UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Žiga Tomažič

Socialna omrežja kot orodje nadzora nad prebivalstvom

Magistrsko delo

Ljubljana, 2018

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Žiga Tomažič

Mentor: izr. prof. dr. Iztok Prezelj

Socialna omrežja kot orodje nadzora nad prebivalstvom

Magistrsko delo

Ljubljana, 2018

Zahvala

Zahvaljujem se staršem, saj so mi omogočili študij ter me vseskozi podpirali na moji študijski poti.

Zahvala gre tudi profesorjem, še posebej mentorju izr. prof. dr. Iztoku Prezlju, ki so mi pomagali na moji akademski poti.

Zahvaljujem se tudi vsem prijateljem, ki so me spremljali skozi študijska leta.

Socialna omrežja kot orodje nadzora nad prebivalstvom

Države se pri svojem delovanju poslužujejo različnih metod in oblik nadzora nad prebivalstvom. V novejši zgodovini so primeri, ko so politične elite uvedle popoln nadzor v državi predvsem za dosego svojih ožjih političnih ciljev. Njihovo glavno orožje so predstavljale varnostno-obveščevalne službe, katerih temeljne naloge so pridobivanje, vrednotenje, analiziranje in posredovanje podatkov. Skupaj z razvojem informacijske tehnologije se razvijajo tudi metode in načini pridobivanja ter eksploatacije podatkov. Varnostno-obveščevalne službe so se za uspešno zagotavljanje nacionalne varnosti morale prilagoditi in skupaj z družbo preseliti na svetovni splet. Socialna omrežja so v informacijski dobi postala integralni del vsakdanjega življenja. Velike količine osebnih in drugih podatkov, ki jih te platforme zbirajo, se izrabljajo v dva namena. Prvi namen je povečevanje dobička podjetij, drugi pa izvajanje nadzora s strani države. To magistrsko delo poskuša dokazati, da se socialna omrežja lahko izrablja za izvajanje nadzora nad uporabniki, kar lahko vodi v policijsko državo. Na podlagi zgodovinskih primerov policijskih držav je prikazan teoretični model z osnovnimi elementi, ki določajo policijsko državo. Nadalje je na ta teoretični model aplicirano delovanje socialnih omrežij, ki zaradi zbiranja osebnih podatkov nudijo možnost njihove uporabe za nezakonito izvajanje nadzora nad prebivalstvom in prehod v policijsko državo. Kot je bilo v tem delu ugotovljeno, socialnih omrežij zaenkrat ni mogoče uporabljati kot orodje popolnega nadzora nad državljani. V prihodnosti pa bi se lahko, v kombinaciji z ostalo tehnologijo, današnja družba spremenila v obliko globalne policijske države, ki bi v določenih vidikih spominjala na klasične primere nadzorovanih družb v nedemokratičnih režimih.

Ključne besede: policijska država, tajne službe, socialna omrežja, nadzor.

Social networks as a tool for people surveillance

States are using different methods and forms of surveillance. In recent history some political elites had introduced the full control of the state, primarily to achieve their narrow political goals. Their primary weapon were intelligence and security services, whose basic functions are to collect, evaluate, analyse and disseminate intelligence. Along with the development of informational technology, methods and ways for obtaining and exploiting data are also being developed. In order to successfully ensure national security, intelligence and security services had to adapt and moved together with society to the internet. In the informational age, social networks became a vital part of everyday life. Vast amounts of personal and other data collected by these platforms are used for two purposes. The first purpose is to increase the profits of companies, while the second one is to exercise state surveillance. This master's thesis attempts to prove that social networks can be used to exercise control over its users, what can lead into a police state. On the basis of historical examples of police states, a theoretical model with the basic elements defining the police state will be shown. Further on, this theoretical model will be applied to social networks, which through the collection of personal data offer the possibility of their illegal use for surveillance and the transformation to a police state. As has been found in this thesis, social networks for the time being can't be used as a tool for total control over citizens. In the future, in combination with other technology, today's society could be transformed into a global police state, which in certain aspects would resemble the classic examples of surveillance societies in non-democratic regimes.

Keywords: Police state, secret services, social networks, surveillance.

KAZALO

SEZNAM KRATIC **7**
1 UVOD **9**
2 METODOLOŠKO-HIPOTETIČNI OKVIR **12**
2.1 OPREDELITEV TEME MAGISTRSKEGA DELA 12
2.2 CILJI DELA 14
2.3 HIPOTEZA 14
2.4 STRUKTURA ANALIZE IN METODOLOGIJA 14
3 OPREDELITEV OSNOVNIH POJMOV **16**
3.1 DRŽAVA 16
3.1.1 Avtoritarizem *18*
3.1.2 Totalitarizem *20*
3.1.3 Demokracija *28*
3.2 SOCIALNA OMREŽJA 31
4 TEORETIČNI MODEL POLICIJSKE DRŽAVE **37**
4.1 TAJNE SLUŽBE 37
4.2 NADZOR 39
4.3 POLICIJSKA DRŽAVA 41
4.3.1 Nacistična Nemčija *42*
4.3.2 Nemška demokratična republika in Stasi *44*
4.3.3 Sovjetska zveza *45*
4.3.4 Združene države Amerike *48*
4.4 MODEL POLICIJSKE DRŽAVE 49
5 ZBIRANJE PODATKOV S STRANI SOCIALNIH OMREŽIJ **52**
5.1 FACEBOOK 52
5.2 INSTAGRAM 54
5.3 TWITTER 55
5.4 GOOGLE+ 57
5.5 LINKEDIN 59
6 UPORABA SOCIALNIH OMREŽIJ S STRANI DRŽAVE **61**
6.1 OSINT, WEBINT, SOCMINT 61
6.2 VARNOSTNO-OBVEŠČEVALNE SLUŽBE 64
6.3 DRUGI DRŽAVNI ORGANI 69

7 SINTEZA IN ZAKLJUČEK 72
8 VIRI 76

SEZNAM KRATIC

COINTELPRO	*Counter Intelligence Program*	Protiobveščevalni program
DARPA	*Defense Advanced Research Projects Agency*	Agencija za napredne obrambne analize
DST	*Direction du Surveillance Territorie*	Francoska notranja obveščevalna služba
ESTA	*Electronic System for Travel Authorization*	Elektronski sistem za odobritev potovanj
FBI	*Federal Bureau of Investigation*	Zvezni preiskovalni urad
FISA	*Foreign Intelligence Surveillance Act*	Zakon o nadzoru tujih obveščevalnih služb
FSB	*Federal'naya sluzhba bezopasnosti*	Federalna varnostna služba
GCHQ	*Government Communications Headquarters*	Vladna uprava za komunikacije
GPU	*Gosudarstvennoye politicheskoye upravlenie*	Državna politična uprava
GUGB	*Glavnoe upravlenie gosudarstvennoi bezopasnosti*	Glavni direktorat za državno varnost
HUMINT	*Human Intelligence*	Pridobivanje podatkov s človeškimi viri
IRA	*Irish Republican Army*	Irska republikanska vojska
IRS	*Internal Revenue Service*	Davčna uprava ZDA
KGB	*Komitet gosudarstvennoy bezopasnosti*	Komite državne varnosti
MGB	*Ministerstvo gosudarstvennoy bezopasnosti*	Ministrstvo za državno varnost
NDR	Nemška Demokratična Republika	
NKGB	*Narodny komissariat gosudarstvennoi bezopasnosti*	Ljudski komisariat za državno varnost
NKVD	*Narodnyi komissariat vnutrennikh del*	Ljudski komisariat za notranje zadeve
NSA	*National Security Agency*	Nacionalno varnostna agencija
NSDAP	*Nacionalsozialistische Deutsche Arbeiterpartei*	Nacionalsocialistična nemška delavska stranka
OGPU	*Obyedinyonnoye gosudarstvennoye politicheskoye upravleniye*	Združena državna politična uprava
OSINT	*Open Source Intelligence*	Pridobivanje podatkov iz javno dostopnih virov
SD	*Sicherheitsdienst*	Varnostna služba
SIGINT	*Signal Intelligence*	Pridobivanje podatkov s tehničnimi sredstvi

SOCMINT	*Social Media Intelligence*	Pridobivanje podatkov z uporabo socialnih omrežij
SS	*Schutzstaffel*	Eskadron za zaščito
WEBINT	*Web Intelligence*	Pridobivanje podatkov z uporabo interneta

1 UVOD

Nagel razvoj informacijske tehnologije ob koncu 20. stoletja, začetki katere segajo v leta po koncu druge svetovne vojne, je privedel do tega, da se je postindustrijska družba korenito spremenila in je na podlagi ustvarjanja, širjenja, integriranja in manipuliranja z informacijami z novimi tehnologijami privedla do informacijske družbe, v kateri živimo. Na prelomu tisočletja je internet prešel v vsesplošno uporabo, sledil je razvoj drugih z njim povezanih tehnologij, kot so pametne mobilne naprave. Oba dejavnika sta tako postavila temelje delovanja socialnih omrežij, ki so pri ljudeh postala sestavni del modernega načina življenja. Tako je v letu 2016 internet aktivno uporabljalo 3,7 milijarde ljudi, kar je polovica svetovnega prebivalstva. Razvoj pametnih mobilnih naprav in brezžičnega interneta (Wi-Fi) in mobilni podatkovni prenos sta privedla do tega, da na mobilnih napravah internet uporablja 3,4 milijarde ljudi, kar pomeni, da imajo skoraj vsi uporabniki internet vedno na dosegu roke in so praktično ves čas *on-line* (Kemp, 2017). V povprečju se v 60 sekundah na svetovnem spletu zgodi naslednje: poslanih je 149.513 sporočil elektronske pošte, objavljenih je 3,3 milijona objav na Facebooku, opravljenih je 3,3 milijona iskanj na Googlu, na Instagram je naloženih 65.972 fotografij, na Twitterju je objavljenih 448.800 objav, na Wordpressu je 1440 novih objav, prek aplikacije Whatsapp je poslanih 29 milijonov sporočil in na YouTube je naloženih 500 ur videoposnetkov (Allen, 2017).

Varnostno-obveščevalne službe praviloma vseskozi iščejo nove načine pridobivanja podatkov in so se bile primorane prilagodit razvoju informacijske tehnologije. Če so se v daljni preteklosti osredotočale zgolj na podatke, pridobljene s človeškimi viri – HUMINT (angl. *Human Intelligence*) , je z razmahom uporabe novih tehnologij pomembno vlogo pridobil segment pridobivanja podatkov s tehničnimi sredstvi – SIGINT (angl. *Signal Intelligence*). Podobno so tajne službe začele uporabljati in nadzirati storitve, ki so dostopne prek svetovnega spleta, ne glede na področje, s katerim se ukvarjajo, bodisi kot obveščevalno ali varnostno dejavnost, te podatke pa opredeljujejo kot javne vire – OSINT (angl. *Open Source Intelligence*). Skupaj z globalizacijo se je spremenilo tudi dojemanje terorizma, ki se je iz nacionalno-političnega in separatističnega spremenil v mednarodni terorizem, kjer državne meje in nacionalnost ne igrajo več vodilne vloge. V praksi se je izkazalo, da se tudi teroristi in ekstremisti pri svojem delovanju poslužujejo informacijske tehnologije, kar je sprožilo

pričakovan odziv in legitimnost eksploatacije teh tehnologij tudi za zagotavljanju nacionalne, regionalne in globalne varnosti, predvsem s strani varnostno-obveščevalnih služb.

Neposreden dostop do širokega nabora podatkov o posameznikih pa lahko kar hitro premami posamezne države in njihove tajne službe, da pričnejo izkoriščati podatke še za druge dejavnosti kot pa samo v primerih, ko gre za dejansko ogrožanje nacionalne varnosti. Tako se ti podatki pričnejo uporabljati za razreševanje notranjih težav, ki so družbeno-politično motivirane, ko govorimo o ohranjanju nadvlade političnih elit in onemogočanje opozicije. Takšne pojave lahko spremljamo v nedemokratičnih državah, kjer nad internetom in socialnimi omrežji vladata oster nadzor in državna cenzura. Na drugi strani pa ravno te storitve omogočajo aktivacijo ljudi in večjo ozaveščanje ter informiranje glede aktivnosti, kot so protesti in manifestacije. V skoraj vseh državah zahodnega sveta se izvajanje množičnega nadzora opravičuje predvsem z grožnjo islamskega terorizma, ki velja za največjo sodobno grožnjo njihovi nacionalni varnosti.

V zadnjih letih je vse več polemik okrog tega, ali so se ljudje pripravljeni odreči delu svoje zasebnosti v zameno za večjo varnost ali ne. Ta problematika je še posebej prišla v ospredje po razkritju dejstev, da nekatere države izvajajo ali sodelujejo v programih množičnega globalnega nadzora. Med drugim je bil razkrit program ECHELON, za katerim stoji t. i. skupina petih oči.[1] Program se je v času hladne vojne uporabljal za zbiranje vojaških in diplomatskih komunikacijskih podatkov, potem pa prešel v globalni sistem za prestrezanje zasebne in komercialne komunikacije oziroma v množični nadzor in industrijsko vohunjenje (Schmid, 2001, str. 11). Podobno se je v okviru projekta PRISM na podlagi zakona ZDA FISA (angl. *Foreign Intelligence Surveillance Act*) komunikacija zbirala prek interneta neposredno od ponudnikov storitev. V javnost so prišli še drugi podobni projekti, ki so se ali se še vedno izvajajo s strani služb SIGINT, kot je ameriška Nacionalno varnostna agencija NSA (angl. *National Security Agency*) in britanska Vladna uprava za komunikacije GCHQ (angl. *Government Communications Headquarters*).

"Sodobno nadzorovanje se nanaša na posameznike, ki niso ničesar osumljeni. Opazovani so zato, ker so del nadzorovane množice in prostora ali pa uporabljajo določeno tehnologijo, kot je internet" (Završnik, 2010, str. 35). Svet se iz tega zornega kota spreminja v globalni zapor,

[1] Skupino Five Eyes sestavljajo Združene države Amerike, Kanada, Velika Britanija, Avstralija in Nova Zelandija.

ki ga je Jeremy Bentham v svoji teoriji nadzora poimenoval Panoptikon, v katerem so zaporniki ves čas nadzorovani tako s strani paznikov kot tudi s strani drugih zapornikov, poleg tega pa niso nikoli zares prepričani, ali so v danem trenutku dejansko pod nadzorom ali ne.

2 METODOLOŠKO-HIPOTETIČNI OKVIR

2.1 Opredelitev teme magistrskega dela

Socialna omrežja so v sodobnem načinu življenja postala integralni del posameznikovega vsakdana, saj združujejo različne človeške potrebe. Tako se lahko uporabljajo za zabavo, komunikacijo, lajšajo vsakdanja opravila, informiranje in še mnogo drugih storitev. Za delovanje teh platform pa je pomembno zbiranje podatkov o uporabnikih, saj na tak način omogočajo prikazovanje vsebin, osebno prilagojenih za določenega uporabnika, pa naj bo to prikazovanje informacij s področij, ki ga zanimajo, ali oglaševanje izdelkov, za katere se predvideva, da bi ga morebiti zanimali. Takšno zbiranje osebnih podatkov pa bi lahko pomenilo, da bodo podjetja začela izkoriščati te podatke za drugačne namene, kot so v osnovi zastavljeni za delovanje socialnih omrežij. Poleg vrste vprašanj, ki se pojavljajo o delovanju teh platform, se najpogosteje govori o osebnih podatkih, ki jih socialna omrežja zbirajo, kako jih hranijo ter kaj z njimi počnejo. V prvi vrsti jih izkoriščajo ustanovitelji platform sami. Ustvarjajo psihološke profile o uporabnikih z namenom neposrednega oglaševanja ter vplivanja na odločitve uporabnikov, ob tem pa osebne podatke uporabnikov prodajajo tretjim osebam. Po drugi strani pa lahko te podatke izkoriščajo posamezne države in njene institucije. Državne institucije, ki delujejo na področju zagotavljanja varnosti, tako aktivno spremljajo in uporabljajo socialna omrežja pri svojem delovanju, predvsem na področjih preprečevanja kriminala in protiterorističnega delovanja. Zato obstaja upravičena bojazen, da bi države z dostopom do baz podatkov in uporabo različnih orodij lahko množično nadzorovale uporabnike, kar bi privedlo do popolnega nadzora nad prebivalstvom s strani državnih institucij ter oblikovanje policijske države.

"Socialna omrežja skozi možnosti, ki jih ponujajo, zbirajo ogromno osebnih podatkov o uporabnikih" (Črnčec, 2009, str. 227). Socialna omrežja, kot so Facebook, Google+ in Twitter, shranjujejo nešteto vrst osebnih podatkov o svojih uporabnikih. Ne samo da se shranjujejo podatki, ki jih uporabnik sam preda prek registracije in aktivnosti na omrežjih, temveč tudi informacije, do katerih uporabnik zavestno ali nezavedno odobri dostop. Te informacije prihajajo iz njegovega celotnega delovanja na spletu, dostop pa omogočajo internetni piškotki, zgodovina iskanja in korespondenca spletne pošte. Vse te informacije so shranjene v bazah podatkov, ki jih podjetje med drugim uporablja tudi za neposredno

oglaševanje (Weidemann in Swift, 2013, str. 21). "Razvoj dejavnosti je omogočil povečanje in pocenitev zbiranja in obdelave podatkov ter informacij, zato je nadzor lahko postal večji. Hkrati je predvsem zaradi nadzorovanja potrošnikov prišlo do tega, da imajo podatki in informacije, ki so bili včasih popolnoma vsakdanji in nezanimivi, zdaj veliko tržno vrednost" (Kovačič, 2003, str. 31). Facebook, Twitter, Google+ in LinkedIn so primeri hitrega prenosa življenja ljudi, interakcij, identitet, argumentov in pogledov na novo vrsto javne in zasebne sfere; so široke digitalne socialne javnosti (Omand, Bartlett in Miller, 2012, str. 803). "Vsaka storitev na internetu je izpostavljena določenemu tveganju nepooblaščenega zbiranja podatkov" (Črnčec, 2009, str. 224).

Leta 2012 je Facebook izvedel eksperiment, ki je vključeval 689.000 uporabnikov, v katerem je s filtriranjem objav, ki so se uporabniku pojavljale pri njegovi uporabi platforme, poskušal manipulirati z uporabnikovimi čustvi. Eksperiment je bil izveden brez vednosti in soglasja uporabnikov. Podjetje je ob razkritju svoje dejanje upravičevalo s strinjanjem vsakega uporabnika s pogoji uporabe, s katerimi so seznanjeni ob registraciji (Booth, 2014). Z izvedbo tega eksperimenta so dokazali, da se določeno čustveno stanje lahko od ene osebe prenese na druge uporabnike prek t. i. čustvene okužbe, ki povzroči, da imajo podobne občutke. Tako je dokazano, da se lahko z določenimi metodami prek socialnih omrežij vpliva na razpoloženje uporabnikov (Kramer, Guillory in Hancock, 2014). Torej obstaja možnost vplivati na uporabnike tudi v času političnih kampanj in posledično na izid volitev. Na tak način bi lahko tudi obveščevalne službe v tretjih državah s pomočjo uporabnikov izvedle revolucijo (Booth, 2014).

Obveščevalna dejavnost na socialnih omrežjih se deli v dve kategoriji, ki se ločita po ciljni domeni. To sta posameznik in množica. Pri posamezniku se išče behavioristične in interakcijske značilnosti posameznika v digitalnem okolju. V primeru množice pa je iskanje usmerjeno v agregatne behavioristične in interakcijske značilnosti številnih posameznikov v okviru določene skupine (Géczy in drugi, 2014, str. 47). Obveščevalno-varnostne službe se vse bolj poslužujejo taktičnega zbiranja obveščevalnih podatkov, saj s t. i. "*open-source*" načinom uporabljajo socialna omrežja, kot so Facebook, Twitter, Youtube in številna druga, za pridobivanje koristnih podatkov v obveščevalni dejavnosti (Fitsanakis in Bolden, 2012, str. 28). Obveščevalni skupnosti lahko nova generacija orodij pomaga pri zbiranju dragocenih informacij iz javno dostopnih socialnih omrežij po vsem svetu. Obveščevalci iščejo trende in opozorilne znake morebitnih nacionalnovarnostih kriz. Tako lahko analitiki iz sporočila na Twitterju ali drugih objav odkrijejo povezave med avtorjem in drugimi stiki v navideznem

okolju, ki ga predstavlja socialno omrežje. Določijo lahko fizično lokacijo, kje se določena tarča in njeni stiki nahajajo, kar socialno omrežje spremeni v realni svetovni zemljevid (Barnes, 2014).

2.2 Cilji dela

Cilj magistrske naloge je na podlagi delovanja socialnih omrežij, njihovega zbiranja podatkov in preteklih dogodkov, v katerih so državne varnostne institucije uporabile socialna omrežja, pokazati, da ta predstavljajo orodje, s katerim se lahko vsakodnevno vohuni za uporabniki, spremlja njihove aktivnosti ter izvaja množični nadzor nad prebivalstvom. Znano je, da varnostni organi v primerih odkrivanja kaznivih dejanj in preprečevanja teroristične dejavnosti med drugimi pristopi uporabljajo tudi socialna omrežja. Na podlagi najizrazitejših zgodovinskih primerov delovanja tajnih policijskih služb bom izdelal teoretični model, ki predstavlja policijsko državo. Poskušal bom dokazati, da živimo v času, ko je državam omogočen vsakodnevni nadzor nad prebivalstvom, kar predstavlja primer globalne policijske države.

2.3 Hipoteza

Zbiranje in uporaba osebnih podatkov uporabnikov socialnih omrežij v obveščevalne namene poleg vdora v posameznikovo zasebnost prinaša tudi popoln nadzor nad uporabniki, kar vodi v policijsko državo.

2.4 Struktura analize in metodologija

V tretjem poglavju so predstavljeni temeljni pojmi, ki so potrebni za razumevanje teme in analize podatkov, zbranih v magistrski nalogi. Najprej predstavim državo in tri vrste režimov, ki so se pojavili v času moderne države. Natančneje sta opisana dva nedemokratična režima, avtoritarni in totalitarni. Tretji režim pa je demokracija, ki je popolno nasprotje tako v ideološkem, institucionalnem in ustavnem oziru. Z vidika nedemokratičnih režimov so dodatno opredeljene tri najbolj znane vrste ideologij, ki so se pojavile v 20. stoletju. Drugi pojem, pomemben pri raziskovanju, pa je socialno omrežje. Skozi nalogo je večkrat

uporabljen izraz platforma, ki služi kot sopomenka besedni zvezi socialno omrežje, saj z razvojem mobilnih tehnologij niso več dostopna samo prek osebnih računalnikov, ampak ima že vsak ponudnik socialnega omrežja razvite aplikacije za prenosne naprave, kot so tablice in pametni mobilni telefoni. Četrto poglavje opredeljuje delovanje tajnih služb, opiše zgodovinske primere uporabe tajne policije in predstavi teoretični model policijske države, ki je poglavitni del analize. Peto poglavje zajema predstavitev delovanja petih največjih socialnih omrežij in njihovega zbiranja osebnih podatkov uporabnikov. V šestem poglavju so zajeti primeri, v katerih je država prek svojih institucij uporabljala ali izkoriščala socialna omrežja v svoje namene. V sedmem poglavju so predstavljene ugotovitve raziskovalnega dela in podan zaključek magistre naloge.

Metodološki pristopi, ki so uporabljeni pri delu, zajemajo deskriptivno metodo, s katero so predstavljeni temeljni pojmi in teoretični model policijske države, ter primerjalno metodo, s katero se primerja na zgodovinskih primerih vzpostavljeno teorijo policijske države in uporabo socialnih omrežij s strani države. V analizi so uporabljeni primarni in sekundarni viri. Primarni viri vključujejo pravilnike, po katerih delujejo socialna omrežja, in poročila vladnih organov, sekundarni pa znanstvene knjige, članke in medijske objave.

3 OPREDELITEV OSNOVNIH POJMOV

3.1 Država

Moderna država je vseobsegajoče prisotna v življenju vsakega posameznika. Zanemarljivo število ljudi živi zunaj njenega dosega, kot tudi je na planetu zelo malo ozemelj, nad katerimi ta ne bi imela teritorialnega nadzora. Na globalni ravni je država temeljna enota političnega organiziranja in interakcija država proti državi je temelj mednarodnih odnosov. Z razvojem moderne države je ta pridobila možnost, da se na veliko načinov dotika in upravlja z življenjem vsakega posameznika. Tako je ob rojstvu osebi dodeljena unikatna številka, zatem je oseba vključena v šolski sistem, ki temelji na državnem izboru programov in obravnavanih tem, zagotavlja socialno varstvo, od zaslužka osebe vzame določen znesek, s katerim se financirajo državne storitve, in ob smrti v evidencah zabeleži njegov fizični neobstoj. Država tako posega skoraj v vse vidike posameznikovega življenja, tako v šolstvo, državno birokracijo, sodstvo, plačevanje obveznih dajatev v obliki davkov in tudi v zagotavljanje varnosti. Lahko trdimo, da je država glavna institucija neke družbe, ki kot celota obstaja na določenem teritoriju, nad katerim ima monopol upravljanja zadev. Nasproti drugim institucijam ima moč prisile in nasilja, ki ga lahko generira v primerih, za katere meni, da je to upravičeno. Zaradi teh karakteristik govorimo o državi kot centralni politični instituciji v moderni družbi (Hislope in Mughan, 2012, str. 2–3).

Mirovna pogodba, sklenjena v Vestfaliji leta 1648, s katero se je končala tridesetletna vojna med rimokatoliškim in protestantskim taborom, velja za prelomnico v politični zgodovini države. Ta dogodek predstavlja konec dotedanje družbene ureditve in postavlja temelje moderni državi. Oblikovala sta se dva principa razumevanja suverenosti države. Prvi je, da ima država absolutno oblast nad ozemljem, ki je omejeno s teritorialnimi mejami druge države. Drugi princip pa je, da so vse države enakopravne v odnosu druge do druge in da se tako nobena ne sme vmešavati v notranje zadeve drugih držav (Hislope in Mughan, 2012, str. 11). Webrovo razumevanje države je najpogosteje opisano v njegovi definiciji, kjer je država človeška družba, ki uspešno terja monopol nad legitimno uporabo fizičnega nasilja na določenem teritoriju (Gerth in Mills, 1946, str. 78). Njegova bolj natančna opredelitev države pa je, da so primarne formalne značilnosti moderne države naslednje: upravni in pravni red se lahko spremeni z zakonodajo, ki določa, da je usmerjena v organizirane dejavnosti

administrativnega osebja, ki je pod nadzorom s predpisi. Ta sistem reda zahteva zavezujočo avtoriteto ne le nad člani države, ki so v tem pogledu državljani, katerih večina je pridobila članstvu ob rojstvu, ampak tudi v veliki meri nad vsemi ukrepi, ki potekajo v okviru svoje pristojnosti. Gre torej za obvezno organizacijo s teritorialnimi načeli. Poleg tega se danes uporaba sile šteje za legitimno samo, če je dovoljena ali predpisana s strani države (Weber, 1978, str. 56). Zartman (1995, str. 5) podobno kot Weber (1978) razume državo kot institucijo politične avtoritete, ki ima suverenost nad določenim teritorijem. Tretji steber, ki se pojavlja pri Webrovem razumevanju države, pa je ta, da država uspešno izvaja monopol nad legitimno uporabo fizične prisile. Države nadzirajo legalna sredstva prisile in nasilja prek raznih institucij, kot so vojska, carina, tajne službe in celoten kazenski sistem (policija, zapori) (Hislope in Mughan, 2012, str. 15).

Izrazito nasprotje pri gradnji države se pojavi pri razlikovanju notranjih in zunanjih zadev, ki se navezujejo na meddržavnih odnose. Pri notranji stopnji je izgradnja države v večini primerov utemeljena na pacifizmu družbe, saj država kot sama monopolizira legitimno uporabo nasilja in se zavezuje, da sankcionira dejavnosti, ki kršijo pravila. Poleg legitimne uporabe nasilja tudi edina vzpostavlja pravni sistem in upravno administracijo. Na stopnji zunanjih zadev pa se pojavi stopnja nepredvidljivosti, saj države sprejemajo lastne pobude *vis-a-vis* druga druge (vključno z dostopom do nasilja), glede na lastne avtonomne opredelitve nacionalnih interesov. Za vsako državo je glavno zasledovanje cilja lastne varnosti, ki pa lahko ima za posledico, da ogroža drugo državo oziroma ji povzroča zmanjšanje njene lastne varnosti. Ti pogoji vsako državo vodijo v stanje, kjer na prvem mestu poskrbijo za lastno varnost, koliko je mogoče na osnovi danih pogojev (Poggi, 2011, str. 2490).

Avtoriteta je moralna pravica vladati in daje vzajemno dolžnost vladanim, da sprejmejo to pravico podrejeno. V modernih demokratičnih državah avtoriteta sloni na soglasju vladanih. To soglasje daje avtoriteti legitimnost. Legitimnost prihaja s strani vladanih, ki prostovoljno sprejemajo dano avtoriteto. Avtoriteta pa mora imeti moč, s katero lahko nekoga prisili, da stori nekaj, česar drugače ne bi naredil. Moči pa ni mogoče izvajati brez določenih prisilnih instrumentov, ki jih ima na voljo država, kot so policija in oborožene sile, nadzor, zapori, denarne kazni in drugo (Hislope in Mughan, 2012, str. 11–12).

Klasični liberalni filozofi, med katerimi sta najvidnejša predstavnika Thomas Hobbes in John Locke, zagovarjajo idejo družbene pogodbe. Ideja družbene pogodbe temelji na tem, da svobodni ljudje v naravnem stanju doživljajo pomanjkanje varnosti, ki drugim omogoča njeno

eksploatacijo. Tako si varnost in svobodo lahko zagotovijo na način, da zagotavljanje varnosti prenesejo na umetno tvorbo, državo, ki bo skrbela za varnost vsakega posameznika. Po drugi strani pa se s to predajo pooblastil odpovedo delu svojih pravic (Hislope in Mughan, 2012, str. 13). Cilj razumevanja družbene pogodbe je v racionalnem okviru nastanka družbe in politične moči. Prav tako povzroča normativni razmislek o legitimnosti oblasti. Podniz predsodkov izhaja iz te široke obravnave pojma, ki se razumejo kot ključne teme politične teorije, kot so prostor religije v družbi, vprašanje suverenosti, vloga ljudi in oblasti ter temeljnih pravic in svoboščin (Leterre, 2011, str. 436). Jedro družbene pogodbe v političnem smislu je temeljna intuicija, da so vsi družbeni posli na podlagi prvotne pogodbe med posamezniki, da ti pripadajo isti družbi in spoštovanju določene oblasti. Pogodba tako daje možnost vsakemu posamezniku, ki vidi vrednost v tem, da je del družbe, ki ima določena pravila, ki omejujejo posameznikovo svobodo. Namesto da bi ostal sam v popolni svobodi, se raje vključi v to družbo. Teorije družbene pogodbe temeljijo na ideji, da posameznik prepozna večjo korist v pripadnosti določeni družbi kot pa v individualizmu. Posameznik je tako dolžan spoštovati pravila družbe. Tako kot pri vsaki drugi pogodbi se svobodno odločimo in strinjamo s pravili, ki nas potem zavezujejo, da jih spoštujemo, drugače se moramo sprijazniti s posledicami, ki nas doletijo ob kršitvi pravil (Leterre, 2011, str. 437).

V osnovi režime na prvi stopnji ločimo na demokratične in nedemokratične. Razlika se izraža v treh vidikih. Ti so:

1. svobodne kompetitivne volitve,
2. univerzalna volilna pravica,
3. odgovornost izvoljene vlade do ljudi.

V primerjalni politični literaturi najdemo tri osnovne vrste režima. To so demokracija, avtoritarizem in totalitarizem.

3.1.1 Avtoritarizem

Vse do začetka 60. let 20. stoletja je v politični znanosti veljala fundamentalna klasifikacija sistemov na demokratičnega in totalitarnega. Tako je avtoritarni politični sistem veljal za tip totalitarnega režima vse do takrat, ko je postal prevladujoči sistem v nedemokratičnih državah (Özbudun, 2011, str. 107–108). V avtoritarnem sistemu politično organizirana skupina, ki se v različnih državah lahko izraža v obliki stranke, vojske ali vplivne družine, nadzoruje državo in vlado ter tako manipulira z njenimi institucijami za dosego svojih ciljev. Politična

participacija tekmujočih si skupin ni dovoljena ali pa je precej omejena (Hislope in Mughan, 2012, str. 47).

Uvrstiti posamezno državo med avtoritarne režime pomeni, da sta moč in nadzor v državi nepošteno koncentrirani, uveljavljeni in vzdrževani. Represija, tako politična kot fizična, se uporablja za ohranjanje obstoječega stanja, s katerim se preprečuje, da bi v državi prišlo do političnih in družbenih sprememb. Eno od najmočnejših orožij, ki ga lahko poseduje avtoritarni režim, je propaganda. V notranji politiki se uporablja za združevanje ljudi in ustvarjanje populistične podpore ter posledično kot nekakšna vrsta legitimnosti obstoječi vladi. V tej propagandi se nasprotne države prikazuje v negativni luči, označuje se jih kot sovražnike, ki ogrožajo obstoj naše države. S tem se preusmeri in odvrača pozornost od notranjih problemov, ki pestijo državo. Cilj propagande v zunanji politiki pa je mednarodni skupnosti prikriti določene lastnosti režima, ki ne sovpadajo z mednarodnimi normami in pogodbami. Na ta način države pred svetom skrivajo različne kršitve človekovih pravic in državljanskih svoboščin (Murphy, 2014, str. 47–48).

Juan J. Linz (2000) je razvil dokaj natančno teorijo o avtoritarnih režimih, v kateri jih loči od demokratičnih oblik vladavine in totalitarnih režimov kot tudi drugih oblik nedemokratičnih vladavin (tradicionalne avtokracije, oligarhičnih demokracij, sultanističnih režimov …). Tako je avtoritarne režime definiral po treh značilnostih, ki takšno obliko vladavine ločijo od drugih, predvsem totalitarnih režimov:

1. omejena pluralnost,
2. prisotnost miselnosti nasproti ideologiji,
3. odsotnost ali nizka stopnja politične mobilizacije.

Omejena pluralnost je srednja točka med neomejeno pluralnostjo v liberalnih demokracijah in njeno popolno odsotnostjo v totalitarnih režimih. Tako je v primeru avtoritarnega režima izključena določena politična opozicija ali pa gre za izključitev nekaterih delov civilne družbe. Miselnost se od ideologije razlikuje v sestavi in dojemanju prvin, ki jo sestavljajo. Tako je ideologija bolj sistematično urejena, miselnost pa zgolj abstraktno in se osredotoča bolj na emocionalno kot racionalno raven. Ta se potem odraža tudi na tretji značilnosti, politični mobilizaciji, saj ravno zaradi odsotnosti ideologije težko oziroma nemogoče politično mobilizira in privabi mlade, študente in intelektualce (Özbudun, 2011, str. 108).

Linz (2000) nadalje na osnovi svojih dveh kriterijev omejene pluralnosti in pomanjkanje mobilizacije razlikuje naslednje podtipe avtoritarnih režimov:

- birokratsko-vojaški avtoritarni režim,
- organski statizem,
- mobilizacijski avtoritarni režim v postdemokratičnih družbah,
- postneodvisni mobilizacijski avtoritarni režim,
- rasna in etnična demokracija,
- posttotalitarni avtoritarni režim.

V praksi je te podsisteme težko razlikovati med seboj, saj se dejansko medsebojno prepletajo in si delijo skupne točke v različnih obdobjih svojega obstoja (Özbudun, 2011, str. 109).

V tretjem valu demokratizacije 20. stoletja se pojavi nova oblika avtoritarnega režima, ki leži v sivem območju med liberalno demokracijo in zaprtim avtoritarnim režimom (Özbudun, 2011, str. 108). Ta oblika predstavlja t. i. hibridni sistem in je v sodobnem svetu pogosta predvsem zato, ker si določeni avtoritarni režimi želijo, da bi bili navzven videti kot neke vrste demokracija. V času globalizacije in prevlade zahodnih idej ter članstva v mednarodnih organizacijah, ki so jih ustanovile zahodne države, ki tako promovirajo demokratične vrednote, je demokratična vladavina postava nekakšen standard in zato avtoritarni režimi želijo posnemati njene določene prvine. Najpogosteje se to kaže v dopuščanju volilne konkurence, ki pa se od liberalne demokracije razlikuje, predvsem v stopnji omejevanja.

Nadzor nad mediji je pomembna prvina avtoritarnih držav. Večina takšnih režimov ima v lasti celotno medijsko mrežo v državi. V primerih, ko ta ni pod popolnim nadzorom vlade, pa velja velika omejenost in stroga cenzura za nedržavne medije. S pomočjo medijev režim izvaja svojo načrtovano propagando ter sam odloča, katere in kakšne informacije in dezinformacije bo poslal med prebivalce. Prav tako določeni režimi nadzirajo internet in na njem izvajajo cenzuro ter onemogočajo dostop do posameznih spletnih strani ali socialnih omrežij. Cenzura in nadzor nad mediji skupaj z nadzorom posameznika omogočata avtoritarnemu režimu, da sam po lastni presoji poustvarja zgodovino ter določa, kaj je resnica in kaj ne (Murphy, 2014, str. 50).

3.1.2 Totalitarizem

Izraz totalitarizem se pojavi v 20. in 30. letih 20. stoletja kot del ideologije fašistične Italije. V 50. letih se izraz znova pojavi kot prominentni koncept zahodne politične znanosti, ki je s tem terminom začela označevati tako fašistični in nacistični kot tudi komunistični režim (Brooker, 2000, str. 8). Totalitarizem predstavlja nasprotje modernim liberalnim in

demokratičnim režimom, utemeljen je na monopolu moči ene stranke, na čelu katere je karizmatični voditelj in ki dominira nad državo in družbo z uporabo terorja in propagande. Za izvajanje politike totalitarnega režima se uporabljajo institucije, ki so pod nadzorom stranke: visoko centralizirana birokracija, splošna in tajna policija, strankarska milica, manipulacija kulture in javnega mnenja skozi izvajanje monopola nad množičnimi mediji ter omrežje organizacij stranke, ki delujejo po celotni državi z nalogami organizirati, indoktrinirati in permanentno mobilizirati tako posameznika kot množice (Gentile, 2011, str. 2627). Propaganda je eden najpomembnejših dejavnikov totalitarizma za boj proti netotalitarnem svetu, teror pa predstavlja bistvo oblike vladavine (Arendt, 1962, str. 344).

Osnovna značilnost totalitarizma je enostrankarski režim, ki je prišel na oblast s protidemokratičnim gibanjem, ki je za svoj vzpon na oblast in ohranitev politične moči uporabil nasilje in teror paravojaških skupin. Prevlada karizmatičnega vodje in oligarhične stranke ustvari diktaturo, ki se izvaja prek policijske države. Napredek v tehnologiji in organiziranju se uporablja za mobilizacijo množic in intenzivno ter nenehno kolektivno indoktrinacijo skozi množične organizacije. Za ohranjanje monopola moči se uporablja militarizacija politike, nasilje, popoln nadzor države nad družbo in pranje možganov prek propagande (Gentile, 2011, str. 2629). "Totalitarni režim zahteva popolno mobilizacijo družbe v zasledovanju ciljev, ki temeljijo na ideologiji vladajoče stranke" (Hislope in Mughan, 2012, str. 52). V totalitarnih režimih, kjer vlada visoka in konstantna represija, se uspešno izogibajo notranjim konfliktom, kot sta državljanska vojna in množični protesti (Zimmermann, 2011, str. 2710).

Politična represija (politična cenzura, prepoved opozicijskih strank, kršenje osnovnih državljanskih pravic, velike notranje varnostne sile ...) se kaže z nasprotujočim in odvračalnim učinkom, ko stopnja represije doseže kritično točko, na kateri se protestniki začnejo zavedati svoje fizične varnosti. Tako stanje v liberalnih demokracijah velikokrat privede do še večjih protestov, nasprotno pa je v avtoritarnih državah, kjer več represije zmanjša in utiša nastali konflikt (Zimmermann, 2011, str. 2710).

Carl Friedrich in Zbigniew K. Brzezinski (1965) sta postavila parametre, po katerih se določena država uvršča met totalitarne režime. Podala sta klasifikacijo na podlagi šestih točk:

1. izdelana vodilna ideologija,
2. enostrankarski sistem, na čelu katerega je diktator,
3. sistem terorja, ki se upravlja prek nasilja in tajne policije,

4. monopol nad orožjem,
5. monopol nad sredstvi komuniciranja,
6. centralni nadzor in upravljanje ekonomije skozi državno načrtovanje.

Brzezinski (1962) dodaja, da je totalitarna oblika režima oblika vlade, ki je v osnovi diktatura, ki se s pomočjo tehnološko naprednih instrumentov politične moči izraža v neomejenem, centraliziranem elitnem gibanju, katerega namen je ustvariti totalno družbeno revolucijo. Diktatura je oblika vladavine, v kateri ima ena oseba ali skupina absolutno oblast, neomejeno po ustavi ali zakonih, in ne temelji na tradicionalni legitimnosti (Wiatr, 2011, str. 653).

Sam izraz diktatura oziroma diktator se prvič pojavi že v antičnem Rimu. Izraz znova zasledimo v 16. stoletju, ko Niccolo Machiavelli v okviru svojega razmišljanja o združitvi Italije zagovarja stališče, da je diktatura kot oblika vladavine popolnoma sprejemljiva, če diktator ne postane tiran in če vlada v dobro ljudstva. Najbolj izstopajoča primera diktature v začetnem obdobju moderne države sta vladavini Oliverja Cromwella (1649–1658) v Angliji in Napoleona Bonaparta v Franciji. Oba sta si s pomočjo vpliva v oboroženih silah in zaradi šibkosti državnih institucij podredila celotno državo. V Evropi se diktatura kot oblika vladavine v večjem obsegu začne pojavljati v prvi polovici 20. stoletja, kar je bil za ta del sveta tudi najbolj množičen val prehoda v ta način vladavine. V carski Rusiji je leta 1917 prišlo do revolucije, ki je za posledico prinesla zmago komunistov in vzpostavitev t. i. diktature proletariata pod taktirko Vladimirja Lenina in njegove komunistične partije. Propad Otomanskega cesarstva je na oblast prinesel enopartijski sekularni režim pod vodstvom Mustafa Kemala Pasha. V obdobju med obema vojnama pa se pojavijo fašistični in nacistični režimi. Kot prva pride leta 1922 v Italiji na oblast fašistična stranka pod vodstvom Benita Mussolinija, kasneje pa leta 1933 Hitlerjeva nacionalsocialistična nemška delavska stranka in po španski državljanski vojni leta 1939 še fašistična falanga Francesca Franca v Španiji (Wiatr, 2011, str. 654). Konec druge svetovne vojne pomeni tudi konec fašističnih in nacističnih diktatur v Evropi z izjemo Španije, ki se konča šele leta 1975 s smrtjo Franca. Na drugi strani pa predvsem v vzhodni Evropi komunistična partija postane prevladujoča stranka, ki je na oblasti vse do razpada Sovjetske zveze in Jugoslavije v začetku 90. let 20. stol. S procesom dekolonizacije se po svetu pojavijo diktature, predvsem na afriškem kontinentu in na Bližnjem vzhodu. Tako je v 70. letih od 122 držav, ki so imele več kot milijon prebivalcev, le 30 takšnih, kjer je bila ureditev demokratična (Wiatr, 2011, str. 656).

Juan J. Linz in Leonardo Morlino sta s primerjanjem totalitarne in avtoritarne diktature razdelala razliko med totalitarno diktaturo in drugo obliko diktature. Po njunem se razlika izraža v t. i. totalitarnem sindromu, ki ga sestavljajo naslednje komponente (Wiatr, 2011, str. 655):

1. ideologija se uporablja za spreminjanje družbenih odnosov,
2. enostrankarska vladavina, v kateri je opozicija prepovedana,
3. državni monopol nad sredstvi prisile in medijev,
4. državni nadzor ekonomije,
5. policijski teror.

3.1.2.1 Komunizem

Komunistični sistemi so se oblikovali v 20. stoletju in temeljijo na zatiralni centralizaciji politične moči, ki zasleduje cilje nadzorovati nacionalizirano gospodarstvo, kulturo in družbo. Izgradnja te pozicije je bila dosežena na račun milijonov žrtev celotnega sistema represije, ki je sestavljena iz policijskega terorja, sodstva pod političnim nadzorom in sistema delovnih taborišč (Rychard, 2011, str. 324). Vzpostavitev komunističnega režima je vedno prinesla obdobje nasilja in terorja, ki je bilo zaznamovano z množičnimi zločini, genocidi, sodbami, deportacijo in oblikovanjem koncentracijskih taborišča za politične, kulturne in verske nasprotnike, prav tako pa so se izvajale čistke proti nasprotnikom znotraj same stranke. Lazar (2011, str. 311) zagovarja stališče, da se komunistični režimi med seboj razlikujejo, vendar imajo določene skupne lastnosti:

- vzpostavitev enostrankarske vladavine ali hegemonske vloge komunistične partije z nekaj nepomembnimi zavezniki, ki služijo za navidezni vtis pluralistične ureditve;
- monopoliziranje vseh dejavnosti, vključno s politiko, gospodarstvom, socialnimi, intelektualnimi in kulturnimi dejavnostmi ter mediji, ki so glavno sredstvo za izvajanje intenzivne propagande;
- poudarek je na pomenu ideologije, tako za samo stranko kot za celotno prebivalstvo;
- strog in popoln nadzor nad družbo;
- prizadevanje za ustvarjanje "novega človeka", ki je ideološko prepričan ter popolnoma predan stranki in je zanjo pripravljen žrtvovati svoje življenje;
- centralizacija vseh pristojnosti, zlasti v državah z veliko kulturno, etnično, versko in geografsko raznolikostjo;
- potrjevanje vodstva, ki lahko pripelje do kulta osebnosti.

Okrog komunističnega režima so se vedno ustvarjale polemike, kam naj bi se ta uvrstil: ali pod klasično diktaturo ali pod avtoritarni sistem oziroma totalitarizem. Podporniki totalitarnega koncepta vztrajajo, da komunizem skupaj z nacizmom in fašizmom spada med totalitarne režime. Nasprotno pa trdita Hannah Arendt in Raymond Aron, da se je po letu 1956 komunistični sistem, za primer navajata Sovjetsko zvezo, spremenil v posttotalitarno obliko oziroma je dobil lastnosti avtoritarnega režima. Drugi kritiki pa zagovarjajo načelo, da je totalitarna oblika vladavine preširoka in ne zajema posameznih ločnic med fašizmom in nacizmom kot tudi ne med posameznimi oblikami komunističnih režimov (Lazar, 2011, str. 311). Če za uvrstitev komunističnega režima vzamemo Linzov (2000) kriterij določanja avtoritarnih režimov, potem lahko sklepamo, da je v nekaterih primerih prva kategorija politične pluralnosti izpolnjena, saj nekateri komunistični režimi dopuščajo omejeno pluralnost, vendar je ta še vedno pod nekakšnim nadzorom režima. Za drugi dve kategoriji pa ne moremo trditi, da se skladata, saj ima v tem režimu veliko vlogo ideologija, ki naj bi bila v avtoritarnem režimu odsotna, prav zaradi njene prisotnosti pa je v komunističnih državah možna obsežna politična mobilizacija. Na podlagi te distinkcije razlikovanja med avtoritarnimi in totalitarnimi režimi komunističnega režima ne moremo uvrstiti pod avtoritarnega. Seveda pa Linz (prav tam) razlikuje tudi med posameznimi podtipi avtoritarnih režimov, in sicer zlasti na osnovi dveh kriterijev, politične pluralnosti in moči mobilizacije. Če se osredotočimo na ti dve lastnosti, potem se določeni komunistični režimi uvrščajo med posttotalitarne avtoritativne režime, kot to na primeru poststalinistične Sovjetske zveze zagovarjata Hannah Arendt in Raymond Aron.

Vladimir Lenin je utemeljitelj prvega prototipa ideološke stranke, ki jo sestavljajo elite revolucionarjev, komponente vojaških in tajnih služb ter časopisne hiše kot ključni element strankarske aktivnosti v propagandi in ideološkem oblikovanju (Lazar, 2011, str. 312). Avtoritarna struktura stranke je vodila ostale delavske organizacije v boju za brezrazredno družbo. Principi delovanja njegove stranke, ki so se izražali v načinu organizacije, strategije in taktike, so postali temelji kasnejšega sovjetskega totalitarnega režima (Krupavičius, 2011, str. 315–316). Propaganda je bila uporabljena za hitrejše in lažje razširjanje komunističnih idej ter kot orodje pridobivanja novih članov stranke. Stranka je popolnoma prevzela državne aparate ter se institucionalizirala znotraj same države, tako da je država kot taka obstajala samo še navidezno, v resnici je bila vsa moč, nadzor in vodstvo v rokah stranke. Stalin si je na podlagi kulta osebnosti, ki ga je ustvaril znotraj komunistične stranke kot tudi Sovjetske zveze, sprva popolnoma podredil Sovjetsko komunistično stranko, kasneje pa tudi

Komunistično internacionalo, ki naj bi predstavljala komunistično stranko na mednarodni ravni in vključevala vse posamezne komunistične režime po svetu, v katerih si je želel vzpostaviti svojo avtoriteto ter neposredni nadzor in usmerjanje posameznih komunističnih strank.

3.1.2.2 Fašizem

Fašizem je oblika radikalnega avtoritarnega nacionalizma (Turner, 1975, str. 162), za katero je značilna diktatorska moč, prisilno zatiranje opozicije in nadzor nad industrijo ter trgovino (Larsen, Hagtvet in Myklebust, 1980, str. 424). Fašizem se pojavi v začetku 20. stoletja kot posledica prve svetovne vojne. Fašisti so ga videli kot revolucijo, ki bo prinesla spremembe na področju vojne, družbe, države in tehnologije. Pojavil se je pojem vojaško državljanstvo, ki izvira iz predpostavke, da so vsi državljani v času vojne na nek način vključeni v vojaške zadeve. Med vojno je prišlo do vzpona moči države. Ta je sposobna uspešno mobilizirati milijone ljudi, ki služijo v prvih vrstah na bojiščih in zagotavljajo gospodarsko proizvodnjo in logistiko v podporo vojaškemu stroju. Država pa ima tudi avtoriteto, s katero lahko neomejeno posega v življenje državljanov (Blamires, 2006, str. 140-41; Mann, 2004, str. 65).

Fašisti verjamejo, da je liberalna demokracija zastarela, in menijo, da je popolna mobilizacija družbe pod totalitarno enostrankarsko državo nujna za pripravo naroda na oborožen spopad in učinkovito odzivanje na gospodarske izzive. Takšno državo vodi mogočni vodja, tj. diktator in vlada, ki jo sestavljajo člani vladajoče fašistične stranke, da bi ustvarili nacionalno enotnost in ohranili stabilno in urejeno družbo (Horne, 2002, str. 237–239).

Lawrence Britt (2003) je na podlagi proučevanja fašističnih režimov v Nemčiji, Italiji, Španiji, Indoneziji in Latinski Ameriki izpostavil 14 lastnosti, ki so značilne za fašistično obliko vladavine in po katerih lahko določen režim uvrstimo v ta nedemokratični sistem:

- močan in kontinuiran nacionalizem. Fašistični režim vseskozi uporablja patriotske slogane, simbole, pesmi in druge oblike komuniciranja, prek katerih lahko izvaja nacionalistično propagando. Velik pomen imajo zastave, ki so eden glavnih simbolov in jih je v fašistični državi mogoče zaslediti na vsakem koraku;
- navidezno priznanje človekovih pravic. Zaradi strahu pred sovražniki in potrebe po varnosti so prebivalci pod fašističnim režimom prepričani, da so v določenih primerih njihove človekove pravice lahko prezrte. Ljudje do neke mere celo podpirajo mučenje, usmrtitve, atentate in dolge zaporne kazni;

- identifikacija sovražnika. Ljudi se združuje na podlagi ustvarjanja skupnega sovražnika. Ta je po navadi oblikovan na osnovi rase, etničnih ali verskih manjšin. Kot sovražnika se lahko predstavlja tudi druge nasprotne oblike političnega delovanja, npr. liberalce, komuniste, socialiste, teroriste …;
- nadvlada vojske. Ne glede na stanje v državi (finančno ali kakšno drugo) je za vojsko vedno dobro poskrbljeno in je na prioritetnem seznamu državnega financiranja, tudi na račun zanemarjanja drugih politik, ki se imajo z vidika oblasti za manj pomembne. Pripadniki oboroženih sil in vojaška služba so prikazani kot ugledni poklici, predvsem visoki častniki in uslužbenci imajo višji družbeni položaj;
- seksizem. Fašistična vlada je po navadi sestavljena izključno iz moških, ki zasedajo vse visoke funkcije in strokovne položaje. Tradicionalne vloge spolov so v takšnih režimih zelo rigidne in je iz vrednot, ki prevladujejo, predpostavljeno, kaj so naloge žensk in kaj moških. Ločitve, splav in homoseksualnost so zatirani in država ima vlogo glavnega varuha, ki bdi nad tradicionalnimi družinskimi vrednotami;
- nadzorovani množični mediji. Večina medijev je pod neposrednim nadzorom vlade, nekateri pa se nadzorujejo posredno z državnimi regulatorji in uredniki. Uporaba cenzure je zelo pogosta;
- nacionalna varnost. Strah se uporablja kot orodje, s katerim vlada opravičuje skrb za nacionalno varnost, da lahko nemoteno izvaja nadzor nad množico;
- prepletanje politike in religije. Vlade fašističnih režimov uporabljajo prevladujočo religijo kot orožje za manipulacijo javnega mnenja. Vodje pogosto uporabljajo in zlorabljajo religijsko retoriko in terminologijo, tudi v primerih, ko je v resnici versko stališče popolnoma nasprotno od političnega;
- korporativna moč. Industrijska in poslovna aristokracija fašističnega naroda je pogosto tista, ki osebam pomaga, da pridejo do oblasti, kar ustvarja vzajemno koristne odnose med podjetji in vlado ter elito moči;
- omejena moč delavcev. Grožnjo fašistični ureditvi predstavljajo organizirani delavci, zato so delavski sindikati prepovedani ali pa zelo močno omejeni;
- zapostavljanje intelektualcev in umetnikov. Fašistični režim spodbuja k odprti sovražnosti do visokega šolstva in akademskega sveta. Svobodno izražanje v umetnosti in znanosti je onemogočeno z izvajanjem cenzure;
- obsedenost z zločinom in kaznovanjem. V fašističnih režimih ima policija skoraj neomejena pooblastila za uveljavljanje zakonov. Ljudje so v imenu patriotizma

pogosto pripravljeni spregledati policijske zlorabe in celo opustiti določene državljanske svoboščine. Skoraj vedno v državi obstaja policija, ki ima neomejeno moč in je brez kakršnegakoli sodnega ali drugega nadzora;

- korupcija. Fašistični režimi skoraj vedno delujejo na principu kronizma, imenovanja na vladna mesta in funkcije na podlagi poznanstev in prijateljstva. Svoje moči, ki jih imajo kot visoki funkcionarji, izrabljajo za zaščito prijateljev pred odgovornostjo. Korupcija je močno prisotna na vseh ravneh delovanja države in uradnikov;
- prirejene volitve. Volitve v fašističnih režimih so skoraj vedno nadzorovane. Uporablja se onemogočanje opozicije, tudi z atentati vodilnih politikov, ter manipulacije volilnega sistema s spreminjanjem volilnih okrajev ali drugih prijemov, s katerimi se da odločujoče vplivati na potek volitev.

3.1.2.3 Nacizem

Nacizem je totalitarno gibanje Nacionalsocialistične nemške delavske stranke (NSDAP) pod vodstvom Adolfa Hitlerja. Nacionalsocializem je v svojem intenzivnem nacionalizmu, vsesplošni mobilizaciji in diktatorski vladavini zelo podoben italijanskemu fašizmu. Razlika med omenjenima režimoma je večja ekstremnost nacizma v svojih idejah in praksah. Svojo vladavino so izvajali in ohranjali skozi moč prisile in množične manipulacije. Nacizem se je neprestano širil skozi propagando v kulturnih in informacijskih medijih. Avro vsemogočnosti so prikazovali skozi organizacijo mitingov, vojaških uniform in simbolov. Propagandni stroj je deloval tudi na principu terorja države, ki ga je izvajala tajna policija in koncentracijska taborišča (*Encyclopedia Britannica*, 2002).

V nacizmu, ki v ospredje daje narod, so bile posameznikove potrebe podrejene družbenim (Birdsall, 2012, str. 31). Tako naj bi bila vsaka dejavnost in vsaka potreba posameznika urejena skozi kolektivnost, ki jo predstavlja stranka. S tem bi se izognili svobodnim področjem, v katerih posameznik pripada samemu sebi (Fest, 2013, str. 408). Legitimnost ustanovitve represivne policijske države, v kateri lahko varnostne sile samovoljno uveljavljajo oblast in zakone, se izraža prek prioritete nacionalne varnosti in vzdrževanja javnega reda pred potrebami in pravicami posameznika (Browder, 2004, str. 240).

Privlačnost nacističnega gibanja kot totalitarne ideologije (s pripadajočo mobilizacijo nemškega prebivalstva) je vzpostavljena v konstruktu pomoči družbi pri reševanju kognitivne disonance, ki je nastala zaradi tragičnega poraza nemške države v prvi svetovni vojni ter ekonomskega in materialnega trpljenja zaradi gospodarske krize. To je družbo, predvsem v

Nemčiji in tudi v drugih državah, pripeljalo do revolucionarnih nemirov. Namesto pluralnosti, ki je obstajala v parlamentarnih demokratičnih državah, je nacizem kot totalitarni sistem podal jasne in konkretne rešitve za zgodovinske probleme, s katerimi se je soočal nemški narod. Podporo je pridobil s spodbijanjem legitimnosti Weimarske republike in njene vlade ter zagotovil politično-biološko pot do boljše prihodnosti, brez negotovosti iz preteklosti naroda. S propagando je stranka razpršene in nezadovoljne množice usmerila v skupno smer in iz njih naredila ideološke privržence ter jih izkoristila, da so ji omogočili priti na oblast (Arendt, 1962, str. 340–389).

NSDAP se v Nemčiji pojavi okrog leta 1919 in od leta 1920 naprej je njen voditelj Adolf Hitler, ki s pomočjo manipulacij in izsiljevanja pride na oblast leta 1933. Z uporabo totalitarnih metod vladanja upravlja celotno državo vse do konca druge svetovne vojne in poraza nacistične Nemčije leta 1945. Po prihodu na oblast lahko nacionalsocializem razdelimo v dve obdobji, ki sta trajali približno enako dolgo. V letih od 1934 do 1939 je stranka vzpostavila popoln nadzor nad vsemi državnimi ustanovami in življenji prebivalcev v Nemčiji. Stranka in njene ideje so si pri prebivalstvu pridobile veliko podporo in večina prebivalstva je z določenim navdušenjem sprejemala novo oblast, ki se je izkazala kot močna, odločna in predvsem učinkovita. Na podporo stranke je v veliki meri vplivalo ekonomsko okrevanje po krizi in zmanjšanje nezaposlenosti na račun odpiranja novih državnih tovarn s poudarkom na vojaški industriji. Drugo obdobje pa je trajalo od 1938 do 1945, ko je nacistični režim poskušal razširiti svoj sistem vladanja in ga vzpostaviti na ozemljih drugih suverenih držav. Načrt je najprej predvideval združitev vseh ozemelj, kjer živi nemško govoreče prebivalstvo. Tako sta bili v prvi fazi bili priključeni Avstrija in Sudeti. Kasneje pa se je začel izvajati načrt, po katerem bi Nemčija pridobila svoj življenjski prostor (nem. *Lebensraum*) na vzhodu in tako vzpostavila samozadostno državo, ki bi si nadalje lahko pokorila Evropo in kasneje ves svet (*Encyclopedia Britannica,* 2002).

3.1.3 Demokracija

"Demokracija je skupek pravil in procesov, katerih glavne značilnosti so konkurenčne volitve, svoboda tiska, večstrankarstvo, pravica do peticij in zbiranja ter pravica do "*habeas corpus*"[2]"(Hislope in Mughan, 2012, str. 42). Politično organizirane skupine in aktivisti želijo

[2] Je pravica priprte osebe, da je pripeljana pred sodno vejo oblasti (sodnika), ki odloča o zakonitosti odvzema prostosti.

voditi državo ali pa vplivati na njeno politiko, politične stranke ciljajo na zmago na volitvah in s pridobljenimi položaji usmerjati politiko države; interesne skupine, lobiji in družbena gibanja iščejo svojo možnost utrditi ali spremeniti smer državnih politik (Hislope in Mughan, 2012, str. 6).

Na splošno razlikujemo dve vrsti demokratičnih režimov, to sta liberalna demokracija in elektoralna demokracija. V tem razlikovanju je pri liberalnih demokracijah zaznati več državljanskih svoboščin, močna in neodvisna sodna veja oblasti, horizontalna odgovornost izvoljenih funkcionarjev do drugih državnih organov in dobro delujoč državni aparat z minimalno korupcijo (Siaroff, 2011, str. 2234-2235).

Vzhodnoazijski komunitarizem, imenovan tudi avtoritarni komunitarizem, zagovarja načela, da je za ohranjanje družbenega reda in harmonije treba omejiti individualne pravice in politične svoboščine. Tako naj bi zahodne vrednote svoboščin pravzaprav privedle do družbene, politične in moralne anarhije. Pravne in politične pravice naj bi tako bile izrecno ideja zahodnih držav, ki jih uporabljajo za uvajanje njihove lastne vizije družbenega razvoja nad državami, ki imajo svoje, drugačne vrednote od zahodnih. Zagovarjajo načela, da je varnost skupna dobrina, ki pretehta individualne pravice, in zato podpirajo politike, ki na račun državljanskih svoboščin uresničujejo varnost države. Na drugi strani pa privrženci t. i. odgovornega (političnega) komunitarizma, ki se je oblikoval v 90. letih 20. stol v ZDA, zagovarjajo načela, da mora med varnostjo in pravicami biti določeno ravnotežje in da se mora to ravnotežje prilagajati spremembam, ki se dogajajo v družbi in mednarodnem okolju (Etzioni, 2011, str. 327–328). Omenjena teorija je postala bolj zanimiva po letu 2001, ko je prišlo do terorističnih napadov s strani do takrat zapostavljenega mednarodnega terorizma. Najprej se je zgodil napad v ZDA, kasneje še v evropskih državah. V tem času glavna nevarnost nacionalni varnosti tako postane transnacionalna grožnja mednarodnega terorizma. Potrebna je bila neposredna percepcija ogrožanja varnosti, da je na zakonodajni ravni prišlo do skoraj radikalnih sprememb v vedno ponavljajočem se ravnovesju med varnostjo in zasebnostjo kot prvino individualnih pravic posameznika.

Tako so teroristični napadi septembra 2001 v ZDA, marca 2004 v Madridu in julija 2005 v Londonu povzročili, da je največja grožnja varnosti postal mednarodni terorizem s svojo kompleksno strukturo, katerega vzroki izvirajo iz družbenih, kulturnih in verskih nazorov (Marotta in Nunzi, 2011, str. 2378). Sistemski protiukrepi so se najbolj spremenili v največjih zahodnih državah, ZDA, Franciji in Veliki Britaniji, ki so tako postavile model varnosti

države v 21. stoletju, ki ga skušajo posnemati ter implementirati tudi druge države, ki so neposredno ali posredno ogrožene s strani mednarodnega terorizma. Takšen model varnosti sloni na dejstvih, da je izvršilna veja oblasti bolj aktivna pri preprečevanju in manj omejena s sredstvi in instrumenti, ki se jih lahko poslužuje v boju proti terorizmu. Države so razširile svoje možnosti prisilnih sredstev in nadzora v zameno za omejitev državljanskih svoboščin in človekovih pravic, vse v imenu nacionalnovarnostnih imperativov. Francija se je za takšno politiko odločila že po letu 1986, ko se je v Parizu zgodil niz terorističnih napadov s strani terorističnih skupin z Bližnjega vzhoda. Napadi so v javnosti povzročili strah in prisilili oblast, da se odzove z novo, bolj zaostreno zakonodajo. Reforme, ki so se pojavile na področju sodstva, so prvostopenjskim sodnikom podelile moč soditi v zadevah, povezanih s terorizmom. Uvedli so specializirane preiskovalne sodnike za terorizem, ki so dobili precejšnja pooblastila pri zasliševanjih, preiskavah in obtožnicah ter za izdajanje nalogov za prisluškovanje, preiskave in sodne pozive. Francoska notranja obveščevalna služba DST (fr. *Direction du Surveillance Territorie*) je začela z nadzorom mošej in obsežnim prisluškovanjem imigrantom iz arabskih in severnoafriških skupnosti. Policija je dobila pooblastilo, da lahko osebo, ki je osumljena terorizma, pripre brez obtožbe za tri leta. Poleg vseh naštetih sprememb so se začeli zavzemati tudi za večjo asimilacijo imigrantov v francosko družbo. V ZDA pa so s sprejetjem zakona *Patriot Act* državni organi dobili pooblastila za prestrezanje komunikacij vseh državljanov. Osebam, osumljenim terorističnih dejanj, pa so odvzeli osnovno pravico "*habeas corpus*". "Ta določba je dolgo časa veljala kot ena temeljnih razlik med svobodno družbo in avtoritativnimi režimi" (Hislope in Mughan, 2012, str. 260). Zakonodajne spremembe so upoštevale tudi tehnološke inovacije in napredek informacijske tehnologije v zadnjih desetletjih, ki so prešle v vsesplošno uporabo. Tako je zakon o tujih obveščevalnih dejavnostih FISA iz leta 1978 določal, da je nalog, izdan za prisluškovanje določeni osebi, vezan na točno določen komunikacijski priključek oziroma napravo. V današnjem času pa ena oseba lahko uporablja več komunikacijskih naprav, zato je bilo v zakonu *Patriot Act* posledično spremenjeno to zakonsko določilo in nalog ni več vezan samo na posamezni priključek oziroma napravo, ampak na vse naprave, ki jih obravnavana oseba uporablja (Etzioni, 2011, str. 329).

Velika Britanija je podobne protiteroristične politike izvajala že v času boja z Irsko republikansko vojsko (IRA) v Severni Irski, kjer so v praski uporabljali določene podobne prijeme, npr. daljše pripore brez obtožnice in sodbe, omejevanje pravic osumljenih, uporabo fizičnega nasilja za pridobitev informacij in priznanj obdolženih. Po terorističnih napadih na

ZDA in kasneje tudi v Londonu pa so te pristope, ki so se prej izvajali samo na območju Severne Irske, razširili tudi na celotno ozemlje Velike Britanije. Organom kazenskega pregona je bilo odobreno povečanje njihove moči in dovoljenj v iskanju, dostopu in zbiranju medicinskih, finančnih, izobraževalnih in poslovnih podatkov (Hislope in Mughan, 2012, str. 257–261).

Etzioni (2011, str. 329) poudarja, da ne glede na to, za kakšne nove oblike varnostnega ogrožanja gre, se nekaterih ukrepov, ki ekstremno posegajo v individualne pravice, kot so mučenje, opustitev pravice do "*habeas corpus*" in množičnih pridržanj na podlagi rase, etničnosti in nacionalnosti, države ne bi smele posluževati. To so temeljne sestavine demokracije, ki jo ločijo od totalitarnih in avtoritarnih režimov.

Razprave o kršenju človekovih pravic in državljanskih svoboščin so v današnjem času močno prisotne. V času globalizacijskega 21. stol. niso na udaru zaradi kršenja osebnih pravic samo države, ampak se na to mesto vse bolj postavlja korporacije. Tako države prihajajo v vlogo zaščitnic človekovih pravic in državljanskih svoboščin, kar pa je zaradi moči korporacij vse težje. Ena pomembnejših tem so pravice posameznika do zasebnosti, ki se v informacijski dobi vse bolj izgublja. Vprašanje za prihodnost je, ali bodo države zaščitile svojega državljana pred vdorom v njihovo zasebnost pred korporacijami ali pa bodo izkoristile potencial informacijske tehnologije in ga uporabile za svoje cilje.

3.2 Socialna omrežja

Pri raziskovanju koncepta socialnih omrežij v velikem številu različnih definicij najdemo štiri skupne značilnosti, ki veljajo za današnja socialna omrežja (Obar in Wildman, 2015):

1. Socialna omrežja delujejo v spletu 2.0, kar pomeni, da uporabniki niso samo potrošniki, ki pridobivajo informacije na spletu, ampak so aktivni udeleženci, ki sooblikujejo informacije. Aplikacije so oblikovane tako, da uporabnikom omogočajo ustvarjanje, interakcijo, sodelovanje in deljenje ustvarjenih vsebin.
2. Vsebina, ki jo ustvarjajo uporabniki, je gonilna sila socialnih omrežij. Brez neposredne dejavnosti uporabnikov, ki se kaže z vpisovanjem osebnih podatkov, deljenjem videoposnetkov, komentiranjem, všečkanjem objav in uporabo drugih možnosti, ki jih omogočajo platforme, ne bi mogli govoriti o socialnih omrežjih.

3. Posamezniki na socialnih omrežjih ustvarjajo profile, prek katerih jih je mogoče identificirati. Storitve zahtevajo vnos določenih osebnih podatkov, ki platformi omogoča, da razlikuje med posameznimi uporabniki in tako lažje ustvarja socialne mreže.

4. Socialna omrežja ustvarjajo socialne mreže na spletu s povezovanjem posameznikov ali skupin. Uporabniki si tako sami ustvarjajo socialno mrežo, v kateri so drugi uporabniki, s katerimi želijo medsebojno komunicirati.

Socialna omrežja so aplikacije, ki omogočajo uporabnikom ustvariti osebne profile, s katerimi se povezujejo s prijatelji, da ti lahko spremljajo njihovo dejavnost ter medsebojno komunicirajo prek zasebnih sporočil. Osebni profili vključujejo različne informacije, ki jih uporabniki delijo z drugimi, kot so slike, videi, zvočni posnetki in blogi. Socialna omrežja ustvarjajo virtualni svet, v katerem uporabniki tako rekoč živijo svoje drugo življenje. V njem uporabniki po navadi bolj svobodno predstavljajo svoje življenje (Kaplan in Haenlein, 2010).

Poenostavljena definicija socialnih omrežij bi bila, da so to na internetu ustvarjene skupnosti, ki uporabnikom omogočajo medsebojno interakcijo na spletu. Njihova popularnost se je začela z uvedbo spleta 2.0, ki je omogočil, da se ustvarjajo bolj dinamične spletne platforme z večjo uporabniško interakcijo. Njihova uporabnost se je povečala s prihodom pametnih telefonov in tablic, ki omogočajo, da uporabniki ves čas dostopajo do socialnih omrežij (Tech Terms, 2013).

Delovanje in uporabo socialnih omrežij lahko predstavimo s t. i. okvirjem satovja (angl. *honeycomb framework*), ki je sestavljeno iz sedmih glavnih funkcionalnih blokov. Ti bloki predstavljajo potrebe angažiranja uporabnikov po uporabi socialnih omrežij. Tako je v primeru LinkedIn večji poudarek njegove uporabe na identiteti, ugledu in medsebojnih odnosih posameznega uporabnika, medtem ko recimo uporabniki YouTuba večji poudarek dajejo funkcijam skupnosti, pogovora, skupinam in ugledu. Bloki so gradniki, ki omogočajo razumeti, katere funkcije so pri socialnih omrežjih pomembne. Med seboj se ne izključujejo, prav tako ni potrebno, da je vseh sedem prisotnih v posameznem socialnem omrežju (Kietzmann, Hermkens, McCarthy in Silvestre, 2011):

1. Identiteta. Predstavlja obseg, v katerem uporabniki razkrijejo svojo identiteto na socialnih omrežjih. Vključuje lahko razkritje različnih osebnih podatkov, kot so ime, starost, spol, poklic, lokacija in informacije, ki prikazujejo uporabnika v določeni luči. Uporabniki prostovoljno delijo svojo identiteto na socialnih omrežjih, nekateri

uporabljajo svojo pravo identiteto, drugi si ustvarijo drugo identiteto, s katero so aktivni na različnih platformah. Da zaščitijo svojo zasebnost, navajajo različne podatke na različnih socialnih omrežjih, skladno z namenom, za katerega uporabljajo določeno platformo. Tako lahko pri istem uporabniku na Facebooku zasledimo drugačne osebne podatke kot pa na njegovem profilu na LinkedInu.

2. Pogovori. Predstavljajo komuniciranje uporabnikov z drugimi uporabniki na posameznih socialnih omrežjih. Mnoga socialna omrežja so v prvi vrsti namenjena ravno medsebojnemu komuniciranju med uporabniki in skupinami, ki se ustvarjajo in dogajajo iz različnih razlogov. Uporabniki objavljajo, pišejo komentarje in pošiljajo neposredna sporočila drugim uporabnikom, da bi spoznali nove podobno misleče uporabnike, našli svojega partnerja, gradili samospoštovanje ali da so vedno aktivno prisotni pri novih idejah in trendih, ki se pojavljajo v družbi. Drugi pa s pomočjo te tehnologije želijo biti slišani in prepoznani na različnih področjih, kot je zavzemanje za humanitarne aktivnosti, okolijska problematika, ekonomska vprašanja in politične razprave.
3. Skupna raba. Predstavlja dejavnik, v katerem uporabniki izmenjujejo, distribuirajo in sprejemajo vsebine, ki so lahko v obliki besedila, povezave do spletnih strani ali digitalne fotografije. Izmenjava informacij je pri socialnih omrežjih ključnega pomena, saj je razlog, zakaj so uporabniki aktivni na spletu, ravno medsebojno druženje. Že samo izmenjavanje informacij je način interakcije na socialnih omrežjih, vendar je cilj deljenja vsebin odvisen od funkcionalnega namena platforme – ali želijo uporabniki sodelovati v pogovorih in ustvarjati medsebojne odnose.
4. Prisotnost. Predstavlja dejavnik, ki uporabnikom omogoča, da izvedo, ali so drugi uporabniki dostopni, tako v virtualnem kot resničnem svetu, na podlagi informacij, kje se nahajajo in ali so na voljo. Nekatera socialna omrežja imajo vgrajene funkcije, ki prikazujejo, ali je uporabnik ta trenutek prisoten na omenjeni platformi.
5. Razmerja. Predstavlja način, kako so lahko uporabniki medsebojno povezani na socialnem omrežju. Dva ali več uporabnikov imajo določeno obliko združevanja, ki vodi interakcije, kot so pogovor, deljenje vsebin iz skupnih zanimanj, pošiljanje besedil in neposrednih sporočil, srečevanje v resničnem življenju, ali pa so preprosto samo označeni kot prijatelji ali navdušenci.
6. Ugled. Na socialnih omrežjih ugled lahko pomeni več stvari in vsako omrežje ima zanj svoj način merjenja. Npr. ugled na Twitterju se lahko meri na podlagi števila deljenja posamezne objave. V LinkedInu se ugled ustvarja na podlagi potrditev (angl.

endorsements) znanj, ki jih ima posameznik navedena v svojem profilu. Na Facebooku se ugled najpogosteje kaže v številu všečkov.[3] Ugled na YouTubu se meri na podlagi števila ogledov ali ocene določenega videa.

7. Skupine. Predstavljajo skupnosti, ki jih sestavljajo uporabniki, ki so del določene skupine. Na podlagi teorije Robina Dunbarja je posameznik zmožen imeti stabilne družbene odnose z največ 150 posamezniki. Socialna omrežja pa znatno presegajo to število. Obstajata dve večji razlikovanji skupin v okviru socialnih omrežij. Prva so seznami, po katerih so razdeljeni posamezniki, npr. sorodniki, prijatelji, sodelavci …, druga skupina pa so skupine, ki so lahko odprte za vsakogar ali pa zaprte in so dostopne samo določenim uporabnikom. Facebook tako razlikuje tri vrste skupin: odprte, zaprte in skrite.

Socialna omrežja ponujajo bogate vire podatkov o naturalističnem vedenju. Iz profila uporabnikov in drugih, z njim povezanih razmerij, se lahko pridobivajo in zbirajo velike količine podatkov, in sicer s pomočjo tehnik samostojnega zbiranja in prek podatkovnih nizov, ki jih neposredno priskrbi podjetje. Ti zbrani podatki omogočajo raziskovalcem izvajanje omrežnih analiz, s katerimi lahko raziščejo vzorce prijateljstva, namene uporabe in druge kazalnike (Boyd in Ellison, 2007). Podjetja pri svojem delovanja in načrtovanju marketinške strategije vedno bolj uporabljajo orodja za spremljanje socialnih omrežij, prek katerih lahko spremljajo, sledijo in analizirajo spletne pogovore o njihovi blagovni znamki, izdelkih ali storitvah, ki jih ponujajo. Podjetja si na tak način pomagajo pri oglaševanju svojih izdelkov in storitev, omogoča pa jim tudi merjenje donosnosti naložb, ki jih usmerjajo v oglaševanje na socialnih omrežjih.

Izraz platforma predstavlja dvignjeno konstrukcijo na nekem prizorišču, kot je na primer oder ali govorniški pult. V digitalnem svetu pa je izraz prenesen v možnost, da vsaj udeleženec izrazi prepričanje in predstavi sebe. Torej si lahko socialna omrežja predstavljamo kot platforme, kjer se lahko vsi posamezniki, ki sodelujejo na določeni platformi, javno izražajo in komunicirajo z drugimi. V teoriji te platforme predstavljajo tehnologijo nevtralnosti in dereguliranosti, kjer je omogočena popolna svoboda govora in izražanje, vendar je v praksi regulirana tako s strani države kot ponudnikov storitev samih. Tako je tudi javna uporaba

[3] Všeček – označitev, da kaj na spletu, zlasti v družabnih omrežjih trenutno ugaja, je všečno (*Sprotni slovar slovenskega jezika*, 2017).

socialnih omrežij za politični diskurz strukturirana na komercialnih imperativih, ki stojijo za to stranjo (Leurs, 2014, str. 972).

Socialna omrežja lajšajo vključevanje v družbeno in politično participacijo, saj posameznik ni več geografsko omejen in lahko prejme informacije z drugega dela sveta ter se tako zavzame za določeno stvar, česar v resničnem življenju zaradi oddaljenosti brez informacijske tehnologije ne bi mogel. Določena socialna omrežja, kot je npr. Twitter, omogočajo vključevanje v družbena gibanja in sodelovanje pri družbenih aktivizmih brez nepotrebnega razkrivanja resnične identitete, kot se razkrije pri neposrednem udejstvovanju na protestih ali zborovanjih (Tindall, 2014, str. 3). Socialna omrežja se pojavljajo kot mehanizem za uporabo protestov in uporov, ki lahko imajo daljnosežne posledice na področju družbenih in političnih reform. Facebook, Twitter in YouTube so se že izkazali kot orodje, ki je bilo uporabljeno za organiziranje in informiranje ljudi, predvsem v avtoritarnih državah. Najbolj nazoren primer je zagotovo Arabska pomlad, ki se je začela leta 2011 v Tuniziji. Predvsem v Egiptu so socialna omrežja pomagala pri mobilizaciji ljudi na proteste in širjenje informacij v svet (Botes, 2014, str. 308–310).

Politična in družbena participacija na internetu oziroma socialnih omrežjih se deli na štiri tipe. Prvi tip predstavlja participacijo, kjer socialna omrežja služijo kot vir informacij o določenem gibanju in organizaciji. Drugi tip je uporaba socialnih omrežij za podporo protestom in shodom v resničnem življenju. Pri tem gre za širjenje informacij, novačenje udeležencev, omogočanje logistične podpore. Internet tako ne predstavlja neodvisnega prostora aktivizma, ampak prostor, kjer se dogaja organizacija in koordinacija dogodka. Tretji tip predstavlja aktivizem na področju peticij, bojkotov, protestnih pisem in kampanj prek elektronske pošte. Četrti tip pa zajema organizacijo celotnih kampanj in gibanj, ki se izvajajo izključno na svetovnem spletu in jih imenujemo e-gibanja. Glavna značilnost teh gibanj je, da se ne dogajajo in niso aktivna v resničnem življenju, ampak samo na internetu (Tindall, 2014, str. 4).

Množična uporaba socialnih omrežij se ne izraža samo v uporabnosti storitev za komuniciranje, ampak tudi v tem, da so ti produkti brezplačni. Seveda se ta brezplačnost odraža v profitu ponudnikov, ki se ustvarja z zbiranjem in nadaljnjo uporabo podatkov njihovih uporabnikov, kar vodi arhitekturo in politike svetovnega spleta primarno v služenje iz zasebnih interesov, ne pa javne sfere (Leurs, 2014, str. 973).

Oglaševanje je osrednji mehanizem, prek katerega platforme socialnih omrežij izvajajo nadzor nad uporabniki. Osebni podatki o uporabnikih teh platform se zbirajo v zameno za dostop do njihovih komercialnih strani in storitev skladno s pogoji uporabe, s katerimi uporabniki soglašajo ob registraciji svojega uporabniškega računa. Posameznikovo obnašanje na spletu, kot so obiski strani, zgodovina iskanja in druge dejavnosti, so tudi nadzorovane in vključene v behavioristično oglaševanje, kjer se išče in želi napovedati prihodnost potrošniškega obnašanja na vzorcih posameznega uporabnika. Večina uporabnikov se ne zaveda dejstva, da njihova dejavnost na platformah ustvarja vrednost podjetij, ki upravljajo s platformo. Politične posledice se odražajo v državni penetraciji obveščevalnih praks v arhitekturo socialnih omrežij, saj se podobne funkcije, ki se uporabljajo za izkoriščanje ciljnega oglaševanja lahko uporabljajo v politične namene, kot je primer Arabske pomladi, kjer so organizatorje demonstracij in manifestacij identificirali na podlagi njihove dejavnosti na platformah socialnih omrežij. Navzven socialna omrežja predstavljajo platformo, kjer imajo vsi uporabniki enake možnosti udeležbe v javnih debatah prek nevtralnih komunikacijskih infrastruktur (Leurs, 2014, str. 973).

4 TEORETIČNI MODEL POLICIJSKE DRŽAVE

4.1 Tajne službe

"Ne glede na vrsto režima ali vlade, ki je na oblasti, vsi uporabljajo birokracijo, policijo, obveščevalne službe, oborožene sile in sodni sistem za pomoč pri upravljanju družbenih konfliktov in ohranjanju domačega reda" (Hislope in Mughan, 2012, str. 40). Širši pojem policije se nanaša na vse ukrepe v notranjih zadevah države, prek katerih se vzpostavlja in vzdržuje blaginja v državi. V ožjem smislu pa se pojem navezuje na vse zadeve, ki so potrebne za ustrezno stanje civilnega življenja, še zlasti za vzdrževanje reda in discipline med subjekti (Maier, 1997, str. 110). Sherman Kent (1966) je definiral tri dimenzije obveščevalnih služb: (1) te službe so organizacije, (2) izvajajo dejavnosti in (3) proizvajajo znanje.

Naloga tajnih služb je tajno zbiranje podatkov. Specializirane so za delovanje na dveh področjih, to sta obveščevalna in protiobveščevalna dejavnost. Tretja dejavnost, ki jo tajne službe tudi opravljajo, pa je izvajanje prikritih akcij. V večini držav so za te naloge zadolžene obveščevalne službe. Zaradi svoje vloge, ki so jo dobile po letu 2001, te niso več samo ena od manj pomembnih državnih služb in politik, kar se tiče državotvornosti, ampak so prevzele primat pri zagotavljanju nacionalne varnosti, ki postaja vse pomembnejša. Povečalo se je njihovo delovanje, tako kadri kot sredstva in posledično proračun. To pa je eden od razlogov, zakaj so demokratične države poostrile nadzor nad svojimi obveščevalnimi službami in odgovornostjo uradnih oseb (Laurent, 2011, str. 2369–2370).

Tajna policija je državna organizacija, ki deluje v tajnosti za dosego političnih ciljev svoje vladajoče elite in pri svojem delu uporablja metode, s katerimi se zavestno krši državljanske in druge pravice prebivalcev. Uveljavljanje zakonov je skoraj v vseh družbah zahtevalo določen del tajnosti, zlasti ko gre za preiskovanje kaznivih dejanj in ugotavljanje zadev, ki so pogosto označene kot zarote. Zgodovinsko gledano, imajo tajne organizacije, ustvarjene s strani vladajoče entitete, ki skrbijo tako za notranjo kot zunanjo varnost, daljšo zgodovino kot pa uniformirane policijske enote, kot jih po večini poznamo v današnjem času. Širši izraz termina tajna policija zajema vse pripadnike policijskih organizacij, ki pri svojem delu ne uporabljajo uniform ali drugih identifikacijskih oznak, poslužujejo pa se tajnih metod, ki osumljencu onemogočajo seznanitve z dejstvom, da je tarča obravnave. Nekatere države imajo takšno delovanje omejeno z zakoni, ki delovanje tajnih policij omejujejo samo na

določene postopke v preiskavi, kot je na primer zbiranje dokazov, s katerimi pa je osumljeni ali obtoženec seznanjen na javnem sojenju in ima njegova obramba popoln dostop do vseh zbranih dokazov proti njemu (*The Columbia Encyclopedia,* 2017).

Tajna policija je v večini primerov samostojna organizacija, ki je neposredno podrejena izvršilni veji oblasti in je nadrejena drugim organizacijam, ki skrbijo za varnost države. Takšne organizacije raziskujejo, ugotavljajo in izvajajo aretacije osumljencev, velikokrat pa tudi same ocenjujejo, ali je osumljenec dejansko kriv nečesa ali ne. V skrajnih primerih ima takšna tajna policija lahko tudi lastna sodišča in zapore, njihove dejavnosti pa se ne prikriva samo pred prebivalstvom, ampak tudi pred lastnimi zakonodajnimi, sodnimi in izvršilnimi organi države, razen na najvišji upravnih nivojih države (*The Columbia Encyclopedia*, 2017).

Dejavnosti tajnih služb, katerih cilj je vladi zagotavljati obveščevalne podatke tako na taktični, še bolj pa na strateški ravni, jim dajejo posebno moč v odnosu do državne uprave. Kljub napredku na področju državljanskih svoboščin in transparentnosti ta del državnega aparata še vedno ostaja skrit pred javnostjo. Na tem področju ima država večjo avtonomnost nad izvajanjem svojih politik in teoretično večjo moč. Zato so obveščevalne službe najpomembnejši del države, kar bi lahko bila t. i. tajna država oz. policijska država (Laurent, 2011, str. 2370).

Država je sama podvržena upoštevanju zakonov in implementacij nevtralnih politik, če govorimo o državah, ki delujejo po sistemu demokratičnega režima. Obstoj tajnih služb in njihove neposredne povezave z vladajočo politično oblastjo pa lahko nakazujejo, da nekateri deli uprave niso neodvisna orodja visokih odločevalcev, ampak so podvrženi točno določeni politiki. Tajne službe so tako del državne uprave, vendar so zelo blizu politične oblasti. Občutljive zadeve, s katerimi se ukvarjajo, službe spreminjajo v vlogo svetovalcev in *think tankov*. To pomeni, da lahko tajne službe izdelajo politične agende ali pa vplivajo na že obstoječe. Tajne službe se lahko uporabljajo kot orodje politične avtoritete, ko gre za izvajanje nacionalne varnosti, tako domače kot mednarodne. Tako je politizacija tajnih služb pogost pojav tudi v demokratičnih državah (Laurent, 2011, str. 2370–2371). V demokratičnih državah je eden pomembnejših dejavnikov v okviru obveščevalnih služb izvajanje nadzora in odgovornosti nad njimi z namenom varovanja in preprečevanja zlorabljanja njihovega delovanja (Johnson, 2011, str. 1213).

Tehnične rešitve zagotavljanja varnosti skozi izvajanje nadzora prevladujejo v politikah in razpravah o zagotavljanju varnosti (Forsberg, 2011, str. 2376). Varnostne in obrambne

politike so tradicionalno obkrožene z zaprtimi sistemi, prek katerih delujejo obveščevalne službe z zbiranjem informacij, ob odsotnosti demokracije in parlamentarnega nadzora. Vendar pa veliko držav svoje doktrine varnosti in obrambe objavi v t. i. beli knjigi ali drugih uradnih dokumentih, ki vladi omogočajo legitimnost in transparentnost izvajanja zastavljenih politik (Forsberg, 2011, str. 2376).

4.2 Nadzor

Množični nadzor v širšem razumevanju predstavlja podreditev populacije ali dela populacije vsesplošnemu nadzoru njihovega življenja. Gre za sistematičen poseg v pravico ljudi do zasebnosti. Vsak sistem, ki ustvarja in zbira podatke o posameznikih, ne da bi poskušal omejiti nabor podatkov na natančno določene posameznike, je oblika množičnega nadzora. V skladu z metodami, ki jih je mogoče uporabiti za množični nadzor, lahko vlade zajamejo praktično vse pore življenja. Danes se vse bolj uporablja nastajanje, zbiranje in obdelava informacij o velikem številu ljudi, pogosto brez kakršnegakoli pravnega obstoja suma kršitve zakonov. Zdi se, da množični nadzor v zadnjem času narašča sorazmerno s hitrim napredkom tehnoloških sprememb, vendar pa obstaja veliko primerov še iz časov pred informacijsko družbo, v katerih že lahko zasledimo zametke množičnega nadzora (Privacy International, 2017).

Nadzora so se v preteklosti po večini posluževale države oziroma vlade posameznih držav, v času informacijskega razvoja pa so se v to vlogo vključile tudi korporacije, ki nadzor izvajajo za svoje cilje ali pa nastopajo kot posredniki oziroma zunanji izvajalci za državo.

Politiki takšno početje opravičujejo in legitimirajo s tem, da je zbiranje informacij z množičnim nadzorom nujno potrebno za boj proti terorizmu, zaščito nacionalne varnosti in preprečevanje drugih kaznivih dejanj, med katerimi je na internetu najpogostejša otroška pornografija. Nasprotniki pa takšni politiki očitajo, da z izvajanjem množičnega nadzora kršijo pravico do zasebnosti, omejujejo državljanske pravice in politične svoboščine. Vsesplošna uporaba množičnega nadzora lahko vodi do spremembe sistemskega delovanja države, kar lahko privede do nadzorstvene države, ki jo iz zgodovine poznamo pod imenom policijska država.

Eden od načinov nadzora je tudi cenzura, ki jo izvajajo državni organi z namenom omejiti obtok določenih informacij, idej in slik ali političnih, kulturnih, religijskih mnenj, ki so v

nasprotju z doktrino trenutne vlade, saj bi ji lahko zmanjšali moč ali škodili na kakšen drugačen način. Cenzura je prisotna predvsem v nedemokratičnih sistemih, srečujemo pa jo tudi v demokratičnih sistemih, predvsem v t. i. mladih demokracijah, ki so se šele pred kratkim izoblikovale iz nedemokratičnih oblik vladavine. Te naj se ne bi utegnile otresti načinov nadzora nad mediji in še vedno menijo, da je cenzura v določenih primerih potrebna za zaščito nacionalne varnosti. Po navadi ima država točno določen organ oziroma uradne osebe, ki skrbijo za spremljanje in širjenje idej, ki bi bile v nasprotju z vladajočo politiko. Pojem cenzura je na splošno v nasprotju z demokracijo, ki je označena z institucionalizacijo državljanskih in političnih pravic, državljanskih svoboščin in obstojem opozicije. Čeprav je svobodno izražanje osrednja demokratična vrednota, nekateri nasprotniki cenzure dopuščajo izjeme, predvsem v primerih, ko gre za otroško pornografijo. Zagovorniki cenzure pa v takih primerih zagovarjajo stališče, da je pravica do svobodnega izražanja izničena s potrebo po preprečevanju izredno škodljivega vpliva na otroke, ki se odraža v ustvarjanju in razširjanju otroške pornografije. Druga izjema, kjer naj bi se dopuščala določena stopnja cenzure, je sovražni govor, saj naj bi ta spodbujal dejansko nasilje in morebitna škoda zaradi tega nasilja znova odtehta vrednost svobode govora (Huneeus, 2011, str. 213).

Z razvojem moderne tehnologije, še posebej interneta, je uvedba cenzure postala težja, kar povzroča težave uradnim osebam pri uveljavljanju cenzure nad informacijami, ki so v nasprotju z vladajočo elito. Internet je prinesel nov kanal komuniciranja med posamezniki v državah, kjer je cenzura vseprisotna, npr. v Ljudski republiki Kitajski v komunikaciji z ostalim svetom, predvsem zahodnimi državami, da lahko uporabniki izpostavijo probleme, s katerimi se spopadajo v svojih državah. Pomembno vlogo igra cenzura predvsem v avtokratskih režimih, kjer se uporablja kot orodje za zagotavljanje omejevanja pluralnosti, kar je eden od temeljev te oblike vladavine. Z njo si pomagajo pri zagotavljanju politične moči in vpliva, poleg tega pa omejujejo dostop do določenih pomembnih informacij (Huneeus, 2011, str. 214).

Nadzor lahko razumemo na dva načina: (1) država spremlja posameznika, v našem primeru je to njegovo aktivnost na internetu oziroma socialnih omrežjih. S tem lahko pride do podatkov, v kakšni družbi se oseba zadržuje, s čim se rada ukvarja, katere stvari so ji všeč in kakšne nazore, tako politične kot druge ima; (2) nadzor lahko razumemo tudi kot dejanje propagande in cenzure. Socialni medij omogoča velik potencial za izvajanje propagande, saj se informacije hitro širijo, poleg tega, pa kot lahko opazimo, države lahko s sprejetimi zakoni uvedejo določeno cenzuro na socialnih omrežjih. Zdajšnja praksa kaže, da se cenzura

uporablja za preprečevanje širjenja sovražnega govora in ekstremizma, kot eden od ukrepov boja s terorizmom oziroma preprečevanja radikalizacije. Kljub temu pa ti primeri nazorno kažejo, kakšno moč imajo države glede tega, kaj se lahko objavlja na socialnih omrežjih in kaj ne. To pa bi lahko v prihodnje izkoristile tudi za druge namene, npr. za politično cenzuro.

4.3 Policijska država

Policijska država je izraz za sistem, v katerem vlada samovoljno uporablja policijo za izvajanje svoje oblasti. V takšni državi se prebivalstvo sooča z omejevanjem državljanskih pravic in svoboščin, onemogočeno je prosto gibanje po vsej državi, izražanje mnenj in politično prepričanje je pogosto nadzorovano s strani policije, ki vsako neskladje z mišljenjem oblasti in njihovimi politikami kaznuje. Za takšno državo je značilna tajna policija, ki deluje zunaj ustavnih in zakonskih okvirov.

Institucija tajne policije je obstajala v večini družb, v katerih si je manjšina morala zagotoviti obstoj in moč nad večino. V času antične Grčije je v špartanski državi delovala dobro organizirana tajna policija, ki je nadzorovala helote in brezobzirno zatirala vse znake upora. V antičnem Rimu, zlati v obdobju vladanja Julijanskih cesarjev, je v državi delovala skupina profesionalnih tajnih obveščevalcev, ki so izdajali t. i. državne sovražnike, za plačilo pa so dobili del zaseženega premoženja. Z razvojem moderne države pa se je dejavnost tajne policije institucionalizirala in se začela posluževati tehničnih napredkov človeštva. Tako je njihovo delovanje prišlo najbolj do izraza v 20. stoletju, predvsem v nedemokratičnih državah, kot sta Sovjetska zveza in Nemčija (*The Columbia Encyclopedia,* 2017).

Različne oblike policijskih držav lahko zasledimo skozi zgodovino, kjer je vladajoča elita uporabljala svojo moč, da si je podrejala prebivalstvo. Vsak takšen primer se razlikuje od države do države in posameznega obdobja. Najbolj znane zgodovinske policijske države so Sovjetska zveza, nacistična Nemčija in Nemška demokratična republika. Ti trije primeri so tudi bolj natančno predstavljeni. Dodan je še primer oblike policijske države v demokratični državi. Med drugimi zloglasnimi primeri so še Južnoafriška republika v času izvajanja apartheida, Čile pod diktaturo Augusta Pinocheta, Kuba pod vodstvom Fulgencia Batiste in Fidela Castra ter Severna Koreja pod vladavino družine Kim.

4.3.1 Nacistična Nemčija

Gestapo (nem. *Geheime Staatspolizei*) je bila organizacija tajne policije v času nacistične Nemčije, ki je bila ustanovljena na podlagi pruske tajne policije leta 1933 in je delovala vse do nemške kapitulacije 1945 na ozemlju Nemčije in njenih okupacijskih območjih. Gestapo je imel pooblastila za preiskovanje primerov izdaje, vohunjenja, sabotaže in kriminalnih napadov na nacistično stranko in Nemčijo. Vlada je leta 1936 sprejela zakon, ki je gestapu omogočil delovanje zunaj sodnega nadzora ter ga tako v praksi in teoriji postavil nad sam zakon (Dams in Stolle, 2014, str. 17). Organizacija je bila posebej izvzeta iz odgovornosti na upravnem sodišču, kjer državljani lahko sprožijo tožbo proti državi, če so bile v skladu z veljavnimi zakoni kršene njihove pravice. Prav tako je že leta 1935 upravno sodišče odločilo, da dejavnosti, ki jih izvaja gestapo, niso predmet sodnega nadzora (McNab, 2009, str. 156). Moč gestapa se je odražala tudi v uporabi t. i. varnega pridržanja (nem. *Schutzhaft*), evfemizma moči zapreti ljudi brez sodnega postopka (United States Holocaust Memorial Museum, 2017). Nenavadnost sistema je bila, da je osumljeni moral podpisati dokument, v katerem je zahteval lastno zaporno kazen iz strahu pred samopoškodbo. Poleg tega je na tisoče zapornikov po vsej Nemčiji in zasedenih ozemljih preprosto izginilo, medtem ko so bili v zaporih gestapa (Snyder, 1994, str. 242).

Gellately (1992) v svoji študiji delovanja gestapovih uradov ugotavlja, da je bila organizacija pretežno sestavljena iz birokratov in uradnikov, ki so bili povsem odvisni od poročanja in posredovanja informacij s strani državljanov. Trdi, da je zaradi široke pripravljenosti in angažiranja nemških državljanov, da vohunijo drug za drugim in posredujejo informacije gestapu, bila Nemčija v času od leta 1933 do 1945 odličen primer panopticizma. Gestapo se je tako spremenil v t. i. reaktivno organizacijo, ki se je vzpostavila in delovala znotraj nemške družbe, njeno delovanje pa je bilo strukturno odvisno od stalnega sodelovanja nemških državljanov. V določenih obdobjih je bil gestapo preobremenjen z informacijami in obtožbami, ki so jih posredovali državljani, in je bilo večino časa porabljenega za verifikacijo verodostojnosti obtožb. Količina informacij in obtožb je obremenjevala lokalne urade, saj so imeli premalo zaposlenih in preveč dela pri preiskovanju (Rees, 1997, str. 65).

Običajne metode preiskovanja so vključevale različne oblike izsiljevanja in groženj za pridobitev priznanja osumljene osebe. Poleg tega so se uporabljale še metode fizičnega in psihičnega mučenja, kot so pomanjkanje spanca in različne oblike nadlegovanja. Mučenje in podtikanje dokazov je bil modus operandi reševanja primerov, še posebej ko se je

obravnavana zadeva nanašala na Jude (Gellately 1992, str. 131–132). Izvajanje nasilnih metod med zasliševanjem so pogosto privedlo do resničnih in neresničnih priznanj in obtožb, kar je gestapu omogočilo, da je odkril številne odporniške mreže. Posledično pa je v javnosti prevladovalo mnenje, da gestapo ve vse in lahko stori karkoli, in to brez kakršnihkoli zakonskih omejitev ali posledic (Ayçoberry, 1999, str. 272). Kot trdi Johnson (1999, str. 483–485), so nacisti izvajali selektivni teror s poudarkom na političnih nasprotnikih, ideološko-religijskih organizacijah, kriminalcih, romskem prebivalstvu, invalidih, homoseksualcih in predvsem Judih. S selektivnim terorjem se strinja tudi Evans (2006, str. 114), ki trdi, da sta se nasilje in zastraševanje redko dotaknila življenja navadnih nemških državljanov. Ovajanje prebivalcev med seboj je bila prej izjema kot pravilo, kar se tiče obnašanja velike večine Nemcev. Učinkovitost gestapa je ležala v zmožnosti prikazovanja vsemogočnosti organizacije, ki je bila odvisna od sodelovanja prebivalstva in njihovih ovajanj, kar je spremenila v svojo korist za prikazovanje sebe kot močne, brezobzirne in učinkovite institucije terorja pod nacističnim režimom, ki je dajala vtis, da je prisotna vsepovsod, v vsakem delu posameznikovega življenja (Delarue, 2008, str. 83–140). Prava učinkovitost gestapa, ki je bil podprt s sodelovanjem prebivalcev, je bila bolj rezultat usklajevanja in sodelovanja med različnimi policijskimi organi v Nemčiji, SS (nem. *Schutzstaffel*) in različnimi organizacijami, ki so spadale pod NSDAP, kar se je odražalo v organiziranem delovanju varnostno-obveščevalnega dela policijske države (Dams in Stolle, 2014, str. 82).

V okviru SS je delovala obveščevalna služba SD (nem. *Sicherheitsdienst*), ki je veljala za prvo nacistično obveščevalno agencijo in je tesno sodelovala z gestapom. Prvi direktor Reinhard Heydrich je želel SD povzdigniti na raven, kjer bi bil vsak posameznik na območjih tretjega rajha pod stalnim nadzorom agencije. SD je bila predvsem agencija za pridobivanje in zbiranje informacij, gestapo pa je bil izvršilna agencija tega sistema politične policije. (Buchheim, 1968, str. 166–176). Zadolženi so bili za odkrivanje dejanskih in potencialnih sovražnikov nacističnega vodstva in za nevtralizacijo te opozicije, kar se je pokazalo v obračunu s SA. SD je za izvajanje svojih nalog ustvaril mrežo agentov in tajnih sodelavcev na območju rajha in okupiranih ozemljih v želji po vzpostavitvi totalitarnega režima na teh območjih (Bracher, 1970, str. 350–362). Poleg obveščevalnih operacij je SD spremljala mnenja iz tujine in kritike nacističnega režima ter po potrebi cenzurirala informacije in objavljala sovražno propagando proti drugim državam (Koonz, 2005, str. 238). Tako SD kot gestapo sta opravljala naloge spremljanja morale nemškega naroda in ob morebitnih odstopanjih od želenih rezultatov sta obe organizaciji imeli na razpolago vsa sredstva, da

odpravita te odklone (Wall, 1997, str. 183–187). Pripravljali so redna poročila sestavljena iz raziskav javnega mnenja, medijskih objav in informativnih biltenov in jih v tajnih dokumentih pošiljali do vrhovnih funkcionarjev nacistične stranke, ki so režimu omogočali, da ocenjuje splošno moralo in odnos nemškega naroda ter temu primerno uporabi propagandi stroj za manipuliranje s prebivalstvom (Ingrao, 2013, str. 107–116).

4.3.2 Nemška demokratična republika in Stasi

V času hladne vojne je v Nemški demokratični republiki (dalje NDR) delovalo ministrstvo za državno varnost (nem. *Ministerium für Staatssicherheit*), v javnosti bolj znano pod imenom Stasi, ki po nekaterih navedbah še vedno velja za eno najbolj učinkovitih in represivnih tajnih policij, ki so obstajale v zgodovini. Ena glavnih nalog, ki jo je agencija izvajala, je bilo vohuniti za prebivalstvom, predvsem z uporabo razširjene mreže tajnih sodelavcev med prebivalstvom. Stasi je bil zadolžen za onemogočanje opozicije in se je lahko posluževal prikritih metod delovanja, med drugimi tudi psihološkega nasilja. Ob koncu delovanja agencije leta 1989 je bilo v njej zaposlenih 91.015 ljudi, poleg tega pa je še 173.081 tajnih sodelavcev v NDR in 1553 v Zahodni Nemčiji. Današnja agencija, zadolžena za arhive Stasija, ocenjuje, da je bilo vseh skupaj 500.000 ljudi, ki so na takšen ali drugačen način posredovali informacije Stasiju. Nekdanji Stasijev polkovnik, ki je bil zaposlen v protiobveščevalnem direktoratu, ocenjuje, da bi bilo število sodelavcev lahko tudi dva milijona, če se upoštevajo tudi občasni sodelavci (Koehler, 2000, str. 8–9).

Stasi je svoje tarče nadzoroval 24 ur na dan, beležil je vsako njihovo početje in vsak njihov obisk. Stanovanja so opremljali s snemalnimi napravami, tako avdio kot video, da so imeli popoln nadzor nad dogajanjem v določenem stanovanju (Koehler, 2000, str. 9). Stasi je imel izdelane posebne kategorizacije vrst tajnih sodelavcev in izdelane natančne postopke, kako od njih pridobiti informacije in jih nadzirati, da so delali po njihovih navodilih (Fullbrook, 2005, str. 228). Stasi se je infiltriral v vse vidike družbenega življenja v Vzhodni Nemčiji. Približno eden od 63 prebivalcev je na določen način kolaboriral z njimi. Tako naj bi Stasi vzdrževal najobsežnejši nadzor nad svojimi prebivalci med tajnimi policijami v zgodovini moderne države (Rosenberg, 2007). Gledano na število prebivalstva v Vzhodni Nemčiji, je statistično en zaposleni na Stasiju nadziral 166 posameznikov. Če se upoštevajo še tajni sodelavci, je imela država z eno osebo potencialno nadzor nad 6,5 prebivalca. Za primerjavo: v obdobju nacistične Nemčije je imel gestapo z enim zaposlenim nadzor nad 2000 prebivalci (Koehler, 2000).

Ena bolj okrutnih metod, ki se je je pri svojem delu posluževal Stasi, je bila t. i. razgradnja (nem. *Zersetzung*). Gre za kompleksno metodo nadzora in psihološkega manipuliranja s tarčo. Natančno poznavanje in proučevanje osebe in njegovih ranljivih lastnosti se uporablja za uničevanje njegove podobe v javnosti, kar posledično vpliva na mentalno in fizično zdravje posameznika, ki naj bi zaradi teh razlogov izgubil voljo po delovanju in izvajanju dejavnosti in aktivnosti proti državi in obstoječemu režimu. Taktike te metode med drugim vključujejo tudi prikrit vstop v ciljno stanovanje, v katerem se z namenom spremeni določeno stvar. Primer je premikanje pohištva, zamenjava predmetov s podobnimi, dostava stvari, ki jih niso naročili, prekinjeni telefonski klici v nočnem času in podobne stvari. Te zadeve so podzavestno delovale na mentalno zdravje posameznikov, veliko jih je doživelo živčni zlom ali podobne psihološke bolezni. Zelo podobne metode je uporabljal kasneje tudi FSB, ki jih je izvajal predvsem nad diplomatskim osebjem ZDA in političnimi nasprotniki. Predvsem na diplomate so imele te tehnike velik vpliv, kar je imelo za posledico veliko število prošenj o njihovi premestitvi iz Ruske federacije.

4.3.3 Sovjetska zveza

Ruski narod je doživljal nekakšne oblike policijske države že vse od 19. stoletja naprej za časa carske Rusije, ko je tajna policija nadzirala in onemogočala politično delovanje vzhajajočega nasprotnika, komunizma. Po zmagi boljševikov v oktobrski revoluciji leta 1917 je bila ustanovljena tajna policijska organizacija Cheka, ki je institucionalna predhodnica KGB in današnje FSB. Organizacija je operirala zunaj vladavine prava in je delovala sama po sebi brez večjega nadzora. Po lastni volji je izvajala preiskave in aretacije brez kakršnihkoli sodnih odredb. Njihove metode so obsegale zasliševanja z mučenjem, usmrtitve in druge grobe kršitve človekovih pravic in državljanskih svoboščin. Obdobje, v katerem je tako rekoč vladala Cheka, 1917–1922, se imenuje tudi rdeči teror. Prvotna naloga organizacije je bila boj proti kontrarevoluciji, sabotaži in finančnim špekulacijam. Domnevne kontrarevolucionarje je klasificirala v pet skupin (Alpha History, 2015):

1. civilisti in pripadniki oboroženih sil, ki so osumljeni dela za carsko Rusijo,
2. družine osumljenih,
3. klerikalci,
4. delavci in kmetje, osumljeni, da ne podpirajo boljševiške oblasti,
5. posamezniki, katerih zasebna lastnina presega vrednost 10.000 rubljev.

Cheka je postala model za tajne policije 20. stoletja v totalitarnih državah, po njenem vzoru so bili vzpostavljeni gestapo, Stasi in KGB.

Leta 1922 je bila transformirana in preimenovana v Državno politično upravo GPU (rus. *Gosudarstvennoye politicheskoye upravlenie*). Del službe, ki je skrbel za notranjo varnost, je dobil določene omejitve v primerjavi z njeno predhodnico. Tako med drugim niso več smeli po svoji volji streljati osumljencev protirevolucijskih dejanj in vsi, ki so bili osumljeni političnih zločinov, so morali biti pripeljani pred sodnika. Z ustanovitvijo Sovjetske zveze leta 1922 se je GPU novembra 1923 znova reorganiziral in preimenoval v Združeno državno politično upravo OGPU (rus. *Obyedinyonnoye gosudarstvennoye politicheskoye upravleniye*), ki je imel v teoriji enake omejitve kot GPU v primerjavi z boljševiško tajno policijsko organizacijo. OGPU so se leta 1926 s sprejetjem Sovjetskega kazenskega zakonika povečale pristojnosti, predvsem z vključitvijo poglavja o protidržavnem terorizmu. Členi zakonodaje so bili napisani zelo splošno in so dopuščali široke interpretacije. Skozi čas je moč OGPU zrasla in je celo presegla svojo predhodnico v obdobju rdečega terorja (Overy, 2004).

Ljudski komisariat za notranje zadeve NKVD (rus. *Narodnyi komissariat vnutrennikh del*) je bil ustanovljen leta 1917 kot organizacija, ki opravlja redne policijske naloge ter nadzoruje državne zapore in delovna taborišča (Huskey, 2014, str. 230). Leta 1930 so organizacijo razpustili in njene naloge razdeli med druge institucije. Štiri leta kasneje pa so znova vzpostavili NKVD z vlogo ministrstva za notranje zadeve. Dejavnosti, s katerimi se je do takrat ukvarjal OGPU, so prišle pod okrilje novonastalega NKVD in s tem se je ustvaril monopol ene institucije na področju kazenskega pregona, ki je trajal vse do konca druge svetovne vojne. Naloge s področja obveščevalnih dejavnosti in tajne policije, ki jih je predtem opravljal OGPU, je sedaj izvajal Glavni direktorat za državno varnost GUGB (rus.: *Glavnoe upravlenie gosudarstvennoi bezopasnosti*). V tem času je organizacija postala orodje v rokah Josefa Stalina in je imela eno glavnih vlog pri izvajanju politične represije v "veliki čistki", s katero je Stalin odstranil svoje dejanske in domnevne sovražnike ter si tako utrdil položaj na čelu stranke in države. V času druge svetovne vojne se je v določenem obdobju GUGB odcepil od NKVD v samostojno institucijo in se preimenoval v Ljudski komisariat za državno varnost NKGB (rus. *Narodny komissariat gosudarstvennoi bezopasnosti*), ki se je še naprej ukvarjal z obveščevalno dejavnostjo in izvajanjem nalog tajne policije (Khlevniuk, 2015, str. 125).

Od leta 1946 pa vse do 1953 je glavna obveščevalna služba postalo Ministrstvo za državno varnost MGB (rus. *Ministerstvo gosudarstvennoy bezopasnosti SSSR*) in tako sta se pred leti dve ločeni službi NKVD in NKGB znova združili pod eno institucijo. Nadaljevalo se je delo na področju tajne policije, ki je izvajala vohunjenje in protiobveščevalno dejavnost kot tudi nadzor, s katerim se je kontroliralo in preprečevalo nelojalnost sistemu. Delovali so po sovjetskih satelitih, kamor so se infiltrirali in uničevali protikomunistično in protisovjetsko delovanje (Rusnet, 2017). MGB je upravljal z mrežo tajnih sodelavcev doma in v tujini in organiziral domačo in tujo protiobveščevalno dejavnost. Odgovorni so bili tudi za uveljavljanje varnostnih predpisov, spremljanje in cenzuriranje informacij, ki so šle iz države ali prihajale vanjo, in za nadzor velikega dela vsakdanjega življenja, vključno z nastavitvijo in aktivacijo tajnih sodelavcev, ki so spremljali in nadzirali javno mnenje. MGB je bil predvsem varnostna organizacija in kot tak je bil zasnovan za tajno izvajanje nadzora. Sposobni so se bili infiltrirati v vse stopnje družbenega organiziranja. Tako so imeli svoje agente v podjetjih in tovarnah, lokalnih oblasteh in na vseh stopnjah sovjetske birokracije. Ministrstvo je imelo visoko stopnjo samostojnosti znotraj državnega sistema in je bilo podrejeno neposredno centralnemu komiteju, kateremu je bilo tudi odgovorno (Fainsod, 1949, str. 710–711). Notranja organizacija je bila razdeljena v devet direktoratov, peti direktorat se je ukvarjal z regulacijo in represijo resničnih in namišljenih disidentov znotraj strankarskih struktur kot tudi sovjetske družbe. Tako so nadzorovali vse vidike življenja, vključno z akademskim svetom, birokracijo, splošnimi upravnimi uradi, kulturnimi organizacijami, izobraževalnimi ustanovami in strankarskim aparatom. Spremljali so politično udejstvovanje celotnega prebivalstva s posebnim poudarkom na komunistični stranki vse do najvišjih funkcionarjev stranke in vlade. Skrivaj so nadzorovali celotni upravni in gospodarski aparat države kot tudi znanstvene, javne, cerkvene in druge organizacije. Cilj je bil pri posameznikih najti odstopanja od sistema in ideologije, opozicijska nagnjena znotraj stranke in preprečiti protisovjetska gibanja pod krinko nacionalizma v sovjetskih satelitih (Wolin in Slusser, 1974, str. 166).

Leta 1954 je nastal Komite državne varnosti KGB (rus. *Komitet gosudarstvennoy bezopasnosti*), ki je upravljal naloge tuje obveščevalne službe in notranje varnosti Sovjetske zveze. Njegove zadolžitve so bile zagotavljanje varnosti politične elite, nadzor nad državnimi mejami in splošni nadzor nad prebivalstvom (Pringle, 2017). Na področju notranje varnosti je imel komite na podlagi zakonov moč aretirati in preiskovati posameznike za določene politične in gospodarske zločine. Odgovoren je bil tudi za izvajanje cenzure, propagando in

zagotavljanje varnosti državnih in vojaških skrivnosti. Poleg aretacij in drugih oblik prisile je KGB izvajal preventivno funkcijo, ki je bila namenjena preprečevanju političnih zločinov in zatiranju deviantnih političnih odnosov. Veliko časa so posvečali politični indoktrinaciji in propagandi. Tako na lokalni kot regionalni ravni so uradniki KGB redno obiskovali tovarne, šole, kolektivne kmetije in druge skupnosti, kjer so predavali o političnih temah. Drug pomemben vidik preventivnega dela, s katerim se je ukvarjal KGB, je bila cenzura literature in medijev, ki se je izvajala na formalni in neformalni ravni. Neformalna cenzura se je izvajala prek nadlegovanja pisateljev, novinarjev in umetnikov, groženj z izgonom iz poklicnih združenj in izgube delovnega mesta v primerih, če so imeli drugačne poglede kot sistem. Takšne oblike zastraševanja so mnoge pisatelje in umetnike prisilile k samocenzuri, tako da so ustvarjali le tisto, kar so menili, da je sprejemljivo. KGB je imel močan nadzor nad združenji pisateljev in sindikatov novinarjev, v katerih so predstavniki KGB zasedali najvišje upravne položaje (Pike, 1997).

Druga pomembna naloga notranjevarnostnega mehanizma je bila zagotavljanje informacij državnemu vodstvu o disidentnem gibanju ter političnih stališčih in mnenju javnosti. Ta naloga je dajala KGB veliko moč, saj je imela zaradi monopola pri dostavljanju informacij vpliv na oblikovanje in izvajanje politik (Pike, 1997).

4.3.4 Združene države Amerike

Obliko policijske države najdemo tudi v ZDA, kjer je Zvezni preiskovalni urad FBI v določenem obdobju od leta 1956 do 1971 pod vodstvom direktorja J. Edgarja Hooverja izvajal program COINTELPRO (angl. *COunter INTELligence PROgram*). Z njim so izvajali tajne in nelegalne dejavnosti nadzorovanja, infiltracije in diskreditacije ter ovirali delovanje domačih političnih organizacij (Jalon, 2006; Murphy, 2002). Program je bil usmerjen na skupine in posameznike, za katere je FBI ocenjeval, da izvajajo subverzivne dejavnosti. Tako so tarče postale organizacije, ki so zagovarjale stališče proti vojni v Vietnamu, aktivistična društva, kot sta Civil Rights Movement in gibanje Black Panther, feministične organizacije, gibanje za samostojnost Portorika (Young Lords) in druga društva v okviru nove levice. Med posamezniki je bil najbolj pod drobnogledom Martin Luther King mlajši (Jeffreys-Jones, 2008, str. 189). Metode, ki so jih uporabljali, se v določenih primerih uporabljajo še danes. Predvsem gre za diskretizacijo z uporabo psiholoških metod, uporabo ponarejenih dokumentov, podtikanje dokazov in negativno prikazovanje v medijih. Taktike vključujejo tudi nadlegovanje, neupravičeno priprtje, nezakonito nasilje in v skrajnih primerih atentate

(Swearingen, 1995). Podoben modus operandi navaja Glick (1999), ki trdi, da se je FBI posluževal štirih glavnih metod, ki so:

1. infiltracija agenta ali tajnega sodelavca v ciljno sredino. Ta metoda ni imela samo funkcije zbiranja podatkov, ampak tudi funkcijo diskreditacije in onemogočanja delovanja organizacije. FBI je med podpornike namerno plasiral informacije o prisotnosti tajnih sodelavcev, da bi na ta način vzbudil strah med podporniki in jih odvrnil od udejstvovanja;
2. psihološka vojna se je odvijala na ravni lažnih informacij o organizaciji v medijih. Ponarejali so korespondenco, opravljali anonimne telefonske klice in pošiljali anonimna pisma v imenu organizacije. Uporabljali so dezinformacije o srečanjih in dogodkih ter ustvarjali podobna gibanja, ki so uporabljala nasilje, s čimer so pravemu gibanju zniževali ugled v javnosti;
3. zloraba pravnega sistema za izvajanje nadlegovanja disidentov, ki se jih prikazuje kot kriminalce. Policisti so lažno pričali in na sodišču prikazovali ponarejene dokaze z razlogom odobritve aretacij in zapornih kazni. Diskriminatorno so uveljavljali zakone in vladne predpise;
4. sodelovanje z lokalno policijo, s katero so grozili disidentom, nelegalno vstopali v njihove prostore ter izvajali fizično nasilje in atentate. Cilj je bil prestrašiti in onemogočiti delovanje gibanj.

4.4 Model policijske države

Iz opisanih zgodovinskih primerov se lahko izpostavi skupne značilnosti različic policijske države v posameznem sistemu. Analiza je narejena na treh zgoraj opisanih primerih Nemčije in Sovjetske zveze. Vse tri oblike policijske države so nastale v nedemokratičnih režimih in so bile odgovor na ohranjanje vladajoče elite na oblasti z onemogočanjem opozicije in izvajanjem terorja nad prebivalci. Primarni namen tajnih služb, ki so bile zadolžene za notranje zadeve, je bil odkrivanje političnih nasprotnikov in onemogočanje njihovega delovanja. Te službe so bile neposredno podrejene vladajoči eliti in so delovale zunaj zakonov. Prav tako niso bile podvržene kakršnemukoli državnemu ali sodnemu nadzoru, kar jim je omogočalo, da so brez posledic kršili človekove pravice in državljanske svoboščine. Pri svojem delu so pogosto uporabljale nekonvencionalne metode pridobivanja podatkov s prakticiranjem fizičnega in psihičnega nasilja kot tudi usmrtitve.

Država pri izvajanju nadzora in ohranjanju stabilnosti svoje ideologije uporablja cenzuro in propagando, ki ju v veliko primerih izvajajo državne tajne službe ali pa kakšen drug specializiran državni organ. Cenzuro se lahko opredeli kot dopolnilno aktivnost izvajanja nadzora nad prebivalstvom. Cenzuri so v takšni državi podvrženi tako mediji kot akademski izdelki in kulturna umetnost. Onemogočeno je svobodno izražanje, še posebej na političnem nivoju, vsaka majhna deviacija od vladajoče politike se konča z negativnimi posledicami. Krutost delovanja tajnih služb v javnosti vzbuja strahospoštovanje do države, kar se uporablja kot preventivna funkcija, s katero se že s samo grožnjo in zavedanjem posameznika o posledicah vpliva na njegovo neaktivnost v izvajanju zadev, ki so v nasprotju z državno politiko.

Tajne službe uporabljajo in izkoriščajo prebivalce kot glavni vir informacij. Njihovo sodelovanje je lahko prostovoljno ali pod prisilo. Iz tega se je razvila teorija, po kateri je vsak posameznik potencialni tajni sodelavec obveščevalnih služb, kar privede do stanja v družbi, kjer vsakdo vsakogar sumi kot sodelavca tajne službe, kar vpliva na vsakdanje življenje. Država to stanje znova izkorišča za preventivno delovanje odvračanja opozicijske participacije, saj so posamezniki zaradi dejstva, da jih lahko izda njihov znanec, sosed ali družinski član, odvrnjeni od političnega aktivizma.

Na podlagi teh enotnih dejavnikov lahko izpostavimo pet skupnih točk, ki veljajo za policijske države:

1. zavestno kršenje človekovih pravic s strani države;
2. obstoj tajne službe, ki je neposredno podrejena vladi in ni pod sodnim nadzorom;
3. izvajanje cenzure in lastne propagande;
4. ustvarjanje videza vsemogočnosti države in tajnih služb za širjenje strahu med prebivalci;
5. aktivna participacija državljanov pri sodelovanju s tajnimi službami.

Pri iskanju skupnih lastnosti je namenoma izpuščen primer policijske države v ZDA, saj je ta drugačen zaradi bistvenega dejavnika, tj. vrste režima. Gre za obliko policijske države v demokratičnem sistemu, v katerem naj bi bile vsem državljanom omogočene enake pravice. V okviru izvajanja programa COINTELPRO so bile metode izvajanja tajnih služb za razliko od ostalih primerov usmerjene na točno določene ciljne sredine in posameznike, nad katerimi se je zaradi opozicijskega političnega udejstvovanja izvajal nadzor, kljub temu da niso kršili obstoječih zakonov in ustave. Delovanje FBI v omenjenem času je dober pokazatelj, kako

lahko država za določene skupine v družbi, ki jih ima za potencialno nevarne, vzpostavi obliko policijske države, kjer državni organi, ki so podvrženi parlamentarnemu in sodnemu nadzoru, zavestno kršijo in izigravajo lastno zakonodajo, celo ob splošnem konsenzu javnosti.

5 ZBIRANJE PODATKOV S STRANI SOCIALNIH OMREŽIJ

5.1 Facebook

Facebook je spletna skupnost, ki posameznim uporabnikom omogoča ustvarjanje osebnih profilov, skupno rabo fotografij in videoposnetkov ter opravljanje medsebojne komunikacije z drugimi uporabniki. Osnovna funkcija Facebooka je olajšati izmenjavo informacij med posamezniki, ki se imajo na platformi za prijatelje. Najpogostejše informacije, ki se izmenjujejo, vključujejo arhivsko gradivo, kot so fotografije in objave v spletnem dnevniku, in tudi informacije v realnem času, to so posodobitve stanja in neposredno sporočanje v okviru okna za klepet. Najdemo pa lahko tudi informacije o prihodnosti, kot so bližajoči se dogodki in rojstni dnevi oseb na seznamu prijateljev (Hogan in Smith, 2011, str. 283). Facebook je leta 2017 presegel mejo dveh milijard aktivnih uporabnikov in ima med socialnimi omrežji daleč največ uporabnikov (Statista, 2017).

Facebook je imel v svoji zgodnji fazi veliko pomanjkljivosti glede varovanja zasebnosti uporabnikov in podatkovnega rudarjenja. Kot sta Jones in Soltren (2005) ugotavljala še dve leti po začetku javne uporabe omrežja, so se gesla uporabnikov pošiljala brez šifriranja, kar je tretjim osebam omogočalo, da so lahko brez večjih naporov prestrezale gesla uporabnikov Facebooka.

Raziskovanje in zbiranje podatkov na Facebooku s strani zunanjega opazovalca je zelo omejeno, saj je platforma zgrajena na temeljih omejenega dostopa do podatkov profilov drugih ljudi. To ne preprečuje analiziranja v celoti, ampak le otežuje dostop do želenega cilja in celotne slike (Hogan in Smith, 2011, str. 284).

Osebno profiliranje uporabnikov in njihovega realnega življenja je eden glavnih konceptov Facebooka in prinaša številne resne skrbi glede politike zasebnosti, ki jo izvaja platforma. Lažni profili so prepovedani in Facebook teži k uporabi resničnih imen. Eden od načinov, kako to dosega, je storitev *Facebook Connect*, ki omogoča, da se uporabnik lahko s Facebookovim računom prijavi na različnih spletnih straneh (Jacobson, 2014, str. 490). Prek te storitve je Facebooku omogočeno zbiranje podatkov tudi o dejavnostih na spletnih straneh tretjih oseb, ki omogočajo storitve, kot so Facebook Connect ali vgrajeni vtičniki za neposredno všečkanje in komentiranje vsebin (Facebook, 2017). V pogojih uporabe je

navedenih več pravil, ki se tičejo uporabe resničnih podatkov, in za vsako kršenje pravil si Facebook pridržuje pravico do izbrisa profila. Facebook osebne podatke vseh uporabnikov, ne glede na državo bivanja, prenaša in obdeluje na strežnikih, ki so v ZDA (Facebook, 2017). Varstvo osebnih podatkov na tem socialnem omrežju se tako obravnava po zakonodaji ZDA.

Podatki, ki se zbirajo o uporabnikih, obsegajo celotno dejavnost posameznika in oseb, s katerimi komunicira. Tako se pri uporabi storitev zbirajo objavljene vsebine in drugi podatki, ki jih uporabniki posredujejo, vključno z ustvarjanjem računov, objav, delitve vsebin in medsebojnim komuniciranjem z drugimi uporabniki. Informacije vključujejo vsebino, ki je objavljena na platformi, ter metapodatke, kot so lokacija fotografije ali datum, kdaj je bila datoteka ustvarjena. Spremlja se uporaba storitev, prek katerih se ugotavlja, kakšne vsebine si posameznik ogleduje, ali sodeluje v neki aktivnosti ter kako pogosto izvaja to početje. Posredno se zbirajo informacije tudi od drugih uporabnikov, s katerimi komunicira, kot so npr. skupne fotografije, zasebna sporočila ali uvoz stikov, v katerih je uporabnik naveden. Ob uporabi plačilnih storitev, ki jih omogoča Facebook v igrah ali donacijah, se zbirajo podatki o kreditnih karticah in fizičnem naslovu kupca. Poleg informacij o dejavnostih se zbirajo tudi informacije o napravah, prek katerih se dostopa do storitev Facebooka. V to kategorijo se uvrščajo operacijski sistemi, strojna oprema, nastavitve naprave, podatki o bateriji in signalu ter identifikacijski podatki o uporabljeni napravi. Prek navigacijskega sistema GPS, Bluetootha in signala brezžičnega interneta se zbira tudi geografske lokacije, kje se naprave nahajajo. Prek povezave do storitev se zabeleži mobilni operater, ISP-ponudnik, tip spletnega brskalnika, jezikovne in časovne nastavitve, številka mobilnega telefona in IP-naslov (Facebook, 2017).

Zbrani podatki o uporabnikih se uporabljajo za nadaljnji razvoj programskih storitev ter izboljšanje uporabniške izkušnje in nadgradnjo platforme. Podatki se analizirajo tudi za osebnostno prilagojeno prikazovanje vsebin, ki posameznega uporabnika zanimajo, torej se vsebine na podlagi profiliranja prilagajajo posamezniku. Algoritmi predvidevajo, kaj bo posameznika zanimalo. Z uporabo lokacijskih storitev platforma prikazuje dogodke in znamenitosti, ki potekajo v bližini, kjer se uporabnik trenutno nahaja. Funkcija prepoznave obraza omogoča predvidevanje in predlaganje označbe uporabnika na prijateljevi sliki. Najpomembnejše področje, za katero se uporabljajo podatki, pa je oglaševanje, ki platformi prinaša glavni dohodek. Oglasi so tako glede na zbrane podatke o posamezniku točno prikrojeni njegovemu zanimanju, zato se v večini primerov prikazujejo samo predpostavljeni relevantni oglasi izdelkov in storitev, ki naj bi uporabnika zanimali (Facebook, 2017).

Nastavitve zasebnosti uporabniku omogočajo nastavitev obsega in javnosti njegovih podatkov, objav in aktivnosti na Facebooku. Popolnoma odprt račun pomeni, da lahko njegove podatke in informacije vidi kdorkoli. Omejitve pa omogočajo nastavitve, da aktivnosti uporabnika vidijo samo določene osebe, skupine ali pa celo nobeden, kar pomeni, da je račun popolnoma zaprt (Facebook, 2017).

Tretje osebe, ki imajo integrirane storitve Facebooka, lahko dostopajo do podatkov, ki so na Facebooku. Tako v primeru komentiranja na spletni strani, ki ima integrirane storitve komentiranja Facebook, lahko ta spletna stran dostopa do podatkov, kot so uporabniško ime, ID-številka, starost, država, jezik in seznam prijateljev, ter informacij, ki so bile deljene z njimi. Ti podatki niso več pod pravili uporabe in zasebnosti Facebooka, ampak so predmet obravnave tiste spletne strani, ki je dostopala in zbrala te podatke (Facebook, 2017).

5.2 Instagram

Instagram je platforma za objavljanje fotografij. Pojavila se je leta 2010. Leta 2012 je podjetje prevzel Facebook lnc. in s prevzemom so bile združene določene funkcionalnosti obeh platform. Instagram v osnovi ponuja uporabniku, da objavlja fotografije, ki jih lahko spreminja in obdeluje z orodji, ki jih platforma ponuja, in komentira fotografije drugih uporabnikov. Storitev omogoča tudi objavljanje kratkih video posnetkov. Geolokacijske storitve uporabniku omogočajo, da k fotografiji pripne tudi kraj, kjer je bila posneta. Instagram je imel septembra 2017 700 milijonov aktivnih uporabnikov (Statista, 2017).

Instagram zbira osebne podatke, ki jih uporabnik navede ob registraciji in ob urejanju svojega profila. Ti podatki so uporabniško ime, geslo in naslov spletne pošte ter fotografija in telefonska številka. Zbirajo se tudi vse vsebine, ki jih ustvari uporabnik, npr. fotografije, komentarji in drugi materiali, ki jih uporabnik objavlja na platformi. Z uporabo funkcije za iskanje prijateljev Instagram neposredno dostopa do telefonskega imenika in imenika spletne pošte, prav tako pa s povezavo računov s Facebookom ali kakšnim drugim socialnim omrežjem dostopa do oseb, navedenih na omenjenih seznamih. Z uporabo piškotkov in drugih podobnih storitev se zbirajo podatki o uporabi platforme kot tudi, katere druge spletne strani uporabnik obiskuje. Zbrani podatki obsegajo IP-naslov, tip brskalnika, obiskane spletne strani, število klikov na posamezno povezavo, imena domen in druge podobne podatke. Pri uporabi mobilnih naprav se zbirajo identifikacijski podatki o napravah, ki obsegajo model

naprave in strojno opremo, operacijski sistem ter drugo programsko opremo, ki je naložena na omenjeni napravi. Iz metapodatkov je mogoče razbrati, kje in kdaj ter kdo je ustvaril in objavil določeno objavo. Pri fotografiji omogoča ugotovitev, kjer je bila posneta, in uporabniku nudi možnost, da javno objavi kraj nastanka fotografije (Instagram, 2017).

Podatki se shranjujejo na strežnikih v ZDA in drugod po svetu. Instagram lahko te podatke nemoteno in brez omejitve prenaša iz enega strežnika na drugega in iz ene države v drugo. Če je podatek prenesen iz EU v ZDA je potem podvržen zakonodaji ZDA in se lahko razlikuje od zakonodaje države v kateri uporabnik živi (Instagram, 2017).

Vse zbrane podatke Instagram lahko posreduje podjetjem, ki spadajo pod isto lastniško strukturo, torej vsem podjetjem, ki so v lasti podjetja Facebook Inc. Določeni podatki so zaradi ciljnega oglaševanja zanimivi za posamezna podjetja in se posredujejo tudi ponudnikom storitev, ki omogočajo oglaševanje. Tretjim osebam se lahko posredujejo tudi podatki, ki so brez identifikacijskih parametrov in iz njih ni mogoče ugotoviti, komu pripadajo. Podjetje lahko na podlagi zakonskega zaprosila odstopi podatke državnim institucijam, če za to obstaja razlog, ki je naveden v zakonu (Instagram, 2017).

5.3 Twitter

Twitter je internetna storitev, ki ljudem omogoča objavo hitrih kratkih sporočil, ogled objav drugih uporabnikov ter odzive na objave v realnem času. Sporočila so omejena na 140 znakov, vendar so leta 2017 to politiko spremenili in po novem lahko posamezno sporočilo vsebuje 280 znakov. Osnovno poslanstvo platforme je omogočanje deljenja informacij posameznikov s svetom. Značilnost te platforma je uporaba ključnikov, kjer se pred ključno besedo vstavi simbol "#". Ključne besede omogočajo iskanje vseh sporočil, ki vsebujejo določen ključnik. Privzete nastavitve so nastavljene, da so vsa sporočila javno vidna vsem uporabnikom, lahko pa se spremenijo, da so vidna samo določenim osebam, za katere posamezni uporabnik želi, da jih vidijo. Platforma je začela delovati leta 2006 in že naslednje leto so uporabniki objavljali v povprečju več kot dva milijona sporočil na dan. Twitter je imel v letu 2017 328 milijonov uporabnikov (Statista, 2017).

Za ustvarjanje računa na Twitterju je treba posredovati podatke, kot so osebno ime, uporabniško ime, geslo, naslov spletne pošte in telefonsko številko. Na platformi sta ime in uporabniško ime, ki je edinstveno, ves čas javno vidna in ju ni mogoče spremeniti v zasebno.

Twitter za razliko od Facebooka dopušča ustvarjanje in upravljanje več računov hkrati. Podjetje meni, da je v našem interesu, da je večina informacij, ki jih predamo prostovoljno, javno dostopnih. Tako so tudi neobvezni podatki, kot so kratek življenjepis, kraj, kjer uporabnik živi, povezava do spletne strani, datum rojstva in fotografija, v osnovi javno prikazani. Za javne informacije se imajo tudi sporočila, ki jih uporabniki objavljajo, kot tudi metapodatki, ki se skrivajo za temi objavami, kot so kdaj in prek katere naprave je bilo sporočilo objavljeno ter podatki o računu uporabnika, npr. kdaj je bil račun ustvarjen, kateri jezik uporablja uporabnik, iz katere države prihaja in časovni pas. Twitter vseskozi razširja javne podatke med drugimi uporabniki, strankami in storitvami, kot so spletni iskalniki, razvijalci in založniki, ki v svojih storitvah uporabljajo integracijo storitev Twitterja. Najpogosteje so to podjetja, ki se ukvarjajo z raziskavo trgov in analizirajo informacije za prikaz trendov in napovedi (Twitter, 2017).

Twitter zbira tudi podatke o lokaciji, kjer se naprava nahaja. Tako je mogoče javno prikazati lokacijo, s katere uporabnik objavlja sporočila, ali pa je v njegovem profilu prikazan kraj, kjer se trenutno nahaja. Platforma lokacijo določa prek podatkov GPS, brezžičnih omrežij in radijskih oddajnikov, na katere je vezana naprava, ter na podlagi IP-naslova. Twitter te podatke zbira, da se lahko uporabniku predlaga prilagojeno prikazovanje sporočil iz lokalnega okolja, kjer se uporabnik nahaja (Twitter, 2017).

Twitter prek piškotkov sledi uporabnikom tudi zunaj svoje platforme. Tako lahko pride do podatkov obiska določene spletne strani, če ima ta spletna stran omogočene storitve Twitterja, ki jih ta ponuja, kot je npr. gumb za neposredno deljenje vsebin na Twitterju. Podatki, ki se zbirajo v tem kontekstu, so IP-naslov, tip brskalnika, operacijski sistem, katere spletne strani je uporabnik obiskal, lokacija, mobilni operater, podatki o napravi, ki obsegajo identifikacijsko številko naprave in aplikacij, ki so na njej naložene, zgodovino iskanja ter podatke o piškotkih. Cilj zbiranja teh podatkov je prilagoditi vsebine posameznemu uporabniku in prikazovati tiste teme, ki naj bi ga zanimale, skupaj s prikazovanjem oglasov. Twitter omenjene podatke za posameznega uporabnika hrani največ 18 mesecev, po tem roku pa jih izbriše. Podatki za posameznega uporabnika niso vezani samo na napravo, s katero dostopa do platforme, ampak veljajo za celoten račun. Torej če uporabnik prek osebnega računalnika obiskuje spletne strani s športno vsebino, bodo predlogi s temi vsebinami kasneje prikazovani tudi v aplikaciji za Android. Podatki o uporabniku se zbirajo tudi prek tretjih oseb. Če je določen uporabnik omenjen v sporočilu drugega uporabnika ali pa je označen na

fotografiji, se ti podatki shranijo in povežejo s podatki, zbranimi neposredno od prvega uporabnika (Twitter, 2017).

Twitter zbrane podatke o uporabnikih deli z drugimi ponudniki storitev, ki jih ima za pomembne in s katerimi lahko izboljšuje svoje storitve in jih razvija. Med podatki, ki jih platforma deli z drugimi, so tudi plačilni podatki, med katere spadajo številka kreditne ali debetne kartice, datum veljavnosti, CVV-številka in fizični naslov za izstavitev računa, in sicer z namenom preprečevanja zlorab in prevar pri plačevanju storitev. Na podlagi zakonskih določil je Twitter obvezan odstopiti podatke določenim državnim institucijam, če so izpolnjene vse pravne obveze, ki veljajo za razkritje osebnih podatkov (Twitter, 2017).

Aplikacija za mobilne naprave zbira podatke o vseh drugih aplikacijah, ki so bile nameščene na tej isti napravi, in shranjuje seznam teh aplikacij. Zbrani so samo podatki o tem, katere aplikacije so nameščene, ne posega pa se v same podatke znotraj teh aplikacij (Twitter, 2017).

5.4 Google+

Google je svoje socialno omrežje predstavil leta 2011. Prvi uporabniki so za ustvarjanje računov potrebovali povabilo že obstoječega uporabnika. Leta 2012 je storitev prešla v splošno rabo, za katero povabila niso bila več potrebna. Google+ je hitro postalo tretje največje socialno omrežje po številu uporabnikov, takoj za Facebookom in Twitterjem. Platforma deluje na principu prijateljstva, s tem da uporabnik lahko razdeli svoje prijatelje v kroge in tako določa, kdo lahko vidi določeno vsebino, ki jo ustvarja ali deli. Google+ Hangouts omogoča avdio in video komunikacijo med uporabniki, omogoča tudi sejo do desetih uporabnikov. Google+ Events pa omogoča organiziranje dogodkov, na katere je mogoče povabiti druge uporabnike. Storitev Google+ je integrirana v celotno Googlovo storitev, za katero se uporablja enoten račun. Tako se prepletajo možnosti uporabe vseh Googlovih storitev. Dogodek, ustvarjen v Google+, se bo samodejno sinhroniziral s Googlovim koledarjem in dogodek uvrstil na uporabnikovo agendo. Če se uporabniki strinjajo z določeno ustvarjeno vsebino drugih uporabnikov, lahko to izrazijo s potrditvijo, ki se na platformi izraža v obliki gumba +1 in ima podobno vlogo kot Facebookov gumb za všečkanje (Google, 2017).

Za platformo Google+ se uporablja enotni Googlov račun, s katerim se lahko dostopa do vseh storitev, ki jih Google ponuja. Za ustvarjanje Googlovega računa je treba posredovati ime,

naslov elektronske pošte, telefonsko številko ter občasno tudi plačilno kartico, prek katere lahko Google preverja starost uporabnika. Za koriščenje vseh funkcij, ki jih podjetje ponuja, je treba ustvariti javno viden profil, ki lahko vključuje ime in fotografijo uporabnika. Google zbira podatke o posameznem uporabniku pri uporabi vseh njihovih storitev, kot so sporočila v Gmailu, profil v Google+, fotografije, video posnetki, zgodovina brskanja, iskanja po zemljevidih ter dokumenti in druge vsebine, ki gostujejo v storitvah Google. Zbrani podatki vključujejo model strojne opreme, različico operacijskega sistema, enolične identifikatorje naprav in podatke o mobilnem omrežju, vključno s telefonsko številko. Google lahko identifikatorje naprav ali telefonsko številko poveže z Googlovim računom. Pri uporabi storitev in ogledovanju vsebine, ki jo zagotavlja Google, se samodejno zbirajo in shranjujejo nekateri podatki v strežniških dnevnikih. Ti podatki vključujejo podatke o tem, kako uporabnik uporablja storitve, npr. iskalne poizvedbe v iskalniku, podatke za dnevnik telefonije, kot so telefonska številka, številka klicatelja, številke za posredovanje, ura in datum klicev, trajanje klicev, informacije o preusmerjanju SMS-ov in vrste klicev, naslov IP, podatke o dogodkih na ravni naprave, kot so zrušitve in aktivnosti sistema, nastavitve strojne opreme, vrsto brskalnika, jezik brskalnika, datum in ura zahteve ter naslov URL (Google, 2017).

Google lahko zbira in obdeluje podatke o dejanski lokaciji uporabnika, še posebej v primerih uporabe storitev Google Zemljevidi. Za ugotavljanje lokacije se uporabljajo različne tehnologije, kot so naslov IP, GPS in drugi senzorji, ki lahko Googlu omogočajo pridobivanje podatkov o bližnjih napravah, dostopnih točkah Wi-Fi in baznih postajah. Google lahko pri mobilnih napravah izkorišča senzorje, s pomočjo katerih dobi podatke za natančnejše ugotavljanje lokacije. Za ugotavljanje parametrov, kot je na primer hitrost, se lahko uporablja merilnik pospeška, za ugotavljanje smeri premikanja pa žiroskop (Google, 2017).

Google in njegovi partnerji, ki jih ima podjetje za zaupanje vredne, dovolijo uporabo piškotkov ali podobnih tehnologij za namene oglaševanja in raziskav v storitvah. Uporabljajo se različne tehnologije za zbiranje in shranjevanje podatkov, ko uporabnik obišče Googlove storitve, na primer uporaba piškotkov ali podobnih tehnologij za prepoznavanje brskalnika ali naprave. Te tehnologije se uporabljajo tudi za zbiranje in shranjevanje podatkov pri interakciji s storitvami, ki jih ponujajo partnerjem, kot so oglaševalske storitve ali Googlove funkcije na drugih spletnih mestih. Podatki, zbrani ob prijavi v storitve Google, vključno s podatki, pridobljenimi od partnerjev, se lahko povežejo z Googlovim računom ter se tako obravnavajo kot osebni podatki (Google, 2017).

Podatki se uporabljajo za zagotavljanje, vzdrževanje, zaščito in izboljšanje Googlovih storitev, razvoj novih storitev ter zaščito uporabnikov. Prav tako se uporabljajo za prikazovanje prilagojenih vsebin, kot so ustreznejši rezultati iskanja in oglasi. Samodejni sistemi analizirajo ogledano vsebino, vključno z elektronsko pošto, da lahko Google ponudi ustrezne funkcije izdelkov, prilagojene uporabniku, kot so prilagojeni rezultati iskanja, prilagojeno oglaševanje ter odkrivanje neželene vsebine in zlonamerne programske opreme. Osebni podatki iz ene storitve se lahko združijo s podatki iz drugih Googlovih storitev, da se omogoči preprostejšo skupno rabo stvari z ljudmi, ki jih uporabnik pozna. Google si jemlje pravico, da obdeluje podatke na strežniku v državi, ki ni tista, iz katere prihaja uporabnik (Google, 2017).

5.5 LinkedIn

LinkedIn je spletno mesto, ki uporabnikom omogoča ustvarjanje profilov ter objavljanje in komuniciranje z drugimi strokovnjaki in iskalci zaposlitve. Profil uporabnika je prikazan kot življenjepis, kjer lahko uporabniki poleg osebnih podatkov dodajo svojo stopnjo uradne izobrazbe, dodatno izobrazbo in pridobljene certifikate, pretekle delovne izkušnje in trenutno delovno mesto. Poleg tega lahko dodajo še različne osebnostne karakteristike, znanja in življenjske filozofije. Platforma je usmerjena predvsem v razvoj kariere posameznega uporabnika in pridobivanje novih zaposlitev. Po drugi strani pa podjetjem omogoča iskanje nove delovne sile (LinkedIn, 2017). Platformo je leta 2017 uporabljalo 106 milijonov uporabnikov (Statista, 2017).

Platforma zbira podatke, ki vključujejo ime, naslov spletne pošte in geslo. Pri uporabi plačljivih storitev med te zbrane podatke sodijo tudi plačilne kartice. Zbirajo se tudi vsi podatki, ki jih uporabniki vnašajo v oblikovanje svojega profila, ki je zaradi namembnosti platforme zelo dovršen življenjepis. LinkedIn svojim uporabnikom ponuja sinhronizacijo telefonskega imenika in spletne pošte ter različnih koledarjev. Na ta način zbira podatke tudi o osebah, ki še niso njihovi uporabniki. Piškotki omogočajo sledenje obiskovanja drugih spletnih strani ter tako omogoča boljše oglaševanje. Platforma dostopa tudi do podatkov, kot so IP-naslov, operacijski sistem, tip brskalnika, identifikacijska številka naprave in ponudnik internetnih storitev. Pri uporabi mobilne aplikacije lahko LinkedIn dostopa tudi do lokacije, kjer se uporabnik ob uporabi njihovih storitev nahaja. Platforma zbira podatke o obiskih

drugih spletnih strani, na katerih se nahajajo njihove funkcije, kot je npr. gumb za neposredno objavo na LinkedInu (LinkedIn, 2017).

Zbrani podatki o uporabnikih se uporabljajo za boljšo izkušnjo z uporabo platforme. Tako sistem na podlagi teh podatkov predlaga morebitne nove osebe, ki bi jih želeli dodati na seznam prijateljev. Uporabljajo se tudi za prikazovanje objav in novic, ki bi nas na podlagi naših zanimanj in drugih podanih podatkov, utegnile zanimati. Predlagajo se tudi delovna mesta, ki bi uporabnika na podlagi njegovega profila utegnila zanimati. Podatki se analizirajo za prikazovanje ciljnega oglaševanja, za katerega se predvideva, da bo zaradi izkazovanja različnih zanimanj zanimalo določenega uporabnika. Zbrani podatki se uporabljajo tudi za izboljšanje in nadaljnji razvoj platforme in njenih storitev ter za raziskovanje različnih družbenih, ekonomskih in delovnih trendov. Podatki se lahko uporabljajo tudi pri odkrivanju prevar in kršenju pravil uporabe, pri čemer se lahko uporabljajo podatki, ki se pridobijo iz uporabnikovega komuniciranja na platformi. LinkedIn zbrane podatke deli med podjetja, ki spadajo pod skupno skupino podjetij oziroma lastništvo. Podjetje lahko prosto prenaša podatke med strežniki v različnih državah (LinkedIn, 2017).

6 UPORABA SOCIALNIH OMREŽIJ S STRANI DRŽAVE

6.1 OSINT, WEBINT, SOCMINT

Izraz OSINT (angl. *Open Source Intelligence*) označuje dejavnost pridobivanja podatkov iz javnih virov, ki se uporabljajo za obveščevalne namene. Predstavlja proces zbiranja in analiziranja podatkov, ki so zbrani iz javnih in odprtih virov. Glede na tok informacij se ti viri delijo na šest temeljnih kategorij (Richelson, 2015):

1. mediji: tiskani časopisi, revije, radio in televizija;
2. internet: spletne publikacije, spletni dnevniki, forumi in socialna omrežja;
3. podatki državnih organov: javna vladna poročila, proračuni, zaslišanja, tiskovne konference, javno dostopne baze podatkov …;
4. akademske publikacije: konference, simpoziji, akademski članki, disertacije …;
5. komercialni podatki: komercialni satelitski posnetki, finančne in gospodarske ocene, podatkovne baze …;
6. siva literatura: tehnična poročila, patenti, poslovni dokumenti, neobjavljena dela, osnutki, delovno gradivo …

Podatki, pridobljeni iz javnih virov, predstavljajo osnovo za razumevanje vsebine, s katero se analitiki srečujejo pri delu s tajnimi podatki. Kljub zadostni količini tajnih podatkov, ki jih ima obveščevalna služba na voljo, je lahko podatkov na določenem področju iz različnih razlogov premalo. Pomanjkanje teh podatkov lahko vodi do napačne interpretacije ali zaključka, kar se odraža v pomanjkljivi obveščevalni informaciji, še posebej v primerih, kjer se analitiki osredotočajo izključno na razpoložljive tajne podatke. Tako lahko npr. pri delu na področju boja proti terorizmu podatki, pridobljeni iz javnih virov, zapolnijo praznine ali ustvarijo nove povezave, ki analitikom omogočajo boljše razumevanje razdrobljenih obveščevalnih podatkov. Podatki iz javnih virov so lahko govorice ali propaganda o terorističnih dejanjih, modus operandi in potencialni cilji terorističnih napadov.

Največji slabosti OSINT sta količina in obseg podatkov, ki se vseskozi ustvarjata in večata, pri čemer je težko oceniti zanesljivost in verodostojnost tako vira kot tudi samih podatkov. Razvoj interneta je dejansko privedel do poplave informacij, zato je včasih težko ločiti resnični podatek od lažnih novic.

Uporaba javnih virov omogoča obveščevalnim službam med drugimi tudi prekriti in zaščititi lastne tajne sodelavce, ki so še vedno poglavitni vir tajnega pridobivanja podatkov. V določenih primerih se lahko obveščevalno informacijo, ki je izdelana na podlagi podatkov, pridobljenih s strani tajnega sodelavca, prikaže kot analizo in oceno podatkov iz javnih virov, s tem pa se prepreči morebitno kompromitacijo tajnega sodelavca.

Varnostno-obveščevalne službe imajo v okviru notranje organizacije na različne načine vzpostavljeno delovanje OSINT-oddelkov. Določene službe uporabljajo osrednjo enoto, ki se ukvarja z zbiranjem vseh za službo relevantnih podatkov iz javnih virov, in z njimi oskrbujejo ostale oddelke, ki delujejo na posameznih vsebinskih področjih. Druge službe pa imajo OSINT-enote integrirane v same oddelke vsebinskih področij, kjer se zbira izključno podatke na dodeljeno temo. Vse več služb pa v današnjem času uvaja tudi specializirane oddelke, ki se ukvarjajo samo s pridobivanjem podatkov z interneta in socialnih omrežij.

Pojem WEBINT (angl. *Web Intelligence*) označuje metode pridobivanja podatkov iz javnih virov na internetu. Pri tem se uporabljajo različne tehnike in orodja, ki so lahko plačljiva ali brezplačno dostopna na spletu. Plačljiva orodja so v večini primerov namenjena podjetjem, ki analitično spremljajo dogajanje v svoji industriji, se z raznimi ukrepi prilagajajo trgom in izboljšujejo svoje poslovanje. Nekatera orodja (Talkwalker, Verint, Maltego) pa so namenjena tudi obveščevalnim dejavnostim, s katerimi se ukvarjajo tako zasebne kot tudi državne varnostno-obveščevalne službe. Brezplačna orodja so prosto dostopna na internetu. Uporaba različnih orodij lahko privede do dobrih podatkov o obravnavanem objektu ob predpostavki, da je ta dejaven na spletu. Tako zbrani podatki imajo v obveščevalnem procesu vlogo preverjanja in potrjevanja ostalih podatkov ali pa odkrivanja novih sledi in spoznanj, ki se lahko uporabijo pri analitičnem delu.

WEBINT-proces je podobno zastavljen kot obveščevalni krog. V prvem koraku se zastavijo cilji, kaj se želi v zadani nalogi doseči in kdo ali kaj je objekt, o katerem se bodo zbirali podatki. Preprosto se postavi vprašanje, kaj raziskovalca zanima. Naslednja dva koraka predstavljata načrtovanje poteka zbiranja podatkov. V enem se vzpostavi načrt, kakšni podatki se potrebujejo in kateri od njih se bodo zbirali, v drugem pa, s kakšnimi orodji in tehnikami se bodo ti podatki lahko zbrali. V četrtem koraku se izvaja zbiranje podatkov na podlagi metodologije, zastavljene v prejšnjih dveh korakih. Peti korak pa zajema vrednotenje in analizo zbranih podatkov ter posredovanje ugotovitev. Pri ugotovitvah rezultatov utegne priti

do vrzeli v zbranih podatkih ali pa je pride do novih dodatnih vprašanj, ki jih po treba na osnovi novih usmeritev znova obdelati v procesu WEBINT.

Do podatkov, ki so na internetu, se lahko dostopa na tri načine. Ti so:

1. prost dostop do javno objavljenih podatkov,
2. zakonski predpisi, s katerimi se od ponudnikov storitev zahteva odstop podatkov,
3. izvajanje prikritih operacij.

Prvi način zajema metode, s katerimi se lahko neposredno dostopa do podatkov na spletu z uporabo orodij in različnih tehnik. Drugi način predstavlja zahtevo varnostno-obveščevalnih služb, ki prek sodišča na podlagi zakonov pridobijo podatke od ponudnikov storitev. Tretji način pa predstavlja uporabo operativnih virtualnih identitet, s katerimi se pridobivajo podatki od drugih oseb ali skupin na internetu.

Povečana uporaba socialnih omrežij skupaj z razvojem analitičnih pristopov ponuja nove priložnosti za ustvarjanje operativnih obveščevalnih podatkov, ki bi lahko pomagali prepoznati kazniva dejanja ter zagotoviti zgodnje opozarjanje na bližajoče se krize in podatke o skupinah in posameznikih. Z uporabo SOCMINT-metod (angl. *Social Media Intelligence*) se lahko izvaja situacijsko zavedanje v realnem času, vpogledi v skupine in identifikacija kriminalnih naklepov ali elementov pri uporabi preprečevanja in preganjanja kaznivih dejanj. Situacijsko zavedanje v realnem času je sposobnost zbirati in obdelati podatke s socialnih omrežij ter jih prikazati na način, ki prikazuje in opisuje dogodke, ki se odvijajo v sedanjem času. Analiza komunikacijskega prometa na socialnih omrežjih omogoča hitrejšo identifikacijo nastajajočih dogodkov kot pa tradicionalni mehanizmi poročanja. Vpogled v skupine omogoča boljše razumevanje dejavnosti in vedenja določenih skupin, ki so že pod nadzorom policije in obveščevalnih služb. Ob zakoniti odobritvi spremljanja teh skupin se lahko SOCMINT uporablja za odkrivanje varnostno zanimivih tem v okviru komunikacije članov. Službe se tako lahko pripravijo na določene aktivnosti, ki jih nadzorovane skupine načrtujejo, in jih uspešno preprečijo. V primeru preprečevanja in odkrivanja kaznivih dejanj lahko službe na podlagi sodnega naloga izvajajo nadzor nad socialnimi omrežji z namenom odkrivanja in zbiranja dokazov proti sodelujočim v kaznivem dejanju, odkrivanja kriminalnih združb in omrežij ter ugotavljanja identitete osumljencev (Omand, Bartlett in Miller, 2012, str. 5–6).

Poleg varnostno-obveščevalnih služb se SOCMINT-metod poslužujejo tudi druge državne institucije, ki pri svojem delu neposredno občujejo z državljani v upravnih postopkih.

6.2 Varnostno-obveščevalne službe

Notranji nadzor nad prebivalci izvajajo vlada in njene službe, v večini primerov gre za tajne službe. V nadzor so tako vključeni vsi ljudje na določenem teritoriju, ne glede na to, ali so državljani omenjene države ali pa so obravnavni kot tujci. V demokratičnih državah so tujci na podlagi zakonodaje lahko legalno podvrženi večjemu nadzoru kot pa državljani. Tehnike, ki jih uporabljajo tajne službe, se v osnovi delijo na dve kategoriji. Prva je pridobivanje podatkov s človeškimi viri – HUMINT. Pri tej tehniki pripadniki varnostnih služb pridobivajo podatke z neposredno udeležbo prek tajnega sodelavca ali drugih razgovorov s ciljnimi osebami, ki bi potencialno lahko imele določen podatek. Druga kategorija pa zajema pridobivanje podatkov s tehničnimi sredstvi – SIGINT, pri čemer se uporablja tehnika za prestrezanje podatkov, ki se producirajo s pomočjo informacijske tehnologije. Najpogosteje je to prisluškovanje telefonskim napravam in prestrezanje podatkovnega prometa na internetu, kot so pogovori, elektronska pošta, zgodovina brskanja in prenos datotek. S pojavom interneta in kasneje socialnih omrežij se je začela uporaba podatkovnega rudarjenja, s katerim se zbira, obdeluje in analizira velike količine podatkov na internetu, ki jih lahko izvaja samo napreden računalnik s specializirano programsko opremo. V tem elementu med varnostnimi službami v ZDA prednjačita predvsem Urad za domovinsko varnost in Nacionalna varnostna agencija.

Varnostno-obveščevalne službe se poslužujejo nadzora socialnih omrežij zaradi dejstva, ker kriminalci uporabljajo te platforme za komuniciranje in kot prostor za izmenjavo informacij. Ta metoda komuniciranja predstavlja bolj konspirativno komunikacijo kot pa srečanja v resničnem življenju. Z uporabo informacijske tehnologije se kriminalci poskušajo izogniti nadzoru države in njenih varnostnih organov, kar povzroča, da varnostni organi ravno zaradi tega dejstva izvajajo nadzor nad socialnimi omrežji in drugimi internetnimi platformami za izmenjavo informacij. Leta 2002 je Urad za informiranje (angl. *Information Awareness Office*) Agencije za napredne obrambne analize DARPA (angl. *Defense Advanced Research Projects Agency*) v okviru enega od svojih številnih projektov sprejel cilj, da ustvari podatkovno bazo vseh državljanov in drugih oseb na ozemlju ZDA s podatki, pridobljenimi na spletu in v resničnem življenju, na osnovi katerih bi lahko predvideli grožnje nacionalni varnosti. Zaradi kritik in pritiskov javnosti ter medijev so program v roku enega leta ustavili (Kte'pi, 2014, str. 410–412).

Orodja za spremljanje socialnih omrežij med drugim omogočajo geografsko sledenje komuniciranju, ugotovijo lahko razmerja med uporabniki in odkrijejo družbena omrežja, v

katerih je posameznik aktiven, ter s kom se druži. Prek teh orodij je omogočeno spremljanje protestov, identificiranje voditeljev političnih in družbenih gibanj in merjenje vpliva posameznih ljudi. Do neke mere ta orodja omogočajo tudi napoved prihodnosti ter zaznavanje groženj in manipulacij javnega mnenja. Če povzamemo vse zgoraj navedeno, se ta orodja lahko uporabljajo za nadzor in ustvarjanje prihodnosti sveta (McCullough, 2016). Kot trdi Van Puyvelde (2014, str. 426), so nekateri strokovnjaki prepričani, da bi boljše razumevanje delovanja in potencialov socialnih omrežij lahko pomagalo obveščevalnim službam predvideti Arabsko pomlad, ki se je začela leta 2011.

Dilema med varnostjo in zasebnostjo je v informacijski dobi privedla do nove dileme, ki se je začela pojavljati po terorističnem napadu v San Bernardinu, ko je Apple zavrnil zahtevo, da preiskovalcem in FBI dovoli dostop do podatkov na napadalčevem telefonu. V politiki se je odprl diskurz o tem, da bi bilo treba uvesti regulacijo šifriranja, ki bi omogočala, da lahko država oziroma njeni varnostni organi kljub določeni stopnji šifriranja dostopajo do podatkov. Ponudniki socialnih omrežij in pametnih telefonov zagovarjajo stališče, da bi takšen univerzalni ključ šifriranja, ki bi dopustil določen dostop do podatkov uporabnikov, lahko izrabljale tako zahodne vlade kot vlade nedemokratičnih držav ter različni hekerji (Yadron, 2016a). Obveščevalne službe težijo k temu, da bi podjetja v svoje šifriranje dodale ključ, prek katerega bi agencije imele dostop do podatkov. Svoje stališče utemeljujejo z razlago, da je to potrebno za boj proti terorizmu, mednarodnemu organiziranemu kriminalu in pedofiliji (MacAskill, 2016). Nekdanji direktor FBI James Comey je izpostavil, da je za uspešen boj proti terorizmu nujno treba urediti dostop do šifriranih sporočil, ki naj bi jih omogočili ponudniki socialnih omrežij in programov za izmenjavo sporočil. Podjetja pa se dobro zavedajo, da bi dopuščanje dostopa do uporabnikovih šifriranih podatkov ljudi odvrnilo od uporabe njihovih produktov, ki jih uporabljajo ravno zaradi šifrirnih metod, s katerimi lahko varujejo svojo zasebnost (Thielman, 2016).

FBI se nagiba k temu, da bi se zakoni, ki opredeljujejo pridobivanje telefonskih podatkov, spremenili v tolikšni meri, da bi dovoljevali tudi dostop do podatkov zgodovine spletnih brskalnikov, podatkov o lokacijah in nekatere evidence elektronske pošte brez odobritve sodnika z uporabo t. i. pisma nacionalne varnosti, ki omogoča pridobivanje podatkov brez odobritve sodne veje oblasti. Facebook, Google in Yahoo so se ostro odzvali na takšne zahteve, ker je po njihovem mnenju že sedaj vse preveč zahtevkov po podatkih z uporabo pisem nacionalne varnosti. To pa pomeni, da je premalo nadzora sodnih organov nad takšnim početjem (Yadron, 2016b).

Ameriško podjetje Dataminr, ki se ukvarja z razvojem analitičnih programov, ima razvita orodja za analizo javnih podatkov na Twitterju v realnem času. Podjetje je prodajalo podatke, ki so bili pridobljeni na Twitterju, državnim organom, predvsem FBI in Cii. Ko so pri Twitterju za to izvedeli, so preprečili nadaljnje posredovanje podatkov, saj so onemogočili dostop tretjim osebam, v tem primeru podjetju Dataminr, da bi še naprej prodajalo takšne podatke državnim organom. Podatki s Twitterja so še naprej dostopni zasebnim podjetjem, kot so medijske agencije in finančnoanalitična podjetja. Kljub izjavam predstavnikov podjetja, da je poslovno sodelovanje z državnimi institucijami dovoljeno, če ne gre za zlorabo podatkov za nadzor, ohranjajo stike z Uradom za domovinsko varnost (Yadron, 2016c).

Direktor Nacionalnega obveščevalnega urada ZDA je v svoji izjavi izpostavil, da internet predstavlja nepredstavljivo orodje v rokah obveščevalnih služb in države. S tem pa bi država v prihodnosti lahko uporabljala internet za svoje dejavnosti, kot so identifikacija, nadzor, spremljanje in sledenje. Nove pametne naprave, ki se počasi že uvajajo v vsakdanjo rabo in so povezane na internet, imajo zmogljivosti, ki bi jih obveščevalne službe lahko izkoriščale za svoje delovanje (Ackerman in Thielman, 2016).

Vse več varnostnih organov uporablja sofisticirana sredstva za spremljanje uporabnikov na socialnih omrežjih. V ZDA se takšnih pristopov poslužujejo federalne službe, med katerimi so NSA, ministrstvo za obrambo, Urad za domovinsko varnost in celo Notranja davčna služba (IRS), ki so vključene v razvoj in uporabo programov in orodij, s katerimi sledijo državljanom na spletu (Rosen, 2012). V poročilu, ki ga je izdal oddelek ministrstva za pravosodje ZDA in se ukvarja z računalniškim kriminalom ter intelektualno lastnino, vključuje priporočila, kako uporabljati socialna omrežja za zbiranje dokazov, ki bi lahko bili uporabljeni ali bi bili vsaj v pomoč pri preiskavah. V njem je navedeno, da se do informacij lahko pride na tri osnovne načine. Prvi je dostop do informacij, ki so javno objavljene in vidne na socialnih omrežjih, drugi predstavlja zakonske vzvode, ki se jih lahko uporabi za pridobitev določenih informacij od ponudnikov, tretji pa omenja prikrite operacije (Lynch in Ellickson, 2010). Gre za ustvarjanje lažnih profilov, prek katerih se vzpostavi stik s tarčo in pride do informacij, ki niso javno objavljene (Rosen, 2012). Dokazi, ki se lahko zberejo s takšnimi metodami, so osebne komunikacije, motivi in osebna razmerja, podatki o lokacijah, potrjen ali ovrženi alibi, kriminal in organizirani kriminal (Lynch in Ellickson, 2010).

Ministrstvo za obrambo je Agenciji za napredne obrambne analize DARPA namenilo 42 milijonov dolarjev za razvoj programa Social Media Strategic Communications (SMISC), cilj

katerega je razvoj orodja, s katerim bi na socialnih omrežjih zbirali in filtrirati informacije. Projekt ima zastavljene štiri cilje (Rosen, 2012):

1. zaznati, klasificirati in meriti nastanek idej, konceptov in skrivnih sporočil na socialnih omrežjih,
2. določiti strukturo kampanje in vpliva posameznih strani na socialnih omrežjih in identificirati skupnost, ki kampanjo ustvarja,
3. identificirati udeležence in namero pri vodenju kampanje socialnih medijev za prepričevanje in merjenje njihovega učinka,
4. razviti učinkovit odziv na ugotovljeno kampanjo proti sovražniku.

FBI se nagiba k programom, s katerimi bi lahko spremljali dejavnost posameznikov na socialnih omrežjih. Težijo k razvoju orodij, ki bi imela sposobnost hitrega zbiranja kritičnih javno dostopnih podatkov in obveščevalnih informacij in ki bi znala hitro varnostno preveriti, prepoznati in ugotoviti lokacijske podatke o prelomnih dogodkih, incidentih in nastajajočih grožnjah. Njihove zahteve glede programa vključujejo tudi geografski prikaz v realnem času in takojšnje formuliranje obveščevalnih informacij po 5K-analizi[4] specifičnih groženj in incidentov. Dokončen cilj ni samo odkriti obstoječe grožnje, ampak na podlagi zbranih informacij predvideti dogodke v prihodnosti. Po mnenju FBI bodo socialna omrežja postala ključni del v obveščevalni analitiki. Njihovo delo naj ne bi bilo usmerjeno na posameznika in skupine, ampak na dogodke in krize ter dejavnosti, ki kršijo zvezne zakone in ogrožajo nacionalno varnost (Rosen, 2012).

Urad za domovinsko varnost pri svojem delu spremlja točno določene besede. V letu 2012 so imeli na seznamu 390 besed. Nadzor se izvaja na spletnih platformah Facebook, Twitter, Flickr, YouTube in Linkedln. Na enem od zaslišanj predstavnikov Urada za domovinsko varnost pred senatnim odborom je prišlo do ugotovitve, da urad nima točno določenih ciljev, zakaj uporablja nadzor nad socialnimi omrežji, kako se zbrane informacije uporabljajo in ali se bodo delile z drugimi agencijami. Predstavniki so vztrajali, da se zbrani podatki uporabljajo izključno za potrjevanje informacij in da se podatki o ljudeh ne zbirajo. Prav tako naj bi se osebni podatki posameznikov redno brisali z njihovih strežnikov. Na zaslišanju je bilo kasneje razkrito, da Urad za domovinsko varnost spremlja določene ljudi, ki pripadajo skupinam s

[4] Kdaj, kje, kdo, kaj, zakaj.

skupnimi nazori in prepričanji, ki so bile takrat aktivne v civilni iniciativi, v kateri so nasprotovali preselitvi zapornikov iz Guantanama v zapor v njihovi bližini (Rosen, 2012).

V ZDA je Urad za domovinsko varnost kot odgovor na vse večjo uporabo socialnih omrežij med ljudmi uvedel program, ki se je osredotočal zgolj na nadzor in pridobivanje podatkov s socialnih omrežij, ki pomenijo grožnjo nacionalni varnosti in terorizem. S pričetkom programa leta 2010 so prve naloge obsegale nadzor nad tremi dogodki, izvajale pa so se z uporabo podatkov, pridobljenih na Facebooku in Twitterju. Ti trije dogodki so bili potres na Haitiju, zimske olimpijske igre v Vancouvru in nesreča izlitja na naftni ploščadi Deepwater Horizon. Obseg virov se je zatem povečal še na ostale javno dostopne vire na internetu, kot so spletne strani, forumi itn. Program, ki ga uporabljajo, v osnovi deluje na podlagi iskanja ključnih besed, s pomočjo katerih iskalnik loči potencialno zanimive objave od tistih, ki imajo povsem drugačno tematiko. Iskanje je splošno in ni ciljno orientirano na posamezno osebo, poleg tega uporabljajo javno dostopne podatke, zato Urad za domovinsko varnost meni, da s tem ne kršijo zakonov o zasebnosti (Glassco, 2014, str. 372–374).

Facebook in Instagram sta marca 2017 spremenila pogoje uporabe in varstvo zasebnosti, ko sta razvijalcem tretjih programov onemogočila razvoj določenih funkcij, ki jih je uporabljala policija pri vohunjenju za aktivisti in protestniki. Programi so omogočali, da so se lahko podatki, pridobljeni na socialnih omrežjih, uporabljali za nadzor nad posamezniki. Med temi orodji najbolj izstopa program Geofeedia, ki lahko na poljubno izbrani lokaciji prikaže in filtrira dejavnost uporabnikov na socialnih omrežjih na določenem geografskem področju. Tako je policija to orodje med drugim uporabljala tudi za nadzorovanje protestov Black Lives Matter (Levin, 2017).

Ekstremistične skupine uporabljajo internet za širjenje svojih radikalnih idej ločevanja ljudi glede na raso, religijo, spol in spolno usmerjenost. V osnovi uporabljajo internet in socialna omrežja kot orodje za javno izražanje svojih stališč, pridobivanje denarja z donacijami in večanje članstva z novačenjem novih posameznikov, ki se poistovetijo z idejami, ki jih skupina zagovarja. Internet tem skupinam omogoča povezavo in komunikacijo, ki presega geografske prepreke ter omogoča določeno zasebnost in anonimnost, ki sta potrebni pri širjenju radikalnih idej, ki odstopajo od splošnih družbenih norm (Bell, 2014, str. 622).

Socialna omrežja so postala ključna komponenta pri komuniciranju terorističnih organizacij. S pomočjo teh platform teroristi razširjajo svojo propagando, pridobivajo nove člane in zbirajo podatke v fazi pripravljanja terorističnih napadov. Prosto dostopna in brezplačna tehnologija

ponuja terorističnim skupinam učinkovit mehanizem distribucije njihove filozofije in sporočil na globalni ravni, kar zmanjšuje potrebo po množičnih medijih kot medijih prenosa njihovega sporočila (Lawson, 2014, str. 1248).

Velike količine podatkov, ki se nahajajo v bazah podatkov platform socialnih omrežij predstavljajo različne probleme in izzive, s katerimi se spopadajo varnostno-obveščevalne službe. Pri svojem delu morajo ločiti bistveno od nebistvenega, da iz vseh podatkov pridobijo informacijo, ki so potrebujejo. Na socialnih omrežjih ljudje objavljajo veliko pomembnih osebnih podatkov. Ta pojav na novo definira meje med zasebno in javno sfero našega življenja. Družbena evolucija bo tako privedla do vse večjih želja in potreb države in njenih tajnih služb, da nadzorujejo dejavnosti posameznika na internetu (Van Puyvelde, 2014, str. 426).

6.3 Drugi državni organi

Facebook je leta 2014 začel objavljati statistiko, koliko zahtev za odstop podatkov so prejeli od državnih organov. Trend, ki se pojavlja, je vsakoletno povečanje teh zahtev. Tako je leta 2014 Facebook prejel 35.051 prošenj, leta 2015 pa kar 41.214, kar je 18 % povečanje. Večina prošenj, ki jih nanje naslovijo varnostni organi posameznih držav, se nanaša na kriminalna dejanja, kot so ropi in ugrabitve. Podatki, ki jih po navadi želijo, se nanašajo na osnovne informacije o določenih uporabnikih, IP-naslovi ali posamezne vsebine, ki jih uporabniki objavljajo. Večina teh prošenj, 60 %, podajo varnostni organi ZDA. Tako so leta 2014 izdali 21.731 zahtev, naslednje leto pa 26.579. Ostale države, ki imajo prav tako večje število zahtevkov, so Francija, Nemčija in Velika Britanija. Tudi pri teh državah je opazno povečano število zahtevkov v primerjavi s prejšnjim letom. V Nemčiji se je največ zahtev navezovalo na zanikanje holokavsta, ki je v tej državi kaznivo dejanje. V zvezi s kršenjem lokalnih zakonov sta največ zahtev podali Turčija (4496) in Indija (15.155). Ob predstavitvi statistike je Facebook izrecno izjavil, da podjetje ne omogoča neposrednih dostopov, prek katerih bi državne varnostne agencije lahko dostopale do podatkov, ki jih hranijo na svojih strežnikih (The Guardian, 2015).

Propaganda se na socialnih omrežjih uporablja za manipulacijo javnega mnenja po vsem svetu. T. i . bot računi umetno zvišujejo popularnost določenih informacij in objav ter povečujejo število všečkov in omenjanje objav, s tem pa vključujejo prave uporabnike v

debate in aktivno sodelovanje. Iluzija spletne podpore določenega političnega kandidata lahko privede do resnične podpore skozi učinek *bandwagoning*. Znana je uporaba propagande prek socialnih omrežij v Ruski federaciji, kjer je vlada že specializirala službe za takšno delo. Na ta način ohranjajo notranjo podporo trenutni vladi in onemogočajo politično opozicijo. Takšne pristope in taktike naj bi uspešno uporabili tudi v zunanjih zadevah, predvsem pri domnevnem vplivanju Rusije na volitve v ZDA in Franciji. Samuel Wooley trdi, da je Rusija najboljši primer, kako lahko določen močni avtoritarni režim uporablja socialna omrežja za nadzor nad ljudmi. Testno območje, kjer izpopolnjuje in raziskuje uporabo socialnih omrežij za propagando, je Ukrajina, kjer Rusija v medsebojnem konfliktu uporablja koncept hibridnega bojevanja, katerega pomemben del je tudi psihološka vojna, ki se v tem primeru izvaja s pomočjo spleta in socialnih omrežij. Širjenje dezinformacij je torej ključno,ko gre za uporabo socialnih omrežij v sestavinah novodobnih vojn (Hern, 2017).

ZDA so pričele zbirati uporabniška imena prosilcev za izdajo vize, razlog, s katerim opravičujejo to ravnanje, pa je potencialna grožnja terorizma. Spletni obrazec za izdajo vize ESTA (angl. *Electronic System for Travel Authorization*), ki ga morajo izpolniti državljani določenih držav pri vstopu v ZDA, zahteva navedbo računov, ki jih ima prosilec na socialnih omrežjih. Tako je treba napisati uporabniško ime za Facebook, Twitter, Google+, Instagram, LinkedIn in YouTube. Kritiki in predvsem organizacije, ki se borijo za človekove pravice in zasebnost, so ostro kritizirali takšen pristop, saj naj bi predstavljal vdor v zasebnost, poleg tega pa bi državne institucije razpolagale z velikimi količinami podatkov o posamezni osebi, kot so posameznikova mnenja, prepričanja, politična usmerjenost, identiteta in njegov socialni krog. ZDA na leto izda okrog 10 milijonov viz, leta 2015 pa je v ZDA pripotovalo 77,5 milijona ljudi. Zbiranje računov socialnih omrežij teh ljudi bi ustvarilo eno največjih podatkovnih baz, s katerimi razpolagajo državne institucije (Helmore, 2016).

Na ameriških letališčih se lahko pri vstopu v državo od tujih državljanov zahteva vpogled v njihov pametni telefon, kjer se med drugim pregleda tudi dejavnost na socialnih omrežjih. Takšnih primerov so v letu 2015 našteli okoli 5000, v letu 2016 pa kar 25.000. Vse to se opravi brez sodnega naloga. Če oseba zahtevo zavrne in noče predati telefona, je lahko pridržana ali pa se ji prepove vstop v državo (Solon, 2017).

Britanska premierka Theresa May je na srečanju G7 maja 2017 pozvala prisotne voditelje, naj države pritisnejo na ponudnike družbenih omrežij, da se ti bolj ostro odzovejo na ekstremistične objave. Njeni predlogi so bili med drugimi, naj države prisilijo podjetja k

ureditvi pogojev in smernic, ki natančno določajo, kaj so škodljive vsebine, ter naj podjetja razvijejo orodja, ki lahko samodejno prepoznajo in odstranijo škodljive vsebine in o njih nemudoma poročajo državnim organom pregona, da lahko sprožijo ustrezne postopke (Asthana, 2017).

Švicarsko sodišče je v eni od obravnav izreklo denarno kazen osebi, ki je na Facebooku všečkala komentar drugega uporabnika. Sodišče je ugotovilo, da gre za žaljive komentarje proti osebi, ki je vložila tožbo, in odločilo, da všečkanje pomeni, da posamezna oseba podpira takšen komentar. Izrek kazni za osebe, ki so objavili žaljive komentarje, ni nekaj novega, saj socialna omrežja veljajo za javne forume. Kar je novo pri tej sodbi, je to, da so všečkanje izenačili z objavo komentarja, s tem pa postavili precedens (The Guardian, 2017).

Avstralske zvezne vladne službe uporabljajo zunanja podjetja, da za njih opravljajo različne nadzorstvene dejavnosti nad posameznimi državljani. V teh primerih gre večinoma za ugotavljanje upravičenosti posameznih državljanov do raznih socialnih pomoči in bonitet. Med informacijami, ki se uporabljajo za takšne ugotovitve, so tudi internetne dejavnosti obravnavanih oseb in njihovo obnašanje na socialnih omrežjih. Zanimiv je primer, v katerem so z uporabo in pregledom Twitterjevega računa dotičnih dveh oseb ugotovili, da se dejansko stanje ne sklada s stanjem, ki sta ga osebi navedli v prošnji za socialno pomoč. Šlo je za par, ki je trdil, da ne živi skupaj, ter da moški in ženska nista v razmerju. Podala sta prošnji za dodatek za samohranilca. Na podlagi informacij, zbranih prek Twitterja, kjer je par skupaj objavljal družinske slike, in objavljenih komentarjev, ki so nedvoumno kazali na to, da gre za družino, so pristojne službe prišle do dokazov, s katerimi so lahko ovrgli njuno prošnjo. Po navedbah naj bi z uporabo takšnih metod država samo na podlagi socialne pomoči prihranila dva milijona avstralskih dolarjev (Farell, 2016).

Ameriški IRS je pri svojem delu začel uporabljati socialna omrežja okrog leta 2009, ko je pričel z načrtnim usposabljanjem svojih zaposlenih o delovanju socialnih omrežij. Pri delu najpogosteje spremljajo dogajanje na Facebooku, Googlu, Twitterju, MySpacu, YouTubu in Second Lifu (Rosen, 2012).

7 SINTEZA IN ZAKLJUČEK

1. Država in njeni organi pri pridobivanju podatkov na socialnih omrežjih, ki so javno dostopni, ne kršijo ustave in drugih zakonskih določb, kar bi lahko imelo za posledico kršenje človekovih pravic. Pri izvajanju svojih dejavnosti uporabljajo razne prijeme in vzvode, s katerimi izrabljajo pravne praznine v zakonodaji in predpisih, kar jim omogoča, da so nekatera njihova dejanja še vedno v skladu z zakoni. Po drugi strani pa so sprejeti zakoni napisani na način, da v točno določenih primerih (izredna stanja, teroristični napadi) dopuščajo ekstremne prijeme, s katerimi se določeni osebi zavestno krši njene pravice in omogoča vstop v njihovo zasebnost.

2. V moderni državi so tajne službe najpomembnejša vladna služba, ki opravlja različne funkcije, med katerimi je na prvem mestu zagotavljanje nacionalne varnosti. V zahodnem svetu je večina varnostno-obveščevalnih služb neposredno podrejena vladi ali pa vključena v eno od državotvornih ministrstev (vojaške obveščevalne službe praviloma delujejo v okviru ministrstva za obrambo in oborožene sile). Prednostne naloge teh služb so zbiranje, vrednotenje, analiziranje in posredovanje informacij. Pri zbiranju se poslužuje vseh možnih načinov pridobivanja podatkov, ki so v okviru obstoječe zakonodaje. Tako je dejavnost tajnih služb v demokratičnih državah podvržena sodnemu in parlamentarnemu nadzoru, ki skrbi za zakonitost delovanja. Varnostno-obveščevalne službe lahko neomejeno pridobivajo podatke o uporabnikih socialnih omrežij, dokler gre za podatke, ki so javno dostopni. Za pridobitev drugih podatkov, s katerimi razpolaga platforma, kot je na primer zasebna korespondenca med dvema ali več uporabniki, pa je treba dosledno upoštevati pravne predpise, ki urejajo to področje. Tako je potreben sodni poziv za odstop podatkov.

3. Ena od temeljnih idej interneta in kasneje socialnih omrežij je bila njihova neodvisnost. V praksi pa je internet podvržen raznim regulacijam države. Regulacija in cenzura interneta še posebej prideta do izraza v nedemokratičnih državah, kjer se izvaja dosleden nadzor nad svetovnim spletom. Vlade teh držav želijo preprečiti širjenje informacij po socialnih omrežjih, zato uvajajo nadzor nad internetom in onemogočajo dostop do platform socialnih omrežij. Prepoved in regulacija interneta pa se v nedemokratičnih državah ne dogajata samo v času revolucij in izrednih razmer, ki bi lahko ogrozile moč njihovih vladajočih struktur, ampak se v teh državah dostop do določenih spletnih vsebin preprečuje neprestano. Iz političnih razlogov

je dostop do socialnih omrežij najbolj onemogočen v Ljudski republiki Kitajski, Egiptu, Iranu, Severni Koreji, Savdski Arabiji in Siriji. Nadzor nad internetom in socialnimi omrežji lahko enačimo z državno cenzuro v medijih in uporabo propagande v nedemokratičnih državah (O'Brien, 2014, str. 325–328). V demokratičnih državah se izvaja t. i. pozitivna cenzura, kjer naj bi se cenzurirale družbeno škodljive vsebine, kot so ekstremistična propaganda, sovražni govor in otroška pornografija. Ker te teme niso dosledno določene, se kaj hitro lahko zgodi, da platforma ali država uvedeta cenzuro nad vsebinami, ki jih imata za grožnjo svoji filozofiji in politiki. Tudi lažne novice so postale orožje v rokah države pa tudi medijev, ki jih lahko uporabljajo za vplivanje na ljudi in ustvarjanje javnega mnenja.

4. V zadnjih letih je v javnem diskurzu velik pomen pridobila tema o izvajanju nadzora nad državljani s strani države, ki nadzor izvaja s pomočjo informacijske tehnologije. Razkritja Wikileaksa in nekdanjega pogodbenega delavca NSA Edwarda Snowdna o programih množičnega nadzorstva so samo še povečala debato o vstopanju države in njenih tajnih služb v zasebnost in vsakdanje življenje posameznikov. Ljudje so zaradi potencialnega nadzora nad njimi do neke mere postali nezaupljivi do uporabe socialnih omrežij, vendar število aktivnih uporabnikov socialnih omrežij kaže na vsakoletno povečanje uporabnikov in uporabe storitev. Uporabniki se samostojno odločajo o uporabi socialnih omrežij, torej lahko v primerih, ko bi šlo za izvajanje zastraševanja s strani države, preprosto prenehajo uporabljati te storitve.

5. Uporabniki socialnih omrežij prostovoljno predajajo in objavljajo svoje osebne in druge podatke ter tako sami omogočajo njihovo obdelavo tako s strani platform kot države in njenih institucij. Ponudniki socialnih omrežij imajo v svojih pogojih uporabe natančno določeno politiko o tem, katere pravice si lastijo za obdelavo in posredovanje podatkov njihovih uporabnikov. S pravnega vidika se posamezniki z registracijo na njihovih storitvah strinjajo s tem početjem. Platforme se poslužujejo aktivne participacije pri odkrivanju spornih vsebin in od uporabnikov pričakujejo, da bodo s prijavljanjem spornih vsebin vključeni v proces izvajanja pozitivne cenzure.

Primerjava izrabe socialnih omrežij s strani države za namene izvajanja nadzora nad prebivalstvom s klasičnim modelom policijske države, ki je opredeljen v tej nalogi, kaže na ugotovitve, da ne gre za policijsko državo, kot smo ji bili priča v preteklosti. Vsekakor pa obstajajo določene vzporednice in predvsem tehnološki potencial, ki bi sčasoma v določenih pogojih in radikalnih spremembah družbenega stanja privedel do vzpostavitve novega

koncepta moderne globalne policijske države ali z drugimi besedami globalne nadzorovane družbe.

Na podlagi raziskovanja, analize in ugotovitev v tem delu lahko zastavljeno hipotezo "Zbiranje in uporaba osebnih podatkov uporabnikov socialnih omrežij v obveščevalne namene poleg vdora v posameznikovo zasebnost prinaša tudi popoln nadzor nad uporabniki, kar vodi v policijsko državo" ovržem. Kljub temu da prvi del hipoteze drži, torej da zbiranje in izraba osebnih podatkov na socialnih omrežjih pomeni vdor države v posameznikovo zasebnost, nisem uspel potrditi drugega dela hipoteze. Uporaba socialnih omrežij s strani tajnih služb namreč ne pomeni popolnega nadzora nad uporabniki, saj podatki, do katerih lahko dostopajo, ne omogočajo nenehnega nadzora. Veliko ljudi tudi ne uporablja socialnih omrežij, torej bi potencialno lahko bil nadzorovan samo določen del družbe. To dejstvo se kaže tudi v trditvi, da prej omenjene dejavnosti vodijo v policijsko državo. Na podlagi zgodovinske analize policijskih držav in izdelave teoretičnega modela policijske države je bilo dokazano, da v primeru izrabe socialnih omrežij s strani države ne moremo govoriti o t. i. klasični policijski državi.

Izvajanja nadzora prek socialnih omrežij tako ne moremo enačiti s tradicionalnim konceptom policijske države, saj se med drugim razlikuje že v kategoriji teritorialne omejenosti oziroma neomejenosti v času globalizacije in tehnoloških inovacij. Če so bili v klasičnih policijskih državah nadzorovani državljani posamezne države, se v današnjem primeru dogaja, da je potencialno nadzorovan ves svet. Vendar trenutna praksa kaže, da večina držav in njihove varnostno-obveščevalne službe zaradi omejenosti virov izvajajo metode SOCMINT izključno na taktični ravni. Torej nadzirajo samo osebe, ki jih operativno obravnavajo v okviru zagotavljanja nacionalne varnosti. Če pa govorimo o strateški ravni izvajanja nadzora, država potrebuje napredno tehnologijo in druge vire, ki bi ji omogočali neprestano izvajanje nadzora nad vsemi osebami na določenem teritoriju ali globalni ravni. V prihodnosti bi lahko prišlo do vzpostavitve globalne policijske države in predpostavka, da vsa največja podjetja, ki upravljajo s socialnimi omrežji, izvirajo iz ene države, vodi v hegemonsko ureditev pri izvajanju globalnega nadzora.

Ljudje ugotavljajo, da jim socialna omrežja omogočajo uživanje ugodnosti, zaradi katerih te platforme hitro vključijo v svoje vsakdanje življenje (Manning, 2014a, str. 1153). Naraščajoča uporaba in pomembnost uporabe socialnih omrežij v 21. stol. še bolj odpirata vprašanje, ki se že vrsto let pojavlja v javnih razpravah, tj. nasprotje med nacionalno varnostjo in zasebnostjo

posameznika. Socialna omrežja so postala pomemben vir informacij za obveščevalne službe, ki iščejo podatke o potencialnih terorističnih organizacijah in političnih trendih v tujih državah. "Socialna omrežja nadaljujejo svojo integracijo v posameznikov zasebni in poslovni del življenja, postajajo manj vidna in vse bolj pričakovana" (Manning, 2014b, str. 1158). Razvoj naslednje ravni interneta, ki ga nekateri imenujejo internet stvari, bo prinesel medsebojno povezanost vseh naprav, ki jih ljudje uporabljajo v vsakdanjem življenju. Dostop do teh podatkov in združevanje z drugimi podatki, kot so npr. bančni izpiski, nadzorne kamere na javnih površinah, zdravstvene kartoteke itd., ter njihovo izrabljanje v politične namene lahko hitro preraste v spremembo svetovne ureditve v orwellovsko družbo.

8 VIRI

1. Ackerman, S. in Thielman, S. (2016, 9. februar). US intelligence chief: we might use the internet of things to spy on you. *The Guardian*. Dostopno prek https://www.theguardian. com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

2. Allen, R. (2017, 6. februar). What happens online in 60 seconds? *Smarth Insights*. Dostopno prek https://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/

3. *Alpha history*. (2015). Dostopno prek http://alphahistory.com/russianrevolution/cheka/

4. Arendt, H. (1962). *The origins of totalitarianism*. Cleveland: The World Publishing Company.

5. Asthana, A. (2017, 25. maj). Theresa May calls on tech firms to lead fight against online extremism. *The Guardian*. Dostopno prek https://www.theguardian.com/politics/2017/may/25/theresa-may-calls-on-tech-giants-to-lead-fight-against-online-extremism

6. Ayçoberry, P. (1999). *The social history of the Third Reich, 1933–1945*. New York: The New Press.

7. Barnes, J. E. (2014, 6. avgust). U.S. Military plugs into social media for intelligence gathering. Dostopno prek https://www.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557

8. Bell, C. V. (2014). Hate speech, online and social media. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 622–625). Thousand Oaks: Sage Publications.

9. Birdsall, C. (2012). *Nazi soundscapes: sound, technology and urban space in Germany, 1933–1945*. Amsterdam: Amsterdam University Press.

10. Blamires, C. (2006). *World fascism: a historical Encyclopedia, Volume 1*. Santa Barbara: ABC-CLIO.

11. Booth, R. (2014, 30. junij). Facebook reveals news feed experiment to control emotions. *The Guardian*. Dostopno prek https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds

12. Botes, J. (2014). Social media and conflict resolution. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 308–310). Thousand Oaks: Sage Publications.

13. Boyd, D. M. in Ellison, N. B. (2007). Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210–230.

14. Bracher, K. D. (1970). *The German dictatorship: The origins, structure, and effects of national socialism*. New York: Praeger Publishers.

15. Britt, L. (2003). *Fourteen defining characteristics of fascism*. Dostopno prek https://ratical.org/ratville/CAH/fasci14chars.html

16. Brooker, P. (2000). *Non-democratic regimes: theory, government, and politics*. New York: St. Martin's Press.

17. Browder, G. C. (2004). *Foundations of the Nazi police state: The formation of Sipo and SD*. Lexington: University Press of Kentucky.

18. Brzezinski, Z. K. (1962). *The Soviet bloc: unity and conflict*. New York: Praeger.

19. Buchheim, H. (1968). The SS – instrument of domination. V H. Krausnik (ur.), *Anatomy of the SS State* (str. 125–188). New York: Walker and Company.

20. Črnčec, D. (2009). *Obveščevalna dejavnost v informacijski dobi*. Ljubljana: Defensor.

21. Dams, C. in Stolle, M. (2014). *The Gestapo: Power and terror in the Third Reich.* New York: Oxford University Press.

22. Delarue, J. (2008). *The Gestapo: A history of horror*. New York: Skyhorse.

23. *Encyclopedia Britannica*. (2017). Dostopno prek https://www.britannica.com/

24. Etzioni, A. (2011). Communitarianism. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 326–331). Thousand Oaks: Sage Publications.

25. Evans, R. J. (2006). *The Third Reich in power*. New York: Penguin Group.

26. *Facebook*. (2017). Dostopno prek https://www.facebook.com

27. Fainsod, M. (1949). Recent developments in Soviet public administration. *The Journal of Politics, 11*(4), 679–714.

28. Farrell, P. (2016, 3. februar). Government monitoring social media accounts to hunt down welfare fraud. *The Guardian*. Dostopno prek https://www.theguardian.com/australia-news/2016/feb/03/government-monitoring-social-media-accounts-to-hunt-down-welfare

29. Fest, J. C. (2013). *Hitler*. Boston: Houghton Mifflin Harcourt.

30. Fitsanakis, J. in Bolden, M. S. (2012). Social networking as a paradigm shift in tactical intelligence collection. V E. Bertacin, S. Ducci in J. M. Nomikos (ur.), *MCIS Yearbook 2012* (str. 28–40). Atene: The Mediterranean Council for Intelligence Studies.

31. Forsberg, T. (2011). Security and defense policy. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 2374–2377). Thousand Oaks: Sage Publications.

32. Friedrich, C. J. in Brzezinski, Z. K. (1965). *Totalitarian dictatorship and autocracy*. Cambridge: Harvard University Press.

33. Fullbrook, M. (2005). *The people's state: East German society from Hitler to Honecker*. New Haven: Yale University Press.

34. Géczy, P., Noriaki, I., Koiti, H., Akira, M., Koichiro, E. in Satoshi, H. (2014). Social intelligence technologies: Menace or aid? *International Journal of Science in Society, 5*(3), 47–56.

35. Gellately, R. (1992). *The Gestapo and German society: Enforcing racial policy, 1933–1945*. New York: Oxford University Press.

36. Gentile, E. (2011). Totalitarian regimes. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 2627–2633). Thousand Oaks: Sage Publications.

37. Gerth, H. H. in Mills, W. C. (1946). *From Max Weber: Essays in sociology*. New York: Oxford University Press.

38. Glassco, D. (2014). Department of Homeland Security social media monitoring initiative. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 372–376). Thousand Oaks: Sage Publications.

39. Glick, B. (1999). *War at home: covert action against U.S. activists and what we can do about it*. Boston: South End Press.

40. *Google*. (2017). Dostopno prek https://www.google.si/

41. Helmore, E. (2016, 26. december). US government collecting social media information from foreign travelers. *The Guardian*. Dostopno prek https://www.theguardian.com/world/2016/dec/26/us-customs-social-media-foreign-travelers

42. Hern, A. (2017, 19. junij). Propaganda on Facebook and Twitter manipulating public opinion – report. *The Guardian*. Dostopno prek https://www.theguardian.com/technology/2017/jun/19/social-media-proganda-manipulating-public-opinion-bots-accounts-facebook-twitter

43. Hislop, R. in Mughan, A. (2012). *Introduction to comparative politics: The state and its challenges*. New York: Cambridge University Press.

44. Hogan, B. in Smith, M. (2011). Facebook. V G. A. Barnett (ur.), *Encyclopedia of Social Networks* (str. 283–286). Thousand Oaks: Sage Publications.

45. Horne, J. (2002). *State, society and mobilization in Europe during the First World War*. New York: Cambridge University Press.

46. Huneeus, C. (2011). Censorship. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 213–215). Thousand Oaks: Sage Publications.

47. Huskey, E. (2014). *Russian lawyers and the Soviet State: The origins and development of the Soviet Bar, 1917–193*9. New Jersey: Princeton University Press.

48. Ingrao, C. (2013). *Believe and destroy: Intellectuals in the SS war machine*. Cambridge: Polity Press.

49. *Instagram*. (2017). Dostopno prek https://www.instagram.com/

50. Jacobson, S. (2014). Facebook. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 489–492). Thousand Oaks: Sage Publications.

51. Jeffreys-Jones, R. (2008). *The FBI*. New Haven: Yale University Press.

52. Johnson, E. (1999). *Nazi terror: The Gestapo, Jews, and ordinary Germans*. New York: Basic Books.

53. Johnson, K. L. (2011). Intelligence. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 1210–1213). Thousand Oaks: Sage Publications.

54. Jalon, A. M. (2006, 8. marec). A break-in to end all break-ins. *Los Angeles Times*. Dostopno prek https://web.archive.org/web/20131203035850/http://articles.latimes.com/2006/mar/08/opinion/oe-jalon8

55. Kaplan, A. M. in Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Bussines Horizons, 53*(1), 59–68.

56. Kemp, S. (2017). *Digital in 2017: Global overview*. Dostopno prek https://wearesocial.com/special-reports/digital-in-2017-global-overview

57. Kent, S. (1966). *Strategic intelligence for American world policy*. New Jersey: Princeton University Press.

58. Kietzmann, J. H., Hermkens, K., McCarthy, I. P. in Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241–251.

59. Khlevniuk, O. V. (2015). *Stalin: New biography of a dictator*. New Haven: Yale University Press.

60. Kramer, A. D. I., Guillory, J. E. in Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788–8790.

61. Koehler, J. O. (2000). *Stasi: The untold story of the East German secret police*. Boulder: Westview Press.

62. Kovačič, M. (2003). *Zasebnost na internetu*. Ljubljana: Mirovni inštitut.

63. Koonz, C. (2005). *The Nazi conscience*. Cambridge: Belknap Press of Harvard University Press.

64. Krupovičius, A. (2011). Communist parties. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 314–320). Thousand Oaks: Sage Publications.

65. Kte'pi, B. (2014). Domestic surveillance and social media. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 410–413). Thousand Oaks: Sage Publications.

66. Larsen, S. U., Hagtvet, B. in Myklebust, J. P. (1980). *Who were the Fascists: Social roots of European fascism*. Bergen: Universitetsforlaget.

67. Laurent, S. (2011). Secret services. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 2369–2372). Thousand Oaks: Sage Publications.

68. Lazar, M. (2011). Communism. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 310–314). Thousand Oaks: Sage Publications.

69. Lawson, D. (2014). Terrorism. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 1248–1250). Thousand Oaks: Sage Publications.

70. Leterre, T. (2011). Contract theory. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 436–446). Thousand Oaks: Sage Publications.

71. Leurs, K. (2014). Platform. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 972–973). Thousand Oaks: Sage Publications.

72. Levin, S. (2017, 13. marec). Facebook and Instagram ban developers from using data for surveillance. *The Guardian*. Dostopno prek https://www.theguardian.com/technology/2017/mar/13/facebook-instagram-surveillance-privacy-data

73. Linz, J. J. (2000). *Totalitarian and authoritarian regimes*. Boulder: Lynne Rienner Publishers.

74. *LinkedIn*. (2017). Dostopno prek https://www.linkedin.com/

75. Lynch, J. in Ellickson, J. (2010). *Obtaining and using evidence from social networking sites: Facebook, MySpace, Linkedln, and more*. Washington: U. S. Department of Justice, Criminal Division. Dostopno prek https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf

76. MacAskill, E. (2016, 7. marec). GCHQ boss calls for new relationship with tech firms over encryption. *The Guardian*. Dostopno prek https://www.theguardian.com/uk-news/2016/mar/07/gchq-boss-new-relationship-tech-firms-encryption

77. Maier, C. S. (1997). *Dissolution: The crisis of communism and the end of East Germany*. Princeton: Princeton University Press.

78. Mann, M. (2004). *Fascists*. Los Angeles: University of California.

79. Manning, J. (2014a). Adoption of social media. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 1153–1155). Thousand Oaks: Sage Publications.

80. Manning, J. (2014b). Definition and classes of social media. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 1158–1161). Thousand Oaks: Sage Publications.

81. Marotta, E. in Nunzi, A. (2011). Security apparatus. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 2377–2383). Thousand Oaks: Sage Publications.

82. McCullough, K. (2016, 6. maj). Why government use of social media monitoring software is a direct threat to our liberty and privacy. *American Civil Liberties Union*. Dostopno prek https://www.aclu.org/blog/privacy-technology/surveillance-technologies/ why-government-use-social-media-monitoring?redirect=blog/speak-freely/why-government-use-social-media-monitoring-software-direct-threat-our-liberty-and

83. McNab, C. (2009). *The SS: 1923–1945*. London: Amber Books Ltd.

84. Murphy, L. W. (2002). *The dangers of domestic spying by feferal law enforcement: A case study on FBI surveillance of Dr. Martin Luther King.* Dostopno prek https://www.aclu.org/files/FilesPDFs/mlkreport.pdf

85. Murphy, T. (2014). Authoritarian states. V T. R. Levine (ur.), *Encyclopedia of Deception* (str. 47–51). Thousand Oaks: Sage Publications.

86. Obar, J. A. in Wildman, S. (2015). Social media definition and the governance challenge: An introduction to the special issue. *Telecommunications policy, 39*(9), 745–750.

87. Omand, D., Bartlett, J. in Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence & National Security, 27*(6), 801–823.

88. Overy, R. (2004). *The dictators: Hitler's Germany, Stalin's Russia*. London: W. W. Norton.

89. O'Brien, P. C. (2014). Countries banning social media for political reasons. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 325–328). Thousand Oaks: Sage Publications.

90. Pike, J. (1997, 26. november). Committee for state security. *Federation of American Scientists*. Dostopno prek https://fas.org/irp/world/russia/kgb/index.html

91. Poggi, G. (2011). State. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 2485–2496). Thousand Oaks: Sage Publications.

92. Pringle, R. W. (2017). KGB. *Encyclopaedia Britannica*. Dostopno prek https://www.britannica.com/topic/KGB

93. *Privacy International*. (2017). Dostopno prek https://www.privacyinternational.org/node/52

94. Richelson, J. T. (2015). *The U.S. intelligence community*. London: Routledge.

95. Rosen, D. (2012, 6. junij). 6 government surveillance programs designed to watch what you do online. *Alternet*. Dostopno prek https://www.alternet.org/story/155764/6_government_surveillance_programs_designed_to_watch_what_you_do_online

96. Rosenberg, S. (2007, 25. maj). Computers to solve Stasi puzzle. *BBC*. Dostopno prek http://news.bbc.co.uk/2/hi/europe/6692895.stm

97. Rees, L. (1997). *The Nazis: A warning from history*. New York: New Press.

98. *Rusnet*. (2017). Dostopno prek http://www.rusnet.nl/encyclo/k/kgb.shtml

99. Rychard, A. (2011). Communist systems. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 320–325). Thousand Oaks: Sage Publications.

100. Schmid, G. (2001). *Report on the existence of a global system fort he interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*. Bruselj: Evropski parlament. Dostopno prek http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

101. Siaroff, A. (2011). Regime (comparative politics). V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 2233–2237). Thousand Oaks: Sage Publications.

102. Snyder, L. (1994). *Encyclopedia of the Third Reich*. Boston: Da Capo Press.

103. Solon, O. (2017, 31. marec). US border agents are doing 'digital strip searches'. Here's how to protect yourself. *The Guardian*. Dostopno prek https://www.theguardian.com/us-news/2017/mar/31/us-border-phone-computer-searches-how-to-protect

104. *Sprotni slovar slovenskega jezika*. (2017). Dostopno prek http://www.fran.si/

105. *Statista*. (2017). Dostopno prek https://www.statista.com/

106. Swearingen, W. M. (1995). *FBI secrets: An agent's expose*. Boston: South End Press.

107. *Tech Terms*. (2013). Dostopno prek https://techterms.com/

108. Tindall, D. B. (2014). Digital activists and activism. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 2–10). Thousand Oaks: Sage Publications.

109. *The Columbia Encyclopedia*. (2017). Dostopno prek https://www.encyclopedia. com/

110. *The Guardian*. (2016, 12. november). Facebook says governments demanding more and more user data. Dostopno prek https://www.theguardian.com/world/2015/nov/12/facebook-says-governments-seek-more-and-more-user-data-and-takedowns

111. *The Guardian*. (2017, 30. maj). Man fined by Swiss court for 'liking' defamatory comments on Facebook. Dostopno prek https://www.theguardian.com/technology/2017/may/30/man-fined-swiss-court-liking-defamatory-comments-facebook

112. Thielman, S. (2016, 9. december). FBI head: terror fight requires open backdoors to encrypted user data. *The Guardian*. Dostopno prek https://www.theguardian.com/us-

news/2015/dec/09/fbi-director-tech-companies-backdoors-user-data-access-counter-terrorism

113. Turner, H. A. (1975). *Reappraisals of fascism*. New York: New Viewpoints.

114. *Twitter*. (2017). Dostopno prek https://twitter.com/

115. *United States Holocaust Memorial Museum*. (2017). Dostopno prek https://www.ushmm.org/wlc/en/article.php?ModuleId=10005467

116. Van Puyvelde, D. (2014). ECHELON. V H. Kerric (ur.), *Encyclopedia of Social Media and Politics* (str. 424–426). Thousand Oaks: Sage Publications.

117. Zartman, W. I. (1995). *Collapsed states: The disintegration and restoration of legitimate authority*. Boulder: Lynne Rienner Publishers.

118. Završnik, A. (2010). Nadzorstvene študije v kulturi bajtov: kaj je "novo" nadzorovanje? V A. Završnik (ur.), *Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?* (str. 21–53). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

119. Zimmermann, E. (2011). Violence. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 2708–2711). Thousand Oaks: Sage Publications.

120. Wall, D. D. (1997). *Nazi Germany and World War II*. St. Paul: West Publishing.

121. Weber, M. (1978). *Economy and society: an outline of interpretive sociology*. Berkeley: University of California Press.

122. Weidemann, C. in Swift, J. N. (2013). Social media location intelligence: The next privacy battle - An ArcGIS add-in and analysis of geospatial data collected from Twitter.com. *International Journal of Geoinformatics*, *9*(2), 21–27.

123. Wiatr, J. J. (2011). Dictatorship. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 653–659). Thousand Oaks: Sage Publications.

124. Wolin, S. in Slusser, R. M. (1974). *The Soviet secret police*. Westport: Greenwood Press.

125. Yadron, D. (2016a, 30. junij). US efforts to regulate encryption have been flawed, government report finds. *The Guardian*. Dostopno prek https://www.theguardian.com/technology/2016/jun/29/government-encryption-regulation-report-criticism

126. Yadron, D. (2016b, 7. junij). Facebook and Google battle latest FBI attempt to expand surveillance. *The Guardian*. Dostopno prek https://www.theguardian.com/world/2016/jun/07/fbi-silicon-valley-fight-surveillance-web-browsing

127. Yadron, D. (2016c, 9. maj). Twitter bars spy agencies from buying bulk user data from analytics firm. *The Guardian*. Dostopno prek https://www.theguardian.com/technology/2016/may/09/twitter-surveillance-fbi-cia-privacy-dataminr

128. Özbudun, E. (2011). Authoritarian regimes. V D. Berg-Schlosser in B. Badie (ur.), *International Encyclopedia of Political Science* (str. 107–117). Thousand Oaks: Sage Publications.