Prikupljanje podataka iz otvorenih izvora i obavještajne službe: pravo na privatnost

Stjepan Novak*

Pregledni članak
Primljeno: 28. veljače 2025.
Prihvaćeno: 18. svibnja 2025.
DOI: https://doi.org/10.46672/po-mest.28.1-2.5

SAŽETAK

Prikupljanje podataka u biti je djelovanja svake obavještajne službe. Najkorisnija, najjeftinija, najplodonosnija te najkorištenija prikupljačka disciplina jest prikupljanje podataka iz javnih izvora. Ovo je rezultat ubrzanog tehnološkog razvoja, informatizacije komunikacije i svakodnevnog življenja te digitalne pismenosti. Općenito se, po prirodi stvari, prikupljanju podataka suprotstavlja pravo na privatnost. Iz tog su razloga i Europski sud za ljudska prava i Sud Europske unije postavili kriterije o tome koje se mjere usmjerene prikupljanju podataka i zakonodavstva koja ih uređuju moraju zadovoljiti kako bi načini prikupljanja bili prihvatljivi u demokratskom društvu. Cilj je ovog rada istražiti je li opisani razvoj mogućnosti prikupljanja podataka iz javnih izvora od strane obavještajnih službi doveo do povećane opasnosti ugroze tog prava odnosno treba li povećana mogućnost nacionalnih obavještajnih službi u navedenom smislu rezultirati i većim ograničenjima u njihovu postupanju.

Ključne riječi: prikupljanje podataka, javni (otvoreni) izvori, obavještajne službe, pravo na privatnost, Europski sud za ljudska prava, Sud Europske unije.

UVOD

Prikupljanje podataka o pojedinim kategorijama ugroza bit je djelovanja sigurnosno-obavještajnih službi (Bilandžić, 1999: 140). Ono je ključni dio obavještajnog ciklusa, procesa kojem je cilj transformacija podataka, odnosno informacija u obavještajni proizvod. Taj proces je sve manje linearnog, a sve više mrežnog oblika, karakteriziran konstantnom suradnjom i interakcijom svih njegovih sudionika (Richards, 2010: 9, Gill, i Phythian, 2014: 23, Warner, 2014: 16, Aydın i Özleblebici 2015, Lucić, 2022, Leško, 2019: 10). Načini prikupljanja podataka od strane obavještajnih službi višestruki su te različito invazivni. Tako članak 25. Zakona o sigurnosno-obavještajnom sustavu Republike Hrvatske („Narodne novine“, broj: 79/06, 105/06, u daljnjem tekstu: ZSS) razlikuje:

- korištenje javnih izvora,

* dr. sc. Stjepan Novak, Ministarstvo unutarnjih poslova Republike Hrvatske, Ministry of the Interior of the Republic of Croatia, Zagreb, Croatia, e-mail: stjepannovak@hotmail.com). Mišljenja i stavovi izraženi u radu autorova su osobna mišljenja i ne predstavljaju stav institucije u kojoj radi.

This work is licensed under a CC BY-NC 4.0 license, © author(s).

- komunikaciju s građanima i potraživanje službenih podataka od državnih tijela, tijela jedinica lokalne i područne (regionalne) samouprave i pravnih osoba, uključujući i uvid u registre i zbirke podataka i službenu dokumentaciju te
- primjenu tajnih postupaka i mjera.

Era ubrzanog tehnološkog razvoja, informatizacije komunikacije i svakodnevnog življenja te digitalne pismenosti dovela je ne samo do ogromnog porasta količine podataka već i do njihove sveopće dostupnosti (Knol Radoja, 2024: 404, Solove, 2002: 1139). Pojedinci, više ili manje svjesno, ostavljaju cijeli niz podataka o sebi u mrežnom prostoru koji, obrađeni na odgovarajući način, mogu rezultirati kvalitetnim obavještajnim informacijama (Wetzling i Dietrich, 2022: 13). Javni izvori postali su puno bogatiji izvor podataka, a time i predmet interesa i obavještajnih službi (usp. Boban, 2012: 594). Posljedično i proporcionalno tome, porasla je i važnost OSINT-a kao prikupljačke discipline. OSINT, odnosno „Open-Source Intelligence", kao obavještajnu informaciju moguće je definirati kao neklasificiranu informaciju koja je namjerno otkrivena, identificirana, odvojena i podijeljena prema određenoj publici, to jest korisnicima s ciljem odgovaranja na određeno pitanje (Steele, 2006: 129). Kada je riječ o OSINT-u kao prikupljačkoj disciplini, najjednostavnija, ali i nesumnjivo najpovršnija definicija koja se može naći u literaturi koja se bavi tom problematikom jest ona prema kojoj je riječ o prikupljanju podataka iz otvorenih izvora (Hwang,, Lee, Kim, Lee, Kim, 2022:1). OSINT, međutim, nije tek bilokakvo prikupljanje podataka s, primjerice, interneta. OSINT, tako, možemo definirati i kao metodičko prikupljanje i iskorištavanje informacija iz javno dostupnih izvora kako bi se ispunili određeni obavještajni zahtjevi (Block, 2024:97). Zakon o osnivanju Centra izvrsnosti za prikupljanje, obradu i analizu podataka iz otvorenih izvora („Narodne novine", broj: 71/2023) OSINT definira kao „disciplinu obavještajnih informacija iz otvorenih izvora koja u širem kontekstu na sustavan način prikuplja informacije i podatke iz javno dostupnih izvora koje se podvrgava utočnjavanju i vrednovanju, to jest obradi i oblikovanju u obavještajne informacije koje se u formi pisanog ili usmenog obavještajnog proizvoda dostavlja krajnjim korisnicima" (Dokman, 2021: 66).

Za razumijevanje ovog rada, u kontekstu iste definicije, važno je istaknuti da će se termin OSINT-u koristiti za prikupljačku disciplinu i to za onaj njezin segment koji se odnosi na prikupljanje podataka, odnosno operativni, a ne i analitički segment obavještajnog ciklusa. U tom smislu, kada se bude govorilo o, primjerice, koliziji OSINT-a s pravom na privatnost, mislit će se samo na prikupljanje podataka iz otvorenih, tj. javnih izvora, ne i na njihovo utočnjavanje i vrednovanje, obradu i oblikovanje u obavještajne informacije. Iako bi se moglo razmatrati i pitanje predstavlja li samo prikupljanje podataka bez daljnjeg dostavljanja korisnicima sukob s pravom na privatnost, ono neće biti predmetom ovog rada.

Radu svake obavještajne službe, po prirodi stvari, suprotstavlja se pravo na privatnost (usp. Bilandžić, 1999: 137) kao temeljno ljudsko pravo (Knol Radoja, 2024: 404, Warren i Brandeis, 1890). Cilj ovog rada je istražiti je li opisani razvoj mogućnosti prikupljanja podataka iz javnih izvora od strane obavještajnih službi doveo do povećane opasnosti ugroze tog prava (Ten Hulsen, 2020: 24; Boban, 2012: 594), odnosno treba li

povećana mogućnost nacionalnih obavještajnih službi u navedenom smislu, rezultirati i većim ograničenjima u njihovu postupanju. Nakon uvodnih razmatranja, u drugom poglavlju analizirat će se glavne karakteristike OSINT-a kao prikupljačke discipline. Nastavno, istražit će se njezini prednosti, nedostaci i specifičnosti iz perspektive obavještajnih službi, u prvom redu u kontekstu hrvatskog zakonodavstva. Potom će se istražiti odnos između ove discipline i prava na privatnost. Na kraju, iznijet će se zaključak.

KARAKTERISTIKE OSINT-A U PRIMJENI OBAVJEŠTAJNIH SLUŽBI

U literaturi postoji sve veći broj kategorizacija podataka iz otvorenih, odnosno javnih izvora. Takve se kategorije više ili manje preklapaju (Lucić, 2022), ali i razlikuju s obzirom na vrijeme svoga nastanka, imajući u vidu internetski razvoj (Dokman, 2021: 73). Tako Hassani i Hijasi kao kategorije otvorenih izvora razlikuju: „1. Internet koji uključuje forume, blogove, društvene mreže, mrežne usluge za razmjenu videozapisa poput YouTubea, Wikipediju, javno dostupne baze Whois, metapodatake, digitalne podatke, dark web, geolokacijske podatke, IP adrese, tražilice ljudi i sve što se može pronaći na internetu, 2. tradicionalne masovne medije poput televizije, radija, novina, knjiga i časopisa 3. specijalizirane časopise, akademske publikacije, disertacije, zbornike radova, profile tvrtki, godišnja izvješća, vijesti o tvrtkama, profile zaposlenika i rezimee 4. fotografije i videozapise s metapodacima, 5. geoprostorne informacije poput karti i komercijalnih fotografija“ (Hassan i Hijazi, 2018: 5, Dokman, 2021: 80, Lucić, 2022).

U kontekstu informatičkog razvoja i sveopće digitalizacije, „eksponencijalni rast broja informacija u javnom prostoru čini prikupljačku disciplinu obavještajnih informacija iz otvorenih izvora sve važnijom disciplinom“ (Dokman, 2021: 68), koja druge prikupljačke discipline, iako ih ne može zamijeniti, može uvelike osnažiti (Mercado, 2004: 48, Macêdo, Peotta i Gomes, 2023: 55). Kako navodi „jedan od najproduktivnijih autora iz područja otvorenih izvora, David Steele“ (Dokman, 2021:35), OSINT može biti i pomoćna disciplina koja je podređena drugim prikupljačkim disciplinama, ali i samostalna disciplina koja kombinira druge (Steele, 2006: 133). Prednosti prikupljanja podataka iz javnih izvora i više su nego očite. Do podataka iz javih izvora, pogotovo kada govorimo o internetu, može se doći jednostavnim pretraživanjem s običnog računala. Vrlo brzo može se doći do širokog spektra podataka iz različitih izvora i na različitim jezicima, kako u realnom vremenu tako i do podataka starijeg datuma nastanka (Ivanjko i Dokman, 2019: 193). Nadalje, ovu prikupljačku disciplinu karakterizira i ekonomičnost jer se do velikog broja podataka dolazi uz gotovo nikakve sigurnosne rizike (Ivanjko i Dokman, 2019: 194) i vrlo male ili nikakve troškove. Tako Steele navodi kako se više novaca troši na 5 % podataka koji su tajni nego na 95 % onih javno dostupnih (Steele, 2006: 134), slijedom čega je utemeljena njegova tvrdnja kako „OSINT štedi živote, vrijeme i novac“ (Steele, 2006: 140). S druge strane, nedostaci podataka prikupljenih iz otvorenih izvora nisu zanemarivi. Riječ je o velikom broju podataka od kojih veći dio može biti nevažan, uslijed čega će se sam obavještajni ciklus pretvorbe sirovog podatka u obavještajnu informaciju značajno usporiti. Podaci, također, mogu

biti kompromitirani neznanjem njihova autora, odnosno osobe koja ih je postavila u javni prostor, njegovom greškom, pristranošću ili namjerom dezinformiranja (Matey, 2005: 8, Ivanjko i Dokman, 2019: 195, Wetzling i Dietrich, 2022: 14).

Na ovom je mjestu, u kontekstu rasprave o OSINT-u kao prikupljačkoj disciplini u primjeni obavještajnih službi, važno istaknuti jednu prikupljačku disciplinu koja je nalik OSINT-u, ali ne mora biti njime obuhvaćena. Riječ je o prikupljanju podataka putem društvenih mreža (Musladin, 2012: 80), odnosno SOCMINT-u. Naime, iako su društvene mreže namijenjene „.za široko komuniciranje prema recipijentima" (Dokman, 2021: 104), nerijetke su situacije u kojima se komunikacija odvija u zasebnim, zatvorenim grupama unutar pojedinog društvenog medija. Dok su podaci koji su prikupljeni iz takvih širih, javno dostupnih komunikacija obuhvaćeni konceptom OSINT-a, prikupljanje sadržaja, „legendiranim ulaskom u određene grupe te socijalnim inženjeringom" (Dokman, 2021: 104) predstavljalo bi puno invazivniji oblik prikupljanja podataka (Putter, Henrico, 2022: 23) te ne bi predstavljalo OSINT u klasičnom smislu. Štoviše, neki autori tvrde da prikupljanje podataka na ovaj način predstavlja novu obavještajnu disciplinu (Ivan, Iov, Lutai i Grad, 2015: 505).[1]

Navedeni prednosti i nedostaci jednaki su u primjeni od strane obavještajnih službi kao i bilo kojeg drugog subjekta. No, kad je riječ o prikupljanju podataka iz otvorenih izvora od strane obavještajnih službi, iste su suočene s dva specifična izazova. Prvi se odnosi na povećano sudjelovanje drugih aktera na tržištu koji mogu konkurirati obavještajnim službama kad je riječ o prikupljanju podataka, ali im i nuditi svoje usluge. Drugi se odnosi na osnovna pravna načela koja službe moraju poštivati, kako općenito tako i prilikom prikupljanja podataka iz otvorenih izvora. U sljedećem će se poglavlju ovi izazovi detaljnije prikazati te, kada je riječ o pravnim načelima koja obvezuju službe, posebno analizirati u kontekstu hrvatskog pravnog sustava.

SPECIFIČNOSTI OSINT-A KAO PRIKUPLJAČKE DISCIPLINE: HRVATSKI PRAVNI KONTEKST

Kao što je navedeno, u prikupljanju podataka iz otvorenih izvora dva su izazova specifična upravo za djelovanje službi u navedenom smislu.

Prvo, prikupljati podatke iz otvorenih podataka mogu i privatni akteri, kao primjerice tzv. informacijski posrednici, pružatelji usluga koji prikupljaju, usklađuju te trguju velikim količinama podataka, a do podataka dolaze prikupljanjem javno dostupnih podataka ili njihovom kupovinom od drugih pružatelja sličnih usluga (Wetzling i Dietrich, 2022: 8). Istom disciplinom prikupljanja podataka mogu se koristiti i privatni detektivi ili bilo koji drugi korisnik interneta (Ten Hulsen, 2020: 3, Ivanjko, Dokman, 2019: 193). Obavještajnim službama ugovaranje bi takvih usluga od takvih subjekata na tržištu moglo biti primamljivo zbog najmanje dva razloga: brzine i fleksibilnosti. Službe bi, na taj način, brže dolazile do kvalificiranog osoblja, a takvi pružatelji usluga ne bi morali zadovoljavati sve one uvjete koje bi morali zadovoljiti zaposlenici službi niti bi nadzor

[1] Navedeni autori govore o novom članu „INT's obitelji".

tijela koji inače vrše nadzor nad službama bio tako striktan kao u slučaju zapošljavanja (Chesterman, 2008: 1058). U tom smislu, Denécé navodi podatak o čak 70 % proračuna jedne američke obavještajne agencije usmjerenog privatnom sektoru te 50 % zaposlenika te agencije iz privatnog sektora (Denécé, 2014: 36.). Ipak, veći dio aktivnosti obavještajnih službi treba ostati inherentan dio državnih aktivnosti (Chesterman, 2008: 1069, Denécé, 2014: 36). Činjenica je da, uz uvjet da je riječ o političkom poretku utemeljenom na demokraciji, upravo država može osigurati najviši stupanj poštivanja načela demokracije i vladavine prava. Upravo nadzor odgovarajućih državnih tijela, koji je s ekonomskog stajališta manje primamljiv, jamči da koncept vladavine prava neće biti zanemaren. Nadalje, iako će se definicija inherentnih državnih aktivnosti možda razlikovati od političkog sustava do političkog sustava, makar svi oni i bili demokratski, nacionalna sigurnost svakako će uvijek ostati u toj kategoriji (Trybus, 2009).

Drugi izazov predstavljaju načelo zakonitosti i načelo razmjernosti. Načelo zakonitosti temelj je djelovanja obavještajnih službi, a njegovo provođenje osiguravaju odgovarajuća nadzorna tijela. Kada je riječ o djelovanju u cilju zaštite nacionalne sigurnosti, a pogotovo ako je pritom riječ o ograničavanju ljudskih prava i temeljnih sloboda, jasno definiranje ovlasti, postupaka, uvjeta za poduzimanje odgovarajućih radnji i provođenje nadzora nad djelovanjem službi u navedenom smislu, neoborivi su aksiomi. Ustavnopravno načelo razmjernosti (Badžim, 2008: 1036) nezaobilazan je uvjet poduzimanja svih obavještajnih radnji kojima se ograničavaju ljudska prava i slobode, a znači da svako ograničenje slobode ili prava mora biti razmjerno naravi potrebe za ograničenjem u svakom pojedinom slučaju. [2]

Kad je riječ o hrvatskom pravnom sustavu, ZSS u prvom članku navodi kako se njime osnivaju sigurnosno-obavještajne agencije radi sustavnog prikupljanja, analize, obrade i ocjene podataka dviju vrsta podataka. Prvo, to su podaci koji su od značaja za nacionalnu sigurnosti u cilju otkrivanja i sprječavanja radnji usmjerenih protiv opstojnosti, neovisnosti, jedinstvenosti i suvereniteta Republike Hrvatske, nasilnom rušenju ustroja državne vlasti, kao i ugrožavanju Ustavom Republike Hrvatske i zakonima utvrđenim ljudskim pravima i temeljnim slobodama te osnova gospodarskog sustava Republike Hrvatske. Drugo, to su svi podaci koji su nužni za donošenje odluka značajnih za ostvarivanje nacionalnih interesa u području nacionalne sigurnosti. Zatim, kao što je već navedeno, ZSS u članku 25. propisuje načine prikupljanja podataka te ih u nastavku detaljno uređuje. Sukladno načelu zakonitosti, posebno detaljno su razrađene mjere tajnog prikupljanja podataka kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode (Juras i Vulas, 2016: 72).[3] Spomenute

[2] Članak 16. stavak 2. Ustava Republike Hrvatske („Narodne novine“ br. 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014)

[3] Članak 33. stavak 3.:
„Mjere tajnog prikupljanja podataka jesu:
1. tajni nadzor telekomunikacijskih usluga, djelatnosti i prometa:
   a) tajni nadzor sadržaja komunikacija,
   b) tajni nadzor podataka o telekomunikacijskom prometu,
   c) tajni nadzor lokacije korisnika,
   d) tajni nadzor međunarodnih telekomunikacijskih veza,
2. tajni nadzor nad poštanskim i drugim pošiljkama,

mjere nabraja po načelu *nuumerus clausus* uvjetujući ih upravo primjenom načela razmjernosti (Badžim, 2008: 1036). Tako se u članku 33., stavku 2., ZSS-a izrijekom navodi kako se mjere kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode mogu provoditi ako se podaci ne mogu prikupiti na drugi način ili je njihovo prikupljanje povezano s nerazmjernim teškoćama. Na istom se mjestu navodi da će se, ako postoji mogućnost izbora između više mjera tajnog prikupljanja podataka, primijeniti mjera kojom se manje zadire u Ustavom zaštićena prava i slobode. U tom smislu, sukladno navedenim načelima, a u svrhu osiguravanja demokracije i vladavine prava, kod najinvazivnijih mjera zahtijeva se i nadzor najviših sudskih tijela. Tako se, temeljem članka 36. ZSS-a, mjere tajnog nadzora sadržaja komunikacija, tajnog nadzora nad poštanskim i drugim pošiljkama, tajnog nadzora i tehničkog snimanja unutrašnjosti objekata, zatvorenih prostora i predmeta te tajnog praćenja i motrenja uz zvučno snimanje sadržaja komunikacija osoba u otvorenom prostoru i na javnim mjestima mogu poduzimati samo na temelju pisanog obrazloženog naloga za njihovo provođenje koje izdaje sudac Vrhovnog suda Republike Hrvatske.

Kada je riječ o prikupljanju podataka posredstvom ljudskih izvora, tzv. HUMINT-u, ZSS prepoznaje i uređuje prikupljanje podataka komunikacijom s građanima uz prethodnu legitimaciju službenom iskaznicom i značkom[4] i posredstvom tajnih suradnika.[5] Također, ZSS predviđa i obvezu „čelnika i zaposlenika državnih tijela i tijela jedinica područne (regionalne) samouprave i pravnih osoba s javnim ovlastima, kao i zaposlenika, odnosno pripadnika Ministarstva obrane i Oružanih snaga, da udovolje zahtjevima sigurnosno-obavještajnih agencija glede podataka kojima raspolažu u okviru zakonom određenog djelokruga.“[6] ZSS navedenim službama omogućuje i pristup registrima i zbirkama podataka ili dokumentaciji, neposrednim uvidom njihovih zaposlenika, odnosno trajnim pristupom računalnoj ili na sličan način ustrojenoj zbirci podataka, uporabom odgovarajućih sučelja.[7] Imajući u vidu navedene relevantne odredbe ZSS-a, načela zakonitosti i razmjernosti su ispunjena. ZSS, naime, detaljno uređuje nadzor nad djelovanjem službi (Badžim, 2008: 1043) [8] kao i prikupljanje podataka.

Naposljetku, kako u svakom drugom tako i u hrvatskom pravnom sustavu, specifičnost OSINT-a kao prikupljačke discipline obavještajnih službi u njegovu je oksimoronskom karakteru (Miller, 2018). Dok je njihovo djelovanje u najvećoj mjeri vezano uz koncept tajnosti, OSINT se temelji na transparentnosti (Ten Hulsen, 2020: 25). Nadalje, kada se govori o ljudskim pravima i temeljnim slobodama koji se privremeno

3. tajni nadzor i tehničko snimanje unutrašnjosti objekata, zatvorenih prostora i predmeta,
4. tajno praćenje i motrenje uz svjetlosno snimanje osoba u otvorenom prostoru i na javnim mjestima,
5. tajno praćenje i motrenje uz zvučno snimanje sadržaja komunikacija osoba u otvorenom prostoru i na javnim mjestima,
6. tajni otkup dokumenata i predmeta.“

4 Članak 27. ZSS-a.

5 Članak 29. ZSS-a.

6 Članak 30. ZSS-a.

7 Članak 31. ZSS-a.

8 Članci 103.-114. ZSS-a.

ograničavaju mjerama prikupljanja podataka koje provode obavještajne službe, u pravilu će riječ biti o pravu na privatnost, odnosno, konvencijskim rječnikom, pravu na poštovanje privatnog i obiteljskog života. Ovo je slučaj i s prikupljanjem podataka iz otvorenih izvora.

OSINT U KONTEKSTU PRAVA NA PRIVATNOST

Zaštita osobnih podataka od presušne je važnosti za uživanje prava na poštovanje privatnog i obiteljskog života.[9] Europski sud za ljudska prava (ESLJP) ustvrdio je da se koncept privatnog života odnosi na sve aspekte povezane s osobnim identitetom kao što su osobno ime, fotografija ili fizički ili moralni integritet, a članak 8. Konvencije za zaštitu ljudskih prava i temeljnih sloboda (EKLJP) osigurava razvoj osobnosti svakog pojedinca unutar njegova odnosa s drugim ljudskim bićima.[10] Navedeni članak štiti pravo na poštovanje privatnog i obiteljskog života te predviđa pravo države da ograniči ostvarivanje tog prava, u skladu sa zakonom i ako je to nužno u demokratskom društvu „radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih."

ESLJP razvio je široku praksu kada je riječ o ograničavanju konvencijskog prava na privatnost u korist nacionalne sigurnosti.[11] ESLJP ustvrdio je da svatko može tvrditi da su mu povrijeđena prava u navedenom smislu ako nacionalni zakon koji uređuje odnosnu materiju ne udovoljava određenim uvjetima.[12] Nacionalno zakonodavstvo mora predviđati učinkovita pravna sredstva za pobijanje mjera prikupljanja podataka koje se nad pojedincima primjenjuju, kao i učinkovit nadzor nacionalnih sudskih tijela[13] (Aljinović, 2022: 84). Država, odnosno službe nisu neograničene u svojoj ovlasti primjene takvih mjera, pogotovo s obzirom na povećan rizik od arbitrarnosti koje tajne mjere nose sa sobom[14] te, sukladno tome, rizik od njihove zlouporabe.[15] Općenito, ESLJP često je naglašavao da pozivanje na nacionalnu sigurnost države članice ne može tu državu članicu osloboditi svih njezinih obveza u smislu obveze poštivanja ljudskih prava i temeljnih sloboda, no istovremeno je bio svjestan važnosti potrebe da nacionalna sigurnost ostane u domeni svake države, odnosno u granicama njezine prosudbe (Novak, 2021: 145).[16] Dakle, dok mjera i zakonodavstvo koje ju omogućava

9 *Podchasov protiv Rusije*, zahtjev 33696/19 2024, para 62.

10 *Von Hannover protiv Njemačke (No. 2),* zahtjev 40660/08 i 60641/08, para 95.

11 Vidi Guide on Article 8 of the Convention – Right to respect for private and family life, Right to respect for private and family life, home and correspondence, Updated on 9 April 2024, str.63., https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng

12 *Roman Zakharov protiv Rusije [GC*], zahtjev 47143/06, para 171–172., 4. 12. 2015.

13 *Kennedy protiv Ujedinjene Kraljevine* zahtjev 26839/05, para 124. , 18.5.2010.

14 *Zoltán Varga protiv Slovačke*, zahtjev 58361/12, para 151.. 20.7.2021.

15 *Weber i Saravia protiv Njemačke,* zahtjev 54934/00, para 106., 29.6.2006.

16 Vidi npr. *Klass i ostali protiv Njemačke*, zahtjev 5029/71, para 48. i 49. od 6.9.1978., *Weber i Saravia protiv Njemačke* , zahtjev 54934/00, para 106. od 29.6.2006., *Kennedy protiv*

zadovoljavaju standarde postavljene EKLJP-om i ESLJP-om, one mogu biti pravdane interesima nacionalne sigurnosti, pa čak i kad je riječ o masovnim presretanjima. Čak niti ova mjera ne mora biti u suprotnosti s EKLJP-om „s obzirom na sve više prijetnji s kojima se države trenutačno suočavaju od mreža međunarodnih aktera, koji za komunikaciju upotrebljavaju internet, i s obzirom na postojanje sofisticirane tehnologije koja tim akterima omogućuje da izbjegnu otkrivanje."[17] Naravno, u istim je slučajevima ESLJP odredio i minimalne standarde koji trebaju biti zadovoljeni kako bi isto bilo prihvatljivo (Burić, Engelhart, Novokmet i Roksandić, 2023: 263).[18]

Prikupljačke metode koje su bile predmet ESLJP-a nisu, same po sebi, obuhvaćale prikupljanje podataka iz otvorenih izvora, iako je ESLJP naglasio da „informacije koje sadrže osobne podatke u posjedu medija korisnici interneta mogu lako pronaći putem tražilica"[19] te, s tim u vezi, kako internetski sadržaj i komunikacija predstavljaju opasnost „za ostvarivanje i uživanje ljudskih prava i sloboda, posebno prava na poštovanje privatnog života, koja je sigurno veća od opasnosti koju predstavlja tisak, posebice zbog važne uloge tražilica."[20]

Dakle, u pravilu će se prikupljanju podataka iz javnih izvora, pa i na društvenim mrežama, suprotstavljati jedino pravo na privatnost. No i ovdje to će biti minimalni zahvati u to pravo, nedovoljno agresivni da bi se prikupljanje podataka iz javnih izvora od strane obavještajnih službi moglo ili trebalo ograničiti. Zapravo, kada je riječ o OSINT-u, sigurnosne službe će najmanje, ako i uopće, zadirati u ljudska prava i temeljne slobode, slijedom čega će i biti najmanje ograničene u primjeni ove prikupljačke discipline (Wetzling i Dietrich, 2022: 13).

Kad je riječ o pravnom sustavu Europske unije, Povelja EU-a o temeljnim pravima u članku 7. navodi kako svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i komuniciranja. Važno je za istaknuti da Sud EU-a posebno štiti pravo na privatnost te mu čak daje načelnu prednost u odnosu na pravo izražavanja. Tako je u predmetu *Google Spain* naveo kako „pravâ osobe čiji se podaci obrađuju… zašti-

---

Ujedinjene Kraljevine zahtjev 26839/05 para 154. od 18.5.2010., *Roman Zakharov protiv Rusije [GC*], zahtjev 47143/06, para 232. od 4.12.2015., *Chahal protiv Ujedinjenog Kraljevstva*, zahtjev 22414/93, para 131. od 15.11.1996., *A i ostali protiv Ujedinjenog Kraljevstva*, zahtjev 3455/05, para 210. od 19.2.2009.

17 *Centrum för rättvisa protiv Švedske*, zahtjev, 35252/08, para 261. od 1.7.2021. i *Big Brother Watch i drugi protiv Ujedinjene Kraljevine*, zahtjev 58170/13 62322/14 24960/15 para 322–323. od 25.5.2021., Vodič kroz sudsku praksu Europskog suda za ljudska prava, Zaštita podataka, str. 87., para 381., https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_hrv.

18 *Big Brother Watch i drugi protiv Ujedinjene Kraljevine*, zahtjev 58170/13 62322/14 24960/15 para 361. od 25.5.2021

19 *M.L. i W.W. protiv Njemačke,* zahtjevi 60798/10 i 65599/10, para 97. od 28.6.2018. Vodič kroz sudsku praksu Europskog suda za ljudska prava, Zaštita podataka, str. 87., para 383. https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_hrv.

20 *M.L. i W.W. protiv Njemačke,* zahtjevi 60798/10 i 65599/10, para 91. od 28.6.2018. Vodič kroz sudsku praksu Europskog suda za ljudska prava, Zaštita podataka, str. 87., para 383. https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_hrv.

ćena općenito prevaguju nad… interesom korisnikâ interneta“ (Carlberg, 2015: 68).[21] S druge strane, kada je riječ o nacionalnoj sigurnosti, članak 4. Ugovora o Europskoj Uniji (u daljnjem tekstu: UEU), izričito propisuje kako ona posebice ostaje isključiva odgovornost svake države članice. Ipak, Sud EU-a se nešto žešće obračunao s konceptom nacionalne sigurnosti nego njegov „stariji brat“ ESLJP. U predmetima *Privacy International*[22] i *Quadrature du Net*[23] Sud EU-a je, lišavajući učinka članak 4. stavak 2. UEU-a, nacionalnu sigurnost podvrgnuo pravu Europske unije, odnosno načelu razmjernosti (Novak, 2021). U konkretnim slučajevima, riječ je bila o prikupljačkim disciplinama obavještajnih službi, odnosno o zakonskoj ovlasti državnih tijela „da radi zaštite nacionalne sigurnosti nalažu pružateljima elektroničkih komunikacijskih usluga da sigurnosnim i obavještajnim službama općenito i neselektivno prenose podatke o prometu i lokaciji.“[24]

Također, osim navedene isključenosti nacionalne sigurnosti iz domene prava Unije temeljem članka 4., stavka 2., UEU-a, nacionalna sigurnost iznimka je kada je riječ o primjeni glavnog europskog, ali trenutno i temeljnog svjetskog akta kojim se uređuje zaštita podatka (Shere, 2020: 14). Riječ je o Uredbi (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka, u daljnjem tekstu: GDPR) uz koju je kao dio istog „zakonodavnog paketa“ (Čizmić, Boban, 2018: 380) usvojena i Direktiva o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka 2016/680. Tako uvodna izjava 16. GDPR-a navodi kako se GDPR ne primjenjuje na pitanja zaštite temeljnih prava i sloboda ili slobodnog protoka osobnih podataka u vezi s djelatnostima koje ne ulaze u područje primjene prava Unije, kao što su djelatnosti u vezi s nacionalnom sigurnošću. S tim u vezi i članak 2., točka 2. a), GDPR-a navodi kako se ova Uredba ne odnosi na obradu osobnih podataka tijekom djelatnosti koja nije obuhvaćena pravom Unije, a nacionalna sigurnost, prema članku 4., stavku 2., UEU-a to „posebice“ nije. Niti spomenuta Direktiva na odnosi se na prikupljanje podataka od strane obavještajnih službi. Sud EU-a potvrdio je kako se zahtjevom zaštite nacionalne sigurnosti mogu opravdati ograničenja u obliku zakonodavnih mjera u pogledu obveza i prava koja proizlaze iz GDPR-a.[25] S druge strane, Sud EU-a također je postavio pravilo da činjenica da se neka odluka tiče

[21] Predmet od 13. 5. 2014., *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317, para 81.

[22] Predmet od 6. 10. 2020., *Privacy International protiv Secretary of State for Foreign and Commonwealth Affairs i ostalih*, C-623/17, ECLI:EU:C:2020: 790.

[23] Predmet od 6. 10. 2020. *La Quadrature du Net i ostali protiv Premier ministre i ostalih i Ordre des barreaux francophones et germanophone i ostali protiv Conseil des ministres*, C-511/18, C-512/18 i C-520/18, ECLI:EU:C:2020:791.

[24] Predmet od 6. 10. 2020., *Privacy International protiv Secretary of State for Foreign and Commonwealth Affairs i ostalih*, C-623/17, ECLI:EU:C:2020:790, para 82.

[25] Predmet od 16.1.2024., C-33/22, *Österreichische Datenschutzbehörde protiv WK*, ECLI:EU:C:2024:46, para 55.

nacionalne sigurnosti države članice ne dovodi, sama po sebi, do neprimjene prava Europske unije, odnosno ne može osloboditi države članice od nužnog poštovanja tog prava.[26] Budući da i EKLJP i Povelja EU-a o temeljnim pravima štite pravo na privatnost i pri prikupljanju podataka, pa i onih iz otvorenih izvora, ono se mora poštivati.

Dužnost je svake demokratske države, pa tako i Republike Hrvatske, osigurati pravilnu ravnotežu između prikupljanja podataka od strane obavještajnih službi i prava na privatnost podataka. Točnije, zakonsko uređenje i nadzor nad tim službama moraju osigurati da takve djelatnosti ne dovedu do povrede ljudskih prava i temeljenih sloboda (Sokol i Smerdl, 2006: 136). Naposljetku, pravo na privatnost podataka, kao vrijednost, zaštićeno je na ustavnopravnoj razini člankom 37. Ustava RH.[27] Taj članak svakom jamči sigurnost i tajnost osobnih podataka te određuje tri razine zaštite. Prva razina odnosi se na obvezu zakonskog uređenja svakog prikupljanja podataka u slučaju izostanka privole ispitanika. Druga se odnosi na obvezno zakonsko uređenje zaštite podataka te nadzora nad djelovanjem informatičkih sustava. Treća razina jest zabrana uporabe osobnih podataka suprotno utvrđenoj svrsi njihova prikupljanja.

ZAKLJUČAK

Prikupljanje podataka u biti je djelovanja svake obavještajne službe, a upravo je prikupljanje podataka iz javnih izvora najkorisnija, najjeftinija i najplodonosnija prikupljačka disciplina. Službe su u prikupljanju podataka na takav način najslobodnije, dok je izbor ponuđenih sirovih podataka, koje tek treba provjeriti, vrednovati i pretvoriti u obavještajni podatak, najširi. Navedeno je nužnost kako bi službe mogle obavljati svrhu radi koje su osnovane.

OSINT, niti sam po sebi niti kao metoda sigurnosnih službi, nije reguliran pravom Unije niti se o njemu, zasad, nije očitovao Sud EU-a, a konkretnije niti ESLJP. U tom smislu, treba ga promatrati kao bilo koju drugu djelatnost služba kojom se potencijalno ograničavaju ili ugrožavaju ljudska prava, odnosno pravo na privatnost (Koops. 2013: 654 i Ten Hulsen, 2020: 3).

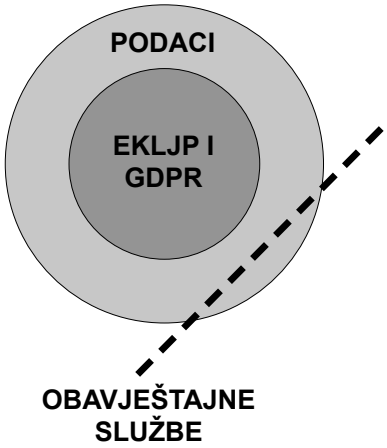
Zapravo, kada je riječ o OSINT-u, sigurnosne službe će najmanje, ako i uopće, zadirati u ljudska prava i temeljne slobode. Donohue, u kontekstu SOCMINT-a, tvrdi kako ljudi, u strahu da su promatrani i praćeni, mogu promijeniti svoje ponašanje, suzdržavati se od izražavanja nekih ideja i mišljenja ili pristupanja određenim grupama istomišljenika. Posljedično, kako tvrdi, udar na privatnost može neizravno negativno utjecati i na slobodu izražavanja tih pojedinaca ili na njihovu slobodu okupljanja i udruživanja. (Donohue, 2015: 1110). Naprotiv, podaci na koje je usmjeren OSINT

[26] Npr. predmeti od 6.10.2020., *Privacy International protiv Secretary of State for Foreign and Commonwealth Affairs i ostalih*, C-623/17, ECLI:EU:C:2020:790, predmet od 6. 10. 2020. *La Quadrature du Net i ostali protiv Premier ministre i ostalih i Ordre des barreaux francophones et germanophone i ostali protiv Conseil des ministres*, C-511/18, C-512/18 i C-520/18, ECLI:EU:C:2020:791, predmet od 15.7.2021., *B. K. protiv Republike Slovenije (Ministrstvo za obrambo)*, C-742/19, ECLI:EU:C:2021:597.

[27] Ustav RH („Narodne novine“ br. 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014).

javni su. Činjenica da je pojedinac neke podatke učinio javnima nesvjesno, odnosno neoprezno ih objavljujući ne vodeći računa o tome da će oni postati dostupni svima, pa tako i obavještajnim službama, nije provjerljiva. U tom kontekstu, i na konvencijskoj razini i na onoj Europske unije, postoji izuzetost nacionalnih službi od strogih zahtjeva zaštite načela privatnosti.

Prikaz: Izuzetost podataka koje prikupljaju obavještajne službe u cilju nacionalne sigurnosti.[28]



Ako takvo izuzeće postoji i kod puno invazivnijih načina prikupljanja podataka, *a maiori ad minus*, još više postoji kod prikupljanja podataka iz otvorenih izvora. Službe će biti najmanje ograničene u primjeni ove prikupljačke discipline (Wetzling i Dietrich, 2022: 13). Takva izuzetost, naravno, nije bez ikakvih ograničenja i uvjeta. Obavještajne službe, u svom su djelovanju, uvijek ograničene načelom zakonitosti te ustavnim i konvencijskom načelom razmjernosti. Posljedično, neće ni prikupljati podatke, pa ni one iz javnih izvora, u slučaju nepostojanja potrebe djelovanja. Također, važan je i sustav nadzora nad radom službi. Preneseno na hrvatski pravni sustav, podaci se neće prikupljati u slučaju nepostojanja potrebe „sprječavanja aktivnosti ili radnji koje se poduzimaju radi ugrožavanja Ustavom utvrđenog poretka, ugrožavanja sigurnosti državnih tijela, građana i nacionalnih interesa."[29] U hrvatskom pravnom sustavu riječ je o terorizmu i drugim oblicima organiziranog nasilja, obavještajnim djelatnostima stranih obavještajnih službi, organizacija i pojedinaca, ekstremističkom organiziranju i djelovanju skupina i pojedinaca, ugrožavanju sigurnosti najviših državnih dužnosnika te štićenih objekata i prostora, organiziranom i gospodarskom kriminalu, neovlaštenom

[28] Većom kružnicom obuhvaćeni su podaci koji postoje u otvorenim izvorima, a manjom oni koji su zaštićeni EKLJP-om i pravom Unije, prvenstveno GDPR-om. Pravac koji siječe veću kružnicu predstavlja djelovanje nacionalnih obavještajnih službi.

[29] Članak 23. ZSS-a.

ulasku u zaštićene informacijske i komunikacijske sustave državnih tijela, odavanju klasificiranih podataka od čelnika i zaposlenika državnih tijela, znanstvenih institucija i pravnih osoba s javnim ovlastima te drugim aktivnostima usmjerenima na ugrožavanje nacionalne sigurnosti.[30] Dakle, zakonska utemeljenost djelovanja sigurnosnih službi, učinkovit nadzor nad njima od strane neovisnog tijela te transparentnost njihova djelovanja nužni su uvjeti opravdanosti ograničavanja prava privatnosti djelovanjem sigurnosnih službi u svrhu zaštite nacionalne sigurnosti.

Sam EKLJP navodi kako je ograničavanje prava na privatnost moguće radi interesa državne, dakle nacionalne sigurnosti, ali i radi zaštite prava i sloboda drugih, čemu ponovno doprinosi nacionalna sigurnost. Odnosno, kako je to ustvrdio i Sud EU, zaštita nacionalne sigurnosti i javnog poretka pridonosi i zaštiti prava i sloboda drugih (Imamović, 2018: 303).[31] Međutim, obavještajne službe će biti ograničene u prvom redu svojom zakonski ustanovljenom nadležnošću, a potom i načelima razmjernosti, racionalnosti, svrsishodnosti i učinkovitosti u radu (Badžim, 2008: 1032).

Zaključno, odgovor na postavljeno pitanje s početka ovog rada je negativan. Povećana dostupnost podataka iz otvorenih izvora te, posljedično, povećane prikupljačke mogućnosti obavještajnih službi u navedenom smislu ne bi trebale rezultirati dodatnim ograničenjima u radu tih službi. Razlozi su minimalno zadiranje u pravo na privatnost, postojeća djelotvorna ograničenja njihova djelovanja proizašla iz načela EKLJP-a i pravnog sustava Unije utjelovljena u praksi ESLJP-a i Suda EU-a.

LITERATURA

Aljinović, N. 2022. Utjecaj odluka i načela Europskog suda za ljudska prava na uređenje instituta posebnih dokaznih radnji u Ujedinjenoj Kraljevini s posebnim naglaskom na presretanje komunikacija, *Pravni vjesnik : časopis za pravne i društvene znanosti Pravnog fakulteta Sveučilišta J.J. Strossmayera u Osijeku*, 38 (2): 75-95.

Aydın, B. i Özleblebici, Z. 2015. Should We Rely on Intelligence Cycle?, *Journal of Military and Information Science*, 3 (3): 93-99.

Badžim, J. 2008. Sigurnosno-obavještajne službe u demokratskom društvu – u povodu reforme sigurnosno-obavještajnog sustava u Republici Hrvatskoj. *Hrvatska i komparativna javna uprava : časopis za teoriju i praksu javne uprave* 8 (4): 1015-1053.

Block, L. 2024. The long history of OSINT. *Journal Of Intelligence History*, 23 (2): 95-109.

Bilandžić, M. 1999. Službe sigurnosti u demokratskom društvu, *Politička misao : časopis za politologiju*, 36 (4): 134-150.

[30] Članak 23. ZSS-a.

[31] Predmet od 15. 2. 2016., J.N. protiv Staatssecretaris van Veiligheid en Justitie, C-601/15 PPU, ECLI:EU:C:2016: 84, para 53.

Boban, M. 2012. Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu, *Zbornik radova Pravnog fakulteta u Splitu*, 49 (3): 575-598.

Burić, Z., Engelhart, M., Novokmet, A., Roksandić, S. 2023. Upotrebljivost rezultata masovnog nadzora komunikacija kao dokaza u hrvatskom kaznenom postupku – slučaj SKY ECC *Hrvatski ljetopis za kaznene znanosti i praksu*, 30 (2): 243-274.

Carlberg, M, 2015. Conflicts between Fundamental Rights in Europe - A study of the CJEU and the ECtHR approach to conflicts between fundamental rights in the light of Google Spain, *Lund University Publications Student Paper*, 1-99.

Chesterman, S. 2008. We Can't Spy … If We Can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing ' Inherently Governmental Functions. *European Journal of International Law*, 19 (5): 1055-1075.

Čizmić, J., Boban, M. 2018. Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 39 (1): 377-410.

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

Dokman, T. 2021. *Analitički okvir primjene obavještajnih informacija iz otvorenih izvora u protuterorizmu* (doktorska disertacija). Sveučilište u Zagrebu, Filozofski fakultet. Zagreb.

Donohue, L. K. 2015. The dawn of social intelligence (SOCINT). *Drake Law Review*, 63 (4): 1061-1112.

Gill, P. i Phythian, M. 2014. From Intelligence Cycle to web of intelligence: Complexity and the conceptualisation of intelligence, u: Phythian, M., *Understanding the Intelligence Cycle*. Routledge, Taylor and Francis Group. London/New York: 21-42.

Hassan, N. A. i Hijazi, R. 2018. *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*. Apress, New York.

Hwang,,YW., Lee, IY., Kim, H., Lee, H., Kim, D. 2022. Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing*:1-14.

Imamović, Š. 2018. *Resolving Conflicts in European Fundamental Rights Protection National and European Courts' Perspectives* (doktorska disertacija). Maastricht University, Universiteit Hasselt. Maastricht.

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.

Ivanjko T. i Dokman, T. 2019. Open Source Intelligence (OSINT) : issues and trends, u: Bago, Petra; Hebrang Grgić, Ivana; Ivanjko, Tomislav; Juričić, Vedran; Miklošević, Željka; Stublić, Helena, *INFuture 2019 : knowledge in the digital age*. FF press. Zagreb: 191-196.

Juras, D., Vulas, A. 2016. Pravni okvir provjere uspostavljanja telekomunikacijskog kontakta. *Policija i sigurnost*, 25 (1): 69-82.

Knol Radoja, K. 2024. Pravo na zaštitu privatnosti vs. načelo javnosti zemljišnih knjiga, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 45 (2): 403-419.

Koops, BJ. 2013. Police Investigations in Internet Open Sources: Procedural-Law Issues. *Computer Law & Security Review* 29, (6): 654-665.

Leško, L. 2019. Analitičke tehnike primjenjive u sigurnosno-obavještajnim agencijama, *Strategos : Znanstveni časopis Hrvatskog vojnog učilišta „Dr. Franjo Tuđman“*, 3 (2): 7-35.

Lucić, D. 2022. Open-source information – the basis for business intelligence (BI), *Informatologia*, 55 (3-4): 219-231.

Macêdo, A., Peotta L. i Gomes, F. 2023. A Review of the Intersection Techniques on Humint and Osint, *International Journal on Cybernetics & Informatics (IJCI)*, 12 (1): 53-63.

Matey, G.D. 2005. Intelligence Studies at the dawn of the 21st century: new possibilities and resources for a recent topic in International Relations, UNISCI *Discussion Papers*, 8: 1-15.

Mercado, C. S. 2004. Sailing the Sea of OSINT in the Information Age, S*tudies in Intelligence, Journal of American Intelligence Professional*, 48 (3): 45-55.

Miller, B.H. Open source intelligence (OSINT): an oxy-moron?. 2018. *International Journal of Intelligence & Counter In-telligence*, 31 (4): 702–719.

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

Novak, S. 2021. Sigurnosno osjetljivi podaci država članica u praksi Suda Europske unije, *Hrvatska i komparativna javna uprava : časopis za teoriju i praksu javne uprave* , 21 (1): 129.-153

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.

Richards, J. 2010. *The Art and Science of Intelligence Analysis*, Oxford University Press Inc. New York.

Shere, A. 2020. *Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and opensource intelligence gathering and analysis*, u: Gable, H. *The New Collection*. Harry Gable, Oxford: 3-21.

Sokol, S. i Smerdl, B., 2006. *Ustavno pravo.* Pravni fakultet Sveučilišta u Zagrebu. Zagreb.

Solove, D.J. 2002. Access and Aggregation: Public Records, Privacy and the Constitution, *Minnesota Law Review*, 86 (6): 1137-1209.

Steele, R. D. 2006. Open source intelligence. u: L. K. Johnson, Handbook of Intelligence Studies. Routledge. New York: 129-147.

Ten Hulsen, L., Open Sourcing Evidence From the Internet – the Protection of Privacy in Civilian Criminal Investigations using OSINT (Open-Source Intelligence). *Amsterdam Law Forum*, 12 (2): 1-45, dostupno na: https://amsterdamlawforum.org/articles/353/files/submission/proof/353-1-696-2-10-20200611.pdf 11 jun. 2020. 9. listopad 2024.

Trybus, M. 2009. A Response to Simon Chesterman “We Can’t Spy….If We Can’t Buy!” EJIL: Talk!, dostupno na: https://www.ejiltalk.org/a-response-to-simon-chesterman-%E2%80%9Cwe-can%E2%80%99t-spy%E2%80%A6if-we-can%E2%80%99t-buy%E2%80%9D/ 10. listopad 2024.

Warner, M. 2014. The past and future of Intellignce Cycle, Gill, P. i Phythian, M. From Intelligence Cycle to web of intelligence: Complexity and the conceptualisation of intelligence, u: Phythian, M., *Understanding the Intelligence Cycle*. Routledge, Taylor and Francis Group. London/New York: 9-20.

Wetzling, T. i Dietrich, C. 2022. *Disproportionate use of commercially and publicly available data: Europe’s next frontier for intelligence reform?*. Stiftung Neue Verantwortung: 3-66., dostupno na: https://www.interface-eu.org/publications/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier 9. listopad 2024.

Warren, S.D. i Brandeis, L.D. 1890. The right to privacy, *Harvard Law Review,* 4 (5).

Information Gathering from Open Sources and National Intelligence Services: Right to Privacy

Stjepan Novak

EXTENDED SUMMARY

Data collection is essentially the core activity of any intelligence service, and the collection of information from public sources is precisely the most useful, cost-effective, and productive intelligence-gathering discipline. Neither in itself nor as a method of security services is OSINT (Open Source Intelligence) regulated by Union law, nor has the Court of Justice of the European Union (CJEU), or more specifically the European Court of Human Rights (ECtHR), issued a ruling on it to date. In this sense, it should be regarded like any other activity of the services that potentially limits or threatens human rights, in particular the right to privacy.

Regarding OSINT, security services will minimally, if at all, interfere with human rights and fundamental freedoms. The fact that an individual has made certain information public—either unknowingly or by imprudently publishing it without considering that it could become accessible to everyone, including intelligence services—is not verifiable. In this context, both at the level of the ECHR and at the level of the European Union, there is an exception for national services from strict requirements for the protection of privacy principles. If such an exception exists for much more invasive methods of data collection, a fortiori, it exists even more for the collection of data from open sources. Consequently, services are least restricted in applying this intelligence-gathering discipline.

Of course, such an exception is not without limitations and conditions. Intelligence services, in their operations, are always bound by the principle of legality as well as the constitutional and Convention-based principle of proportionality. Accordingly, they will not collect data, including from public sources, in the absence of an operational necessity.

The increased availability of data from open sources, and consequently the enhanced intelligence-gathering capabilities of intelligence services in this context, should not result in additional restrictions on their operations. The reasons are minimal intrusion into the right to privacy and the existence of effective limitations on their actions arising from the principles of the ECHR and the legal system of the Union, as reflected in the case law of the ECtHR and the CJEU.

Keywords: data collection, public (open) sources, intelligence services, right to privacy, European Court of Human Rights, Court of the European Union.