizu podataka iz otvorenih izvora. Međunarodni Centar izvrsnosti za prikupljanje, obradu i analizu podataka iz otvorenih izvora odgovor je SOA-e (Sigurnosno-obavještajna agencija) na rastući broj obavještajnih podataka, koji se generiraju iz otvorenih izvora, te veću potrebu europskih sigurnosnih i obavještajnih agencija za razvojem i jačanjem sposobnosti izdvajanja, prikupljanja, obrade i analize podataka iz otvorenih izvora (SOA, 2022.).

3.2. Ne-državni akteri i javno dostupni podaci

Obavještajna djelatnost, uključujući otvorene izvore obavještajnih informacija, više nije obilježje koje pripada samo državi. Prikupljanje, analitička obrada i proizvodnja relevantnog i djelotvornog obavještajnog znanja sada su tipični i za državne i za ne-državne aktere (Dokman i Ivanjko, 2019: 195). U posljednjih nekoliko godina pristup novim *online* alatima učinio je istraživanje otvorenog koda nečim što svatko može raditi iz vlastitog doma (Higgins, 2016: 190). Zahvaljujući Google-u i drugim tvrtkama za tehničke usluge moguće je pristupiti satelitskim snimkama cijelog planeta, geo-označenim fotografijama, fotografijama na razini ulica te je dostupna velika količina videosadržaja svakog kutka Zemlje (Higgins, 2016: 190). Jednostavnim pristupom alatima svatko ima potencijal biti istraživač otvorenog koda. Novi (često besplatni) alati i platforme nerijetko se stvaraju, a rastuća internetska zajednica istraživača otvorenoga koda brzo ih usvaja (Higgins, 2016: 190). Istraživanje koje se koristi informacijama otvorenoga izvora, poput javno dostupnih dokumenata, statistika, podataka, novinskih izvješća ili karti nije ništa novo. To je praksa na koju su se organizacije za ljudska prava, vlade i pojedinačni istraživači oslanjali desetljećima, ako ne i stoljećima (Dubberley i ostali, 2020: 12).

Novinarstvo i OSINT

Novinarstvo javno dostupnih informacija pojavilo se kao novi fenomen u medijskom ekosustavu. Ono upotrebljava *crowdsourcing* (hrv. masovna podrška) za provjeru činjenica i generiranje istraživačkih izvješća o svjetskim događajima koristeći se otvorenim izvorima (Bär i ostali, 2023: 1). *Crowdsourcing* je krovni izraz za nekoliko vrsta *online* suradnji. Obično se odnosi na otvoreni poziv za zajedničko stvaranje (prije svega istraživanja) preko internetskih mreža (Aitamurto, 2019: 2). To je dinamičan i interaktivan proces u kojem novinari i korisnici interneta, koji su odlučili sudjelovati u njemu, strukturirano i sistematski surađuju na stvaranju novinarskog proizvoda (Aitamurto, 2019: 2). Najbolji primjer istraživačkog novinarstva je *Bellingcat*, neovisan i međunarodni kolektiv istraživača i novinara preko 20 zemalja. *Bellingcat* je poznat po istragama o ilegalnoj uporabi kemijskog oružja tijekom sirijskog rata, ruskoj odgovornosti za obaranje leta MH17 te ratnim zločinima u rusko-ukrajinskom ratu (Bär i ostali, 2023: 1). Ključni za takvu vrstu istraga i novinarstva su društveni mediji kojima se šire informacije i provjeravaju činjenice. Većina takvih istraga, koje istražuju novinari ili slobodni istraživači, sada se provode isključivo *online* s dodatnim izvorima podataka kao što su: informacije iz državnih arhiva, evidencije poduzeća i porezna prijava, podaci o biračkom popisu, informacije učitane *online* s *briefinga* i konferencija, elektronički tiskana izdanja (Ganguly, 2022: 26). Za početak OSINT-a u novinarstvu može se navesti 2009. i novinska agencija *Storyful* koja je razvila nove metode informacijskog rudarenja i praćenja društvenih medija za izvještavanje o sukobima. Nakon toga uslijedilo je Arapsko proljeće koje je pokazalo kako društveni mediji mogu biti legitimna platforma za prikupljanje vijesti, unatoč cenzuri autoritarnih režima na Bliskom istoku (Dubberley i ostali, 2020: 6). Važnost takvog istraživanja najbolje se može vidjeti utjecajem njihovih rezultata. Jedan je primjer rušenje *Malaysian Airlinesa* leta broj 17 iznad istočne Ukrajine 2014. godine. Prvotno je prijavljen kao nesretni slučaj. Koristeći se javno postavljenim videozapisima, satelitskim podacima i novinarima, *Bellingcat* je uspio otkriti da je MH17 oboren projektilom BUK ruskih separatističkih snaga, lansiranim iz okupiranog teritorija Ukrajine koji podržava Rusija (Ganguly, 2022: 27). Također su uspjeli odrediti točno polje odakle je projektil lansiran čime su dokazali umiješanost ruske vojske, koja to i danas negira (Ganguly, 2022: 27).

Provjera sadržaja društvenih medija postala je temeljni dio istrage otvorenog izvora. Kombinacijom različitih vrsta informacija otvorenog izvora moguće je provjeriti tvrdnje korištenjem istrage otvorenog izvora (Higgins, 2016: 192). U slučaju fotografija i videozapisa potvrda geolokacije postala je ključna metodologija u procesu verifikacije. Geolokacija u

kontekstu istraživanja otvorenog izvora koristi se tragovima u fotografijama za utvrđivanje područja na kojoj je snimljena (Higgins, 2016: 192). Geolokacija je identifikacija geografskog položaja objekta na fotografiji raznim mehanizmima prikupljanja podataka, kao što su satelitske snimke i GPS metapodaci (Mathewson, 2022: 37). Na primjer, može biti jednostavno kao usporedba velikih i jasnih struktura vidljivih na slici sa satelitskih snimki istog područja, sastavljanje tragova s fotografija, kao što su pozivni telefonski brojevi na reklamnim pločama, zatim traženje sve više detalja za sužavanje položaja do točnog mjesta na kojem je fotografija snimljena (Higgins, 2016: 192).

Poslovni subjekti i financijski sektor

Privatizacija dijela poslova koje obavljaju obavještajne službe dramatično se proširila porastom obavještajnih aktivnosti nakon napada na Sjedinjene Američke Države 11. rujna 2001. (Chesterman, 2008: 1056). Razni privatni subjekti sve su više uključeni u nacionalnu, ali i privatnu sigurnost, prije svega prikupljanjem obavještajnih podataka (Eijkman i Weggemans, 2012: 288). Povećano eksternaliziranje prikupljanja informacija, rudarenja podataka i analize privatnih tvrtki trend je unutar sigurnosne industrije (Eijkman i Weggemans, 2012: 288). Ugovaranje hardverskih i softverskih poslova jedna je od najvećih pojedinačnih stavki eksternaliziranja, ali se značajno ne razlikuje od drugih oblika državnog ugovaranja (Chesterman, 2008: 1058). Privatizacija dovodi do komercijalizacije sigurnosnih dimenzija i alata, poput satelitskih snimki. One su postale demokratizirane, dostupne svim korisnicima interneta (Weinbaum i ostali, 2017: 1). Veliki broj privatnih obavještajnih tvrtki oslanja se na OSINT za pružanje obavještajnih analiza jer nerijetko nemaju pristup tajnim informacijama, čime se povećava važnost i ulaganje u OSINT (Campbell, 2022: 25).

Privatizacija sigurnosti općenito ima svoje dobre i loše strane. Podugovaranje određenih poslova i zadataka s privatnim tvrtkama može doprinijeti ubrzavanju, poboljšavanju i funkcionalnom unapređenju rada sigurnosnih institucija koje su povezane u sustav nacionalne sigurnosti (Mikac i Sajko, 2009: 67). Nacionalna je sigurnost temeljno pitanje i interes svih država, stoga je nužna doza opreza kad je obavlja netko zbog financijske koristi (bez obzira na njihove kompetencije). Može doći do sukoba interesa, da privatizacija postane sama sebi svrhom i da te tvrtke počnu preuzimati funkcije države (Mikac i Sajko, 2009: 67-68). Pitanje sukoba interesa posebno je važno, zato što privatne tvrtke mogu dati prednost financijskoj dobiti nad javnim interesom, što dovodi do potencijalnih etičkih dilema. Općenite ugroze i dileme

koje se javljaju kada privatizacija postane sama sebi svrhom su: ugrožavanje demokratskih vrijednosti, sigurnosti i sloboda te zabrinutosti oko odgovornosti i nadzor nad njima (Mikac i Sajko, 2009: 68).

Neki se zagovornici zalažu za veću učinkovitost, stručan pristup i potencijalne uštede troškova, ali se ne smije zanemariti zabrinutost oko odgovornosti, sukoba interesa i nejednakosti, koje može proizvesti privatizacija sigurnosti. Ključni je zadatak uspostaviti ravnotežu između navedenih prednosti uključenosti privatnog sektora i potrebe za učinkovitim mehanizmima nadzora i odgovornosti, kako bi se osiguralo da nacionalna sigurnost ostane prioritet. Uz to se istovremeno mora posebno paziti na očuvanje demokratskih načela i ljudskih prava.

U financijskom sektoru poduzeća koriste OSINT izvore za istraživanje novih tržišta, praćenje aktivnosti konkurenata, planiranje marketinških aktivnosti i predviđanje svega što može utjecati na trenutno poslovanje i budući rast (Yong-Woon i ostali, 2022: 5). Porast korištenja OSINT-a među poslovnim subjektima objašnjava se pojavom i širenjem interneta, a posljedično i pojavom dostupnih informacija (Tuominen, 2019: 19). U prošlosti je korištenje OSINT izvora bilo ograničeno na velike korporacije s dovoljnim proračunima za obavještajne poslove. Danas ga, zbog široke upotrebe interneta, koriste i male tvrtke s ograničenim proračunima (Yong-Woon i ostali, 2022: 5). Financijski sektor, također, upotrebljava javno dostupne podatke za borbu protiv curenja podataka. Znaju da je poslovna izloženost povjerljivih informacija i sigurnosna ranjivost njihovih mreža uzrok budućih kibernetičkih prijetnji. Analizom OSINT izvora, unutar i izvan organizacije, koriste se za stvaranje strategija obavještavanja o prijetnjama. Zatim kombiniraju te informacije s drugim informacijama kako bi se postigla učinkovita politika upravljanja kibernetičkim rizikom, koja im pomaže zaštititi financijske interese, ugled i bazu klijenata (Hassan i Hijazi, 2018: 12).

Konkretan primjer korištenja sadržaja objavljenog na društvenim mrežama ne-državnih aktera (u ovom slučaju nevladinih organizacija) američki je *think tank Atlantic Council*. Koristili su se amaterskim fotografijama vojnika kao dokazom ruske agresije u Ukrajini. Time se zamagljuje granica između zagovaranja mira i obavještajnih podataka (Saugmann, 2019: 350). *Amnesty International* reagirao je na dostupnost civilnih fotografija, ne samo za njihovo korištenje za dokumentiranje ratnih zločina, već i za upozoravanje civila da moraju paziti što snimaju i dijele na internetu kada su u blizini sukoba (Saugmann, 2019: 350).

Digitalizacija je dodatno povećala rizike za privatnost povećanjem kapaciteta rudarenja podataka i pohrane podataka. Tehnološke inovacije[5] omogućuju kompjutorizaciju običnih kućanskih predmeta povezanih na internet zbog čega se povećava moguće prikupljanje i zadržavanje podataka (Feldman i Haber, 2020: 198). Ova je promjena omogućila pružateljima usluga prikupljanje golemih količina osjetljivih podataka o svojim korisnicima poput razgovora, fotografija, videozapisa, biometrijskih podataka, pa čak i vitalnih znakova (npr. krvni tlak ili otkucaji srca) (Feldman i Haber, 2020: 198).

Terorističke skupine i skupine organiziranog kriminala

Još je nedovoljno istražena tema kako se terorističke skupine koriste javno dostupnim podacima. No, postoji puno istraživanja kako navedene skupine upotrebljavaju društvene mreže u svoju korist. Prije ekspanzije interneta sposobnost terorističkih organizacija objavljivanju vlastitog propagandnog sadržaja bila je minimalna te su većinom ovisili o tradicionalnim medijima (Klausen, 2015: 3). Međutim, pojavom interneta i društvenih medija samooglašavanje, promocija terorističkih skupina i učitavanje njihovih materijala znatno se povećalo na platformama kao što su Facebook i Twitter, uključujući i forume, mrežne stranice i *video hosting* (Klausen, 2015: 3). Društveni su mediji terorističkim organizacijama pružili puno prednosti u koordinaciji operacija, dosezanju potencijalnih džihadista i uključivanju onih koji se dvoume pridruživanju terorističkim organizacijama (Bertram, 2016: 244). Terorističke organizacije mogu koristiti javno dostupne podatke za planiranje napada, prikupljanje informacije o meti (tijekom istraživanja ciljanog područja) prije napada, analiziranje i praćenje stranica na društvenim mrežama za regrutiranje boraca, dobivanje vojnih podataka koje je slučajno otkrila pojedina vlada (npr. metoda izrade eksploziva) te širenje propagande po svijetu raznim medijskim kanalima (Hassan i Hijazi, 2018: 13). Al-Quaida je dobar primjer korištenja društvenih mreža u terorističke svrhe. Al-Quaida se koristila Facebookom i YouTube kanalima za regrutacije novih članova i povećanje broja simpatizera, posebice na Zapadu. To se očitovalo širenjem fotografija i videouradaka „uspješnih" terorističkih napada, objavom liste i biografija samoubojica, propovijedanjem ideoloških tekstova i slično (Musladin, 2012:73 prema Montagnese, 2012:16).

Uz besplatne i dostupne informacije kriminalci i hakeri mogu lako identificirati te napasti ranjive i pogrešno konfigurirane sustave. Kibernetički terorizam relativno je novi pojam.

[5] Naziv za takvu vrstu tehnologije je *Internet of Things* (IoT) što je u prijevodu Internet stvari.

Kibernetički je terorizam konvergencija terorizma i kibernetičkog prostora. Označuje nezakonite napade i prijetnje napadima na računala, mreže i pohranjene informacije kako bi se zastrašila ili prisilila vlada ili njezin narod u promicanju političkih ili društvenih ciljeva (Diaz i Merlos, 2008: 6). Kibernetički se napadi sve više smatraju ozbiljnim prijetnjama nacionalnoj sigurnosti. Takvi napadi ometaju zakonite mrežne operacije i uključuju namjerne štetne učinke mrežnim uređajima, preopterećenje mreže i uskraćivanje mrežnih usluga legitimnim korisnicima (Tabatabaei i Wells, 2016: 218). Izviđanje je preduvjet, ali i mjesto gdje počinje većina kibernetičkih napada. Prije izvršenja ciljanog napada cilj je napadača izvršiti izviđanje obuzdavanjem moći slobodno dostupnih informacija izvučenih korištenjem različitih načina prikupljanja obavještajnih podataka (Enbody i Sood, 2014: 101). Tajnost i neotkrivanje počinitelja ključni je dio svakog organiziranog kibernetičkog napada (Tabatabaei i Wells, 2016: 218).

Nadalje, napadači se mogu koristiti obavještajnim podacima otvorenog koda za pronalaženje informacija o ljudima pri osmišljavanju napada društvenim inženjeringom (engl. *social engineering attacks*). Primjer daje *Etay Maor* u svom članku: napadači mogu pronaći rukovoditelje ciljane tvrtke jednostavnom Google pretragom, zatim mogu pronaći njihove profile na društvenim mrežama kako bi saznali više o njihovoj obitelji, prijateljima, mjestima, interesima i hobijima (TechTarget, 2021). Kada napadači znaju određene detalje o svojoj žrtvi, lako mogu osmisliti napad društvenog inženjeringa, koji se teško može otkriti. Primjer je zaposlenik koji objavljuje svoje kuharske vještine na društvenim mrežama. Napadači mu mogu poslati e-poštom kupon za popust za navodnu novu gurmansku trgovinu (TechTarget, 2021). Ta će elektronička pošta izgledati kao bezopasna promidžbena e-pošta, ali može isporučiti zlonamjerni softver koji će potajno infiltrirati uređaj zaposlenika (TechTarget, 2021). Posljedice mogu biti katastrofalne ako je žrtva povezana s kritičnom infrastrukturom ili partnerom treće strane (TechTarget, 2021).

Nedavni (2020.) primjer korištenja OSINT-a grupe organiziranog kriminala zabilježen je u Srbiji. Članovi kriminalne grupe metodom geo-lociranja saznali su položaj protivnika. Internetskom pretragom locirali su restoran iz kojeg se vidi prizor kakav je vidljiv s fotografije koju je objavio protivnik (Krik, 2023). Nakon što su otkrili gdje se nalazi i kako provodi vrijeme, kriminalci su uspješno organizirali njegovo ubojstvo. Primjer dokazuje kako je prikupljanje podataka iz otvorenih izvora postalo široko rasprostranjeno te se relativno lagano i brzo uči.

Zaključno, istrage su, s novim dostupnim alatima i resursima otvorenog koda, postale neprocjenjiv izvor informacija za svakoga tko istražuje širok raspon tema iz različitih razloga (Higgins, 2016: 195). Posljednjih godina organizacije za ljudska prava, aktivisti i novinari prihvaćaju ove nove alate i resurse. Sada je već jasno da će istraživanje javno dostupnim podacima postati ključni dio rada mnogih istražitelja bez obzira na vrstu istraživanja kojom se bavi.

4. Ljudska prava i privatnost u bespućima društvenih mreža

Globalizacija, tehnološki napredak i suvremeno okruženje u kojem se društvo nalazi donose mnoge prepreke ljudskoj privatnosti i individualnim pravima čovjeka. U današnje je vrijeme, dojam je, granica između pravog i virtualnog života gotovo izbrisana. Stoga će ovo poglavlje odgovoriti na pitanje: „Može li se upotreba podataka, objavljenih na društvenim mrežama, koji se koriste u obavještajne svrhe okarakterizirati kao kršenje ljudskih prava i privatnosti?“ Od početka informacijskog doba privatnost je postala česta tema o kojoj se raspravlja, zato je cilj prikazati preobliku pojma privatnosti te kršenja ljudskog prava na privatnost u kontekstu uporabe sadržaja objavljenog na društvenim mrežama u obavještajne svrhe.

4.1. Pojam ljudskih prava i pojam privatnosti

Ljudska su prava norme koje teže zaštiti sve ljudi od teških političkih, pravnih i društvenih zloporaba, a sama se filozofija bavi pitanjima o postojanju, sadržaju, prirodi, univerzalnosti, opravdanosti i pravnom statusu ljudskih prava (Nickel, 2021: 461).

Ljudska su prava osnovna prava i slobode koje pripadaju svakoj osobi na svijetu, od rođenja do smrti. Pojam i koncept ljudskih prava postoji stoljećima te se tijekom vremena mijenjao i preoblikovao. Zaštita temeljnih ljudskih prava jedno je od važnijih pitanja međunarodne zajednice. Prije Drugog svjetskog rata međunarodna prava, koja su štitila ljudska prava, nisu bila razvijena, a države su ograničile svoje međunarodne pravne obveze na izjave namjere i mali broj ugovora i konvencija (Hafner-Burton i Tsutsui, 2005: 1373). Danas u svojoj suvremenoj manifestaciji ljudska prava označavaju skup individualnih i kolektivnih prava koja su službeno promicana i zaštićena međunarodnim i domaćim pravima od 1948. godine i Deklaracije UN-a o ljudskim pravima (Landman, 2006: 8). Transformacija i evolucija ljudskih prava rezultirala je naglim porastom pravne i institucionalne zaštite ljudskih prava. Nadalje, razvoj doktrine ljudskih prava promijenio je međusobno djelovanje nacionalnih država na međunarodnoj i regionalnoj razini, ali i načine na koje vlade, pojedinci i grupe na domaćoj razini djeluju jedne prema drugima (Landman, 2006: 8). Ove nove vrste djelovanja i interakcije pokrivaju široko područje, uključujući politička prava, građanska prava, socijalna, ekonomska i kulturna prava, kao i pitanja siromaštva i raspodjele socio-ekonomskih resursa (Landman,

2006: 8). Nakon Deklaracije UN-a i dalje se izrađuju razni međunarodni ugovori o ljudskim pravima koje potpisuje sve veći broj država.

Pojam privatnosti koristi se u filozofskim, sociološkim, etičkim, političkim, pravnim i ekonomski orijentiranim raspravama, ali ne postoji jedinstvena analiza, značenje ili definicija (Hugl, 2010: 1). Većina ljudi ima vlastite koncepte privatnosti. Načelno je jasno što je privatnost i na što se zaštita privatnosti odnosi. No, kao što je slučaj s mnogim drugim konceptima u društvenim znanostima, spuštanje s načelne razine na konkretniju razinu dovodi do zaključka kako ne postoji univerzalni dogovor oko definicije privatnosti (Pavuna, 2019: 12).

Ukratko, ljudska su prava važna jer priznaju temeljnu vrijednost svakog pojedinca, štite individualne slobode i dostojanstvo, promiču jednakost, štite osnovne potrebe, uspostavljaju odgovornost te pridonose miru i stabilnosti. Ljudska prava zapravo čine temelj za pravedno, uključivo i skladno društvo.

4.2. Transformacija pojma privatnosti u informacijskom dobu

Na početku ovog stoljeća čuvanje privatnosti osobnih podataka značilo je oprez pri razgovoru sa strancima (npr. u sobama za razgovor na internetu) i ograničavanje broja osobnih podataka koje pojedinac dijeli na internetu. Danas je, međutim, neobuzdano praćenje podataka zakompliciralo i promijenilo definiciju privatnosti. Većina današnjih tvrtki i mrežnih stranica prati digitalno ponašanje građana (vrlo često bez njihovog znanja ili pristanka) i bilježe mrežne stranice koje posjećuju, stranice društvenih medija koje im se sviđaju, proizvode koje kupuju i popise e-pošte na koje se prijavljuju.

Povijest i razvoj pojma privatnosti velika je i široka tema, stoga će biti naznačeni samo neki od važnijih razdoblja u povijesti pojma. U drevnim društvima, poput antičkog, ljudi su imali relativno ograničenu mogućnost samoodređenja jer su im privatni životi bili pod snažnim utjecajem države i društva (Lukács, 2016: 257). Taj dio povijesti uspješno ilustrira Platon u svom dijalogu *Zakoni* gdje je cjelokupni život pojedinca bio određen državom i njezinim ciljevima te nije postojalo mjesto za individualnu slobodu i autonomiju (Lukács, 2016: 257). Životi pojedinaca pod utjecajem su društva te se oni ne mogu samoostvariti. U srednjem vijeku nije postojala privatnost kao društvena vrijednost u današnjem smislu. Tada je pojedinac postojao kao član zajednice pa je njegov privatni život i ponašanje bilo pod stalnim nadzorom

drugih članova (Lukács, 2016: 257). Pojava privatnosti kakvu danas znamo povezana je s pojavom gradova. Tijekom 19. stoljeća nove promjene u gospodarstvu i društvu promijenile su način ljudskog života. Novonastale promjene imale su posljedice za privatnost jer su fizička i mentalna privatnost odvojene te su se počele razvijati na dva različita načina (Lukács, 2016: 257). Selidbom iz sela u grad počela je rasti populacija gradova. To je dovelo do fizičkog gubitka privatnosti jer su ljudi u gradovima morali živjeti na prenapučenim mjestima. Građani su morali iskusiti novi tip privatnosti jer su prestali živjeti pod uvijek budnim okom svojih seoskih susjeda i stalnom moralnom kontrolom koju su uspostavili (Lessig, 1999: 57). Prije urbanizacije ljudi su živjeli u malim mjestima gdje su poznavali svoje susjede. Ako ste ostali vani prekasno ili ste popili previše, odnosno ako ste na bilo koji način prekršili razrađen skup normi ponašanja građanina, kršenje bilo bi primijećeno i pojedinac bi snosio posljedice (Lessig, 1999: 57). Društvene norme regulirale su pojedince tog društva pa su mogle utjecati na veliki dio njegovog života jer je on zapravo bio javan (Lessig, 1999: 57). Druga vrlo važna promjena bila je pojava i rast tabloidnih novina koje su bile plodno područje za promicanje glasina, tračeva, fotografija, vijesti i sl. (Lukács, 2016: 257). Samuel D. Warren i Louis D. Brandeis prvi su istaknuli prijetnje privatnosti uzrokovane tehnološkim i društvenim razvojem u poznatom članku *Pravo na privatnost* iz 1890. godine (Lukács, 2016: 257). Prepoznali su dvije prekretnice koje su tada predstavljale prijetnju privatnosti: tehnološki razvoj (prije svega fotografija) i trač, koji su sve više bili objavljivani u novinama (Bratman, 2002: 628). Prvi su zahtijevali da se pravo na privatnost (definirano kao pravo da se pojedinca 'pusti na miru') prizna kao zasebno i opće pravo koje osigurava zaštitu, između ostalog i, od emocionalne patnje (Bratman, 2002: 631). Već spomenuto, ne postoji univerzalno prihvaćena definicija privatnosti. Stoga interpretacija i definicija privatnosti ovisi o duhu vremena, kontekstu sadašnjeg doba te se u obzir moraju uzeti sve prepreke i izazovi tog doba.

Informacijsko doba dovodi do primjene niza tehničkih mjera za ublažavanje kršenja privatnosti kojima se nastoje očuvati podaci korisnika (Nissimi i Wood, 2018: 2). Uobičajene mjere uključuju potiskivanje, zamjenu podataka, dodavanje buke, sintetičke podatke, agregaciju alata za statistiku i strojno učenje, bilježenje upita i reviziju, i više (Nissimi i Wood, 2018: 2). S proširenim oslanjanjem na tehnološke pristupe, privatnost, koja je nominalno bila normativni koncept, sve više postaje i tehnički koncept (Nissimi i Wood, 2018: 2).

Teorije informacijske privatnosti razmatraju dvije interpretacije. To su redukcionistička interpretacija i interpretacija utemeljena na vlasništvu. Prema redukcionističkom tumačenju informacijska je privatnost vrijedna jer štiti od neželjenih posljedica uzrokovanih povredom

privatnosti (Yun, 2022: 1). Tumačenje temeljeno na vlasništvu smatra da svaka osoba posjeduje svoje informacije. Prema teoriji ograničenog pristupa ljudi imaju informacijsku privatnost kada mogu ograničiti ili zabraniti drugima pristup informacijama o njima (Yun, 2022: 1). U teoriji kontrole osobni je izbor važan, a privatnost je izravno povezana s kontrolom nad informacijama o sebi (Yun, 2022: 1). Unatoč njihovoj širokoj upotrebi, ni teorija ograničenog pristupa ni teorija kontrole ne pružaju zadovoljavajuće objašnjenje informacijske privatnosti, iako svaka primjećuje nešto važno o njoj (Yun, 2022: 1). Teorija koja pokušava spojiti važne elemente u jednu teoriju već je spomenuta teorija ograničenog pristupa/ograničene kontrole (engl. *Restricted Access/Limited Control theory*, u daljnjem tekstu RALC). RALC teorija naglašava da su privatnost i kontrola odvojeni pojmovi. Privatnost u osnovi štiti od upada drugih i njihovog prikupljanja informacija, a definira se u kontekstu određene situacije (Hugl, 2010: 5). Osoba ima normativnu privatnost kada je zaštićena eksplicitnim normama, politikama ili zakonima uspostavljenima za zaštitu pojedinaca u takvim situacijama (Hugl, 2010: 5). Stoga se privatnost usredotočuje na ograničeni pristup i zaštitu. Pojam kontrole i odgovarajuće politike privatnosti trebaju pojedincima pružiti ograničene kontrole potrebne za upravljanje njihovom privatnošću (Hugl, 2010: 5). Prema RALC teoriji ne postoji ništa u osobnim podacima što određuje treba li ih klasificirati kao javne ili privatne (Tavani, 2007: 14-15). Umjesto toga kontekst ili situaciju, u kojoj drugi koriste ili mogu koristiti osobne podatke, treba uzeti u obzir pri proglašenju određene vrste osobnih podataka normativno privatnom (Tavani, 2007: 14-15). Dakle, situacija je od presudne važnosti u teoriji privatnosti RALC teorije (Moor, 1997: 30). Primjer korištenja RALC teorije je kontroverza o privatnosti koje okružuju internetske kolačiće. Odgovarajuća politika privatnosti na internetu, koja utječe na rudarenje podataka, morala bi jasno navesti zahtjeve privatnosti za *online* potrošače u komercijalnim transakcijama s mrežnim stranicama koje se koriste tehnologijom rudarenja podataka (Tavani, 2007: 16). Ti potrošači prvo moraju biti obaviješteni da se mrežne stranice koriste tehnikama rudarenja podataka. Stranice trebaju istaknuti da se korisnički podaci dobiveni rudarenjem mogu naknadno koristiti iako ih korisnici možda nisu izričito odobrili te da takva upotreba može ugroziti njihovu privatnost (Tavani, 2007: 16). Tvrtka, čija je mrežna stranica, imala bi dužnost obavijestiti potrošače koriste li se praksom rudarenja podataka i kako to može utjecati na osobne podatke potrošača (Tavani, 2007: 16). Primjenom RALC-a možemo upotrijebiti proceduru pri odluci trebaju li osobni podaci, kojima trenutno pristupa tehnologija kolačića, biti zaštićeni kao normativno privatna situacija (Tavani, 2007: 19-18). Upotrebom RALC-a nema potrebe uokviriti novu kategoriju zaštite privatnosti ili ovisiti o novim alatima za rješavanje pitanja privatnosti povezanih s kolačićima (Tavani, 2007: 19-18). Na ovaj način RALC nudi

sveobuhvatnu i sustavnu proceduru za rješavanje pitanja privatnosti na internetu koja mogu utjecati na širok raspon tehnologija (Tavani, 2007: 19-18).

Definicija privatnosti, koja se koristi u ovom radu, obuhvaća ideju informacijskog samoodređenja koje za rezultat omogućava pojedincu procjenu osobnog rizika privatnosti, poduzimanje odgovarajuće radnje za zaštitu vlastite privatnosti i sigurnost da su poduzete odgovarajuće mjere zaštite privatnosti izvan njegove sfere kontrole (Ziegeldorf i ostali, 2014: 2).

Opća uredba o zaštiti podataka (engl. *General Data Protection Regulation*, u daljnjem tekstu GDPR) zakon je o zaštiti privatnosti i osobnih podataka koji se od 2018. godine primjenjuje u Europskoj uniji. GDPR određuje koja su prava pojedinaca, a u skladu s tim i obveze subjekata koji obrađuju osobne podatke poput voditelja obrade, odnosno izvršitelja obrade. GDPR se primjenjuje na sve poslovne subjekte i pojedince koji obavljaju određenu aktivnost prikupljanja i/ili obrade osobnih podataka (npr. udruge, bolnice, osiguravajuća društva, fizičke osobe i sl.) (Gov.hr, 2018). Iako GDPR štiti samo građane Europske unije, njegov je utjecaj globalan jer utječe na sve organizacije koje ciljaju na europsko tržište ili pružaju usluge i posjeduju osobne podatke o stanovnicima EU (Li i ostali, 2019: 1). GDPR daje potrošačima visok stupanj kontrole npr. pravo povlačenja privole (čl. 7) i pravo na zaborav (čl. 17) (Li i ostali, 2019: 1). Također, postavljaju se zahtjevi za voditelje obrade podataka i izvršitelje obrade kao što su zaštita podataka prema dizajnu i prema zadanim postavkama (čl. 25) te bilježenje svih aktivnosti obrade (čl. 30) (Li i ostali, 2019: 1). Organizacija ili tvrtka smije obrađivati podatke korisnika samo ako zadovoljava jednu od nekoliko pravnih osnova obrade podataka. Jedna je osnova izričito odabiranje pristanka korisnika (Acquisti i ostali, 2020: 2). Na primjer, kada korisnik pregledava mrežnu stranicu u vlasništvu izdavača, izdavač mora zatražiti izričito korisničko dopuštenje za postavljanja kolačića na njegovo računalo i, ako odobrava, dopušta li i praćenje kolačića trećih strana (Acquisti i ostali, 2020: 2).

4.3. Kršenje ljudskih prava tijekom uporabe podataka dobivenih preko društvenih mreža u obavještajne svrhe

Postoji veliki broj ugovora, konvencija i zakona koji se brinu o državnom poštivanju privatnosti i njezinom ograničenom uplitanju u privatnost. Dobar je primjer *Europska konvencija o*

ljudskim pravima[6] koja navodi pravo na privatnost, ali i ograničenja koja mu se mogu postaviti. Sva ograničenja koja države postavljaju na pravo na privatnost moraju biti zakonita (McMenemy, 2016: 2). Za upad i kršenje prava privatnosti pojedinca mora postojati pravna osnova i ona mora biti opravdana postojećim zakonodavstvom (McMenemy, 2016: 1-2). Trenutno postoje tehnologije s potencijalom i utjecajem na pitanja privatnosti, a odnose se na video (CCTV) i internetski nadzor, profiliranje podataka, nadzor na radnom mjestu, biometrijsku identifikaciju, radiofrekvencijsku identifikaciju i globalni sustav pozicioniranja (GPS) (Hugl, 2010: 1).

Većina popularnih mrežnih stranica, aplikacija, programa i usluga zahtijevaju od korisnika prije uporabe potpisivanje dugačkih pravnih uvjeta korištenja usluge. Ti uvjeti korištenja znaju biti nekoliko tisuća riječi dugački. Pristanak unutar *online* sustava digitalna je manifestacija društvene interakcije. To je korisnikova pozitivna indikacija pristanka koja postaje istovjetna potpisivanju njegovog imena na pravnom dokumentu (Luger i ostali, 2013: 2688). Većina korisnika ne čita uvjete i odredbe, nego se jednostavno slože s njima kako bi se odmah mogli koristiti aplikacijom ili uslugom (Juul, 2013: 3). Ova pravila privatnosti govore korisnicima, koji ih pročitaju, da pružatelji usluge žele prikupljati ogromne količine njihovih osobnih podataka (Juul, 2013: 3). Nadalje, ona jasno navode da tvrtke otkrivaju prikupljene osobne podatke trećim stranama (Juul, 2013: 3). Na primjer, utvrdi li se potreba, Appleova politika privatnosti navodi moguće otkrivanje korisničkih podataka u svrhe nacionalne sigurnosti, provođenja zakona ili drugih pitanja od javnog značaja (Apple, 2022). Do otkrivanja dolazi u skladu sa zakonom, pravnim postupkom, parnicom i/ili zahtjevima javnih i vladinih tijela unutar ili izvan zemlje prebivališta pojedinca (Apple, 2022). Prisiljavanjem korisnika na pristanak ovih ugovora o uvjetima korištenja prije pristupanja usluzi, privatne tvrtke dobivaju dopuštenje za prikupljanje i rudarenje osobnim podacima, kao i dozvolu davanja podataka vladi ako smatraju da je potrebno (Juul, 2013: 3). Politike privatnosti često služe više kao odricanje od odgovornosti za tvrtke nego kao jamstvo privatnosti za potrošače (Tene i Polonetsky, 2012: 68). Čitljivost odredbi i uvjeta ključnih digitalnih usluga u osnovi je pitanje uključenosti i pristupačnosti pojedinaca te samim time njihovih prava. Usluge bi trebale biti dostupne svima, no uvjeti i odredbe napisani su vrlo složenim i kompliciranim jezikom što ih čini nerazumljivim velikom dijelu društva, a uglavnom onima koji su već isključeni na razne načine (Luger i ostali, 2013: 2678). Točka pristanka, gdje pojedinci moraju biti dovoljno informirani i smisleno se

[6] engl. *The European Convention on Human Rights* (ECHR).

odreknu svojih prava te prihvate prava stranice, dramatično je osiromašena ako je razumijevanje korisnika nepotpuno ili uopće ne postoji (Luger i ostali, 2013: 2687).

Tehnološki napredak, kako je ranije rečeno, doveo je do učinkovitog i jeftinog prikupljanja, pohranjivanja i razmjenjivanja informacija. Informacije koje su objavljene na internetu čuvaju se u elektroničkim bazama podataka koje im daju postojanost, fleksibilnost i prenosivost, koja je postala zaštitni znak tehnologije. Posljedično, napravljene su ogromne baze podataka i internetski zapisi informacija, npr. o individualnoj financijskoj i kreditnoj povijesti, medicinskoj dokumentaciji, kupnjama i sl. (Joinson i Paine, 2007: 244).

U pogledu tehnologija i značajki razvojna priroda interneta, kao i pojavljivanje novih načina interakcije, dovodi do specifičnih prijetnji i izazova privatnosti. Prema Ziegeldorfu i ostalima (2014) to su:

1. Identifikacija – označava prijetnju povezivanja trajnog identifikatora, npr. ime i adresu ili pseudonim bilo koje vrste, s pojedincem i podacima o njemu. Prijetnja leži u povezivanju identiteta s određenim kontekstom koji narušava privatnost. Također, omogućuje i pogoršava druge prijetnje, npr. profiliranje i praćenje pojedinaca ili spojeve različitih izvora podataka.
2. Lokalizacija i praćenje – prijetnja je određivanja i bilježenja položaja osobe u vremenu i prostoru. Praćenje zahtijeva identifikaciju kako bi se kontinuirane lokalizacije vezale za osobu. Prije svega koristi se GPS, internetski promet i položaj mobilnog telefona.
3. Profiliranje – označava prijetnju sastavljanja informacijskih spisa pojedinaca zaključujući njihove interese na temelju povezanosti s drugim profilima i podacima. Metode profiliranja uglavnom se koriste za personalizaciju u e-trgovini, ali i za internu optimizaciju na temelju demografskih podataka i interesa kupaca. Primjer je diskriminacija cijena i neželjeni oglasi.
4. Interakcija i prezentacija koja narušava privatnost – prijetnja se odnosi na prenošenje privatnih informacija javnim medijima i njihovo otkrivanje neželjenoj publici u procesu. Primjer je pametna maloprodaja koja predviđa i zahtijeva snažnu interakciju s korisnikom. U takvim je slučajevima moguće zamisliti pružanje informacije korisnicima koji se u svom okruženju koriste pametnim uređajima npr. uporaba videozaslona. Ono postaje prijetnja privatnosti kada se privatni podaci razmjenjuju između sustava i njegovog korisnika.

5. Prijelazi životnog ciklusa – privatnost je ugrožena kada pametni uređaji (mobitel, prijenosno računalo i sl.) otkriju privatne podatke tijekom promjena kontrolnih sfera u životnom ciklusu. Problem se uočava kod kompromitirajućih fotografija i videozapisa koji se često nalaze na rabljenim fotoaparatima ili pametnim telefonima. U nekim su slučajevima uznemirujući podaci pronađeni čak na novim uređajima.
6. Napadi na inventar – odnose se na neovlašteno prikupljanje podataka o postojanju i karakteristikama osobnih stvari.
7. Povezivanje – ova prijetnja povezuje različite prethodno odvojene sustave. Kombinacija izvora podataka otkriva (istinite ili pogrešne) informacije koje subjekt nije otkrio, niti želio otkriti, prethodno izoliranim izvorima. Korisnici se boje loše prosudbe i gubitka konteksta kada se spajaju različiti podaci prikupljeni u različitim kontekstima i dopuštenjima (Ziegeldorf i ostali, 2014: 7-10).

Prve dvije prijetnje odavno su poznate, a ostale su relativno nove koje se tek moraju istražiti.

Prateći društvene odnose na društvenim mrežama država riskira iznenadni ulazak u privatnu sferu. Kao posljedica, ako pojedinci misle da ih se promatra, korisnici mijenjaju svoje ponašanje, što utječe na njihovu sposobnost razvijanja ideja i šteti intimnosti među pojedincima (Donohue, 2010: 1010). Ako se ljudi boje vladinog praćenja, jer razgovaraju s pojedincima sumnjive etničke ili vjerske skupine, tada veze između pojedinaca u skupini i onih izvan mogu značajno oslabiti. Stoga OSINT i SOCMINT ne povrjeđuju samo pravo na privatnost, već i prava koja su srodna privatnosti, kao što su pravo na slobodno udruživanje i pravo na slobodu govora (Donohue, 2010: 1010). Ako netko ne može komunicirati s drugima zbog straha od uplitanja države, šteti se njegovoj sposobnosti artikuliranja različitih uvjerenja, misli i ideja (Donohue, 2010: 1010).

Većina onoga što nas čini ljudima proizlazi iz naših interakcija s drugima unutar privatne sfere, pretpostavljajući da ju nitko ne promatra. Privatnost se odnosi na ono što govorimo, što radimo, pa čak i na ono što osjećamo (McMenemy, 2016: 1-2). Zaključno, bez privatnosti autonomija pojedinca je ugrožena. Jedino autonomijom pojedinac može biti stvarno slobodan. Dakle, kršenje privatnosti u jednu ruku krši i slobode pojedinaca.

Konkretni primjeri kršenja prava

Akteri, koji se koriste obavještajnim podacima otvorenog koda, mogu preoblikovati svakodnevnu fotografiju ili videozapis objavljen na internetu i učiniti ih dokazom u istrazi ratnih zločina ili sukoba. Tada fotografija ili videozapis ima različito djelovanje u odnosu na

svog tvorca i subjekta koji ju dijeli (Saugmann, 2019: 345). Kada pojedinačne snimke ili videozapisi postanu ključni element koji dokazuje ratni zločin, stvaralac takve fotografije postaje važan akter stranama u sukobu i samim time ulazi u sukob (Saugmann, 2019: 345). Proizvođači fotografija, odnosno korisnici interneta postaju dodatno izloženi nesigurnosti zbog njihove prenamjene u svrhu obavještavanja sukoba (Saugmann, 2019: 345). Dobar je primjer civilna snimka koja prikazuje dimni trag rakete prema lansirnom mjestu pri rušenju MH17. Ona pokazuje odakle je i s čijeg teritorija počinjen ratni zločin (Saugmann, 2019: 346). Prema *Bellingcatu* originalni videozapis brzo je izbrisan s YouTubea iz nepoznatih razloga. Nagađa se da je nestao zbog straha od odmazde prema objavljivaču (Saugmann, 2019: 346).

Sljedeći primjer jest skandal *Cambridge Analytica* i njihovo korištenje podataka korisnika Facebooka. Negodovanje javnosti koje je uslijedilo pokazuje dio potencijala za prikupljanje informacija na platformama društvenih medija, očekivanja korisnika platforme i primjer kršenja privatnosti korisnika (Rønn i Søe, 2019: 363). *Cambridge Analytica* iskoristila je Facebookov poslovni model, pristanak korisnika, tijekom rješavanja testa ili kviza. Pravni problem *Cambridge Analytica* nije bio u tome što su prikupljali informacije i ciljali na korisnike koji su rješavali testove i kvizove. Oni su također prikupljali informacije i ciljali na prijatelje korisnika koji nisu dali pristanak da se koristi njihovim podacima (Rønn i Søe, 2019: 363). Nadalje, nezadovoljstvo javnosti pokazuje kako se ljudi općenito ne osjećaju ugodno zbog sustavnog prikupljanja osobnih podataka i informacija (Rønn i Søe, 2019: 363). U slučaju *Cambridge Analytica* osjećali su da im je privatnost narušena i da su njihovi osobni podaci iskorišteni protiv njih (Rønn i Søe, 2019: 363).

Dobar primjer prekoračenja ovlasti i kršenja prava države dogodio se u SAD-u 2013. godine kada je Edward Snowden razotkrio načine i razmjere nadzora države nad svojim građanima. Snowden je, preko novinara, objavio preko tisuću klasificiranih dokumenata američke vlade. NSA i GCHQ nekritički su prikupili podatke građana te potkopavali sigurnost informacijskih sustava i elektroničkih uređaja (Pavuna, 2019: 56). Nekritičkim prikupljanjem podataka skupljano je znatno više podataka nego što je nužno, a prikupljani su i podaci o osobama bez opravdanoga razloga (Pavuna, 2019: 56). Nadalje, NSA[7] i GCHQ[8] namjerno su potkopavali enkripciju i oslabljivali sigurnost popularnog hardvera i softvera kako bi lakše pristupali podacima o osobama od interesa. Time su napravili nemjerljivu štetu milijunima drugih

[7] Nacionalna sigurnosna agencija SAD-a (engl. *National Security Agency*).
[8] Centar za komunikacije Velike Britanije (engl. *Government Communications Headquarters*).

korisnika, koji nikada neće biti predmet njihova interesa, narušivši njihovu privatnost (Pavuna, 2019: 56).

Iz navedenih primjera može se zaključiti kako ljudska prava te privatnost na internetu i društvenim mrežama još uvijek nisu dovoljno zaštićeni. Postoji puno ugroza i aktera koji na sve načine žele prikupiti osobne korisničke podatke bez dopuštenja. Njihovi su motivi navedeni u prethodnim poglavljima. Vlasnici društvenih mreža i mrežnih stranica ne čine dovoljno dobar posao kako bi zaštitili korisnike. Neki, čak aktivno i svjesno, upotrebljavaju i prodaju podatke svojih korisnika. Privola koju korisnik daje prije korištenja pojedine stranice ili društvene platforme promašen je pokušaj upoznavanja korisnika s načinom na koji vlasnici stranica upotrebljavaju njihove podatke, kao i za saznavanje njihovih korisničkih prava i moguće zaštite podataka dostupnih na stranicama.

5. Zaključak

Veliki se broj ljudi koristi internetom, prije svega društvenim mrežama, te su sve skloniji objavljivanju privatnog sadržaja na njima. Podaci dobiveni iz javnih izvora postaju bitni u procesu prikupljanja podataka. Razne tvrtke, vlade i akteri sve više sudjeluju u prikupljanju takvih podataka. Stoga napreduju OSINT metode prikupljanja podataka i rast njezine važnosti. Značaj OSINT-a u suvremenom okruženju je: laka dostupnost, učinkovitost, niska cijena, korištenje u različite svrhe, poput borbe protiv terorizma, u istraživačkom novinarstvu, obavještajnom i protuobavještajnom djelovanju i sl. S druge je strane važno napomenuti, iako OSINT pruža obilje informacija, on postavlja određena etička pitanja. Ona se prije svega odnose na privatnost i prava pojedinaca čiji se podaci prikupljaju. Odgovorno i etičko korištenje OSINT-a ključno je kako bi se osiguralo poštivanje privatnosti pojedinaca. Korištenje podataka ne smije uzrokovati štetu. Utjecaj i važnost OSINT-a i njegovih alata rast će usporedno s tehnološkim napretkom te većim i intenzivnijim korištenjem društvenih mreža.

Cilj je ovog rada bio prikazati aktere koji se koriste društvenim mrežama u različite svrhe, njihove motive, različite načine prikupljanja i obrade podataka otvorenog koda te ugroze i prijetnje privatnosti korisnika društvenih mreža i interneta. Rad je prikazao kako se internet koristi u svrhu prikupljanja obavještajnih podataka. Objašnjeno je koji osjećaji i motivacije potiču korisnike na objavljivanje veće količine podataka koji su privatnog sadržaja. Nadalje, navedeni su korisnici podataka, načini njihovog korištenja te ciljevi koje žele postići. Posljednji se dio rada bavio kršenjem ljudskih prava i privatnosti. Privola koju korisnik daje, kibernetička zaštita od tvrtke u čijem je vlasništvu društvena mreža i slični pokušaji zaštite podataka korisnika, ne pružaju dovoljno dobru sigurnost i zaštitu. Veliki broj aktera s malicioznim namjerama žele eksploatirati javno dostupne podatke. Stoga pitanje sigurnosti na internetu postaje bitno za svakog korisnika. Prikazalo se na raznim primjerima kako oni koji imaju zadaću zaštititi svoje korisnike, u velikoj mjeri nisu uspjeli. Razni skandali, poput *Camebrigde Analytica*, zorni su primjeri nedovoljne kontrole i regulacije tvrtki, vlasnika velikih društvenih mreža. Provedenim istraživanjem potvrđena je hipoteza. Porastom korištenja društvenih mreža i sklonosti njihovih korisnika objavljivanju privatnih podataka povećava se upotreba podataka u obavještajne svrhe različitih aktera te se krši privatnost korisnika. Navedeni rizici; kršenje privatnosti i razvoj tehnologije (prije svega umjetne inteligencije, engl. *Artificial Intelligence* – A.I.) čini ovu temu važnom za razvoj čitave ljudske civilizacije. Internet je od nastanka imao veliki utjecaj na razvoj ekonomije, gospodarstva, tehnologije, društva, države i svega ostalog.

Puno je dobrih strana interneta, no one loše strane postaju sve izraženije (*hakiranje*, prodaja ilegalnih stvari, *cyberbullying* i ostalo). Internet je velik, bogat i nepresušan izvor podataka čiji značaj svakim danom samo još više raste.

Gledajući iz perspektive obavještajnog djelovanja države, korištenje podataka dobivenih iz javnih izvora trebalo bi biti integrirano kao dio šire strategije prikupljanja obavještajnih podataka. To se prije svega odnosi na prikupljanje podataka iz više izvora, provjeru informacija te poštivanje privatnosti i etičkih pitanja tijekom cijelog procesa. Bitno je održati ravnotežu između prednosti koju daju podaci javnog koda i potencijalnih rizika koji vrebaju.

Problem kršenja ljudskih prava i privatnosti na internetu suvremeni je problem koji se još uvijek razvija i još uvijek nije smišljen učinkovit način zaštite korisnika. Korisnici, tj. njihovi podaci ostaju na (ne)milost vlasnika mrežnih stranica i društvenih mreža. Bitan zadatak za sve države, tvrtke i organizacije u budućnosti bit će osmisliti način zaštite privatnosti korisnika, a da pri tome ne utječu na bit interneta, odnosno brzi prijenos informacija, znanja, poruka, podataka i slično.

Zaključno, privatnost na internetu postaje temelj modernog društva u kojemu je granica između stvarnoga i virtualnog vrlo često izbrisana. Zaštita privatnost zahtijeva stalnu pozornost i odgovorne postupke korisnika, tvrtki, organizacija, ali najviše tvorca politika. Zbog svoje prirode, načina korištenja i količine osobnih podataka koje korisnici često dijele, društvene su mreže najplodnije tlo prikupljanja podataka i kršenja privatnosti. Uživajući u prednostima društvenih medija, a istovremeno smanjujući potencijalne rizike povezane s izloženošću podataka i kršenjem privatnosti, korisnici društvenih mreža moraju voditi računa o svojoj prisutnosti na internetu. Povreda i kršenje privatnosti države je neizbježna. Kada se dogodi, mora biti što manje invazivna te zahvatiti manji broj građana. Naposljetku, svaka povreda privatnosti koja je opravdana kao nužna za višu vrijednost, npr. u svrhu zaštite nacionalne sigurnosti, isključivo se mora koristiti samo u tu svrhu i imati obzira za individualne građanske slobode.

6. Popis literature

Acquisti, A. Cheyre, C. Lefrere, V. Marotta, V. Warberg, L. 2020. The impact of the GDPR on content providers. *The 2020 Workshop on the Economics of Information Security*.

Ahmet, A. T. E. Ş. 2020. Current challenges and trends in intelligence. *Güvenlik Bilimleri Dergisi.* 9(1): 177–204.

Aitamurto, T. 2019. Crowdsourcing in journalism. *Oxford Research Encyclopedia of Communication*.

Akhgar, B. 2016. Osint as an integral part of the national security apparatus. *Open Source Intelligence Investigation: From Strategy to Implementation*. 3–9.

Alhabash, S. Ma, M. 2017. A Tale of Four Platforms: Motivations and Uses of Facebook, Twitter, Instagram, and Snapchat Among College Students?. *Social Media + Society.* 3(1): 1–13.

Bartes, F. 2013. Five-phase model of the intelligence cycle of competitive intelligence. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*. 61(2), 283–288.

Baumeister, R. F. Leary, M. R. 1995. The need to belong: desire for interpersonal attachments as a fundamental human motivation. *Psychological bulletin*. *117*(3): 497–529.

Bär, D. Calderon, F. Lawlor, M. Lickleder er, S. Totzauer, M. Feuerriegel, S. 2022. Analyzing Social Media Activities at Bellingcat.

Benes, L. 2013. OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm. *Journal of Strategic Security*. 6(3), 22–37.

Bertram, L. 2016. Terrorism, the Internet and the Social Media Advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violent extremism. *Journal for deradicalization*. (7), 225–252.

Best, C. 2011. Challenges in Open Source Intelligence. *European Intelligence and Security Informatics Conference*. 58–62.

Bondad-Brown, B. A. Rice, R. E. Pearce, K. E. 2012. Influences on TV viewing and online user-shared video use: Demographics, generations, contextual age, media use, motivations, and audience activity. *Journal of Broadcasting & Electronic Media*. *56*(4): 471–493.

Boyd, D. M. Ellison, N. B. 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication.* 13(1): 210–230.

Bratman, B. 2002. Brandeis & Warren's 'The Right to Privacy and the Birth of the Right to Privacy'. *Tennessee Law Review.* 62: 623–651.

Bryant, K. Sheldon, P. 2016. Instagram: Motives for its use and relationship to narcissism and contextual age. *Computers in Human Behavior*. 58: 89–97.

Campbell, A. 2022. Legitimate actors or security concern? How Open-Source Intelligence hobbyists are changing the nature of conflict.

Chauhan, S. Panda, N. K. 2015. *Hacking Web Intelligence - Open Source Intelligence and Web Reconnaissance Concepts and Techniques*. Elsevier Inc. Waltham.

Chen, M. Ebert, D. Hagen, H. Laramee, R. S. Van Liere, R. Ma, K. L. Silver, D. 2008. Data, information, and knowledge in visualization. *IEEE computer graphics and applications*. 29(1): 12–19.

Cheng, L. Li, K. Teng, C. I. 2020. Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Information Processing & Management*. *57*(1): 1–14.

Chesterman, S. 2008. We Can't Spy … If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions. *The European Journal of International Law.* 19(5): 1055–1074.

Čavalić, A. 2016. Utjecaj kvalitete podataka i informacija na kvalitetu odluke. *Ekonomska misao i praksa*. 25(2): 495–513.

Day, T. Gibson, H. Ramwell, S. 2016. Fusion of OSINT and non-OSINT data. *Open source intelligence investigation: From strategy to implementation*. 133–152.

Denécé, E. 2014. The Revolution in Intelligence Affairs: 1989– 2003. *International Journal of Intelligence and Counterintelligence*. 27(1): 27–41.

Díaz, G. Merlos, A. 2008. The role of intelligence in the battle against terrorism on the Internet: revisiting 3/11. *Research Paper*. (117).

Dokman, T. Ivanjko, T. 2020. Open source intelligence (OSINT) issues and trends. *The Future of Information Sciences*. 1(2020): 191.

Donohue, L. K. 2015. The dawn of social intelligence (SOCINT). *Drake L. Rev.* 63, 1061.

Donnelly, J. 2000. *Realism and international relations*. Cambridge University Press.

Dubberley, S. Koenig, A. Murray, D. 2020. *Digital witness: using open source information for human rights investigation, documentation, and accountability*. Oxford University Press.

Edwards, L. Urquhart, L. 2016. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? *International Journal of Law and Information Technology*. 24(3): 279–310.

Eijkman, Q. Weggemans, D. 2012. Open source intelligence and privacy dilemmas: Is it time to reassess state accountability. *Sec. & Hum. Rts.* 23, 285–296.

Ellison, N. B. Steinfield, C. Lampe, C. 2007. The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication.* 12(4): 1143–1168.

Feldman, D. Haber, E. 2020. Measuring and protecting privacy in the always-on era. *Berkeley Tech. LJ*. 35(197): 198–250.

Ganguly, M. 2022. *The Future of Investigative Journalism in the Age of Automation, Open-Source Intelligence (OSINT) and Artificial Intelligence (AI).* Doctoral dissertation. University of Westminster.

Hafner-Burton, E. M. Tsutsui, K. 2005. Human rights in a globalizing world: The paradox of empty promises. *American journal of sociology*. 110(5), 1373–1411.

Hammond-Errey, M. 2022. Big data and national security: A guide for Australian policymakers. *Lowy Institute for International Policy*.

Haridas, M. 2015. Redefining military intelligence using big data analytics. *Scholar Warrior*. 72–78.

Hassan, N. A. Hijazi, R. 2018. *Open source intelligence methods and tools.* Apress. New York.

Higgins, E. 2016. A New Age of Open Source Investigation: International Examples. *Open Source Intelligence Investigation: From Strategy to Implementation*. Str. 189–196.

Hobbs, C. Moran, M. Salisbury, D. 2014. *Open-Source Intelligence in the Twenty-First Century*. Palgrave Macmillan. New York.

Holtzman, D. H. 2006. *Privacy lost: how technology is endangering your privacy*. John Wiley & Sons. New Jersey.

Hugl, U. 2010. Approaching the value of Privacy: Review of theoretical privacy concepts and aspects of privacy management. *Americas Conference on Information Systems.*

Hulnick, A. S. 2002. The Downside of Open-Source Intelligence. *International Journal of Intelligence and CounterIntelligence.* 15(4): 565–579.

Ivan, A. L. Iov, C. A. Lutai, R. C. Grad, M. N. 2015. Social Media Intelligence: Opportunities and Limitations. *CES Working Papers*. 7(2a): 505–510.

Joinson, A. N. Paine, C. B. 2007. Self-disclosure, privacy and the Internet. *The Oxford handbook of Internet psychology*. 237–252.

Jolić, T. 2011. Politički realizam i anarhija u međunarodnim odnosima. *Prolegomena: časopis za filozofiju*. 10(1): 113–130.

Jones, K. S. 2003. Privacy: what's different now?. *Interdisciplinary Science Reviews*. 28(4), 287–292.

Jović, D. 2013. Uvod u studij realizma. U: Jović, D (ur.). *Teorije međunarodnih odnosa – realizam* (str. 15–38). Politička kultura. Zagreb.

Jović, D. 2014. Liberalizam u međunarodnim odnosima: teorija i praksa. U: Jović, D (ur.). *Liberalne teorije međunarodnih odnosa* (str. 15–55). Političke analize. Zagreb.

Jović, D. 2016. Konstruktivizam u teorijama međunarodnih odnosa i praksi oblikovanja vanjskih politika. U: Jović, D (ur.). *Konstruktivističke teorije međunarodnih odnosa* (str. 7–36). Političke analize. Zagreb.

Juul, P. 2013. Adapting to the Future of Intelligence Gathering. *Center for American Progress*. 1–9.

Klausen, J. 2015. Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*. 38(1), 1–22.

Lakomy, M. 2022. *Assessing the potential of OSINT on the Internet in supporting military operations.*

Leary, M. R. Kowalski, R. M. 1990. Impression management: A literature review and two-component model. *Psychological Bulletin.* 107(1): 34–47.

Lessig, L. 1999. The Architecture of Privacy: Remaking Privacy in Cyberspace. *Vanderbilt Journal of Entertainment and Technology Law.* 1(1): 56–65.

Leško, L. 2019. Analitičke tehnike primjenjive u sigurnosno-obavještajnim agencijama. *Strategos.* 3 (2), 7–35.

Li, H. Yu, L. He, W. 2019. The impact of GDPR on global technology development. *Journal of Global Information Technology Management*. 22(1), 1–6.

Luger, E. Moran, S. Rodden, T. 2013. Consent for all: revealing the hidden complexity of terms and conditions. In *Proceedings of the SIGCHI conference on Human factors in computing systems.* 2687–2696.

Lukács, A. 2016. What is privacy? The history and definition of privacy. University of Szeged.

Mathewson, A. 2022. Open-source research and mapping of explosive ordnance contamination in Ukraine. *The Journal of Conventional Weapons Destruction*. 26(1), 3.

McMenemy, D. 2016. Rights to privacy and freedom of expression in public libraries: squaring the circle.

Moor, J. H. 1997. Towards a theory of privacy in the information age. *ACM Sigcas Computers and Society*. 27(3), 27–32.

Musladin, M. 2012. Utjecaj društvenih mreža na nacionalnu sigurnost. *Međunarodni Anali: međunarodni znanstveni časopis za pitanja medija, novinarstva, masovnog komuniciranja i odnosa s javnostima*. 6(11): 67–85.

Nadkarni, A. Hofmann, S. G. 2012. Why do people use Facebook?. *Personality and individual differences*. *52*(3): 243–249.

Nickel, J. W. 2012. *On Human Rights*. (2012): 461–464.

Nissim, K. Wood, A. 2018. Is privacy privacy?. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 376(2128).

Omand, D. Bartlett, J. Miller, C. 2012. Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security.* 27(6): 801–823.

O'Reilly, T. 2007. *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software.* International Journal of Digital Economics. 65: 17–37.

Pastor-Galindo, J. Nespoli, P. Gomez Marmol, F. Martinez Perez, G. 2020. The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE.* 8: 10282–10304.

Pavuna, A. 2019. *Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova.* Doktorska disertacija. Fakultet političkih znanosti. Zagreb.

Petronio, S. 2002. *Boundaries of privacy: Dialectics of disclosure*. Suny Press. New York.

Putter, D. Henrico, S. 2022. Social media intelligence: The national security–privacy nexus. *Scientia Militaria: South African Journal of Military Studies*. 50(1): 19–44.

Phythian, M. 2013. Introduction: Beyond the Intelligence Cycle?. U: Pythian, Mark (ur.). *Understanding the intelligence cycle* (str. 15-22). Routledge. New York.

Quan-Haase, A. 2012. Is the uses and gratifications approach still relevant in a digital society? Theoretical and methodological applications to social media. *Journal of Mass Communication & Journalism*. 2(7): 1:3.

Ramwell, S. Day, T. Gibson, H. 2016. Use cases and best practices for LEAs. *Open Source Intelligence Investigation: From Strategy to Implementation*. 197–211.

Ratcliffe, J. 2008. *Intelligence-led policing*. Cullompton. Willan Publishing.

Rathbun, B. C. 2007. Uncertain about uncertainty: understanding the multiple meanings of a crucial concept in international relations theory. *International studies quarterly*. 51(3), 533–557.

Ruggiero, T. E. 2000. Uses and Gratifications Theory in the 21st Century. *Mass Communication and Society.* 3(1): 3–37.

Rønn, K. V. Søe, S. O. 2019. Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security.* 34(3): 362–378.

Sajko, J. Mikac, R. 2009. Privatizacija sigurnosti kao trend novog doba: privatna industrija sigurnosnog sektora kao integralni dio nacionalne sigurnosti SAD-a. *Polemos.* (23), 51–72.

Saugmann, R. 2019. The civilian's visual security paradox: how open-source intelligence practices create insecurity for civilians in warzones. *Intelligence and National Security*. 34(3): 344–36.

Schaurer, F. Störger, J. 2013. The evolution of open-source intelligence (OSINT). *Journal of U.S. Intelligence Studies.* 19: 53–56.

Scott, L. Jackson, P. 2004. The study of intelligence in theory and practice. *Intelligence & National Security*. 19(2), 139–169.

Seidman, G. 2013. Self-presentation and belonging on Facebook: How personality influences social media use and motivations. *Personality and individual differences*. *54*(3): 402–407.

Sood, A. Enbody, R. 2014. *Targeted cyber attacks: multi-staged attacks driven by exploits and malware*. Syngress.

Staniforth, A. 2016. Open source intelligence and the protection of national security. *Open Source Intelligence Investigation: From Strategy to Implementation*. 11–19.

Steele, R. D. 2007. Open-source intelligence. *Handbook of intelligence studies*. 147–165.

Sweetser, K. D. Weaver Lariscy, R., Tinkham, S. F. 2011. Kids these days: Examining differences in political uses and gratifications, internet political participation, political information efficacy, and cynicism on the basis of age. *American Behavioral Scientist*. *55*(6): 749–764.

Tabatabaei, F., Wells, D. 2016. OSINT in the Context of Cyber-Security. U: Akhgar, B., Bayerl, P., Sampson, F. (ur.). *Open-Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications* (str. 213-231). Springer.

Tavani, H. T. 2007. Philosophical theories of privacy: implications for an adequate online privacy policy. *Metaphilosophy*. 38(1): 1–22.

Ten Hulsen, L. 2020. Open sourcing evidence from the internet – the protection of privacy in civilian criminal investigations using OSINT (Open-Source Intelligence). *Amsterdam Law Forum*. 12(2), 3–48.

Tene, O. Polonetsky, J. 2011. Privacy in the age of big data: a time for big decisions. *Stan. L. Rev. Online*. 64, 63.

Thomsen, C. Pedersen, T. B. 2009. A survey of open-source tools for business intelligence. *International Journal of Data Warehousing and Mining (IJDWM).* 5(3): 56–75.

Trottier, D. 2015. *Open source intelligence, social media and law enforcement: Visions, constraints and critiques. European Journal of Cultural Studies.* 18(4-5): 530–547.

Tuominen, S. 2019. *Open Source Intelligence and OSINT Applications*. Oulu University of Applied Sciences.

Quirine, E. Weggemans, D. 2012. Open-source intelligence and privacy dilemmas: Is it time to reassess state accountability. *Security and Human Right.* 23(4): 285–296.

Unver, A. 2018. Digital Open-Source Intelligence and International Security: A Primer. *EDAM Research Reports, Cyber Governance and Digital Democracy.* 8: 1–26.

Waltz, K. N. 2010. *Theory of international politics*. Waveland Press.

Weinbaum, C. Berner, S. McClintock, B. 2017. *Sigint for anyone: the growing availability of signals intelligence in the public domain*. Rand National Defense Research Inst Santa Monica Ca.

Whiting, A. Williams, D. 2013. Why people use social media: a uses and gratifications approach. *Qualitative market research: an international journal*. 16(4): 362–369.

Yong-Woon, H. Im-Yeong, L. Hwankuk, K. Hyejung, L. Donghyun, K. 2022. Current status and security trend of OSINT. *Wireless Communications and Mobile Computing*.

Yun, S. 2022. Magnitude of Benefits in Privacy: Data Protection. *Journal of Civil & Legal Sciences*. 11(8): 1–2.

Ziegeldorf, J. H. Morchon, O. G. Wehrle, K. 2014. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*. 7(12), 2728–2742.

Ziółkowska, A. 2018. Open source intelligence (OSINT) as an element of military RECON. *Security and Defence Quarterly*. 19(2): 65–77.

Mrežne stranice

https://datareportal.com/reports/digital-2023-global-overview-report Pristupljeno 22.4.2023.

https://www.statista.com/statistics/617136/digital-population-worldwide/ Pristupljeno 22.4.2023.

https://www.soa.hr/hr/vijesti/ Pristupljeno 9.6.2023.

https://www.techtarget.com/searchsecurity/post/How-attackers-use-open-source-intelligence-against-enterprises Pristupljeno 10.6.2023.

https://www.krik.rs/skaj-poruke-ubistvo-na-krfu/ Pristupljeno 10.6.2023.

https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf Pristupljeno 11.6.2023.

https://gov.hr/hr/sto-je-opca-uredba-o-zastiti-podataka-eng-general-data-protection-regulation-gdpr/1868 Pristupljeno 12.7.2023.

7. Sažetak

Korištenje podataka prikupljenih iz otvorenih izvora, prije svega s društvenih mreža, suvremeni je izazov obavještajnim agencijama. Suvremeni je to problem koji negativno utječe na privatnost korisnika. Danas, ponajprije zbog velikog tehnološkog napretka te većeg korištenja interneta i društvenih mreža, granica između stvarnog života i života u digitalnom svijetu gotovo je izbrisana. Korisnici interneta često nisu svjesni svih prijetnji i ugroza koje vrebaju na internetu.

Ovaj rad prikazuje na koje se načine krše ljudska prava na internetu s naglaskom na privatnost. Analizom aktera, njihovih motivacija, razloga i načina korištenja podataka dobivenih iz javnih izvora nastoji se prikazati kako se korištenjem tih podataka krše ljudska prava i privatnost. Provedeno istraživanje pokazalo je tko se, kako i zašto koristi tim podacima. Navode se konkretni primjeri kršenja ljudskih prava. U konačnici prikazana je promjena pojma privatnosti u suvremenom okruženju, sve veća važnost podataka prikupljenih iz javnih izvora (OSINT) i sklonost korisnika objavljivanju privatnog sadržaja.

Razvoj tehnologije, korištenje interneta i društvenih mreža nameće problem kršenja ljudskih prava kao jedan od temeljnih problema suvremenog društva. S njim se tek treba uhvatiti u koštac jer raniji pokušaji nisu dali dovoljno dobre rezultate. Vlade, vlasnici mrežnih stranica, ali i sami korisnici, čija se prava krše, ne pridaju dovoljno pažnje i napora za osmišljavanje učinkovitih načina zaštite prava na internetu.

Ključne riječi: otvoreni izvori, ljudska prava, privatnost, internet, društvene mreže, OSINT, obavještajna djelatnost, SOCMINT.

8. Summary

The use of data collected from open sources, primarily from social networks, is a modern challenge for intelligence agencies, but it is also a modern problem that negatively affects user privacy. Today, primarily due to great technological progress and the increasing use of the Internet and social networks, the border between real life and life in the digital world has almost been erased. Internet users are often unaware of all the dangers and threats lurking on the Internet.

This paper tries to show all the ways in which human rights are violated on the Internet with an emphasis on privacy. By analyzing the actors, their motivations, reasons and ways of using data obtained from public sources, this paper tries to show how and in what way the use of these data violates human rights and privacy. The conducted research showed who, how and why uses this data and concrete examples of human rights violations. Finally, the transformation of the concept of privacy in the modern environment, the increasing importance of data collected from public sources (OSINT) and the tendency of users to publish more and more private content are presented.

The further development of technology and the increasing use of the Internet and social networks imposes the problem of human rights violations as one of the fundamental problems of modern society, which has yet to be tackled, since all earlier attempts did not give sufficiently good results. Governments, owners of websites, but also users whose rights are violated do not give enough attention and efforts to devise effective ways to protect rights on the Internet.

Key words: open sources, human rights, privacy, internet, social networks, OSINT, intelligence, SOCMINT.