UNIVERZITET U SARAJEVU
FAKULTET POLITIČKIH NAUKA
ODSJEK SIGURNOSNE I MIROVNE STUDIJE

„Digitalna transformacija humane sigurnosti“

-Master teza-

Kandidat:

Mirza Hindija

Broj indeksa: 854/II-SPS

Mentor:

prof. dr. Emir Vajzović

Sarajevo, august 2022. godine

Sadržaj

I METODOLOŠKI DIO RADA

Uvod

Svakim danom tehnologija napreduje i prevazilazi dosadašnje granice i tehnološke limite. Ni nauka ni tehnologija nisu statične, šta više, najbolje se razvijaju zajedno; nauka-tehnika-tehnologija. U zadnjih 20 godina svjedočimo ogromnom razvoju i ekspanziji tehnologije u oblasti računara, interneta i pametnih telefona koji su danas u suštini džepni kompjuteri. Cilj digitalizacije u osnovi jeste da olakša svakodnevni život ljudi. „Danas se preko 90% posto svjetske komunikacije na daljinu odvija preko elektronskih uređaja..“(Karahmetović, 2020:189) Digitalizacija i pojava cyber prostora tako predstavljaju ogroman društveno-tehnološki napredak koji je otvorio brojne nove mogućnosti za dalji razvoj društva. Tako se javila potreba za novom granom sigurnosti pod nazivom cyber sigurnost, i novim razumijevanjima humane sigurnosti. Sigurnost je jedno od najsloženijih područja djelovanja savremenih država. U različitim kontekstualnim uvjetima države različito pristupaju oblikovanju sigurnosnih politika i sigurnosnom upravljanju.

Sigurnosne studije, a sa time i humana sigurnost, se još uvijek nisu razvile u dovoljno koherentnu i zaokruženu naučnu disciplinu sa jasno određenim predmetom, izgrađenim teorijskim pristupima i razvijenom istraživačkom praksom, tako da proučavanje pojava koje ugrožavaju sigurnost zahtijeva široka znanja i pristupe koji prevazilaze usko disciplinarno usmerenje (Lipovac, 2013.). Teorijski napori savremenih istraživača sigurnosnih pojava se, između ostalog, odnose i na primjenu širih paradigmi opštijih nauka poput sociologije, psihologije, informatike i dr. Proces digitalne transformacije predstavlja veliki korak koji se dešava jako brzo, pri čemu mnoge ostavlja u „digitalnom raskoraku”, koji samim tim povećava nejednakost i ranjivost društva, te tako direktno utiče na njegovu sigurnost. Savremeno doba sa sobom nosi savremene izazove i rizike koji zahtijevaju drugačiji pristup od dosadašnjih tradicionalnih metoda. Pojavom savremenih prijetnji i višestrukih oblika ugrožavanja, samo poimanje humane sigurnosti više nije isto. Na osnovu činjenice da živimo okruženi digitalnim tehnologijama koje se koriste u svim aspektima ljudskog djelovanja, javila se i ambicija za istraživanjem jedne ovakve teme. Humana sigurnost kao nauka, usko je vezana za čovjeka, njegov razvoj i djelovanje, te sama po sebi pruža mogućnost izučavanja novih sigurnosnih fenomena i reakciju čovjeka na iste.

Prvi dio rada, izuzimajući uvod i teorijsko – metodološki okvir istraživanja, fokusirat će se na pojmovno određenje koncepta humane sigurnosti, njegov nastanak, razvoj, te osnovne postulate i principe.

*Drugi dio rada*odnosit će se na svjetski napredak tehnologije i nauke koji su omogućili digitalnu transformaciju društva i doveli do postepene digitalizacije humane sigurnosti. Ovaj dio rada predstavit će digitalizaciju svakodnevnog života ljudi kao bitnog činioca u sagledavanju i razumijevanju savremene humane sigurnosti.

Treći dio rada predstavit će glavne izazove za humanu sigurnost kroz analizu uticaja digitalizacije na društvene procese. U ovom dijelu rada govorit će se o zloupotrebama digitalnih tehnologija i medijsko-platformskog okruženja koje mogu izazvati veliku pometnju u digitalnom okruženju iz kojeg događaji ostvaruju snažne implikacije na realni svijet, što bi moglo dovesti u pitanje opću globalnu sigurnost, a samim time i sigurnost pojedinca.

Posljednji dio rada analizirat će odnos između digitalizacije, demokratije i sigurnosti kroz prizmu digitalnog okruženja u kojem aktivno djeluju algoritmi, umjetna inteligencija i mašinsko učenje na osnovu ogromnih baza podataka. Ti odnosi bit će sagledani i iz ugla međunarodne saradnje na pitanjima sigurnosti kroz različite vladine i nevladine međunarodne organizacije, dokumenate, regulative, strategije, konvencije i naučne studije o sigurnosti, kako bi se napravio uvid u položaj čovjeka kao referentnog objekta humanocentrične sigurnosti. Za kraj ukazat će se na važnost preventivnog djelovanja u zaštiti ljudskih prava i sloboda, te integriteta individue u digitalnom okruženju.

1. Problem i predmet istraživanja

1.1. Problem istraživanja

Problem ovog istraživanja predstavlja promjena izvora nesigurnosti kao i uloge, odnosno položaja čovjeka u savremenom digitalnom okruženju. Diskutabilno je pitanje kako te promjene utiču na humanu sigurnost, ljudska prava i slobode, te u konačnici na život dostojan čovjeka. Koristeći se metodom analize dolazimo do određenja problema istraživanja rada, a koji se može definisati kroz pitanje: "Kakve implikacije na humanu sigurnost ostvaruje novo digitalno sigurnosno okruženje?"

Digitalna transformacija društva uzrokovala je ne samo tehničko-tehnološke promjene u oblasti sigurnosti, nego i promjene u sagledavanju demokratskog diskursa kao i novih rizika, prijetnji i izvora nesigurnosti koji će biti detaljnije obrađeni u nastavku rada. Uloga čovjeka je promijenjena i od nosioca vlasti i moći u društva postao je roba resurs. Taj resurs eksploatišu i prodaju tehnološke kompanije koje od korisničkih informacija zarađuju ogromna bogatstva, te koriste iste te informacije za predviđanje i upravljanje ljudskim ponašanjem. U savremenim uvjetima sigurnosti sve je više neizvjesnosti i nepredvidivosti, što naposlijetku utiče na poteškoće u reagovanju na ugrožavanje sigurnosti.

Tehnološke kompanije ne preuzimaju odgovornost za javno mnijenje, pravdajući se da su platforme samo prostor za informacije a ne platforme za mjerenje valjanosti informacija. Tehnološke kompanije koje prikupljaju i obrađuju podatke o svakom korisniku vrše profilisanje i predviđanje budućih ponašanja u cilju monetizacije društva, bitno mijenjajući položaj čovjeka u savremenom okruženju, praveći od njega robu na kojoj profitiraju i čiju pažnju usmjeravaju u željenom smjeru, što zahtijeva poseban angažman humane sigurnosti. Ljudsko ponašanje je zbog količine podataka koja se može prikupiti i obraditi postalo predvidivo i upravljivo. Ako se to preslika na polja ekonomije, politike i medija onda to predstavlja savremenu prijetnju vrijednostima, zajednici i svakom pojedincu.

Iz ovakvih početnih postavki mogu se definisati sljedeća istraživačka pitanja:

1. Da li digitalizacija i prikupljanje podataka više doprinose ili ugrožavaju sigurnost?
2. Predstavlja li digitalizacija prednost ili prepreku humanoj sigurnosti?
3. U kojoj mjeri je percepcija sigurnosti u digitalnom okruženju podložna manipulacijama?

4. Kakve posljedice digitalizacija ostavlja na prirodno stanje društva, te psihički i mentalni razvoj čovjeka?

1.2. Predmet istraživanja

Predmet istraživanja ovog rada je uticaj jedne savremene pojave kao što je digitalizacija na nastanak potpuno novog sigurnosnog okruženja koje generiše brojne izvore nesigurnosti i predstavlja izazov za humanu sigurnost i njen zadatak da pruži sigurnost svakom pojedincu. Procesi globalizacije i tehnološkog razvoja naročito u sferi informacionih i komunikacionih tehnologija omogućili su četvrtu industrijsku revoluciju i nove mogućnosti za napredak i razvoj društvene zajednice. Digitalna transformacija i njen uticaj na svakodnevni život i razvoj društva dovela je do proširenja sigurnosnih potreba društva, kao i izvora nesigurnosti.
U novom normalnom sigurnosnom okruženju važnu ulogu u oblikovanju javnog mijenja i društvene stvarnosti imaju informacijski mediji i platformsko okruženje sa društvenim mrežama. Događaji u virtualnom svijetu, zbog enormne ekspanzije broja korisnika, mnogo brže ostvaruju implikacije na društvenu realnost. U novom sigurnosnom okruženju omogućene su masovne kampanje destabilizacije društva, cyber hibridno ratovanje, te razni oblici manipulacije društva koji ostvaruju uticaj na politiku, ekonomiju i sigurnost društva. Položaj demokratskog građanina u digitalnom okruženju uveliko ovisi o informacijskim medijima i širokom platformskom okruženju u kojem dominantnu ulogu igraju umjetna inteligencija, cyber hibridni ratovi, te medijska i informacijska pismenost. Potrebno je shvatiti da su u pitanju rizici koji ne prave razliku na osnovu nacionalnosti, bogatstva ili društvenog porijekla, već kao takvi predstavljaju prijetnju svima. Oni su ujedno lokalni i globalni, tj. glokalni. Postoji više vrsta prijetnji koje su se pojavile tokom digitalnog doba, uključujući digitalnu nejednakost, cyber hibridne napade, ugrožavanje privatnosti, zloupotrebu podataka, prevare ili krađe, digitalnu koncentraciju moći i moć društvenih mreža. Sve navedene prijetnje potencijalno ugrožavaju ljudska prava i slobode savremenog društva. Savremena sigurnost se transformira od očuvanja teritorija prema očuvanju vrijednosti, a u današnjem svijetu informacije predstavljaju ogromnu vrijednost. U magli globalizacije nestala je mogućnost kontrole a sa tim i vjera da se napredak može kontrolisati. Pojedinac je podvrgnut do sada nepoznatoj društvenoj nesigurnosti, pri tome sama raspodjela rizika između države, privrede, tehnike, nauke i ljudi je sve problematičnija, stoga humana sigurnost u budućem razvoju tehnologije ima presudnu ulogu.

1.3. Operacionalno određenje predmeta istraživanja

Bitni činioci predmeta dotičnog istraživanja su:

1. Uslovi: Glavni uslov je postojanje tehnološko-informacione infrastrukture koja omogućuje pristup umreženom svijetu i novom posmatranju humane sigurnosti.
2. Subjekti: Korisnici interneta i drugih informacionih mreža, tehnološke kompanije, organizacije, te državne institucije na čelu sa sigurnosnim sektorom.
3. Motivi, interesi i ciljevi: Zaštita temeljnih ljudskih prava, zaštita privatnosti, informacija i podataka, zaštita pojedinca u digitalnom svijetu, suzbijanje hibridnih prijetnji i ugrožavanja lične i kolektivne sigurnosti u digitalnom prostoru.
4. Aktivnosti: Sve aktivnosti koje pomažu boljem razumijevanju savremene humane sigurnosti i procesa digitalizacije, istraživanje, anketiranje lica i otklanjanje mogućih problema i nejasnoća na ovu temu.
5. Metode i sredstva: Metoda informisanja i metoda prikupljanja podataka, te metoda sređivanja i obrade podataka, razni razvojni i humanocentrični programi, planovi, strategije sigurnosti i projekti koji rade na zaštiti pojedinca i njegovog integriteta.
6. Efekti: Efekti djelovanja tiču se rezultata koji utiču na savremeno shvatanje sigurnosti i spoznaju odnosa digitalizacije, demokratije i humane sigurnosti.

1.4. Vremensko i prostorno određenje predmeta istraživanja

Vremenska odrednica predmeta istraživanja pozicionira se na period od 1994. do 2022. godine.

Prostorno određenje predmeta istraživanja, zbog pojavne specifičnosti, posmatrat će se na globalnom nivou.

1.5. Disciplinarno određenje predmeta istraživanja

Istraživanje je interdisciplinarnog karaktera iz razloga što se ova problematika odnosa enormnog napretka tehnologije i ljudske sigurnosti proučava kroz sigurnosne studije, specifičnije kroz humanu sigurnost. Stoga je u ovom istraživanju naglasak stavljen na ugrožavanje svakodnevne sigurnosti pojedinca i društva, te na zaštitu društva od ugrožavanja, prevenciju, realizaciju i disciplinarno izučavanje na akademskom polju, koja će u narednom periodu utjecati na razvijanje i unapređenje humane sigurnosti u digitalnom okruženju.

2. Ciljevi istraživanja

2.1. Spoznajni ili naučni ciljevi

S ciljem davanja što boljeg i validnijeg odgovora na društveni i sigurnosni problem vrši se naučna elaboracija pojava koje utiču na, odnosno, dovode do nove paradigme o ljudskoj sigurnosti u nauci. Istraživanje uzroka i posljedica izazvanih savremenim tehnološkim trendovima u društvima koja ostvaruje suživot sa tehnologijom. Naučna predodžba o tome u kojem smjeru se kreće digitalno-tehnološki napredak u 21.stoljeću, pokazat će promjene koje su nastale u konceptu humane sigurnosti. Kroz pisanje rada nastojat ćemo ukazati na odnos između digitalizacije i koncepta humane sigurnosti, te položaj i ulogu čovjeka u digitalnom platformskom okruženju.

2.2. Naučna deskripcija

Naučna deskripcija podrazumijeva detaljan opis manifestnih formi. U okviru ovog naučnog cilja nastoji se opisati proces digitalizacije, te njegova integracija u svakodnevni život, kao i promjene koje je unijela u posmatranje humane sigurnosti. Osim toga, istraživanje će biti usmjereno na opisivanje rada tehnoloških korporacija, državnih i međunarodnih organizacija i agencija za pružanje zaštite korisnika, te informacijsko-platformskih medija koji imaju veliku važnost u kreiranju javnog mnijenja.

3. Hipoteze i indikatori

3.1. Generalna hipoteza

Glavna hipoteza ovog rada glasi:
Tehnologija, koja se uvukla u svakodnevni život čovjeka, sa svojim potencijalom da ga oblikuje i manipuliše, duboko zadire u humanu sigurnost i ljudska prava.

3.2. Posebne hipoteze i indikatori

a) Društvo u digitalnom okruženju, zadovoljavajući svoje prirodne potrebe za informisanjem i upoznavanjem, podložno je ugrožavanju humane sigurnosti.
b) Brzina proizvodnje i lahkoća širenja neprovjerenih informacija u medijsko-platformskom okruženju onemogućuje potpunu zaštitu od iznenadnih i štetnih poremećaja svakodnevnice.
c) Ljudsko ponašanje je zbog količine podataka koja se može prikupiti i obraditi uz pomoć algoritama i umjetne inteligencije postalo predvidivo i upravljivo.
d) Percepcija, osjećaj i stanje sigurnosti u umreženom svijetu podložni su različitim informacijskim i medijskim interpretacijama stvarnosti.
e) Informacijsko-komunikacijske tehnologije su sila novog ekosistema koja utiče na našu percepciju sebe i društvenih vrijednosti, interakcije, međusobne odnose, kao i na predstavu stvarnosti i sigurnosti.
f) Zloupotreba tehnologija može biti egzistencijalna prijetnja po društvo.

g) Razvoj i podizanje nivoa medijske i informacijske pismenosti postaje nezaobilazno u podizanju nivoa nacionalne sigurnosti.
h) Medijska i informacijska pismenost, naročito u digitalnom okruženju, postaje ključna kompetencija u ostvarenju sigurnog i otpornog društva.
i) Sigurnost digitalnog prostora predstavlja važan faktor stabilnosti mira i sigurnosti.

3.3. Indikatori

Osnovni pravni dokumenti koji će se koristiti u izradi magistarskom rada su: UNDP-evi programi i izvještaji o ljudskom razvoju i humanoj sigurnosti, sigurnosne politike i smjernice za cyber sigurnost, evropske i druge međunarodne regulative i propisi o zaštiti privatnosti i sigurnosti. Kao primarni izvor korisnih informacija biće predstavljena analiza raznih međunarodnih konvencija i međunarodnih dokumenata, strategija i izvještaja o cyber sigurnosti, te stručne preporuke koje daju jasne smjernice za sigurno djelovanje u digitalnom okruženju i smanjenje sigurnosnih rizika na internetu. Analizom ovih dokumenata iznositi ćemo zaključke koji se tiču položaja čovjeka u digitalno uvjetovanom okruženju.

4. Naučni pristup – Paradigme i metode

Imajući u vidu koncept i karakter ovog rada, posebno će biti stavljen akcenat na metod analize sadržaja kao metodu prikupljanja podataka, odnosno prikupljanje podataka uz pomoć korištenja raznih informacijskih sredstava. Kao primarni izvor korisnih informacija biće predstavljena analiza UNDP-ijevih izvještaja o humanoj sigurnosti (1994.-2022.godine), razvojnih planova i međunarodnih konvencija, strategija, preporuka, te smjernica za sigurno djelovanje u digitalnom okruženju, na temelju kojih ćemo iznositi zaključke koji se tiču položaja čovjeka u digitalnom okruženju.

4.1. Opće naučne metode

U radu će se koristiti analitičko-deduktivna metoda. Na osnovu prikupljenih podataka putem ove metode pokušat ćemo pružiti naučna objašnjenja za uticaj digitalizacije na humanu sigurnost, promjenu uloge i položaja čovjeka, te promjene izvora nesigurnosti.

5. Naučna i društvena opravdanost

5.1. Naučna opravdanost istraživanja

Naučna opravdanost istraživanja proizilazi iz bitnih pojedinosti i karakteristika kako pozitivnih, tako i negativnih uticaja digitalizacije na humanu sigurnosti. U zemljama koje su tehnološki lideri u svijetu, istraživanja ovog tipa su česta i intenzivna, te im se predaje velika važnost upravo zbog činjenice da se digitalni svijet širi iz dana u dan i da se broj korisnika eksponencijalno povećava. Ova vrsta istraživanja može pružiti doprinos budućim naučnim istraživanjima ove aktualne teme i pomoći da akademska zajednica ne oskudijeva podacima koji su vrlo značajni za ovu nauku.

5.2. Društvena opravdanost istraživanja

Društvena opravdanost istraživanja proizlazi iz prethodnog naučnog saznanja, njegovog društvenog značaja i cilja, te mogućnosti praktične primjene i potencijalno dobijenih rezultata istraživanja. Ovo istraživanje je društveno opravdano s razlogom da će osigurati rezultate na osnovu kojih bi se moglo zaključiti kakav uticaj je ostvarila digitalizacija svakodnevnice na humanu sigurnost i posmatranje sigurnosti čovjeka, njegovog integriteta, digitalne imovine i dostojanstva. Rezultati mogu da unaprijede koncept humane sigurnosti prema zaštiti ljudi od novih vidova ugrožavanja njihove sigurnosti, kao i dovesti do toga da se i društvena sredina aktivnije uključi u rješavanje ovog aktuelnog društvenog problema, prvenstveno podizanjem svijesti o savremenim izvorima društvenih rizika i nesigurnosti.

6. Kategorijalni, pojmovni i terminološki sistem

HUMANA SIGURNOST ili ljudska sigurnost, predstavlja relativno novi pristup nacionalnoj i međunarodnoj sigurnosti koji, kao što i sama riječ navodi, daje primat ljudskim bićima i njihovim složenim društvenim i ekonomskim interakcijama. U izvještaju UNDP iz 1994. definiše se kao „stanje u kojem su ljudi oslobođeni od trauma koje opterećuju ljudski razvoj. Humana sigurnost znači, kao prvo, sigurnost od takvih kroničnih prijetnji kao što su glad, bolest i represija. A kao drugo, znači zaštitu od iznenadnih i štetnih poremećaja svakodnevnice – bilo u domovima, na radnim mjestima ili u zajednicama." (Izvještaj UNDP, 1994.)

DIGITALIZACIJA - digitalizacija (engl. digitalization, od digit: znamenka), u najširem smislu, prevođenje analognog signala u digitalni oblik (analogno-digitalno pretvaranje). U užem smislu, pretvaranje teksta, slike, zvuka, pokretnih slika (filmova i videa) ili trodimenzijskog oblika nekog objekta u digitalni oblik, u pravilu binaran kôd zapisan kao računalna datoteka sa sažimanjem podataka ili bez sažimanja podataka, koji se može obrađivati, pohranjivati ili prenositi računarima i računarskim sistemima. Postupci digitalizacije, kao i uređaji kojima se ona obavlja (analogno-digitalni pretvarači), ovise o vrsti gradiva koje se digitalizira. (*Hrvatska enciklopedija*, 2021.)

DIGITALNA TRANSFORMACIJA- Digitalna transformacija je transformacija poslovnih aktivnosti, procesa, proizvoda i modela koji u potpunosti iskorištavaju mogućnosti digitalnih tehnologija. Glavni cilj je poboljšanje efikasnosti, upravljanje rizikom ili otkrivanje novih mogućnosti monetizacije podataka. Digitalna transformacija radi stvari na novi (digitalni) način. Digitalna transformacija odnosi se na promjene koje primjena digitalne tehnologije izaziva u svim društvenim oblicima. Može se zamisliti kao treći stepen primjene digitalne tehnologije u nizu: digitalna sposobnost (digital competence) - digitalna upotreba (digital usage) - digitalna transformacija (digital transformation). Stepen digitalne transformacije označava da upotreba digitalne tehnologije po svojim karakteristikama omogućuje nove vrste inovacija i kreativnosti u pojedinim društvenim područjima, a ne samo poboljšanje i podržavanje tradicionalnih metoda. Digitalna transformacija je temeljita i ubrzana transformacija poslovanja, procesa, sposobnosti i modela s ciljem potpunog iskorištavanja mogućnosti digitalnih tehnologija i njihovog utjecaja na društvo i to na strateški i prioritetni način. Digitalna transformacija djeluje kako na pojedinačno poslovanje tako i na društvene cjeline

kao što su naprimjer gospodarstvo, uprava, masovne komunikacije, umjetnost, medicina ili nauka. (Hrvatska enciklopedija, 2021.)

CYBER PROSTOR- virtualni prostor stvoren uz pomoću globalno umreženih računara, tj. svijet interneta s njegovim okružjem; također cyber prostor (engl. cyberspace). U njemu, kao i u stvarnom prostoru ljudi mogu jedni s drugima komunicirati, družiti se, razmjenjivati, razvijati i ostvarivati ideje, trgovati i dr. Naziv je skovao američki pisac znanstvene fantastike William Gibson (1948), a postao je popularan zahvaljujući njegovu romanu Neuromancer (1984), koji predstavlja osnovu cyberpunk smjera u znanstvenofantastičnoj literaturi. Pojam cyber prostor djelomično se poklapa s pojmom virtualna stvarnost, koji se ipak više odnosi na tehničke aspekte realizacije takvog prostora. (*Hrvatska enciklopedija,* 2021.)

II HUMANA SIGURNOST

1. Uvod u Humanu sigurnost

U uvodnom dijelu ovog poglavlja govorit će se o nastanku i definisanju humane sigurnosti te njenom procvatu između državne i međunarodne sigurnosti.

Humana sigurnost prvi put se spominje sredinom devedesetih godina prošlog stoljeća u UN-ovim a posebnije u UNDP-jevom izvještaju iz 1994. godine (UNDP – Program Ujedinjenih nacija za razvoj). Ovaj dokument humanu sigurnost definiše kao stanje u kojem su ljudi oslobođeni od trauma koje opterećuju ljudski razvoj. Humana sigurnost znači, kao prvo, sigurnost od takvih kroničnih prijetnji kao što su glad, bolest i represija. A kao drugo, znači zaštitu od iznenadnih i štetnih poremećaja svakodnevnice – bilo u domovima, na radnim mjestima ili u zajednicama. (Izvještaj UNDP, 1994., Colins, 2010.; u Smajić, 2012.)

Kada je uveden 1994. godine, pristup ljudske, odnosno humane sigurnosti, preusmjerio je debatu o sigurnosti sa teritorijalne sigurnosti na sigurnost ljudi. Ova ideja pozvala je stručnjake za sigurnost i kreatore politike da pogledaju dalje od zaštite nacionalne države do zaštite onoga do čega nam je u životu najviše stalo: naših osnovnih potreba, našeg fizičkog integriteta i ljudskog dostojanstva.

Shvaćena u ovim terminima, ljudska sigurnost je također sadržana u aksiomu politike "sloboda od straha" i "sloboda od oskudice", iz čega možemo zaključiti da humana sigurnost ima dva glavna aspekta (freedom from fear i freedom from wear). Kroz ovakve ideje naglašava se važnost svačijeg prava na slobodu od straha, slobodu od oskudice i slobodu od poniženja, kao i bliska povezanost između sigurnosti, razvoja, zaštite i osnaživanja pojedinaca i zajednica. Humana sigurnost, kako smatra Smajić, "može biti ugrožena u sedam područja, koja ujedno čine temelj ljudske sigurnosti: ekonomska sigurnost, prehrambena sigurnost, zdravstvena, ekološka, osobna, politička i sigurnost zajednice."(Smajić, 2012:181) U današnje vrijeme, svaka od ovih sigurnosti direktno je povezana sa digitalnim medijskim i platformskim okruženjem koje uveliko određuje stanje i percepciju sigurnosti koja je podložna različitim medijskim i informacijskim interpretacijama stvarnosti, o čemu će se u trećem poglavlju rada detaljnije govoriti.

1.1. Od tradicionalne do humane sigurnosti

Radi što boljeg razumijevanja evolucije koncepta humane sigurnosti, na samom početku, neophodno je osvrnuti se na širu sliku nauke o sigurnosti i sagledati različite pristupe, stavove i fundamentalne postavke na putu od tradicionalne do humanocentrične sigurnosti. Sigurnost predstavlja izuzetno širok i poprilično neuhvatljiv pojam. Ukoliko bismo obuhvatili svaki sigurnosni aspekt ne bi ostala društvena pojava koja ne bi mogla biti predmet istraživanja sigurnosnih studija i predstaviti u nekom trenutku potencijalnu sigurnosnu prijetnju ili izvor nesigurnosti. Stoga ćemo u ovom dijelu rada predstaviti razliku između tradicionalne i humane sigurnosti koja se ogleda u njihovom referentnom objektu i različitom pristupu prijetnjama.

Do sada još uvijek ne postoji zvaničan konsenzus o pojmu sigurnosti. Iako je u posljednjih šezdeset godina istražen i objavljen veliki broj sigurnosnih tema, nijedna općenito prihvaćena definicija sigurnosti nije izrađena. Sigurnost kao pojam ima mnogo značenja, pri čemu nije nužno da svako bude logički povezano sa konvencionalnim shvatanjem tog pojma. (Dalby, 1997). Pojam sigurnosti je dvojben u svome sadržaju i u formatu, te se odnosi na različite skupove pitanja i vrijednosti. Wolfers je (1952: 483) opisao nacionalnu sigurnost kao "dvosmislen simbol" koji, ako se koristi bez dodatnih pojašnjenja, "ostavlja prostora za veću zbrku." Za Wolfersa sigurnost predstavlja „nepostojanje prijetnji stečenim vrijednostima“, čime je obuhvatio većinu upotrebe izraza sigurnost. (Mihalinčić, 2020: 24)

U te stečene vrijednosti ubrajaju se društvene i individualne, materijalne, intelektualne, duhovne i druge društvene vrijednosti. “Sigurnost je kompleksan i integralan pojam, za nju možemo reći da je „optimalana, poželjna i ohrabrujuća izvjesnost“. (Masleša, 2001., prema Vajzović, Hibert, Turčilo i dr. 2021. :247); Sigurnost „podrazumijeva općenito stepen zaštićenosti: ljudi od različitih oblika njihova ugrožavanja, zaštitu materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelokupnu zaštitu države od svih vidova njenoga ugrožavanja, a naposlijetku sigurnost podrazumijeva stepen zaštite od ugrožavanja na planetarnom i kosmičkom nivou života općenito i ljudskoga roda u cijelosti. Svi nivoi sigurnosti čovjeka: planetarni, državni i sigurnost čovjeka-pojedinca, te materijalnih i kulturnih dobara predstavljaju neraskidivu cjelinu. U političkom smislu sigurnost podrazumijeva stepen zaštite države od ugrožavanja iznutra i izvana (unutarnja i vanjska sigurnost)”. (Beridan, 2001 : 348)

„Haf studije sigurnosti vidi kao „poddisciplinu međunarodnih odnosa“ (Hough, 2008: 2), dok Majkl Vilijams studije sigurnosti predstavlja kao „najdinamičnije i najosporavanije područje

međunarodnih odnosa“ (Williams, M. 2003: 511). Postoji saglasnost u smislu preciznog definisanja istraživačkog polja sigurnosti. Mnogi teoretičari su, u nastojanju da obuhvate sve ono što sigurnost „treba“ da podrazumijeva, dali tako široka određenja u kojima se pod sigurnošću može podrazumevati gotovo svaka pojava. Tako na primjer, Lipman sigurnost određuje kao „sposobnost da se zaštite ključne vrednosti“ (Lippmann, 1944: 51 prema Ayoob, 1984: 41), Martin je definiše kao „garanciju budućeg blagostanja“ (Martin, 1983: 12), dok Ulman sigurnost shvata kao odsustvo ranjivosti, što implicira obrazac po kojem se smanjivanjem sigurnosti povećava ranjivost (Ullman, 1983: 146). Jedno od najčešće navođenih određenja sigurnosti dao je Mroz, koji smatra da je „sigurnost relativna sloboda od štetnih pretnji (Mroz, 1980: 105, prema Lipovac, 2013. : 444)

„Sigurnost stoji naspram ugrožavanja, prijetnji i obrnuto“ (Beridan 2008: 25); ona je preduslov za razvoj i ostvarenje ljudskih prava i sloboda, ali i osnov razvoja društva u ekonomskom, kulturnom i političkom smislu.

Maslow u svojoj piramidi potreba sigurnost svrstava odmah iza fizioloških potreba, te pod sigurnošću podrazumijeva: tjelesnu odnosno fizičku sigurnost, radnu, resursnu, moralnu, porodičnu, zdravstvenu i imovinsku sigurnost. (Maslow, 1943.) Važnost sigurnosti se očituje i iz činjenice da se tek poslije potrebe sigurnosti navodi potreba za ljubavlju i pripadnošću, poštovanjem i samoaktualizacijom. Zaključujemo da su jedino fiziološke potrebe važnije od potrebe za sugurnoću.

U naučno-istraživačkom području sigurnost je najčešće definisana kao „stanje bez opasnosti i ugrožavanja, sigurnost podrazumijeva i osjećaj sigurnosti, ali i aktivnosti odnosno sistem za ostvarenje sigurnosti“ (Mangold, 1990; Mitar, 1994, prema Mihalinčić, 2020:2 i prema Vajzović, 2020: 16). Pored rasprava o konstituciji novog međunarodnog poretka, otvorena je i rasprava o sigurnosnim sadržajima koji su se mijenjali zajedno sa stanjem u sigurnosnoj nacionalnoj i međunarodnoj okolini. „Na općoj razini oblikovala su se tri pristupa sigurnosti: ljudska sigurnost (human security), nacionalnu sigurnost (national security) i transnacionalnu sigurnost (transnational security)“ (Hellmann, 2017: 250). Ovdje treba naglasiti da je samo ljudska sigurnost bila novi koncept, dok su nacionalna i transnacionalna postojale i ranije, ali im se promijenio sadržaj prijetnji, organizacijski oblici i modeli upravljanja. Hellmann (2017: 240) se fokusirao upravo na analizu ova dva tipa, te je ponudio tri zapažanja koja upućuju na razlike među njima: prvo, „u konceptima nacionalne sigurnosti uvijek je postojala središnja razlika između domaćeg i inozemnog, između unutarnjeg i vanjskog“. Drugo, zbog toga su „granice igrale presudnu ulogu u definiranju sigurnosti“. Treće, „pojam 'prijetnje' bio je gotovo uvijek usko povezan s teritorijalno određenim akterima, što je podrazumijevalo praćenje vojnih

aktivnosti i potencijalnih napada s vanjskog teritorija i organizaciju teritorijalne obrane…“ . (Mihalinčić, 2020: 100)

Richard Ullman bio je jedan od prvih znanstvenika koji je kritizirao gotovo isključivi fokus na vojnu prijetnju u konvencionalnom (realističkom) razmišljanju o sigurnosti. Ullman (1983: 123) naglašava da "definiranje nacionalne sigurnosti samo (ili čak prvenstveno) u vojnom smislu daje duboko lažnu sliku stvarnosti." Stephan Blank (Foreign Policy Research Institute) posebno ističe da su najveće sigurnosne prijetnje danas zapravo mobilne, a najveće prijetnje u 21. stoljeću neće biti one od kojih se možemo braniti stajaćom vojskom ili sofisticiranim oružjem.(Dijanović, 2020: 3) Bit će potrebno preispitati samu prirodu nacionalne sigurnosti i međunarodne sigurnosti, a za suzbijanje ugroza bit će potrebna globalna suradnja.

1.2. Koncept ljudske sigurnosti

Nakon završetka Hladnog rata i naizgled prestanka konvencionalnih prijetnji, otvorio se prostor za nova razumijevanja uzroka ljudske ranjivosti. Došlo je do promjene sigurnosnih politika i paradigmi – vojne prijetnje koje predstavljaju primarni oblik ugrožavanja odbrane i sigurnosti društva i države, postaju tek jedna od komponenti savremene sigurnosti (Mikac, 2013). Koncept ljudske sigurnosti predstavlja odmak od tradicionalnih ortodoksnih sigurnosnih studija koje svoj fokus usmjeravaju isključivo na sigurnost države. Subjekti pristupa ljudske sigurnosti su pojedinci, a krajnji cilj mu je zaštita ljudi od tradicionalnih (tj. vojnih) i netradicionalnih prijetnji kao što su strah, siromaštvo, bolesti, represija i tako dalje. Pomicanje sigurnosne agende izvan državne sigurnosti ne znači njezinu zamjenu, već uključuje njeno nadopunjavanje i nadgradnju. Pregledom pristupa koji obuhvataju nekonvencionalnu sigurnosnu paradigmu uočava se potreba za fokusiranjem na prijetnje opstanku pojedinca i sredstva za postizanje sigurnosti koja neće dodatno ugrožavati niti pojedinca ni zajednicu u kojoj se on nalazi. To znači da se sadržaji nacionalne sigurnosti moraju proširiti izvan vojne sigurnosti i to uključivanjem političkih, socijalnih, ekonomskih i društvenih sadržaja sigurnosti. Važno je razumjeti da uskraćivanje ljudske sigurnosti može potkopati mir i stabilnost kako unutar država tako i na međunarodnom planu, dok pretjerano naglašavanje državne sigurnosti može biti štetno za ljudsko dobro. U sistemu u kojem humana sigurnost ima primarnu ulogu, država ostaje središnji davatelj sigurnosti, ali državna sigurnost nije dovoljan uvjet za dobrobit ljudi. (Britanica, Gregoratti, 2018.)

Postavljen je temelj novoj paradigmi koja koncept sigurnosti širi izvan vojno-političkih odgovora jer opasnosti kao što su: klimatske promjene, migracije, epidemije zaraznih bolesti, terorizam, cyber napadi, cyber criminal, organizovani criminal, trgovina drogom, prirodne i tehnološke nesreće i katastrofe, zahtijevaju drugačije politike i sistemske odgovore. Sve te pojave zahtijevaju nove pristupe i načine djelovanja sigurnosnih struktura, kao i formiranje odgovarajućeg sigurnosno-naučnog stave. Savremena paradigm trebala je ponuditi relativno novi pristup nacionalnoj i međunarodnoj sigurnosti koji, kao što i sama riječ navodi, daje primat ljudskim bićima i njihovim složenim društvenim i ekonomskim interakcijama. (Izvještaj UNDP, 1994.)

Kako Collins, u Savremenim sigurnosnim studijama (2010 :20) navodi: "Jedna od novijih poštapalica u literaturi o sigurnosti je ljudska sigurnost. Ona dijeli mnoge sličnosti sa kritičkim pristupima sigurnosti." Kao što samo ime govori, referentni objekat ove sigurnosti su ljudi, ali kao što Pauline Kerr u šestom poglavlju iste knjige navodi da promjena referentnog objekta otkriva blisku vezu između razvoja i sigurnosti, također ona donosi mnoge nove izazove održavanju analitičke strogosti. Dijeleći zagovarače ljudske sigurnosti na posebne i općenite škole moguće je prepoznati ogromni niz prijetnji koje postoje za ljude i njigove živote i time se omogućuje stvaranje vaših vlastitih sudova o onome što čini sigurnost. Humana sigurnost predstavlja ideju zaštite vitalne srži svih ljudskih života na načine koji poboljšavaju ljudske slobode i ljudsko ispunjenje. Ljudska sigurnost znači zaštitu osnovnih sloboda – sloboda koje su suština života. To znači zaštitu ljudi od kritičnih, teških, sveprisutnih i široko rasprostranjenih prijetnji i situacija. (IIHR, UNDP, 2010.) Williams navodi da se u većini literature koja se bavi pitanjima ljudske sigurnosti može vidjeti zajedničko uvjerenje da je „ljudska sigurnost od presudne važnosti za međunarodnu sigurnost i da međunarodni poredak ne može počivati samo na suverenosti i vitalnosti država – taj poredak ovisi i od pojedinaca i njihovog osjećaja sigurnosti." (Williams, 2008: 232, prema Mihalinčić, 2020. :48)

1.3. Subjektivna i objektivna sigurnost

Odsustvo osjećaja straha od ugrožavanja društvenih vrijednosti prema Wolfersu subjektivna je dimenzija sigurnosti dok se odsustvo prijetnji prema društvenim vrijednostima odnosi na objektivu dimenziju sigurnosti (Wolfers, 1952). Na osnovu toga Vajzović zaključuje da "osiguranje i subjektivne i objektivne dimenzije sigurnosti (Safety i Security) podrazumijeva

istodobno i zaštitu vrijednosti uz očekivano očuvanje teritorijalnog integriteta." (Vajzović, 2020:16)

1.4. Uži i širi pristup humanoj sigurnosti

Evolucijom humane sigurnosti postigao se opći konsenzus oko referentnog objekta ljudske sigurnosti, ali sporenje u pravcu određivanja prijetnje koja će biti primarna za ovaj koncept podijelilo je zagovornike na uži i širi pristup ljudskoj sigurnosti.(Kerr, 2010B; Tigerstrom, 2007; Hampson, 2008; u Smajić, 2012.).

Škola užeg pristupa ljudskoj sigurnosti i njen zagovornik Mack, (kako bilježi Smajić, 2012.:186) "tvrde kako je prijetnja političkog nasilja ljudima, od države ili bilo kojeg drugog organiziranog političkog subjekta, prikladan predmet koncepcije ljudske sigurnosti. Pritom zastupnici užeg pristupa ljudsku sigurnost definiraju kao zaštitu pojedinca i zajednica od rata i ostalih oblika nasilja (Collins, 2010.) Mack i njegovi sljedbenici ne negiraju postojanje i drugih prijetnji ljudima osim sistemskog političkog nasilja, ali naglašavaju da su one samo korelati nasilju (npr. uzajamna veza siromaštva i loše vladavine)." Za zastupnike škole šireg pristupa ljudskoj sigurnosti, pored političkog nasilja, nezaobilazna prijetnja sigurnosti je i siromaštvo. U tome se ogleda definisanje humane sigurnosti kao „sloboda od straha" i „sloboda od siromaštva" uz ostale ljudske slobode i vrijednosti. (Smajić, 2012)

Tako, Tahkur (2004., u Smajić, 2012) "smatra da ljudska sigurnost treba da se bavi „zaštitom ljudi od kritičnih, po život opasnih prijetnji, bez obzira na to jesu li uzroci prijetnji ljudske aktivnosti ili prirodni događaji, nalaze li se one unutar ili izvan država". Širi pristup je zbog svoje difuznosti vrlo često izložen mnogim kritikama, što potvrđuje i Paris (2004, u Collins, 2010.) te zaključuje da ovakvo shvatanje ljudske sigurnosti pokriva dijapazon od „zloupotrebe opojnih sredstava do genocida", što suštinski onemogućuje fokusiranje na njegovu efikasnu implementaciju u praksi.

Obzirom na široku lepezu izvora prijetnji ljudskoj sigurnosti koju preferiraju zastupnici šireg pristupa te ograničenost na političko nasilje kao izvor ljudske nesigurnosti kod predstavnika užeg pristupa, "ljudska sigurnost predstavlja stanje u kojemu je osiguran uravnotežen fizički, duhovni, društveni i materijalni opstanak pojedinc.." (Smajić, Seizović, Turčalo 2017.)

Važan iskorak u razvoju koncepta ljudske sigurnosti učinila je Opća skupština UN-a 1998. godine, kada je osnovana neformalna grupa zemalja mreže ljudske sigurnosti (Human Security

Network). „Osnovni cilj te mreže je poticanje rješavanja međunarodnih problema koji predstavljaju neposrednu opasnost za sigurnost ljudi.“ (Price & Zacher, 2004: 254, prema Smajić, 2012: 187).

Koalicija država i nadnacionalnih organizacija koje su podržale ovaj pristup doprinose razvoju mnogih društvenih postignuća, poput Ottawske konvencije (tj. Ugovora o zabrani mina), uspostave Međunarodnog kaznenog suda i Fakultativnog protokola uz Konvenciju o pravima dijete i drugim. Snažnu potporu razvoju humane sigurnosti predstavljaju i redovni UNDP-jevi izvještaji, koji izvještavaju o dostignućima humane sigurnosti, o načinima na koje nova generacija prijetnji koje se pojavljuju u antropocenskom[1] kontekstu i djeluju u interakciji, utječu na ljudsku sigurnost i šta učiniti u vezi s tim (Specijalni izvještaj UNDP, 2022.).

1.5. Odnos sigurnosti i emancipacije

Prema Boothu, navodi Mihalinčić u svome radu: “ljudska emancipacija” omogućava dublje spoznavanje sigurnosti. Ken Booth (2007: 8) opisuje odnos sigurnosti i emancipacije na sljedeći način: „Sigurnost znači odsustvo prijetnji. Emancipacija je oslobađanje ljudi (kao pojedinaca i grupa) od onih fizičkih i ljudskih ograničenja koja ih zaustavljaju u izvršavanju onoga što bi slobodno izabrali. Rat i prijetnja ratom su jedno od tih ograničenja, zajedno sa siromaštvom, lošim obrazovanjem, političkim ugnjetavanjem i tako dalje. Emancipacija ne daje moć ili red, ona stvara istinsku sigurnost.“ Ljude bi trebali tretirati kao svrhu sigurnosti, a državu kao sredstvo. Pojedinci i njihova zajednica koja im ispunjava potrebe, a ne države kao takve, krajnji su cilj razvoja i sigurnosti.

Na kaju ovog poglavlja, a na osnovu prezentiranih definicija možemo zaključiti da je humana sigurnost ključna karika u lancu sigurnosnog sistema. Iako imaju drugačije referentne objekte i koncepte, humana sigurnost ne predstavlja zamjenu za tradicionalni pristup sigurnost, nego njegovu dopunu. Humana ili ljudska sigurnost jasno naglašava svoj stav o zaštiti čovjeka od novih prijetnji i drugačijih ugrožavanja sigurnosti. Savremena sigurnost, zbog svoje

[1] Antropocen- termin kojim se opisuje era u kojoj su ljudi postali centralni pokretači planetarnih promjena, radikalno mijenjajući biosferu Zemlje. U centru tih promjena ljudi imaju dobar razlog da se osjećaju nesigurno.

dinamičnosti**,** svakim danom postaje sve kompleksnija, uvjetovana zbivanjima u međunarodnoj okolini i promjenjivom ulogom države koja gubi monopol nad sigurnosću u korist novih centara moći, tehnoloških korporacija i privatnih kompanija koje raspolažu ogromnim količinama podataka o svakom svom korisniku. Savremena sigurnost se očigledno transformiše od očuvanja teritorija prema očuvanju vrijednosti, a u današnjem svijetu informacije imaju veliku vrijednost. Savremeni rizici prijete vrijednostima, zajednici i svakom pojedincu.

III HUMANA SIGURNOST – STANJE I PERSPEKTIVE

U 21. stoljeću, kada se skoro sve ljudske djelatnosti obavljaju uz pomoć nekog vida digitalne tehnologije ili u digitalnom prostoru, nauka o sigurnosti ima veliki zadatak da isprati taj tehnološki napredak, odnosno obuhvati i digitalni prostor, a to može postići samo evolucijom koncepta i stavova prema osiguranju šire društvene sigurnost. U ovom poglavlju želi se, između ostalog, istražiti i utvrditi jesu li i zašto nastupile promjene u konceptu humane sigurnosti u odnosu na UNDP-jev izvještaj iz 1994.godine i izvještaj iz 2022. godine, te kakve promjene se mogu očekivati u budućem sve bržem i širem digitalnom razvoju društva koji iziskuje etičko promišljanje razvoja.
U uvodnom dijelu ovog poglavlja napaviti će se kratak pregled digitalnog napretka društva i integrisanja tehnologije duboko u smisao svakodnevnog života čovjeka.

1. Globalizacija i informacijsko-tehnološki napredak i razvoj

UNDP je razvojni program Ujedinjenih nacija koji prvenstveno pomaže zemljama u razvoju, u uklanjanju siromaštva i postizanju održivog gospodarskog rasta i ljudskog razvoja, te prati humani razvoj čovjeka, razvoj sigurnosti i zaštite, ljudskih prava, tehnologije itd. (Mingst, K. Britanica, (2018)

Najbolji primjer civilizacijskog razvoja i napredovanja čovječanstva predstavljaju upravo tehnologija i mogućnosti koje nudi internet. Globalizacija je, potpomognuta tehnološkim napretkom u sferi informacionih i komunikacionih tehnologija i prenosa podataka, povezala svijet u jedno „globalno selo“. Procesi koji su pokrenuti takvim povezivanjem

omogućili su nove načine za napredak i razvoj društvene zajednice. Tako ubrzan razvoj društva kreirao je različite sadržajne i transformacijske pomake prema novim tehnologijama koje zahtijevaju novi model upravljanja rizicima. Dogodio se pomak u sadržajima sigurnosti, proširivanjem i produbljivanjem područja koje treba zaštiti. Nestale su granice koje su definirale gdje počinju i prestaju međunarodna, nacionalna ili lična sigurnost. Ipak, uočljivo je da se nije dogodila temeljna promjena ukupnog koncepta koji bi se značajno odmaknuo od klasičnog modela nacionalne sigurnosti. Tehnološki razvoj promijenio je poimanje prostora i vremena, omogućio je industrijske revolucije i povezivanje ljudi na sve modernije načine. Kroz historiju, čovjekova svakodnevna komunikacija i razmjena informacija prošle su put od usmene, klesane, pisane, štampane i radio-talasne komunikacije, pa sve do e-maila i video poziva, koji su komunikaciju i prijenos informacija naizgled doveli do vrhunca, te svakodnevni život ljudi učinili lakšim.

1.1 Digitalizacija

Digitalizacija je zahvatila gotovo sve sfere ljudskog društva: industriju, privredu, medije, umjetnost, obrazovanje i sigurnost. Svojom sveprisutnošću ubrzano mijenja i društva i ljudske aktivnosti širom svijeta. Digitalizacija se općenito smatra pozitivnom silom. Vlade zemalja kao što je Estonija, Japan, Kina, Norveška te mnoge druge, na primjer, prihvataju digitalnu tehnologiju kako bi postale učinkovitije i transparentnije za svoje građane.[2] Digitizacijia i digitalizacija su dva konceptualna pojma koja su usko povezana. Digitizacija se odnosi na „radnju ili proces digitizacije; pretvaranje analognih podataka (posebno u kasnijoj upotrebi slika, videa i teksta) u digitalni oblik.” Digitalizacija se, naprotiv, odnosi na "usvajanje ili povećanje upotrebe digitalne ili računarske tehnologije od strane organizacije, industrije, zemlje itd." (Chakraborty, 2022.). Bez digitalnih informacija nije moguće rješenje temeljeno na velikim podacima koji će biti detaljnije obrađeni u jednom od naslova narednog poglavlja.

Digitalizacija kao koncept se može tumačiti kao “korištenje digitalnih tehnologija za promjenu poslovnog modela i pružanje novih mogućnosti za prihod i stvaranje vrijednosti; to je proces prelaska na digitalno poslovanje (Ibid.). Ako tome dodamo širenje računarstva u Cloud-u, umjetnu inteligenciju i milijarde digitalno povezanih uređaja, stvari se podižu na potpuno novi

[2] O građanskoj transparentnosti i iskorištavanju takvih ideja za nadziranje svakog umreženog pojedinca, kao i o prijetnjama koje mogu iz toga proizići, podrobnije će se govoriti u narednim poglavljima.

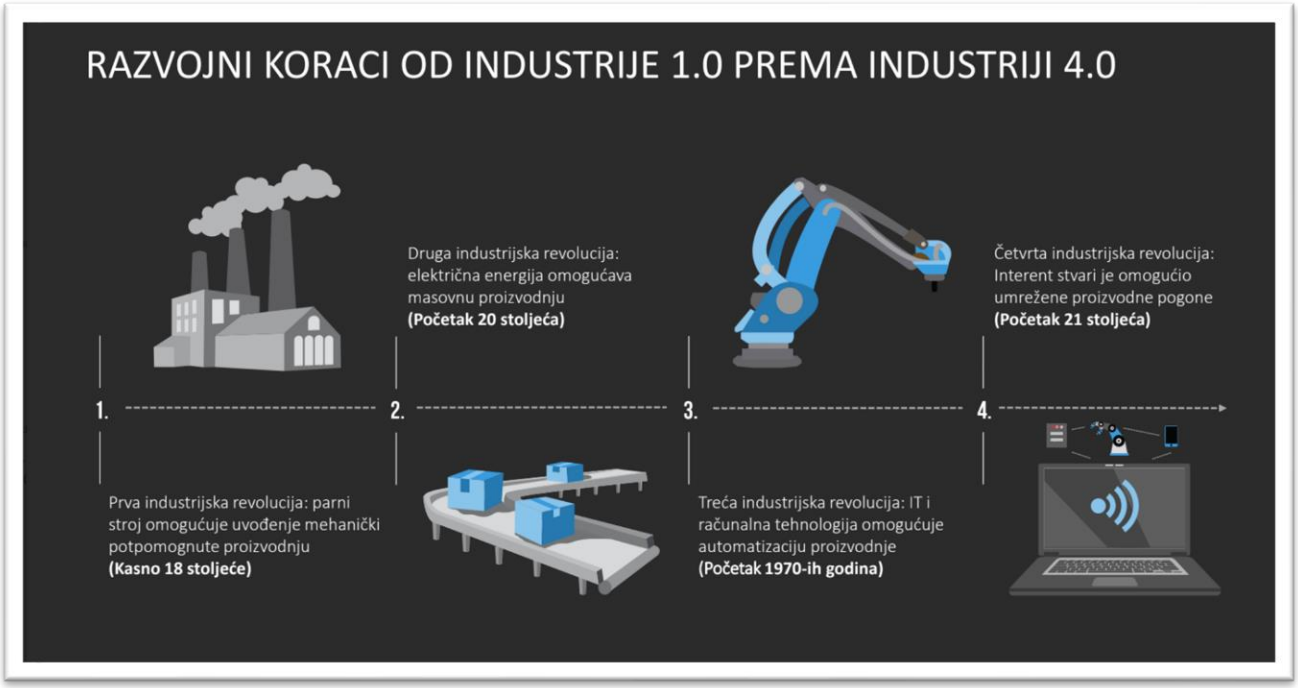
nivo. Ovi trendovi samo su se ubrzali od početka pandemije COVID-19, o čijim uticajima na humanu sigurnost će se detaljnije govoriti u narednom poglavlju. Digitalizacija transformiše sve tokove i proširuje mogućnosti za učestvovanje i manjih igrača. Uspon digitalnih tehnologija ne samo da pokreće protok podataka i komunikacija, već i transformiše i omogućuje protok roba, usluga, kapitala, pa čak i ljudi. Neosporno je da digitalizacija nudi brojne prednosti, a kako bi iskoristile potencijal digitalne tehnologije u svrhu pružanja užitka ljudima širom svijeta, kompanije su razvile ideju pod nazivom „Digital Dream Kids“. Oni zahtijevaju uočavanje snova mlade, digitalno pismene generacije potrošača i njihovo prevođenje u jedinstvene, zabavne proizvode i uzbudljive aplikacije, isporučujući proizvode koji ispunjavaju snove njihovih kupaca. Kako bi se postigao ovaj cilj, potrebno je besprijekorno spajanje sadržaja, hardvera i tehnologije (Chakraborty, 2022.). Ova ideja postala je središnja u strategijama poslovanja širom svijeta.

1.2. Digitalni razvoj društva

Početak „digitalnog doba“ Hilbert, (2020; A) procjenjuje na 2002. godinu, kada je svijet prvi put mogao pohraniti više digitalnih nego analognih informacija u svoje tehnološke alate. Sveobuhvatna digitalizacija proizvela je vidljive društveno-kulturne, ekonomske i političke promjene u svijetu. Ove promjene stvaraju nove prilike, ali i izazove i brige za ljude i zajednice koje se svakim danom sve više okružuju pametnim uređajima. Digitalni razvoj vođen je nadnacionalnim, nacionalnim i regionalnim digitalnim politikama i osiguran je nacionalnim programima cyber sigurnosti. Ti se okviri prvenstveno fokusiraju na unapređenje ukupnog gospodarskog rasta i zaštitu kritične informacijske infrastrukture i informacijske sigurnosti, ali ne posvećuju odgovarajuću pozornost interesima, potrebama i strahovima ljudi i zajednica koje doživljavaju digitalizaciju u svakodnevnom životu. (Salminen, Hossain, 2018.) Kako bi se stvorio sveobuhvatniji program cyber sigurnosti koji je orijentisan prema ljudskoj sigurnosti i osnaživanju ljudi da utječu na digitalni razvoj, potreban je istraživački okvir koji naglašava stvarne načine na koje ljudi koriste, žele koristiti ili ne mogu koristiti informacijske i komunikacijske tehnologije.

1.3. Digitalna revolucija

Noviju historiju razvoja čovječanstva obilježile su 4 industrijske revolucije (slika br.1.), koje su iz dana u dan vodile čovjeka u sve brži ritam svakodnevnice



Slika br.1.“Razvojni koraci industrije”
(Hrvatska gospodarska komora, 2017.)

Svjedoci smo digitalne revolucije koja obuhvata sve sfere našeg zivota, koja prvenstveno štedi vrijeme i novac, skraćuje udaljenost i olakšava svakodnevni život ljudi. Digitalnu revoluciju u naučnim i akademskim krugovima može se opisati kao eksplozija informacijskih tehnologija koje preuređuju svijet, ostavljajući samo nekoliko aspekata društva netaknutim. Smatra se da je u proteklih 50 godina digitalni svijet postao ključan za funkcioniranje društva. Revolucija je napredovala vrtoglavom brzinom i sa sigurnošću se može reći da nijedna tehnologija nije dosegla više ljudi u tako kratkom vremenskom razdoblju kao Internet, i još nije završila (Hodson, Nature; 2018). Digitalizacija je dovela do proširenja sigurnosnih potreba jednog čovjeka, zbog proširenja oblika ugrožavanja i pojave novih prijetnji. Svijetu koji se dinamički mijenja, zahtijeva od nas da osiguramo da digitalna revolucija služi društvu, a ne obrnuto.

Hilbert (2020.A) smatra da se nova tehno-ekonomska paradigma postepeno oblikuje kao drugačiji „zdrav razum“ za efikasno djelovanje u bilo kojoj oblasti nastojanja. Autor također smatra da konkurentske snage, traženje profita i pritisci za opstanak pomažu u širenju promjena u ekonomiji i društveno-institucionalnoj sferi u kojoj su promjene također potrebne. Te promjene su sputane snažnom inercijom koja proizlazi iz rutine, ideologije i stečenih interesa. „Upravo ta razlika u ritmu promjena, između tehno-ekonomske i socio-institucionalne sfere, objašnjava turbulentni period (Perez, 2003.; prema Hilbert, 2020.A). Poznato je da su industrijske revolucije doprinijele velikom bogatstvu, ali i mnogim nejednakostima i ekonomskim problemima. Isto vrijedi i za sadašnji period digitalne tehnologije i društvenih promjena” (Hilbert, 2020.B).

Digitalna revolucija 21. stoljeća određena je promjenjivom ulogom neposrednog posmatrača ili korisnika, s relevantnom zabavom unutar prethodnog broja godina. Ono što je započelo kao privatna iskustva gledanja između gledatelja, a time i emitera, sada se prebacilo na gledatelja. Interaktivni mediji poput mobilnih i tablet uređaja uz pomoć kojih potrošači mogu stvarati, prilagođavati i dijeliti sadržaj, sljedeći su val budućnosti. Platforme društvenih medija kao što su: YouTube, Snapchat, Facebook, Instagram, Twitter, Tik Tok i mnogi drugi, omogućuju većem broju potrošača s digitalnom tehnologijom, da brzo i vrlo jednostavno emitiraju sadržaj koji sami generiraju. Širenje računarstva Cloud-u[3], umjetne inteligencije i milijardi digitalno povezanih uređaja podižu stvari na novu visinu. (Chakraborty, 2022.)

U prethodnih 20 godina odvijala se nova digitalna revolucija. Povećanje snage i konvergencije prenosnih, računalnih i skladišnih kapaciteta, te opseg do kojeg digitalne tehnologije prožimaju gospodarstvo, pokreću transformacijsku fazu temeljenu na Internet stvarima i analitici velikih podataka. Pojava pametnih telefona i tableta potaknula je masovan razvoj aplikacija i rješenja u Cloud-u koja su omogućila nove inovacije u poslovnim modelima i pružanju usluga. Zbog stalnog razvoja brzih pristupnih mreža, sveprisutnosti pristupa s više uređaja, računarstva u Cloud-u, te eksplozije informacija koje generiraju pojedinci, strojevi i objekti, može se zaključiti da je svakodnevno funkcionisanje čovjeka sve više oslonjeno na digitalnu tehnologiju (Ibid.) Analitika velikih podataka omogućuje poboljšanje segmentacije tržišta usmjeravanjem zaliha i proizvoda i u poslovnim i proizvodnim modelima, uz stvaranje novih proizvoda (kombinujući proizvodnju s personalizacijom) i novih poslovnih i državnih modela

[3] Cloud predstavlja pohranjivanje sadržaja na internet, koji se ne nalazi na tvrdom disku i dostupan je vlasniku u svakom trenutku.

usluga (Chakraborty, 2022.). Osim povećanja transparentnosti i učinkovitosti, oni omogućuju bolju i tačniju analizu učinka brojnih i različitih varijabli te mogu regulisati strukture i ponašanja u stvarnom vremenu.

1.4. Digitalna transformacija

Digitalna transformacija najnoviji je dugi val socioekonomske evolucije čovječanstva. Na velika vrata donijela je ogromno unapređenje svakodnevnog života, očuvanje znanja i podataka za budućnost kojima se može pristupiti uz par klikova. Tokom svoje evolucije, čovjek ni u kojem periodu nije mogao za kratko vrijeme prikupiti veći broj informacija kao što mu je omogućeno danas. Informacije igraju važnu ulogu u modernim društvenim odnosima, te su tehnološkim napretkom i digitalnom transformacijom postale glavna pokretačka snaga globalnog sistema. Njihov utjecaj na sve sfere društva generira promjene u moralnoj, kulturnoj i vrijednosnoj orijentaciji čovjeka. Široko širenje informacija posljedica je razvoja i poboljšanja savremenih digitalnih tehnologija koje su značajno pojednostavile njihovo pretraživanje, prikupljanje i analizu. Digitalna transformacija društva uzrokovala je ne samo tehničko-tehnološke promjene u oblasti sigurnosti nego i promjene u sagledavanju demokratskog diskursa, kao i novih rizika i prijetnji, odnosno izvora nesigurnosti. Digitalizacija i uticaj digitalne transformacije zauzimaju važno mjesto u razumijevanju sigurnosti savremenog čovjeka. (Specijalni izvještaj UNDP, 2022).[4] Svaki čovjek u sklopu svojih ljudskih prava bi trebao imati pristup tehnologiji koja ima za cilj ujediniti, a ne podijeliti ljude. Digitalna transformacija, kako smatra Europska komisija, trebala bi doprinijeti pravednom društvu i ekonomiji u Uniji. (Ibid.)

Europska komisija predložila je definisanje posebnog skupa načela za digitalnu transformaciju koja je usmjerena na čovjeka, u svojoj deklaraciji o digitalnim pravima i načelima iz 2022. godine. Ova deklaracija predstavlja referentni okvir za ljude i vodič za preduzeća i kreatore politike, s ciljem povećanja sigurnosti. Primarni zadatak ove deklaracije je sigurnost i osnaživanje pojedinaca, kao i promicanje održivosti digitalne budućnosti (IT Professionalism Europe 2022., Mirigliano, 2022.). Stoga dotična deklaracija snažno i od svog korijena doprinosi razvoju humane sigurnost u Evropi.

---

[4] Dodatni izvori vezani za Izvještaj mogu se naći na mreži na: http:// hdr.undp.org.

Digitalna transformacija utiče na svaki aspekt života ljudi. Nudi značajne mogućnosti za bolji kvalitet života, inovacije, ekonomski rast i održivost, ali također predstavlja nove izazove za strukturu, sigurnost i stabilnost društava i ekonomija. S ubrzanjem digitalne transformacije, došlo je vrijeme da Evropska unija (EU) navede kako se njene vrijednosti i osnovna prava trebaju primjenjivati u online svijetu. EU je u ranije pokazivala spremnost za aktualiziranje ovakvih tema, kroz prethodne inicijative kao što su Talinska deklaracija o e-vladi, Berlinska deklaracija o digitalnom društvu i digitalnoj vladi zasnovanoj na vrijednosti. Vijeće je kroz Lisabonsku deklaraciju koja se još naziva i digitalna demokratija sa svrhom pozvalo na model digitalne transformacije koji jača ljudsku dimenziju digitalnog ekosistema sa jedinstvenim digitalnim tržištem kao njegovom jezgrom (Evropska komisija, 2022.). Vijeće je također pozvalo na model digitalne tranzicije koji osigurava da tehnologija pomaže u potrebi poduzimanja klimatskih mjera i zaštite okoliša. Vizija EU za digitalnu transformaciju, kao i humana sigurnost, stavlja ljude u centar, osnažuje pojedince i potiče inovativna preduzeća. Komisija je nedavno predstavila prijedlog odluke o svom putu u digitalnu deceniju, koji "postavlja konkretne digitalne ciljeve zasnovane na četiri kardinalne tačke:

- digitalne vještine,
- digitalna infrastruktura,
- digitalizacija poslovanja.
- digitalizacija javnih usluga;

Ove kardinalne tačke će pomoći ostvarenju ove viziju i osigurati put Unije za digitalnu transformaciju naših društava i privrede koji bi trebao obuhvatiti digitalni suverenitet, inkluziju, jednakost, održivost, otpornost, sigurnost, povjerenje, poboljšanje kvalitete života, poštovanje prava i aspiracija ljudi, te osnažiti dinamičnu, resursno- efikasnu i pravednu ekonomiju i društvo u Uniji. (Evropska komisija, 2022.)

Još jedan sjajan primjer odnosa prema digitalnoj transformaciji predstavlja i "Strategija za digitalnu transformaciju mirovnih snaga UN-a", koja posmatra digitalnu transformaciju kao "proces promjene koji je potaknut i omogućen digitalnim tehnologijama, ali uključuje značajnu mjeru kulturne promjene. Pod digitalnim tehnologijama podrazumijeva elektronske alate, sisteme, uređaje i resurse koji generšu, hvataju, pohranjuju ili obrađuju podatke. U skladu s četiri oblasti koje su identificirale američke vlade, strategija se fokusirala na digitalnu

transformaciju koja direktno poboljšava i preventivnu i nacionalnu sigurnost, osnažuje i obogaćuje provedbu mandata, pomaže u otkrivanju prijetnji i prilika u okruženju sukoba, te na obuku i izgradnju kapaciteta koja je potrebna da omogući ove napore" (Strategija za digitalnu transformaciju mirovnih snaga UN, 2021:11).

1.5. Digitalna transformacija ljudskih prava

Nakon sto smo se kroz prethodne naslove upoznali sa tehnoloskom transformacijom i konceptom humane sigurnosti, koji snažno promoviše i štiti ljudska prava i slobode, u ovom poglavlju propitivati ćemo uticaj tehnoloske transformacije na ljudska prava.

Razvoj industrije, posebno vojne, je do kraja Drugog svjetskog rata očigledno bio važniji od razvoja i priznavanja ljudskih prava. Na svu sreću, nakon toga Ujedinjeni narodu su period mira i naučene lekcije iskoristili za proglašenje Univerzalne deklaracije o ljudskim pravima (eng. Universal Declaration of Human Rights - UDHR), koja predstavlja veliku prekratnicu u modernoj historiji i dokument koji je utemeljio osnovna i neotuđiva ljudska prava, koja pripadaju svakom ljudskom biću i koja mu se ne mogu oduzeti. Univerzalna deklaracija o ljudskim pravima je jedno od prvih značajnih dostignuća Ujedinjenih naroda i predstavlja osnovu za mnoge pravno obavezujuće i neobavezujuće međunarodne dokumente koji su, slijedeći istu ideju, kasnije nastali: Međunarodna konvencija o ekonomskim, socijalnim i kulturnim pravima, Međunarodni pakt o građanskim i političkim pravima, Europska konvencija o ljudskim pravima i skraćena Europska socijalna povelja, Konvencija o uklanjanju svih oblika diskriminacije žena, Konvencija o pravima djeteta, te brojni drugi dokumenti.
Povelja Europske unije o temeljnim pravima iz 2000. godine sadrži popis od 50 temeljnih, ličnih, gospodarskih, socijalnih i političkih ljudskih prava od kojih su nama posebno zanimljiva sljedeća:

1. Pravo na ljudsko dostojanstvo,
2. Pravo na život,
3. Pravo na integritet osobe,
4. Pravo na slobodu i ličnu sigurnost,
5. Pravo na poštovanje privatnog i porodičnog života, doma i komuniciranja,
6. Pravo na zaštitu ličnih podataka,

7. Sloboda izražavanja i informiranja,
8. Sloboda okupljanja i udruživanja,
9. Pravo na zdravstvenu zaštitu,
Itd. (Povelja Europske unije o temeljnim pravima, 2007.)

Najčešća kategorizacija ljudskih prava je podjela na građanska i politička prava te ekonomska, socijalna i kulturna prava. Građanska i politička prava sadržana su u člancima 3. do 21. Opće deklaracije o ljudskim pravima i u Međunarodnom paktu o građanskim i političkim pravima (Eng. International Covenant on Civil and Political Rights – ICCPR). Ekonomska, socijalna i kulturna prava sadržana su u člancima 22. do 28. Opće deklaracije o ljudskim pravima i u Međunarodnom paktu o ekonomskim, socijalnim i kulturnim pravima (International Covenant on Economic, Social and Cultural Rights - ICESCR). Univerzalna deklaracija o ljudskim pravima (UDHR) je uključivala i ekonomska, socijalna i kulturna prava te građanska i politička prava jer se temeljila na načelu da različita prava mogu uspješno postojati samo u kombinacij.

"Ideal slobodnih ljudskih bića koja uživaju građansku i političku slobodu i slobodu od straha i oskudice može se postići samo ako se stvore uvjeti u kojima svatko može uživati svoja građanska i politička prava, kao i svoja socijalna, ekonomska i kulturna prava" (Međunarodni pakt o građanskim i političkim pravima i Međunarodni pakt o ekonomskim socijalnim i kulturnim pravima, 1966.), (UN, 1966.). To se smatra tačnim jer bez građanskih i političkih prava javnost ne može ostvariti svoja ekonomska, socijalna i kulturna prava. Naprimjer, čovjeku bez sredstava za život i radnog društva, građanska ili politička prava ili neka deklaracija ne pomaže baš mnogo.
U samu suštinu koncepta humane sigurnosti ugrađeno je poštivanje ljudskih prava, jer je to prepoznato kao uslov za ostvarenje sigurnosti društva. Kada je riječ o sigurnosti i ljudskim pravima, nekoliko je ograničavajućih faktora. Jedan od njih ogleda se u sigurnosnom paradoksu da ako želimo više sigurnosti imati ćemo manje slobode. Zatim princip koji kaže da čovjek može uživati sva svoja prava, sve dok ta prava ne ugrožavaju tuđa prava ili slobodu.
Odnos ljudskih prava i ljudske sigurnosti neophodno je promatrati kroz prizmu sigurnosnih izazova koji individualnu sigurnost i ljudska prava postavljaju kao osnovu nacionalne sigurnosti, a nacionalnu sigurnost postavljaju kao osnovu međunarodne sigurnosti. U Povelji Ujedinjenih nacija posebno je naglašena potreba unapređivanja i podsticaja poštovanja ljudskih prava i osnovnih sloboda za sve, bez obzira na rasu, pol, jezik ili vjeru (Povelja Ujedinjenih nacija, 1945.). Članice se obavezuju da će raditi na unapređenju općeg poštovanja i uvažavanja

ljudskih prava kao i osnovnih sloboda za sve članove. U zajednici u kojoj ne vladaju pravila i zakoni, nema ni prava, što dovodi do prirodnog stanja u kojem vlada zakon jačeg. U takvom sistemu vrijednosti opstanak bi bio težak, a bilo kakav razvoj društva vjerovatno nemoguć.

Od formiranja UN-a prije više od 70 godina, smatra se da principi ljudskih prava igraju ključnu ulogu u pružanju međunarodnog mira i sigurnosti. Vlade koje poštuju ljudska prava takođe su generalno shvatile da poštovanje ljudskih prava i vladavine prava jača njihovu snagu, a ne umanjuje je (Human rights watch, 2016.). Važan zadatak UN-a u ovom kontekstu je okupiti narode svijeta oko minimuma standarda ljudskih prava i sigurnosti koji se nalaze u Općoj deklaraciji o ljudskim pravima. Prava štite čovjeka od države i od drugih ljudi, a i državu od čovjeka, međutim, to se dodatno usložnjava pojavom različitih i mnogobrojnih državnih i nedržavnih aktera. Posebno u digitalnom okruženje u kojem, kako neki autori smatraju, država sve više gubi svoju ulogu i značaj, ovi akteri mogu predstavljati sigurnosni izazov. Poduzeća, nevladine organizacije, političke stranke, neformalne grupe i pojedinci poznati su kao nedržavni akteri. Nedržavni akteri također mogu počiniti kršenje ljudskih prava, ali ne podliježu zakonu o ljudskim pravima osim međunarodnom humanitarnom pravu, koje se primjenjuje na pojedince.

Razumijevanje sigurnosti i zaštite ljudskih prava uveliko je promijenjena u periodu terorističkih napada na SAD. Famozni događaji 11. septembra, doveli su do strogog odgovora nacionalne sigurnosti, u kojem je zaštita države stavljena ispred zaštite ljudskih prava. Jedan od negativnih narativa, koji se pojavio u kontekstu digitalne tehnologije i rastućeg terorizma, je da postoji nulti izbor između zaštite nacionalne sigurnosti i poštovanja ljudskih prava. Javno uokvirivanje ovih pitanja naišlo je na žestoka suprotstavljanja, jer u tom slučaju ili dajemo prednost borbi protiv terorizma ili štitimo prava i privatnost, ali ne možemo učiniti oboje, posebno kada je tehnologija uključena. Sa realne tačke gledišta, može se zaključiti da je obezbjeđivanje sigurnosti prioritet ljudskih prava, a zaštita privatnosti i ljudskih prava važna dimenzija sigurnosti. Dok je veći dio javne rasprave uokviren u pojednostavljene binarne opozicije (Human rights watch, 2016.).

UN priznaje da se ljudska prava mogu ograničiti ili čak pomaknuti u vrijeme izvanrednog stanja ali izvanredno stanje mora: biti stvarno, utjecati na cijelo stanovništvo i prijetnja mora biti samoj opstojnosti nacije. Proglašenje izvanrednog stanja također mora biti posljednje sredstvo i privremena mjera (UN, 2003.). Pandemija Covid-a 19, kao svježi primjer je ograničavanje ljudskih prava dovela na jedan novi nivo. Privremeno su ograničavana prava na

slobodno kretanje, okupljanje, komuniciranje i mnoga druga ljudska prava. Sagledano iz drugog ugla, takva ograničavanja služe državnim sistemima da uvide do koje mjere su građani poslušni, upravljivi, i tolerantni na ukidanje prava uslijed straha, panike i životne ugroženosti. Nacionalna sigurnost i međunarodni mir i sigurnost zavise od spremnosti vlada da svoje tehnološke kapacitete za borbu protiv terorizma, migracija, pandemija i drugih globalnih prijetnji stave pod vladavinu prava i da pomire svoju odgovornost za borbu ovih protiv prijetnji sa svojim obavezama u vezi sa ljudskim pravima (Human rights watch, 2016.). Takve promjene zahtijevaju promjenu paradigme u globalnom pristupu borbi protiv savremenih prijetnji u međusobno povezanom digitalnom kontekstu, kako bi se zaštita sloboda i ljudskih prava ponovo shvatila kao ključna za zaštitu nacionalne i međunarodne sigurnosti.

Shodno tome, naredni dio rada biti će posvećen regionalno kontekstualiziranim i globalnim digitalnim prilikama i prijetnjama kakve mogu iskusiti lokalni ljudi i zajednice u novom ekosistemu 21.-og stoljeća. Predstaviti će se sile novog normalnog sigurnosnog okruženja i njihov uticaj na humanu sigurnost. Cilj je uvesti pitanja ljudske sigurnosti u programe digitalnog razvoja, za sveobuhvatnije razumijevanje odnosa između društvenih promjena, koje digitalna transformacija ostvaruje, i ljudskih prava.

2. Digitalni ekosistem 21.stoljeća

U samoj suštini čovjekovog bića nalazi se instink za preživljavanjem, koji je kroz historiju tjerao čovjeka na prilagođavanje, razvoj, otkrivanje i pravljenje novih stvari. To je tako još do kamenog, bronzanog i željeznog doba, kada je transformacija materijala bila pokretačka snaga i uvod u nove kreativne načine destrukcije. Još od transformacije materijala pa sve do društvene modernizacije, preko perioda transformacije energije (poznatog kao "industrijske revolucije"), do perioda transformacije informacija, čovjek je taj koji oblikuje svoj ekosistem. Da li je došlo vrijeme da ekosistem oblikuje čovjeka? U duhu ovog pitanja, u ovom poglavlju baviti ćemo se ulogom i položajem čovjeka u savremenom digitalnom okruženju, te pitanjem kako te promjene utiču na humanu sigurnost, ljudska prava i slobode, te u konačnici na život dostojan čovjeka. Također, pokušat će se dati naučno utemeljen odgovor na pitanje: Kakve implikacije na humanu sigurnost ostvaruje novo digitalno sigurnosno okruženje?

Internet predstavlja najveće civilizacijsko otkriće koje, kao što je već evidentno, ubrzava ljudski razvoj nezamislivom brzinom i omogućava stvaranje virtualnog prostora (Cyberspace). Doveo je globalizaciju do istinski globalne dimenzije i praktički je izbrisao relevantnost postojanja različitih rasporeda ili razlika u vremenskim zonama u svijetu. Tokom 20. stoljeća, rast tehnološkog napretka dramatično se povećao, a digitalna transformacija, koja se upravo odvija, iziskuje velike korake u 21. stoljeću.

Današnje normalno sigurnosno okruženje karakteriše činjenica da ljudi i mašine žive u sve bliskijem odnosu, utoliko da se može reći da su ljudi “nadograđeni” tehnologijom. Taj odnos očigledno pruža velike mogućnosti, ali i prijetnje. Može se zaključiti da tehnologija nikada nije neutralna. Vrlo je lična jer nosi etičke, političke i pravne implikacije (Mijatović, 2019.). Pogrešno je stajalište da tehnologija predstavlja nešto nužno lose i opasno, tehnologija sama po sebi nije problem, ali ‘mi’ je činimo “lošom”, zloupotrebljavajući je u cilju postizanja neke prednosti ili profitiranja. Rasprava o digitalnoj tehnologiji i društvenim promjenama dio je šire literature teorije inovacija (Freeman, 1990.) . Teorija inovacija se najčešće zasniva na Schumpeterovom pojmu socioekonomske evolucije kroz tehnološke promjene (Schumpeter, 1939., 1942.). Sam autor dao mu je ilustrativno ime: „kreativno uništenje“. Kreativna

destrukcija može djelovati na različitim nivoima, od ciklusa proizvoda, preko modnih i investicijskih životnih ciklusa, do takozvanih poslovnih ciklusa (Schumpeter, 1942.). Primjeri kreativne destrukcije najbolje se mogu uočiti analizom medijsko-platformskog okruženja koje je postalo glavno sredstvo informisanja. Društvo u digitalnom okruženju, zadovoljavajući svoje prirodne potrebe za informisanjem i upoznavanjem, podložno je ugrožavanju humane sigurnosti. U takvim uslovima njen zadatak da pruži sigurnost svakom pojedincu, postaje multidimenzionalna i sve teža za ispratiti. Uzrok toga leži u novom sigurnosnom okruženju u kojem su omogućene masovne kampanje destabilizacije društva, cyber hibridno ratovanje, te razni oblici manipulacije društva koji ostvaruju uticaj na politiku, ekonomiju i sigurnost društva. Položaj demokratskog građanina u digitalnom okruženju uveliko ovisi od informacijskih medijia i širokog platformskog okruženja, u kojem dominantnu ulogu igraju umjetna inteligencija, cyber hibridni ratovi, te medijska i informacijska pismenost. Savremena sigurnost se transforormira od očuvanja teritorija prema očuvanju vrijednosti, a u današnjem svijetu informacije predstavljaju ogromnu vrijednost.

Napredak čovječanstva može se posmatrati i kroz mogućnosti pohranjivanja informacija, pa je tako 1980-tih godina, manje od 1% pohranjenih informacija bilo u digitalnom formatu, dok je do 2012. godine 99% pohranjenih informacija bilo u digitalnom obliku. Svake 2,5 do 3 godine, čovječanstvo je u stanju pohraniti više informacija nego od početka civilizacije (Hilbert, 2020.A) Informacijsko društvo može se sagledati kao "pretpostavka održivog razvoja, ali i pokretačka sila novog svjetskog poretka. Dok se, sjedne strane, primarni focus stavljao na razvoj infrastrukture, s druge je fokus na društvene aspekte znanja u prvi plan isticao pravo na informaciju kao jedno od najvažnijih ljudskih prava" (Vajzović, Hibert, Turčilo, 2021. : 120). Svakim danom sve više vremena provodimo u cajber prostoru, prividno ostvarujući svoje pravo na informaciju, jer u moru neprovjerenih ili izmanipulisanih informacija teško je pronaći pravu. Ljudi donose odluke na osnovu informacija kojima raspolažu. Stoga, uzmemo li u obzir pretpostavku da su sve digitalne informaciju koje do nas dolaze prošle pažljivu selekciju i filtriranje, možemo zaključiti da je takvim uticajem, teoretski moguće "upravljati" ljudskim životima i sudbinama. Potrebno je shvatiti da su u pitanju prijetnje i rizici koji ne prave razliku na osnovu nacionalnosti, bogatstva ili društvenog porijekla, već kao takvi predstavljaju prijetnju svima, na lokalnom i globalnom planu. Postoji više vrsta prijetnji koje su se pojavile tokom digitalnog doba, uključujući: digitalnu nejednakost, ugrožavanje privatnosti, zloupotrebe podataka, prevare ili krađe, digitalnu koncentraciju moći i moć društvenih mreža itd.. Sve ove prijetnje potencijalno ugrožavaju ljudska prava i slobode savremenog društva.

Proces digitalne transformacije predstavlja veliki korak koji se dešava jako brzo, pri čemu mnoge ostavlja u „digitalnom raskoraku", koji dodatno povećava nejednakost i ranjivost društva, te tako direktno utiče na njegovu sigurnost. Ideju umreženog i informisanog demokratskog građanin ponajviše osporava neravnomjeran pristup vitalnim tehnologijama.

Dugi niz godina postoji briga o ljudskim pravima, koja je uveliko pogoršana digitalnom tehnologijom. Najveću prijetnju u tom smislu predstavlja globalna nejednakost koja je uzrokovana prvenstveno nedostatkom pristupa tehnologiji, a ne samom tehnologijom. Dok se stanovništva razvijenih zemalja, koja žive u digitalnom ekosistemu, ne mogu sjetiti kakav je svakodnevni život bez internetske veze ili digitalnih uređaja, većina ljudi na svijetu ipak nema digitalno iskustvo. Nedostatak digitalnog iskustva ili nedostupnost interneta predstavljaju ogromanu kočnicu u razvoju društvene zajednice i globalnom povezivanju.

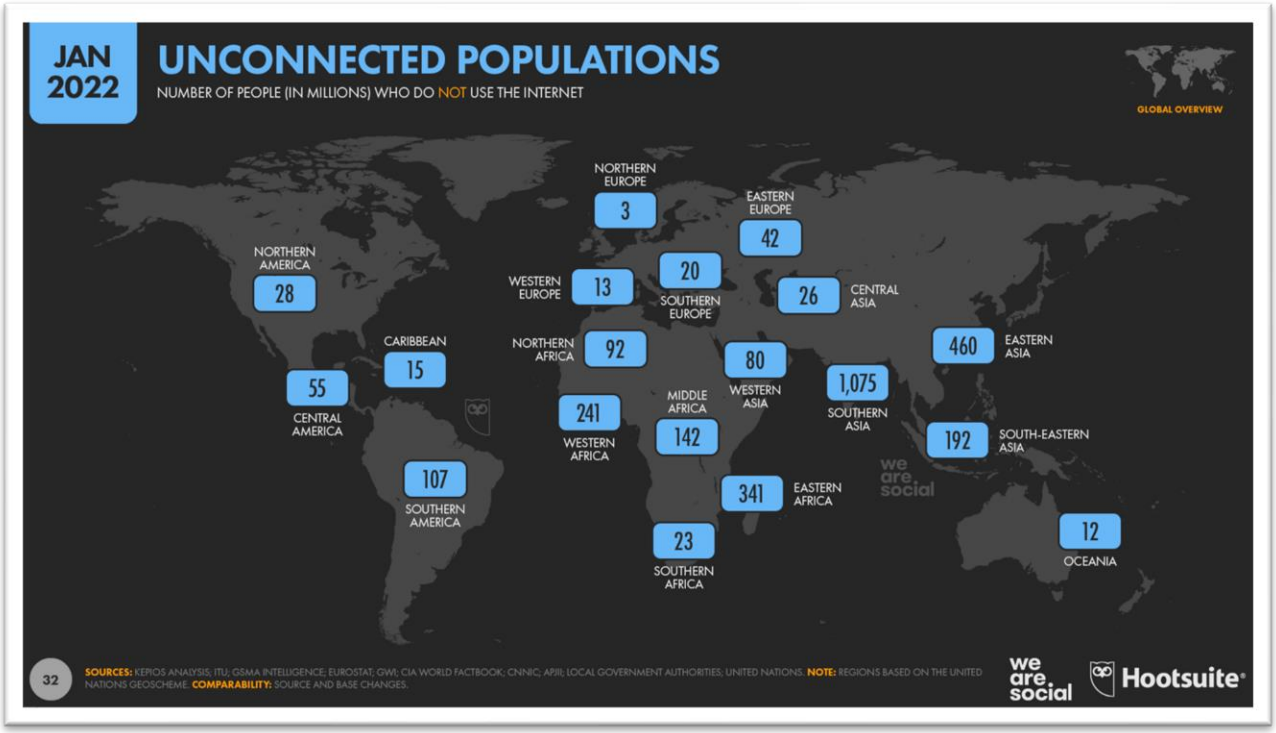
Na globalnom nivou, skoro šest od deset ljudi nije povezano na internet. Još oštrija je činjenica da otprilike 65 posto ljudi u zemljama u razvoju još uvijek ne koristi internet. Primjetno je da ljudi koji žive u nerazvijenim i ruralnim područjima općenito imaju manji pristup internetu, kao i činjenica da veliki broj žena u svijetu uopšte nema pristup istom, što je još jedan izraz rodne nejednakosti. Ovakve digitalne podjele imaju veliki potencijal da značajno pogoršaju postojeću globalnu nejednakost i međuljudsko nerazumijevanje, te u konačnici dovedu do uslova u kojima je još vjerovatniji sukob. Sužavanje digitalnog jaza mora biti rangirano kao glavni prioritet ljudskih prava (Human rights watch, 2016.). Snažnu potporu smanjenju digitalnog jaza pružio je UN kroz svoje razvojne programe i ciljeve održivog razvoja. Ključan iskorak predstavlja UN-ov cilj o univerzalnom pristupu internetu, u zemljama u razvoju. Svi razvojni programi i ciljevi zavise upravo od proširenja pristupa infrastrukturi informacijske i komunikacijske tehnologije širom planete.

Podaci koje je iznio DataReportal u izvještaju za digitalnu 2022. godinu, otkrivaju da je broj ljudi koji ostaju "nepovezani" s internetom sada po prvi put pao ispod 3 milijarde.

Ovo označava značajnu prekretnicu na svjetskom putu ka jednakom digitalnom pristupu i ima posebnu važnost jer je uloga povezanih uređaja prešla od nečeg što se smatra luksuzom i privilegijoom do nečega što je dostupno svima i spašava živote, posebno tokom pandemije COVID-19.

Međutim, iako se brojka smanjuje, najnoviji podaci pokazuju da ima još mnogo posla na realizaciji globalne mreže. "Više od milijardu ljudi ostaje van mreže širom južne Azije, dok skoro 840 miliona ljudi tek treba da dođe na mrežu širom Afrike. U međuvremenu, uprkos tome što čini otprilike 1/5 svjetske povezane populacije, Kina je još uvek dom za više od 400

miliona „nepovezanih“ ljudi u svetu. Broj ljudi u svijetu koji ne koriste internet, izražen u milionima prikazan je na slici br. 2.(Kemp, Datareportal, 2020)



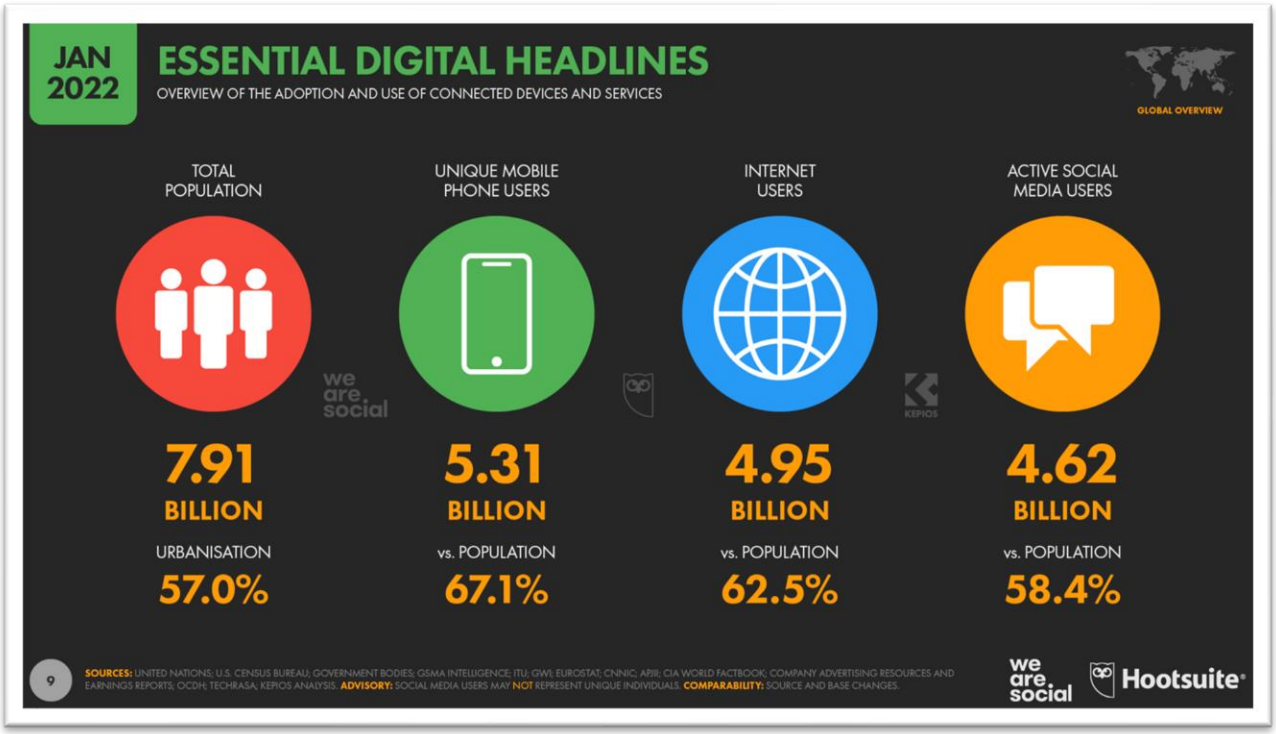
Slika br.2. Broj ljudi u svijetu koji ne koristi internet, izražen u milionima (Datareportal, 2022.)

Nadalje, odličan izvještaj o stanju mobilnog internet povezivanja za 2021. GSMA Intelligence otkriva da 1 od 4 osobe u zemljama s nižim i srednjim prihodima još uvijek nije svjestan postojanja mobilnog interneta. Drugim riječima, stotine miliona ljudi širom svijeta možda još uvijek ne znaju da internet postoji. Dakle, iako su UN možda proglasile pristup internetu „osnovnim ljudskim pravom“, još je dug put da se osigura da svi imaju jednak pristup onome što je vjerovatno najvažnija inovacija našeg doba. (GSMA, 2021)

3. Digitalno sigurnosno okruženje

Navedene tehnološke i društvene promjene dovode do novog kompleksnijeg određenja sigurnosne paradigme od tradicionalno-ortodoksnog fokusa državno-centričnog shvatanja sigurnosti, gdje je pitanje sigurnosti razmatrano u relaciji odnosa rata i mira. (Tačno.net, Bašić, 2016.) Očigledno je da digitalna transformacija dovodi do promjene osnovnih pretpostavki i stavova tradicionalne nauke o sigurnosti. Pojavom savremenih tehnologija i nastankom cyber prostora, čiji broj korisnika se povečava eksponencijalno, pojavila se i jasna potreba za zaštitom društvene sigurnosti jer su se pojavili i novi oblici ugrožavanja.

Brojke koje nam daju početnu preglednost digitalnog okruženja (Slika br.3.), iznio je Simon Kemp u ovogodišnjem izvještaju pod nazivom 'Digital 2020', na svome portalu 'Datareportal'.



Slika br.3. Digitalno okruženje (Datareportal, 2022.)

(S lijeva na desno: Broj globalne populacije, broj korinika mobilnih telefona, broj korisnika interneta, broj aktivnih korisnika socijalnih medija)

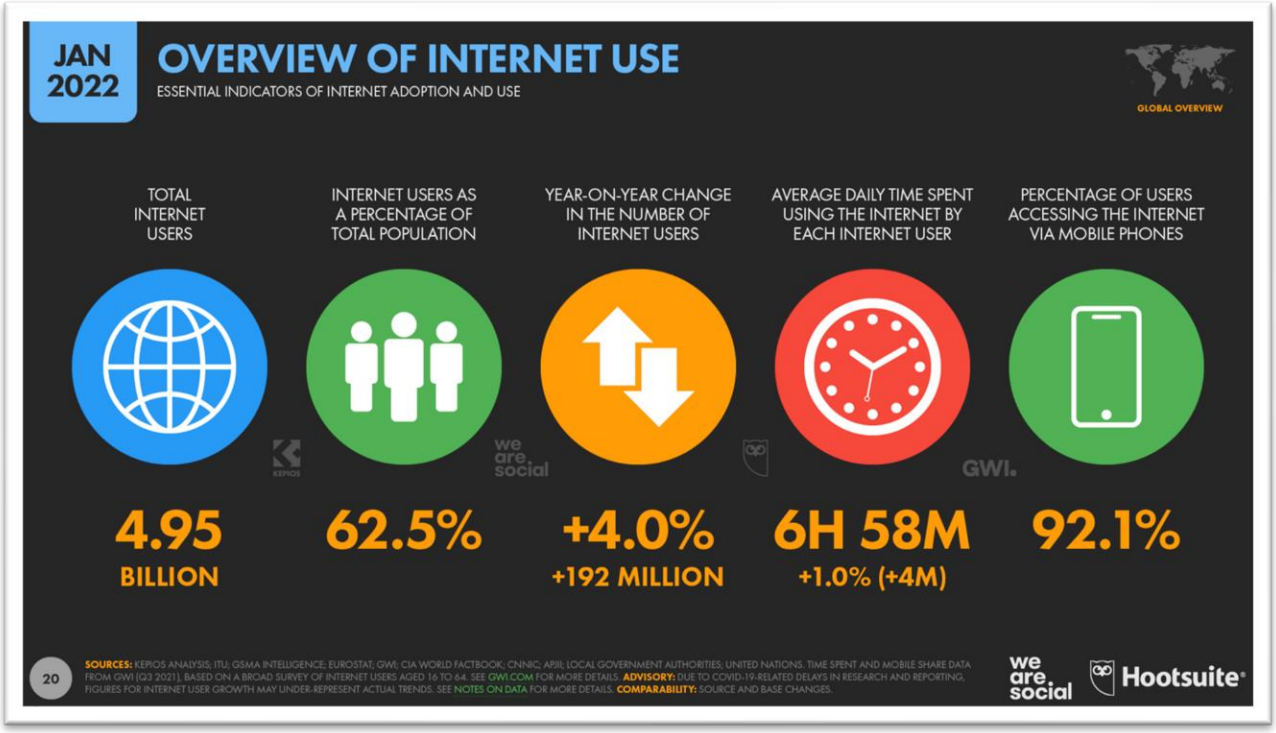
"**Globalna populacija**: Svjetska populacija iznosi 7,91 milijardu u januaru 2022. godine, sa godišnjom stopom rasta od 1,0 posto što sugerira da će ta brojka dostići 8 milijardi negdje

sredinom 2023. godine. Više od polovine (57,0 posto) svjetske populacije sada živi u urbanim područjima.

Globalni korisnici mobilnih uređaja: Više od dvije trećine (67,1 posto) svjetske populacije sada koristi mobilni telefon, a jedinstveni korisnici će dostići 5,31 milijardu do početka 2022. Ukupan globalni broj porastao je za 1,8 posto u protekloj godini, sa 95 miliona novih mobilnih korisnika od ovog doba prošle godine.

Globalni korisnici interneta: Globalni korisnici interneta popeli su se na 4,95 milijardi početkom 2022. godine, a penetracija interneta sada iznosi 62,5 posto ukupne svjetske populacije. Podaci pokazuju da su korisnici interneta porasli za 192 miliona (+4,0 posto) u protekloj godini, ali stalna ograničenja istraživanja i izvještavanja zbog COVID-19 znače da bi stvarni trendovi rasta mogli biti znatno veći nego što ove brojke sugeriraju.

Globalni korisnici društvenih medija: U januaru 2022. godine postoji 4,62 milijarde korisnika društvenih medija širom svijeta. Ova brojka je jednaka 58,4 posto ukupne svjetske populacije, iako je vrijedno napomenuti da „korisnici“ društvenih medija možda ne predstavljaju jedinstvene pojedince. Globalni korisnici društvenih medija porasli su za više od 10 posto u posljednjih 12 mjeseci, a 424 miliona novih korisnika započelo je svoje putovanje društvenih medija tokom 2021. godine.“(Kemp, Datareportal, 2020)



Slika br.4 Osnovni pokazatelji usvajanja i korištenja interneta (Datareportal, 2022.)

Na osnovu ovog prikaza sa Datareportal-a, uviđamo da je broj korisnika interneta, početkom 2022. godine iznosio 4.95 milijardi, odnosno 62,5% ukupne globalne populacije. Iz godine u godinu broj Internet korisnika raste za oko 4%, odnosno godišnje se umreži više od 192 miliona novih korisnika interneta. Svaki korisnik interneta u prosjeku dnevno provede 6 sati i 58minuta koristeći ga, a taj broj se godišnje povečava za oko 1%. I za kraj, zanimljiv je podatak koji nam govori da čak 92,1% korisnika Internet, istom pristupa putem pobilnog uređaja. Kepios analiza otkriva da su se korisnici interneta više nego udvostručili u posljednjih 10 godina, popevši se sa 2,18 milijardi na početku 2012. na 4,95 milijardi početkom 2022. (Kepios Analiysis, 2021, prema Kemp, Datareportal, 2022)

U novom normalnom sigurnosnom okruženju važnu ulogu u oblikovanju javnog mninja i društvene stvarnosti imaju informacijski mediji i platformsko okruženje sa društvenim mrežama. Događaji i dešavanja u virtualnom svijetu, zbog sve većeg broja korisnika, mnogo brže ostvaruju implikacije na društvenu realnost. Te implikacije često mogu biti negativne i generisati brojne prijetnje po humanu sigurnost. U takvim uslovima opstanka, kada rat (u svom izvornom obliku) više ne predstavlja najveću sigurnosnu prijetnju, sigurnosna paradigma se svodi prije svega na obezbjedjenje mogućnosti normalnog preživljavanja pojedinca (grupe) u okviru koje se sigurnost posmatra kao pitanje koje je nužno povezano sa uticajem čovjeka na promjene u globalnom okruženju i uticaj globalnih promjena na njegovo ponašanje. U ovom konceptu sigurnosne paradigme glavni fokus je na "ideji" koja ima moć utjecaja na ponašanje pojedinca, društva i elite, a time i na ponašanje države u međunarodnim odnosima, što vodi stvaranju nove "sigurnosne paradigme", a samim tim i do nove sigurnosne zajednice.
Iza ovog zastora novih tehnoloških promjena, koje dobijaju na novom intenzitetu u eri digitalne industrijske revolucije, Bašić (2022.) smatra da "zajednice koje nisu u stanju da kreiraju adekvatan sistem obrazovanja sopstvenog stanovništva, koje nisu u stanju da kreiraju novu ideološku i interesnu strukturu političkih elita, koje nisu sposobne obezbjediti korišćenje svih benficija koje proističu iz četvrte digitalne revolucije, teško da mogu računati da će preživjeti samim tim što će okrivljivati druge za njohovo sopstveno nestajanje" (Bašić, 2022.) .

Suočeni smo sa razvojnim paradoksom. Iako ljudi u prosjeku žive duže, zdravije i bogatije, ovaj napredak nije uspio povećati lični osjećaj sigurnosti ljudi. Ovo vrijedi za zemlje širom svijeta i zavladalo je i prije neizvjesnosti uzrokovane pandemijom COVID-19. Specijalni izvještaj UNDP-a (2022.) objašnjava ovaj paradoks, naglašavajući snažnu povezanost između pada nivoa povjerenja i povećanog osjećaja nesigurnosti. Ovaj izvještaj a o ljudskoj sigurnosti

otkrio je da u prosjeku 6 od 7 ljudi u bogatim i siromašnim zemljama pati od rastućeg osjećaja nesigurnosti (Kuensell, Tshering Lhamo, 2022.).

Uprkos mnogim godinama značajnog napretka u razvoju i ljudi koji žive zdravije, bogatije i bolje, osjećaj i percepcija sigurnosti nisu mnogo napredovali. To jasno pokazuje da napredak u globalnom razvoju ne dovodi automatski do većeg osjećaja sigurnosti. Kako bismo prevladali ovu zapanjujuću statistiku i riješili se nepovezanosti između razvoja i percipirane sigurnosti, ključno je proširiti naše razumijevanje humane sigurnosti, razumijevanje različitih mehanizama kojima ona djeluje, te u konačnici razumijevanje kako postojećih tako i novih prijetnji ljudskoj sigurnosti. Glad je globalno u porastu, nejednakosti u društvima se svakodnevno produbljuju, klimatske promjene i dalje utječu na najranjivije, prisilno raseljene osobe zbog sukoba dostigle su rekordnu razinu te svijet dovele do migrantske krize. Osim ovih prijetnji, važno nam je identificirati i pripremiti se za različite novonastajuće prijetnje, a posebno razumjeti one koje su jedinstvene za složenost 21. stoljeća.

Ranije spomenuti izvještaj, identificirao je negativnu stranu digitalne tehnologije kao jednu od pet skupina prijetnji koje su se pomaknule i postale istaknutije posljednjih godina. Svjedoci smo značajnog tehnološkog napretka u nizu područja uključujući informacijsko komunikacijsku tehnologiju, umjetnu inteligenciju i kvantno računanje. Ovi proboji već donose poremećaje i promjene u poslovanju, upravljanju i funkcioniranju društva (Ibid.).

Pametni telefoni (eng.Smartphone), na tržištu se pojavljuju od 2007. godine, a prvi smartphone uređaj koji je pušten na tržište je iPhone. iPhone je bio prvi mobilni telefon koji je pokrenuo tehnološku revoluciju pametnih telefona, pa su zahvaljujući Steve Jobsu danas pametni telefoni Iphone-a najmoćniji na tržištu. Pametni telefoni, toliko su uznapredovali, da su postali nezaobilazan dodatak za svaku priliku.

Stoga i ne čudi njihova globalna rasprostranjenost, da budemo precizni, „više od dvije trećine (67,1 posto) svjetske populacije sada koristi mobilni telefon, a jedinstveni korisnici će dostići 5,31 milijardu do početka 2022.godine. Ukupan globalni broj porastao je za 1,8 posto u protekloj godini, sa 95 miliona novih mobilnih korisnika od ovog doba prošle godine. Novi izvještaj App Annie State of Mobile za 2022.godinu, otkriva da tipični mobilni korisnik sada u prosjeku provede 4 sata i 48 minuta dnevno koristeći svoj telefon. (Datareportal, Kemp, 2022.)

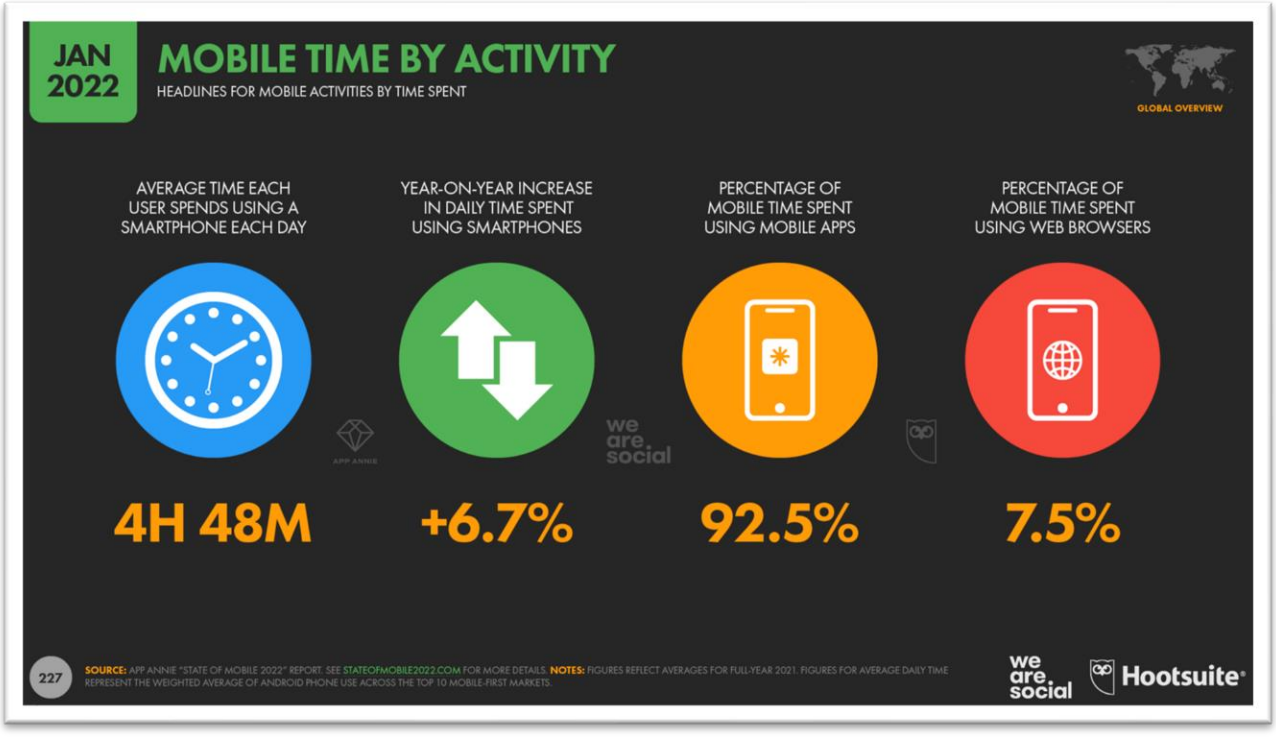
To znači da će 5,3 milijarde mobilnih korisnika u svijetu provesti više od milijardu godina zajedničkog ljudskog vremena koristeći mobilne telefone 2022. godine.

U tako rastućem tržištu ostvaruju se i ogromne zarade. Pored prihoda od prodaje i servisiranja mobilnih uređaja, (koji su pomogli da se Apple Inc. podigne na tržišnu vrijednost od 3 triliona

dolara) prije samo nekoliko mjeseci, korisnici pametnih telefona u svijetu ukupno su potrošili 170 milijardi dolara na mobilne aplikacije i kupovinu unutar aplikacija u 2021.(Ibid.)

Richard Hodson (Nature Outlook, 2018) smatra da postoji zabrinutost zbog uticaja pametnih telefona, videoigara i društvenih medija na našu mentalnu dobrobit . Te su zabrinutosti toliko izražene da tehnološki divovi iz Silicijske doline već počinju poduzimati korake ka iznalaženju rješenja za negativne uticaje tehnologije. No mnogi istraživači tvrde da još uvijek nedostaju dokazi o šteti i o samoj učinkovitosti korektivnih intervencija, te da sve veći dio naše kulture postoji samo u digitalnom obliku.

U današnje vrijeme, pametni telefoni su postali mali đepni kompjuteri, jer na 'malom' ekranu mogu obavljaju sve radnje koje može i suvremeni računar ili laptop. Jedan pametni telefon u digitalnom okruženju pruža nezamislive mogućnosti: komuniciranja, informisanja, i izražavanja, pa se vrijeme koje ljudi provode aktivno koristeći svoj uređaj, iz dana u dan povečava (Slika br.5.)



Slika br.5. Potrošnja vremena na mobilnom telefonu (Datareportal, 2022.).

Zaključujemo, na osnovu prethodne slike (br.5.), da dnevno u prosjeku svaki korisnik smartphona provede 4 sata i 48 minuta, sa godišnjim rastom od 6,7%. Što sa svojom tendencijom još bržeg rasta u budućnosti, može predstavljati ogroman društveni problem. I za

kraj, navodi se da 92.5% vremena na telefonu korisnici provedu koristeći mobilne aplikacije, dok preostalih 7,5% vremena provedu na svojim Internet pretraživačima; (Datareportal, 2022.).

4. Efekti cyber prostora

Ovo poglavlje će osigurati rezultate na osnovu kojih bi se moglo zaključiti kakav uticaj je ostvarila digitalizacija svakodnevnice na humanu sigurnost i posmatranje sigurnosti čovjeka, njegovog integriteta, digitalne imovine i dostojanstva.

Smatra se da cyber prostor ima virtuelnu prirodu, međutim, to nije baš tačno. Cyber prostor se sastoji od apsolutno opipljivih elemenata kao što su personalni računari, mobilni uređaji, serveri, ruteri, optički kablovi, sateliti, operativni sistemi, aplikacije, itd. Kao i mnoge druge stvari, cyber prostor sam po sebi nije ni dobar ni loš, sve zavisi kako ga koristite (Ramírez, Segura, 2017). Moramo priznati da je kreiran i razvijen samo sa svojom funkcionalnošću i prednostima koje donosi svojim korisnicima. Međutim, do nedavno se nije razmišljalo o njegovoj sigurnosti. Njegovo rođenje i vrtoglava evolucija vođeni su idejom slobode i odsustva granica, ograničenja ili bilo kakve regulative. S obzirom na ove okolnosti, bilo je samo pitanje vremena da se pojavi cyber kriminal. To je uključivalo progresivno mijenjajući format: od izolovanog delikventa do organizirane kriminalne grupe, povećavajući transcendaciju cyber napada vrtoglavom brzinom. Znamo da je današnje društvo u cjelini ugroženo kada je cilj cyber napada kritična infrastruktura ili vitalne usluge xi, neophodne za obavljanje naših svakodnevnih aktivnosti.

Cyber prostor je toliko integrisan u svakodnevni život savremenog čovjeka da se može reći da uveliko određuje način na koji čovjek djeluje i rješava probleme u stvarnom svijetu. Uzmimo za primjer jedan hipotetički „digitalni raspored“ prosječnog i običnog dana izmišljene osobe X. Osoba X budi se uz zvuk alarma sa pametnog telefona[5] koji uzima realno vrijeme sa

[5] Prvo su se pojavili fiksni telefoni, koji su predstavljali revolucionarno otkriće. Tehnološkim razvojem telefoni su postali prenosivi, bežićni i mobilni, pa se u njihovom imenu moralo naglasiti mobilni telefon. Sljedeći korak naprijed predstavili su tzv. pametni telefoni kakve danas poznajemo.
Nešto starije modele mobilnih i pametnih telefona, između ostalog karakteriše i njihovo eksterno napajanje u obliku baterije koja se mogla s lahkoćom zamijeniti, popraviti ili odstraniti. Edward Snowden tvrdi da se samo fizičkim odstranjivanjem baterije mogu onemogućiti sve aktivnost uređaja. (Snowden to objašnjava produbljujući

interneta, te u treptaju oka, prije svih fizioloških i ljudskih potreba, ostvaruje svoj prvi kontakt sa svojim pametnim uređajem. Tokom svog sna, osoba X propustila je nesagledivu količinu informacija o najnovijim dešavanjima u svijetu, koja se prenose kroz digitalno okruženje. U prvih sat vremena, još iz topline kreveta osoba X je pisala i odgovarala na mnoge mejlove, obraćala pažnju na društvene mreže, grupe „WhatsApp-a“ i Vibera, i tako dalje. Osoba X će, iako toga vjerovatno nije ni svjesna, ostatak dana svuda sa sobom nositi svoj pametni telefon koji je u svakom trenutku u ruci ili na dohvat ruke. Takav jedan dan završava se naravno sa telefonom u krevetu, koristeći ga kao sredstvo koje može zadovoljiti potrebu za zabavom, informisanjem, komuniciranjem, te potrebu za društvenim, poslovnim, ili drugim ostvarenjem. Nakon ovog primjera, ne možemo a da se ne zapitamo, kako smo živjeli prije nekoliko godina, kada nismo imali e-poštu, pametne mobilne telefone ili World Wide Web? Sa današnjim digitalnim okruženjem, koje ne izostavlja nijednu ljudsku djelatnost, postaje sve teže zapamtiti ili zamisliti svijet bez informacijsko-komunikacijskih i tehnoloških pomagala.

4.1. Razmjena informacija u cyber prostoru

Društvene mreže i socijalne platform zamijenile su nekadašnja dječija igrališta, domove kulture i zabave, te postale glavno mjesto za druženje, upoznavanje i razmijenu ideja. Svojom masovnom upotrebom postale su važan dio čovjekovog informisanja, izražavanja i zabavljanja. Društvene mreže tako imaju direktan uticaj na podizanje ali i oblikovanje svijesti o različitim pitanjima, društvenim, ekonomskim, političkim i dr., jer vrlo brzo privlače pažnju društva, medija i političara. Njihovo uvjerenje u moć društvenih medija i interneta da im pomognu da utiču na političke programe može se sažeti u izjavu: *'Sve što vam treba je kompjuter i internet da promijenite svijet!*'

Stoga i ne čudi podatak da je “današnji broj korisnika društvenih medija došao do 4,62 milijarde, te je 3,1 puta veći od brojke od 1,48 milijardi u 2012. godini, što znači da su korisnici društvenih medija porasli za 12 posto u protekloj deceniji. Za kontekst, najnoviji podaci pokazuju da je 424 miliona korisnika započelo svoje putovanje na društvenim mrežama tokom

priču o prisluškivanju i nadziranju vašeg pametnog uređaja (čija baterija je integrisana u njegovo kućište i pruža konstantnu mogućnost napajanja „pozadinskih procesa“), koji prikuplja informacije čak i onda kada naizgled djeluje u stanju mirovanja.

prošle godine, što je u prosjeku više od milion novih korisnika dnevno, ili otprilike 13½ novih korisnika svake sekunde.” (Kemp, Datareportal, 2020)

Takav cyber prostor, promenio je način na koji se povezujemo, komuniciramo i interaktiramo sa drugima, sa pojedincima, sa kompanijama ili sa vladom i javnim strukturama. Sve društvene promjene nastaju na osnovu društvene komunikacije, stoga je za očekivati da u današnjem svijetu brze i lake komunikacije, društvene promjene cvjetaju. To nažalost nije uvijek tako. Ukoliko je komunikacija nedostupna, onemogućena, loša, zlonamjerna ili obmanjujuća, veća je vjerovatnća da će određena društvena promjena imati negativnu konotaciju.

U 21.stoljeću dešava se poremećaj načina komuniciranja, koju karakteriše zamjena žive riječi i vrijednosti zdrave komunikacije za "mehaničku" komunikaciju, ponajviše dopisivanjem ili u obliku fotografija.

Društvene mreže i samo platformsko okruženje omogućili brzo i lahko pokazivanje svog stava i statusa: socijalnog, ekonomskog, emotivnog, psihološkog, političkog i drugih., ali kroz neki ljepši filter, koji nameće nove i uvrće trenutne društvene vrijednosti. Stoga je uobičajna pojava zaustavljanje „svijeta“ na sekund, kako bi se napravila i objavila fotografija za neku društvenu platformu, koja treba lažno zadiviti nekoga predstavljanjem stvari ljepšim nego što one zapravo jesu.

Kada upotreba digitalnih tehnologija i lični ljudski kontakt nisu u ravnoteži, može doći do nekih kulturoloških nesporazuma. Web tehnologije mogu biti bezlične u smislu da se isti poziv ili informacija šalje masovno. Povjerenje, bliskost i osjećaj zajednice općenito se mogu izgraditi uglavnom na osnovu ličnog pristupa i kroz nekoliko ličnih sastanaka (ELSA, Zhemerov, 2020.).

U savremenoj digitalnoj komunikaciji između subjekata primjetno nedostaje odgovarajuća kontrola od strane tijela javne vlasti u nesavjesnom ponašanju sudionika u digitalnoj komunikaciji. Korištenjm posebnih alata i gotovih software-skih rješenja koji vam omogućuju da stvari radite online pod maskom anonimnosti, gotovo da se onemogućuje identifikacija osobe koja koristi digitalnu tehnologiju. Anonimnost predstavlja predmet žestokih rasprava, dok jedni tvrde da svako zaslužuje pravo da bude anoniman ukoliko to želi, drugi par osjećaju strah jer ne znaju šta da očekuju od anonimnog „identiteta“. U takvim okolnstima međuljudsko povjerenje je sve teže ostvarivo jer kako vjerovati nekome ko se nalazi negdje u svijetu, pod nekim pseudonimom i čudnom slikom profila.

4.2. Platformsko okruženje

Ekspanzija interneta i platformskog okruženja dovela je do ekstremno ubrzog procesa nastanka i širenja informacija. Korisnici digitalnih pratformi i njihovih usluga postali su kreatori sadržaja i njihov konzument, te u konačnici proizvod i predmet trgovine ali i izmanipulisani objekt unutar algoritamske demokratije (McDavid, Jodi, 2020, prema Vajzović, 2020).). U tom slučaju, platforme ne proizvode sadržaj i uglavnom su besplatne i ostavljene korisnicima kao prostor za informisanje i izražavanje. Ipak ekonomski interes kroz platformsko okruženje postavlja nova shvatanja vrijednosti informacija. Došlo je do uviđanja prilike za profitiranjem na informacijama, prvenstveno korisničkim (npr. Za potrebe ciljanog marketinga), a veliki informacijski centri (BigData) u današnjem svijetu predstavljaju veliko bogatstvo. U doba hiperprodukcije sadržaja sve češće svjedočimo informacijskom poremećaju u formi netačnog informisanja, dezinformisanja i zlonamjernog informisanja. Stoga je očigledna i promjena odnosa „interneta“ prema čovjeku, a preciznije bi se reklo prema korisniku, koji će u budućnosti vjerovatno zamijeniti pojam demokratskog građanina. Upravo iz toga se očituje mogući efekat digitalnog platformskog okruženja koje čovjeka više ne posmatra kao individu i jedinku koja ima lični integritet i prava, nego čovjeka posmatra kao korisnika, čije potrebe uz pomoć algoritama i njegovog digitalnog otiska može vrlo precizno i efikasno zadovoljiti, odnosno plasirati mu odgovarajući sadržaj ili produkt. Ljudi, odnosno korisnici koji su stalno vezani za digitalne platforme “obavljaju različite oblike uglavnom nematerijalnog i rijetko plaćenog rada kao što su skrolovanje, lajkanje, dijeljenje, komentarisanje ili kreiranje sadržaja (radna strana ovog trougla)”. Istovremeno, svaki pokret ili emocionalna reakcija se kontinuirano snima (Joler, 2020.). Promijenjena uloga čovjeka, u platformskom okruženju, bez sumnje predstavlja izazov za humanu sigurnost, te zahtijeva široko razumijevanje zaštite čovjeka od negativnih uticaja digitalnog prostora. U takvom sistemu, svakodnevno bismo trebali ispitivati sebe: Koliko su informacije koje dobijam vjerodostojne, provjerene, korisne i dobronamjerne?, te biti svjesni činjenice da u monetizovanom okruženju sve što je naizgled besplatno, ima neki dublji vid interesa.

4.3. Digitalni mediji

Digitalizacija i prelazak medija na online platforme predstavljaju historijske pomake čovječanstva u načinu informisanja, što potvrđuje i masovnost upotrebe digitalnih medijskih platformi. Vrijeme kada su se svakodnevne aktuelne informacije mogle pronaći samo u novinama i na oglasnim pločama je završeno. Internetom i digitalnim informacijskim platformama, vijesti i informacije dolaze do krajnjeg korisnika u treptaju oka, pa danas čovjek za 1 dan može prikupiti informacija iz cijelog svijeta, više nego neki njegov predak za nekoliko godina. Ogromna brzina i količina informacija ipak nas nisu učinili napredijim, nego samo podložnijim različitim medijskim uticajima kroz različite sadržaje. Autori Palmer i Lewis u svom članku (2009.) definisali su društvene medije kao skup internet aplikacija, platformi i medija kojima je primarni cilj omogućiti komunikaciju i saradnju između ljudi, te zajedničko stvaranje uz razmjenu ideja i sadržaja. Njihov značaj ponajviše se ogleda u interakciji između korisnika i zajednice, tj. u omogućavanju vođenja asinhrone, trenutne i interaktivne komunikacije, uz niske troškove.

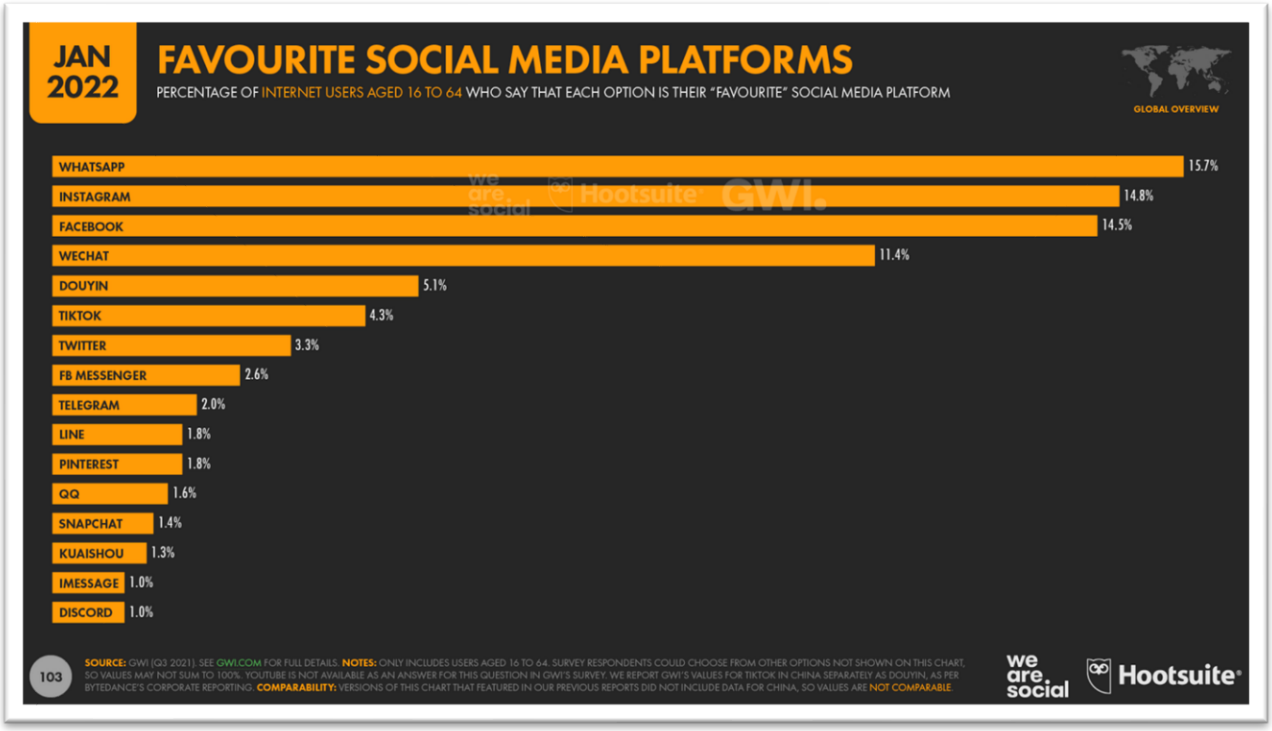
Ipak moramo biti svjesni da svaka informacija koja dođe do nas ostavlja neki trag u našem životu. Stoga ovi mediji imaju veliku moć jer mogu „neprimjetno“ uticati na društvo i javno mnijenje. Koliki uticaj ima javno mnijenje u digitalnom medijskom okruženju, nemoguće je precizno izmjeriti jer vlada privid važnosti mišljenja čovjeka. Primjer za to može biti neki komentar, pojedinca na internet, ispod neke fotografije, videa, članka, bloga ili vijesti. Njegova sloboda izražavanja i uticaja na društvo su zapravo prividni, jer u suštini on ne mijenja ništa, te u velikom broju slučajeva uopšte ne doalazi do kreatora sadržaja, kreatora politika, ili aktera nekog događaja, čak je veća šansa da će doći u konflikt sa korisnicima drugačijeg mišljenja koji će reagovati na njegov komentar, pri čemu je važno naglasiti čovjekovo ubjeđenje da njegov komentar vide široke narodne mase. U današnjem informacijski bogatom platformskom okruženju, kada svaki korisnik internet uz par klikova, ima pristup ogromom broju rezultata, koje ne može pregledati "za dva života", reklo bi se da nauka i društveni razvoj imaju odriješene ruke. Ipak to nije tako, a razlog leži u činjenici da je profit na prvom mjestu. To još jednom pokazuje ulogu i položaj čovjeka u digitalnom sigurnosnom okruženju, te složenost sistema na kojem humana sigurnost mora kontinuirano napredovati.

Na samom početku ovog poglavlja predstavit će se najpopularnije digitalne platforme i brojnost njihovih korisnika, kako bismo imali odgovarajući okvir za posmatranje potencijala i efekata digitalnog medijskog okruženja. Zaključci izvedeni iz ovog poglavlja omogućiti će bolje

razumijevanje digitalnih prijetnji i odnosa između medija i humane sigurnosti o kojima će se govoriti u narednom poglavlju.

4.4. Favoriti društvenih mreža

Najpopularnije društvene medijske platforme danas su naravno one koje imaju naviše aktivnih korisnika. Odličan vizuelni prikaz najpopularnijih društvenih platformi daje slika br.6.



Slika br.6. Najpopularnije platforme društvenih medija (Datareportal, 2022.).

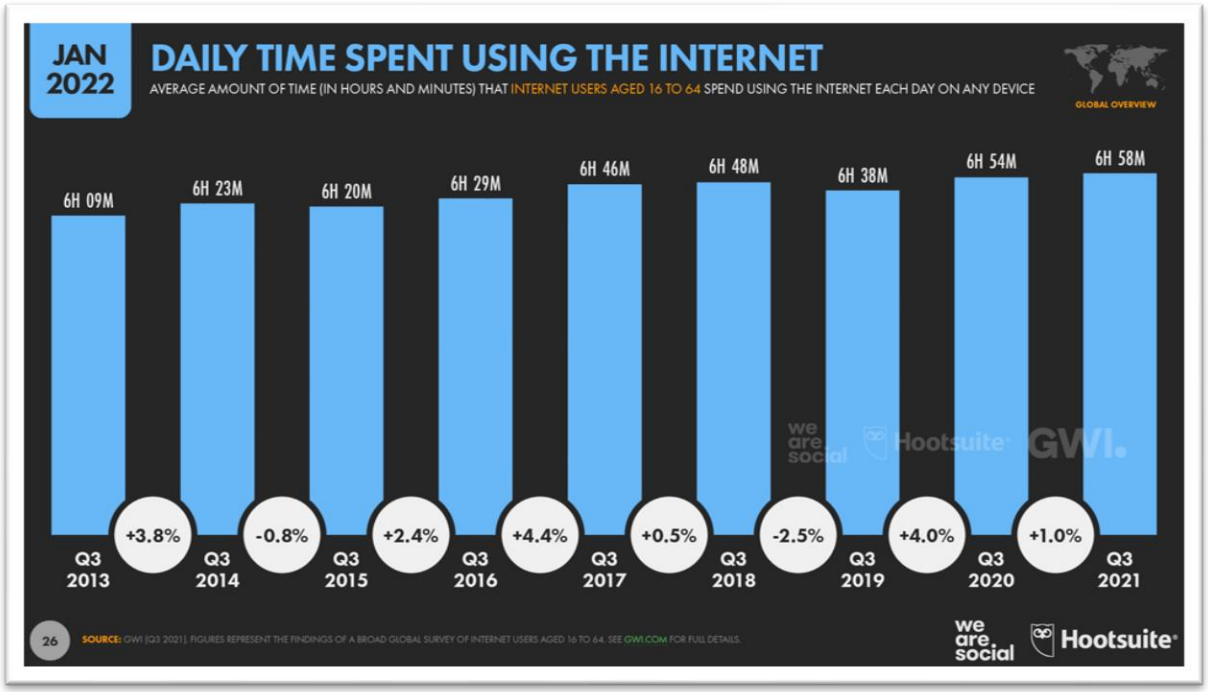
Kada je riječ o svjetskim omiljenim platformama društvenih medija, na vrhu globalne ljestvice nalazi se jedna od Meta[6] platformi –WhatsApp–, sa 15,7 posto radno sposobnih korisnika interneta koji biraju ovu aplikaciju za slanje poruka kao svoju omiljenu društvenu platformu.

[6] Meta je ranije bila poznata kao kompanija Facebook, a ustvari je krovni, multinacionalni tehnološki konglomerat i holding kompanija sa sjedištem u Kaliforniji. To je matična organizacija Facebooka i njegovih podružnica (WhatsApp, Instagram, Messenger i dr.). Jedna je od najvrjednijih svjetskih kompanija i smatra se jednom od pet velikih kompanija u informacijskim tehnologijama, uz Amazon, Google, Apple i Microsoft. Kompanija sav svoj prihod ostvaruje uglavnom prodajom reklamnih mjesta trgovcima (Facebook Reports Second Quarter, 2021).

Također, Instagram je sada pretekao Facebook i zauzeo drugo mjesto na svjetskoj rang listi. Ipak, to je još uvijek blizu jer kao što vidimo, 14,8 posto globalnih korisnika interneta identificira Instagram kao svoju omiljenu platformu, u poređenju sa 14,5 posto korisnika Facebooka. Globalni korisnici društvenih medija porasli su za više od 10 posto u posljednjih 12 mjeseci, a 424 miliona novih korisnika započelo je svoje putovanje društvenih medija tokom 2021. godine.“(Kemp, Datareportal, 2022). Sve ove platforme se međusobno svakodnevno takmiče i bore za čovjekovu pažnju, koja platforma ili aplikacija će mu pružiti najviše sadržaja i na kojoj će provesti najveći dio svog vremena.

4.5 Vrijeme na mreži

Najnoviji podaci na DataReportal-u (iz 2022. godine), pokazuju da ljudi zapravo provode više vremena nego ikada koristeći povezanu tehnologiju. Jedan od razloga koji je doveo do toga svako je pandemija COVID-19, koja je uvela blokade i ograničenja kretanja, pa je tako uvjerila čak i one koji su se premišljali o pridruživanju društvenim platformama, da je to prava stvar. S obzirom na to da korisnici društvenih medija sada čine 58,4 posto ukupne svjetske populacije, trebali bismo očekivati da će stope rasta početi usporavati u narednih nekoliko godina, a ovo bi moglo biti posljednji put da izvještavamo o dvocifrenom godišnjem rastu u korisnika društvenih medija. Istraživanje GWI otkriva da "tipični" globalni korisnik interneta sada provodi skoro 7 sati dnevno koristeći internet na svim uređajima” (Kemp, Datareportal, 2020). To je jasno prikazano na slici br.7,(slika br.7) koja prikazuje godišnje povečanje vremena provedenog na internet, na dnevnoj bazi.

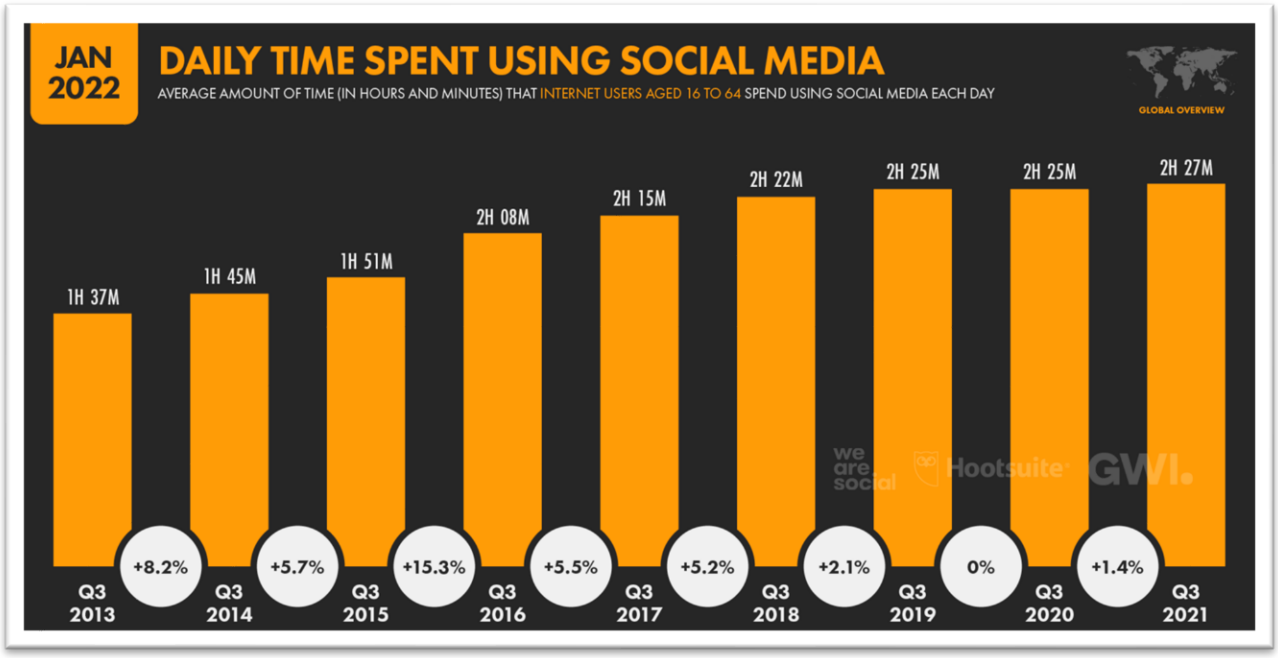


Slika br.7. Dnevna Potrošnja vremena na internetu (Datareportal, 2022.).

Na osnovu ove slike, mogu se izvući zabrinjavajući podaci, jer ako pretpostavimo da prosječna osoba spava otprilike 7 do 8 sati dnevno, zaključujemo da prosječan korisnik interneta (uzrasta od 16 do 64 godine) sada provodi više od 40 posto svog budnog života na internetu.

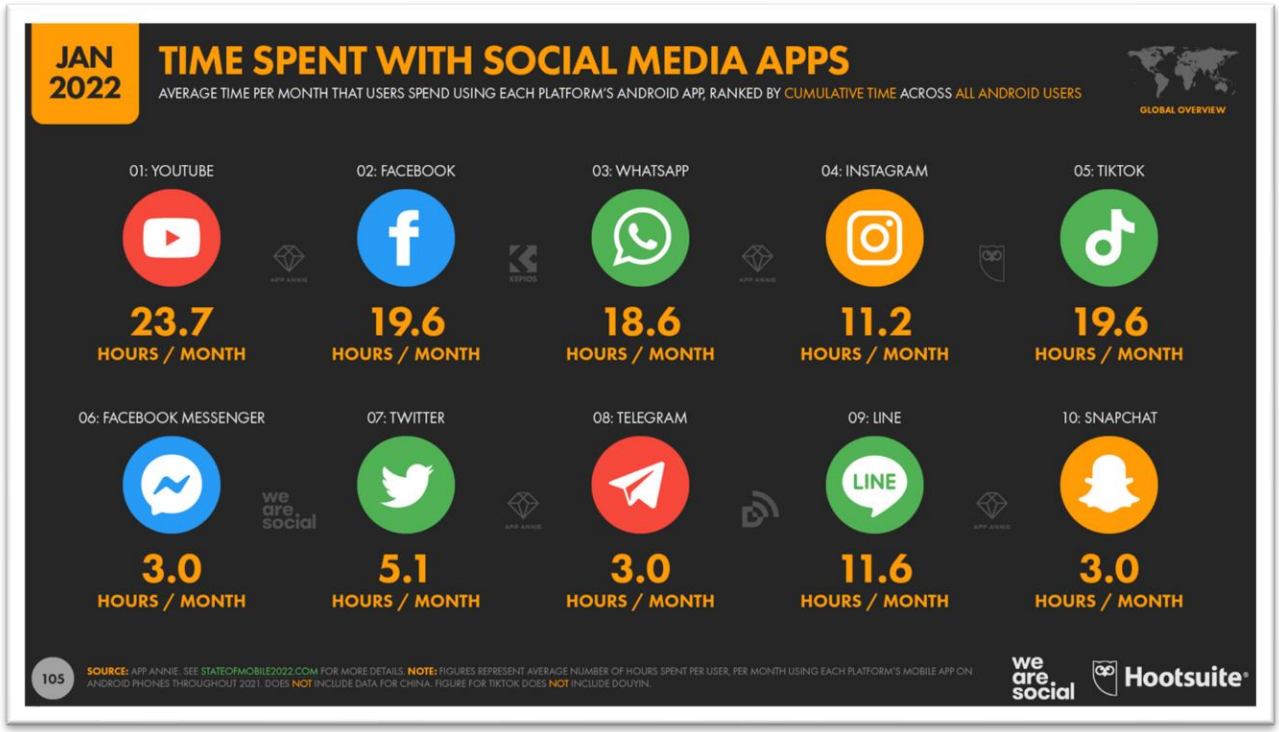
"Količina vremena koje provodimo na mreži također nastavlja da raste, s dnevnim prosjekom koji se povećao za 4 minute dnevno (+1,0 posto) tokom prošle godine. To možda ne zvuči kao veliko povećanje, ali kada se zbroje svi korisnici interneta u svijetu, te 4 dodatne minute dnevno izjednačit će se s više od 5 milijardi dodatnih dana korištenja interneta u 2022. Ukupno, najnoviji podaci govore da će svijet provesti više od 12½ triliona sati na mreži samo 2022. godine." (Kemp, Datareportal, 2022).

Od gore navedenog, ukupnog vremena potrošenog na internetu, veliki dio se troši na društvene medije. Korisnici u prosjeku provedu 2 sata i 27 minuta dnevno koristeći društvene medije. Pa tako "društveni mediji zauzimaju najveći pojedinačni udio našeg vremena za povezane medije, 35 posto ukupnog vremena" (Ibid.). Vrijeme koje provodimo koristeći društvene medije je također poraslo u protekloj godini (slika br.8), za očigledne 2 minute dnevno (+1,4 posto).



Slika br.8. Potrošnja vremena na društvenim medijima (Datareportal, 2022.).

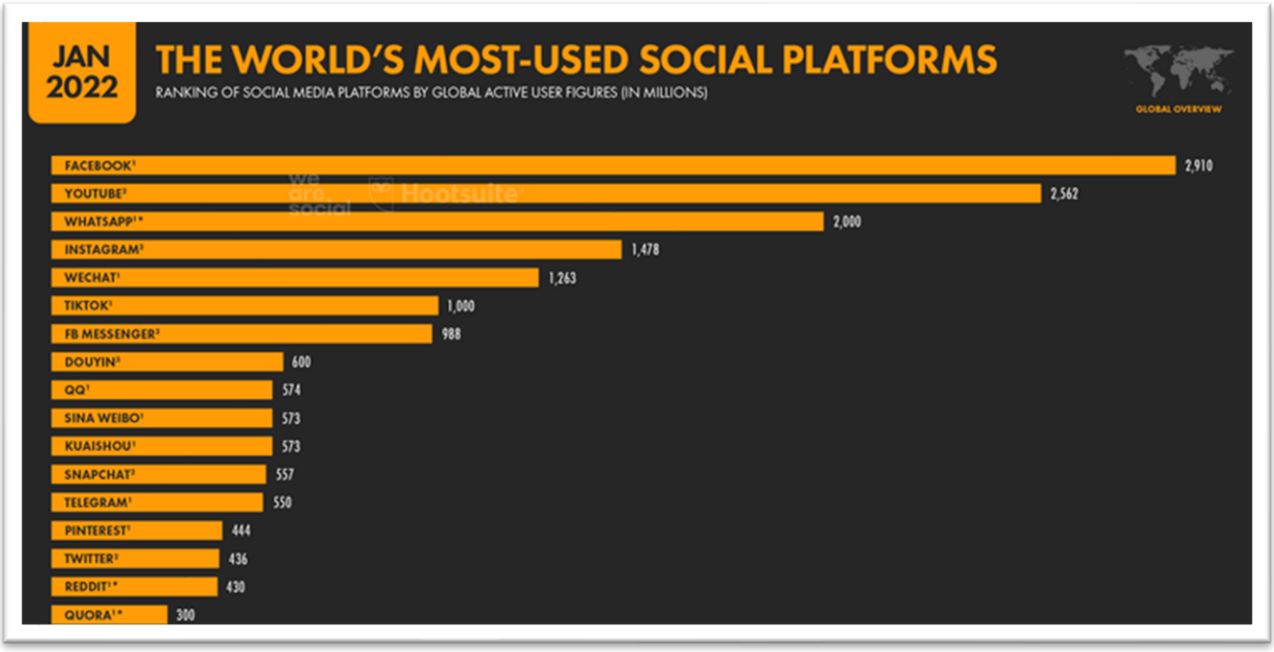
Kako navodi Kemp u svom istraživanju za DataReportal (2022.g) a što se očituje i na slici ispod: (Slika br.9) Aplikacija na kojoj se provodi najviše vremena jeste Youtube, koja mjesečno "uzima" svakom korisniku 23.7 sati njegovog vremena. "Facebook je drugi po ukupnom, kumulativnom vremenu provedenom u aplikacijama društvenih medija, sa korisnicima Androida u prosjeku 19,6 sati u aplikaciji platforme svakog mjeseca. Korisnici TikTok-a također rade u prosjeku 19,6 sati mjesečno koristeći TikTok Android aplikaciju, ali pošto platforma ima manje ukupnih korisnika, TikTok je tek na petom mjestu u ovoj rang listi po kumulativnom vremenu provedenom među svim korisnicima. WhatsApp je treći po ukupnom utrošenom vremenu, sa korisnicima koji provode u prosjeku 18,6 sati mjesečno koristeći messenger aplikaciju na Android telefonima. Instagram je na četvrtom mjestu, ali korisnici provode znatno manje vremena koristeći aplikaciju svakog mjeseca u poređenju s ostatkom prvih 5, sa samo 11,2 sata mjesečno." (Kemp, Datareportal, 2022).



Slika br.9. Prosječna potrošnja vremena na android aplikacijama društvenim mrežama (Datareportal, 2022.).

Ove platforme se međusobno svakodnevno bore za čovjekovu pažnju, koja platforma ili aplikacija će mu pružiti najviše sadržaja i na kojoj će provesti najveći dio svog vremena, jer što više vremena korisnik provede na njihovoj platform, više oglasa mu se može prikazati i više obrazaca ljudskog ponašanja mogu prikupiti.

Podaci koje je kompanija Meta objavila u izvještaju "zarada investitora u trećem kvartalu 2021." (Facebook Reports Second Quarter, 2021), jasno potvrđuju da je Facebook i dalje najkorištenija svjetska platforma društvenih medija, sa 2,91 milijardu korisnika od oktobra 2021. (Slika br.10.).



Slika br.10. Socijalne platform koje se najviše koriste u svijetu (Datareportal, 2022.).

Slična statistika kao na prikazu platformi na kojima se provodi najviše vremena. Na grafikonu uočavamo da je "mjesečna baza aktivnih korisnika Facebooka porasla je za solidnih 6,2 posto (+170 miliona korisnika) u protekloj godini, uprkos tome što je već dosegla više od polovine svoje ukupne potencijalne publike prema starosti i dostupnosti (imajte na umu da je Facebook još uvijek blokiran u Kini). YouTube je smanjio jaz u odnosu na Facebook u protekloj godini, s tim da je publika platforme rasla skoro dvostruko brže od Facebooka. YouTube sada ima najmanje 2,56 milijardi aktivnih korisnika, što je otprilike 88 posto od posljednjeg Facebooka" (Kemp, Datareportal, 2022.).

.

Uz ove impresivne brojke korisnika dolaze ogromna moć, uticaj ali i odgovornost, najčešće u ruke samo nekoliko ljudi. Kada ste na takvoj poziciji, kroz medije možete postavljati i smjenjivati društvene trendove, aktuelne teme, poželjna i nepoželjna lica, te u konačnici oblikovati javno mnijenje i percepciju društvene sigurnosti. Različitim oblicima vizuelno-auditivnog digitalnog izražavanja, omogućena je i olakšana medijska manipulacija, što u pogledu sekuritizacije i desekuritizacije određenih tema ima direktne implikacije na percepciju društvene sigurnosti. Mediji pored sekuritizacije i desekuritizacije, također mogu i zanemarivati određene događaje i teme, te se voditi taktikom da problem o kojem se ne priča i ne postoji.

U poglavlju humane sigurnosti obrađena je i promjena percepcije ljudske sigurnosti pod uticajem digitalne transformacije, a mediji su u tom procesu odigraliključnu ulogu. Mediji mogu zamagliti razliku između realnog stanja na terenu i percepcije sigurnosti do te mjere, da postaje sve teže razlikovati šta su objektvine okolnosti a šta medijsko-platformski i informacijski spektakl. Kada je riječ o objektivnom i subjektivnom osjećaju sigurnosti, subjektivna sigurnost predstavlja odsustvo osjećaja straha od ugrožavanja društvenih vrijednosti, dok se odsustvo prijetnji prema društvenim vrijednostima odnosi na objektivu dimenziju sigurnosti (Vajzović, 2020). Stavovi o sigurnosti društva formiraju se na osnovu informacija koje čovjek dobija od medija, stoga društveni mediji mogu uticati na stabilnost društva i države, nacionalne sigurnosti, sigurnosti cyber prostora itd.

Medijsko ugrožavanje čovjekove slobode od straha i drugih postulata humane sigurnosti, postali su svakodnevnica. To smo uvidjeli i u vrijeme izvještavanja o pandemiji Covid-19, za vrijeme koje smo svakodnevno bili u strahu zbog velikog broja vijesti i informacija o broju smrtno stradalih ili pojavama novih sojeva virusa, posljedica i opasnosti.

Digitalni mediji svoju zaradu svode na finansijere i na broj klikova, a najviše klikova upravo ostavruju naslovi i tekstovi često skandalozne, potresne, kontraverzne ili negativne tematike koje izazivaju sve veći strah i zbunjenost kod ljudi. Odličan primjer za to je platforma Twitter, na kojoj se laži šire 6 puta brže nego istina, jer algoritmi nemaju bolje mjerilo istinitosti od korisničkih reakcija, like-ova, share-ova i klikova (The Great Hack, 2019.).

Mediji imaju vrlo važnu ulogu u svakom demokratskom društvu, jer imaju potencijal za ostvarenje ideala informisanog demokratskog građanina. Međutim brojni su negativni efekti ispoljavanja politike na društvenim platformama jer se društvene mreže sve više koriste kao vid stalne političke kampanje, a nezaobilazan primjer za to su američki izbori 2016. godine i afera umješanosti Cambridge Analytica-e (istraživačkog tima koji se bavio psihografijom, analizom ponašanja i digitalnih podataka 50 miliona korisnika Facebooka iz SAD-a, što im je

omogućilo da doslovce upoznaju umove svojih birača) u ishod američkih demokratskih izbora. Cambridge Analytica je ugovorena s Trumpovom kampanjom i osigurala je potpuno novo oružje za izborno stroj. Pored demografskih segmenata za identificiranje grupa birača, koje je i Klintonova kampanja imala, Cambridge Analytica je također segmentirala pomoću psihografije. Kao definicije klase, obrazovanja, zaposlenja, dobi i tako dalje, demografija je informativna, dok je psihografija uglavnom bihevioralna i koristi se kao sredstvo za segmentiranje prema ličnosti (Wade, THE CONVERSATION, 2018.). Korištenje digitalnih medija u ovakve i slične svrhe potkopava samu srž demokratije i ljudskih prava čovjeka. Također, putem digitalnih medija, politička obračanja npr. Trump-a, Baiden-a, aktuelnog Volodimira Zelenskog i dr. dobijaju na planetarnom značaju, te u takvim obraćanjima stavovi pojedinaca se tumače na različine načine kroz različitu medijsku interpretaciju, te se posmatraju kao stavovi cijele nacije, što naravno u velikom broju slučajeva nije tačno.

Još dublja priča od uticaja društvenih medija na političke procese jeste medijsko i platformsko upravljanje ljudskim životima na osnovu pažljivo filtriranog sadržaja sa kojim se možemo ili ne moramo slagati, ali ljudi ipak donose odluke na osnovu informacija sa kojima se susreće. Ako su ti sadržaji dovoljno precizno servirani odgovarajućim korisnicima, mogu npr. izazvati društvene sukobe nesagledivih razmjera, samo zato što jednoj grupi plasiraju pozitivne a drugoj negativne strane određene teme, ili mogu mijenjati čitav tok društvenih aspiracija, stavova i predrasuda.

Digitalni mediji u procesu apomedijacije u složenom medijskom, informacijskom, obrazovnom i sigurnosnom okruženju, mijenjaju tradicionalnu ulogu gatekeepera (Vratara, čuvara vrata ili ključeva; osoba ili stvari koji kontrolšu pristup nečemu, u ovom slučaju informacijmama). Gatekeeperi u digitalnom okruženju gube svoju pretpostavljenu ili očekivanu ulogu, te većinu tereta poimanja društveno-političke zbilje, sigurnosne kulture ili cyber higijene, građani moraju preuzeti na sebe. U procesu apomedijacije pojavili su se "akteri koji u kontekstu digitalnih medija zamjenjuju posrednike između korisnika i usluga (dakle informacija koje korisnici traže), što znači da sada stoje uz njih, osiguravajući dodatnu vrijednost izvana kao apomedijatori." (Eysenbacha 2008, prema Vajzović, 2019:529).

Digitalni mediji i društvene mreže uvode nas u razdoblje „kreativne destrukcije" koja može djelovati na različitim nivoima, od ciklusa proizvoda, preko modnih i investicijskih životnih ciklusa, do takozvanih poslovnih ciklusa (Schumpeter, 1942.). Primjeri kreativne destrukcije najbolje se mogu uočiti analizom medijsko-platformskog okruženja koje je postalo glavno sredstvo informisanja. Društvo u digitalnom okruženju, zadovoljavajući svoje prirodne potrebe za informisanjem i upoznavanjem, podložno je ugrožavanju humane sigurnosti. U takvim

uslovima njen zadatak da pruži sigurnost svakom pojedincu, postaje multidimenzionalna i sve teža za ispratiti. Uzrok toga leži u novom sigurnosnom okruženju u kojem su omogućene masovne kampanje destabilizacije društva, cyber hibridno ratovanje, te razni oblici manipulacije društva koji ostvaruju uticaj na politiku, ekonomiju i sigurnost društvene zajednice kao i svakog pojedinca. Položaj demokratskog građanina u digitalnom okruženju uveliko ovisi od informacijskih medijia i širokog platformskog okruženja, u kojem dominantnu ulogu igraju umjetna inteligencija, cyber hibridni ratovi, te medijska i informacijska pismenost. Savremena sigurnost se transforormira od očuvanja teritorija prema očuvanju vrijednosti, a u današnjem svijetu informacije predstavljaju ogromnu vrijednost.

Digitalni mediji pružaju nam toliko sadržaja i mogućnosti ispoljavanja svoje ličnosti a pretežno su besplatne, te se od nas zahtijeva samo nekoliko klikova na dugme 'slažem se sa uvjetima korištenja' iza koje se nalazi ogroman tekst, koji čak i onima koji ga uspješno tumače ne govori mnogo. Tekst o uvjetima o korištenju s razlogom je napisan tako, uz pretpostavku da korisnik želi što prije pristupiti nekom softweru, stranici, filmu, igrici, društvenoj mreži ili nečemu drugom, te da neće svaki put čitati šta prihvata, pogotovo ako je sadržaj besplatan. Stoga je važno naglasiti da korisnici moraju biti bolje upoznati sa onime što prihvataju pri "sklapanju ugovora" sa aplikacijama i platformama, jer ukoliko ne plaćamo za neku uslugu, vrlo vjerovatno smo mi produkt.

Sa sve masovnijom upotrebom digitalnih medija i platformi nastali su i brojni sakupljači podataka, odnosno metapodataka u digitalnom okruženju, koji danas predstavlja ogromnu riznicu informacija i korisničkih podataka koje Google, Amazon, Youtube i mnogi drugi koriste za marketinško ciljanje korisnika i druge načine profilisanja korisnika. Detaljnije o temi eksploatacije korisničkih podataka, govorit će se u posljednjem poglavlju ovog istraživačkog rada.

Na kraju ovog poglavlja možemo zaključiti da informacijski nered, koji uzima sve više maha na društvenim medijskim platformama, uz informacijsku nepismenost, prosječnog čovjeka može potpuno zbuniti, ako ne i za(b)luditi. Ljudi donose odluke na osnovu informacija kojima raspolažu. Stoga, uzmemo li u obzir pretpostavku da su sve digitalne informaciju koje do nas dolaze prošle pažljivu selekciju i filtriranje, možemo zaključiti da je takvim uticajem teoretski moguće "upravljati" ljudskim životima i sudbinama, upravljajući njihovim informisanjem. Potrebno je shvatiti da su u pitanju prijetnje i rizici koji ne prave razliku na osnovu nacionalnosti, bogatstva ili društvenog porijekla, već kao takvi predstavljaju prijetnju svima, na lokalnom i globalnom planu. U takvom okruženju javljaju se ideje utemeljene na spoznaji da u društvu postoje ranjivosti od djelovanja rizika iz neizvjesne i nepredvidljive budućnosti,

te kako je potrebno kontinuirano i preventivno razvijati otpornost društva i pojedinaca na buduće nepoznate rizike (Mihalinčić, 2020.). Postoji više vrsta prijetnji koje su se pojavile tokom digitalnog doba, uključujući: digitalnu nejednakost, ugrožavanje privatnosti, zloupotrebe podataka, prevare ili krađe, digitalnu koncentraciju moći, moć društvenih mreža itd. Sve ove prijetnje potencijalno ugrožavaju ljudska prava i slobode savremenog čovjeka.

5. Izazovi digitalnog okruženja

Pored pitanja koja se odnose na tradicionalne sigurnosne prijetnje u kojima se očekuje djelovanje državnih aktera, pojavile su se netradicionalne sigurnosne prijetnje koje istovremeno ugrožavaju više aktera. Prijetnje i izazovi digitalnog okruženja su jedna široka lepeza relacija između korisnika, odnosno čovjeka i „interneta“. Sigurnosne prijetnje do korisnika uglavnom dolaze putem informacijskih medija, društvenih i komunikacijskih mreža, te drugih distributera sadržaja. Ako se pita cyber kriminalce, društvene mreže su najbolja stvar koja se dogodila otkako je interneta. One su odlična podloga za socijalni inžinjering, internet prevare, krađu podataka, špijunažu ili druge vrste cyber napada. U današnjem svijetu kada se sve ljudske djelatnosti obavljaju uz pomoć nekog vida digitalne tehnologije ili u digitalnom prostoru, sigurnost ima veliki zadatak da isprati taj tehnološki napredak, pokrije i digitalni prostor u kojem je zaštita ljudske sigurnosti prijeko potrebna. To može postići samo konstantnim radom i pokretanjem evolucije koncepta humane sigurnosti (digitalnog doba) i stavova prema osiguranju šire društvene sigurnost.

Sudionici smo doba u kojem se prema Colinsu, vojna prijetnja sigurnosti ne smatra jedinim ili isključivim ugrožavanjem sigurnosti društva, nego je samo jedno od širokog spleta ugrožavanja, koja se mogu odraziti ne samo na sigurnost društva, nego i na sigurnost pojedinca. Upravo u navedenom se ogleda proširivanje i produbljivanje koncepta sigurnosti, koji je oznaka kasnije faze razvoja sigurnosnih studija. (Collins, 2010.) Potencijalne prijetnje po živote i dobrobit pojedinaca stoga su proširene s primarnog, vojnog, na općenito ekonomske, društvene, ekološke i zdravstvene probleme. Sve navedene sigurnosne i društvene aktivnosti danas su usko vezane za cyber prostor, što je odlična prilika za bolju komunikaciju i razmjenu ideja, ali i savremeno bojno polje za borbe i napade. Pojava savremenih sigurnosnih (digitalnih) prijetnji

uzrokovala je promjenu sigurnosnog okruženja i samih izvora nesigurnosti. Kako se digitalne tehnologije sve više koriste u trgovini, upravljanju i društvenom životu, one predstavljaju nove izazove za ljudsku sigurnost. O zaštiti sebe i drugih od negativnih efekata digitalnih mreža i medija, govori se malo ili nikako, a mi smo uveliko nadograđeni i okruženi tehnologijom koja je postala naša ekstenzija, stoga je vrlo važno osigurati da tehnologija radi za nas a ne protiv nas. To se može postići samo kroz društveno podizanje i razvijanje svijest o etičnoj i humanoj upotrebi tehnologije, jer tehnologija nije loša, mi je činimo lošom.

Ispitanici u istraživanju Svjetskog ekonomskog foruma, među najneposrednije prijetnje čovjeku naveli su tehnološke rizike kao što su: digitalna nejednakost, cyber napadi, prevare i krađe podataka, te nekontrolisanu i ogromnu digitalnu moć. (UNDP, 3.poglavlje, 2022). Sigurnosne implikacije digitalnih tehnologija često se procjenjuju kroz nacionalnu sigurnosnu leću. Primjena pristupa ljudske sigurnosti unutar nacionalne, nedavno je usredotočena na implikacije za ljude. Na primjer, cyber napadi na komunikacijske mreže utiču ne samo na nacionalnu sigurnost nego i na pristup informacijama i slobodu udruživanja. Digitalne tehnologije također mogu olakšati nanošenje štete ljudima, kao što su: maltretiranje, uznemiravanje, prevara i dezinformacije (UNDP,3., 2022.).

Ostale prijetnje ljudskoj sigurnosti povezane s tehnologijom mogu se povezati s rastućim osjećajem straha uz konstantnu dozu neizvjesnosti koju stvara korištenje tehnologije. Na primjer, „koncentracije kontrole od strane davatelja tehnologije ili vlada mogu obezvlastiti ili zloupotrijebiti korisnike„ (Ibid.). Razmišljajući o tome kako nove tehnologije mogu poslužiti kao digitalno javno dobro, kreatori politike moraju ići korak dalje od tehničkih rješenja i također razmotriti pitanja vrijednosti i etike.

Postojeće i nove sigurnosne prijetnje, rizici i izazovi proširuju odgovornost za sigurnost s države na pojedinca, društvo u cjelini te privatni i javni sektor.(Strategija nacionalne sigurnosti, RH, 73/2017)

Razvojni program UN-a smatra da antropocenski kontekst, sa međusobno povezanim prijetnjama ljudskoj sigurnosti, poziva na hrabru agendu koja će odgovarati veličini izazova i biti znesena sa poniznošću pred nepoznatim (UNDP, 2022.). Spcijalni izvještaj UNDP-ija iz 2022. godine govori o četiri prijetnje ljudskoj sigurnosti koje se posmatraju kroz antropocenski kontekst:

1. Negativne strane digitalne tehnologije,
2. Nasilni sukobi,
3. Horizontalne nejednakosti,

4. Izazovi u razvoju zdravstvenih sistema.

Digitalne tehnologije mogu pomoći u suočavanju sa mnogim izazovima antropocena, ali brz tempo digitalne ekspanzije dolazi s novim prijetnjama koje mogu pogoršati tekuće probleme povezane sa, na primjer, nejednakostima i nasilnim sukobima. Ne samo da je tekuća pandemija ubrzala digitalni pomak u produktivnoj ekonomiji, već je i cyber kriminal naglo skočio, a predviđa se da će godišnji troškovi dostići 6 biliona dolara do kraja 2022.godine (UNDP, 2022.). Iako temeljni izazov svake prijetnje pojedinačno nije nov, prijetnje su nove po izrazu koji dobijaju u antropocenskom kontekstu i njihovoj međusobnoj prirodi, koja se vremenom razvijala.

U tom kontekstu, Specijalni izvještaj za 2022. godinu u produkciji razvojnog programa Ujedinjenih nacija, posvećen je novim prijetnjama ljudskoj sigurnosti u antropocenu i zahtijevima za veću solidarnost. Ovaj izvještaj naglašava snažnu povezanost između pada nivoa povjerenja i povećanog osjećaja nesigurnosti (Ibid.). Također navodi da otkako je pandemija Covid-19 počela, svijet je dostizao neviđene visine 'indeksa ljudskog razvoja' (eng. Human Development Index -HDI-). „Ljudi su u prosjeku živjeli zdravije, bogatije, bolje i duže nego ikad. Ali ispod površine sve je veći osjećaj nesigurnosti puštao korijenje."(UNDP, 2022: 3). Procjenjuje se da se šest od svakih sedam ljudi širom svijeta već osjećalo nesigurno u godinama koje su prethodile pandemiji. Očigledno je Covid-19 učinio da se ljudi osjećaju nesigurnije, ali šta objašnjava zapanjujuću razdvojenost između poboljšanja postignuća u dobrobiti i pada percepcije ljudi o sigurnosti? Očito društveni i tehnološki razvoj ne daju automatski i razvoj sigurnosti, stoga se čini da čovječanstvo čini svijet sve nesigurnijim i nesigurnijim mjestom.

To sugerše i ranije spomenuti izvještaj, navodeći da su tokom antropocena višestruke prijetnje poput pandemije COVID-19, digitalnih tehnologija, klimatskih promjena i gubitka biodiverziteta postale istaknutije ili su dobile nove oblike posljednjih godina. Izvještaj povezuje ove nove prijetnje s nepovezanošću između ljudi i planete, tvrdeći da su oni, kao i sam antropocen, duboko isprepleteni rastućim planetarnim pritiskom (UNDP, 2022.).

Glavni doprinos ovog izvještaja je „ažuriranje koncepta ljudske sigurnosti kako bi odražavao ovu novu stvarnost. Čineći to, izvještaj nudi put naprijed za suočavanje s današnjim međusobno povezanim prijetnjama. Prvo, sprovođenjem strategija humane sigurnosti koje potvrđuju važnost solidarnosti, budući da smo svi ranjivi na proces planetarnih promena bez presedana koji doživljavamo tokom antropocena. I drugo, tretirajući ljude ne kao bespomoćne pacijente,

već kao agente promjene i akcije koji su sposobni da oblikuju vlastitu budućnost i ispravljaju kurs.“ (UNDP, 2022: 4).

Što se tiče budućnosti, Agenda za održivi razvoj 2030 i ciljevi održivog razvoja pružaju ambiciozan skup višedimenzionalnih ciljeva koji trebaju pokrenuti akciju na svim nivoima (od lokalnog do nacionalnog) i mobilisati međunarodnu zajednicu. Ali svi uloženi napori ostaju u velikoj mjeri podijeljeni, baveći se odvojeno klimatskim promjenama, gubitkom biodiverziteta, sukobima, migracijama, izbjeglicama, pandemijama i zaštitom podataka. Te napore treba pojačati, jer dosadašnji su se pokazali nedovoljnim u kontekstu antropocena. Važno je krenuti korak dalje od fragmentiranih napora, te reafirmirati principe osnivačkih dokumenata Ujedinjenih naroda, Univerzalne deklaracije o ljudskim pravima i Povelje UN-a, koji su ujedno i središnje ideje koje podupiru koncept ljudske sigurnosti. Kako smatra i generalni sekretara UN-a: „Naša zajednička agenda, u antropocenu podrazumijeva sistematsku, trajnu i univerzalnu pažnju solidarnosti ne kao neobavezne milostinje ili nečega što pojedinca podvrgava interesima kolektiva, već kao poziv da se traži ljudska sigurnost kroz „oči čovječanstva“. (UNDP, 2022.:7)

5.1 Digitalno potpomognuta represija

Pored svih benefita i olakšica koje nam donosi, digitalna tehnologija takođe može omogućiti novu vrstu represije, terorizam kao i druge oblike ugrožavanja sigurnosti. Terorizam, koji je uz medije doživio i digitalnu transformaciju, sada prelazi u cyber terorizam. Pored toga, terorističke organizacije mogu koristiti internet za širenje svojih poruka putem medija i društvenih mreža, tu mogu vršiti i regrutovanje novih članova, planirati napade, kupovati potrebnu opremu na DarkWebu[7] itd. “Terorizam” u 21. stoljeću može biti rad jedne osobe koja se nalazi negdje u svijetu sjedi za laptopom i terorizira milione ljudi. Autoritarne vlade su sustigle, čak i nadmašile aktiviste za ljudska prava u njihovoj sofisticiranoj upotrebi digitalne tehnologije. Autoritarne države su uspjele da održe svoju moć u cyber prostoru, koristeći

[7] “Dark Web” je termin koji se odnosi na specifičnu kolekciju web-sajtova koji postoje na enkriptovanoj mreži i ne mogu se pronaći uz pomoć tradicionalnih internet pretraživača. Skoro svi sajtovi na tzv. “Dark Web-u” kriju svoj identitet koristeći alat za enkripciju - Tor browser. Tor browser je poznat zbog njegove mogućnosti da sakriva aktivnosti i identitet. Može se koristiti da zavara trag vašoj lokaciji tako da izgleda kao da ste u nekoj drugoj državi, što je slično korištenju VPN servisa (PCPress, Gavrilov, 2017.).

internet u svrhe nadzora i propagande, što se u novinarskim izveštajima često naziva digitalnom diktaturom. Oni sada imaju poboljšane kapacitete za cenzuru izražavanja, blokiranje ili filtriranje pristupa informacijama, praćenje aktivnosti na mreži i efikasnije i efikasnije kontrolu stanovništva nego što su to činili u preddigitalnom svijetu (Human rights watch, 2016.). U demokratskim društvima, s druge strane, prilično mali krug aktera dominira političkim raspravama čak i u cyber prostoru (Hansel, 2010). Neka istraživanja su primijetila da su društveni mediji doveli do ere 'personalizirane politike', koja može potkopati tradicionalnu grupno zasnovanu politiku identiteta društvenih pokreta (Bennet, 2012, prema Castilla, 2019.) Nažalost, digitalna tehnologija je pružila nove komparativne prednosti najsofisticiranijim autoritarnim sistemima. Jedna od najnaprednijih verzija cyber represije viđena u Kini, gdje kombinacija digitalnih alata za masovni nadzor, cenzuru i praćenje društva pruža bogata i sveobuhvatna sredstva društvene i političke kontrole. U svoj digitalni sistem društvenog praćenja, Kina očigledno zapošljava dva miliona internet policajaca koji imaju zadatak da nadgledaju onlajn aktivnosti građana i pregledaju milione poruka na društvenim mrežama i sajtovima za tzv, mikro-blogovanje (Human rights watch, 2016.). Ovi podaci prikupljaju se u različite svrhe, a uglavnom za vladine izvještaje o potencijalu društvenih nemira i za suzbijanje političkih i društvenih aktivnosti. Kineska administracija za cyber prostor suspendovala 580 naloga na društvenim mrežama nakon navoda da su korisnici ignorisali svoje društvene odgovornosti i zloupotrijebili svoj uticaj (Ibid.). Kineski digitalni sistem kreditnog rejtinga je vrhunski primjer gdje bi veliki podaci (BigData) mogli pomoći „Velikom bratu“ na potpuno novom nivou. Ovaj društveno-kreditni rejting kombinuje sveobuhvatno praćenje na mreži sa algoritmima koji imaju za cilj uspostavljanje korelacije između negativnog društvenog ponašanja i internet aktivnosti. „Trenutno se koristi za procjenu financijske kreditne sposobnosti, ali njegova namjeravana buduća upotreba može biti za mnogo širu društvenu kontrolu — navodno za procjenu sveukupne pouzdanosti i poštenja građana, te za dodjelu ocjena državljanstva na osnovu „patriotskih kriterija.“ (Human rights watch, 2016.).

Ukoliko ovakvi sistemi u budućnosti nađu svoju širu upotrebu, bit će to ogroman društveno-naučni sukob između onih koji su za i onih koji su protiv takvog nadzornog sistema. Takve ideje koje već žive u svijetu, korak su do potpune države kontrole, jer hipotetički gledano, u takvom sistemu čovjek je u digitalnom ropstvu. Humana sigurnost u takvom sistemu očito ne bi imala značajnu ulogu, jer privatnost i ljudska prava se zanemaruju zbog toga što je jedina društvena vrijednost socijalni kredit, kojim naravno vlada može manipulisati jer ga ona i daje. Naprimjer ukoliko se čovjek ne slaže sa „partijom“ i ima nizak socijalni kredit, oduzima mu se

kartica ili čip, odnosno zaledi digitalna imovina i on više nema pristup trgovinama, centrima, ili nečemu drugom.

U tako idealističko digitalnom okruženju, veliku sigurnosnu prijetnju po čovjeka i njegovo biće predstavlja „digitalni nestanak“. Digitalni nestanak može se najbolje opisati na način da jednoga dana neko odluči da izbriše sve Vaše račune, naloge, postavljene sadržaje, komunikacije, publikacije, objave ili intelektualne radove, jer se ne slaže s njima ili mu predstavljaju prijetnju. To se može raditi i na način da se određena osoba marginalizira, diskreditуje, proglasi za pseudonaučnika, teoretičara zavjera ili za maskotu koju niko ne shvata ozbiljno. Jedan od primjera za takvo nešto može biti ukidanje Twitter naloga Donalda Trumpa (BBC, 2021.) jer se smatralo da svojim objavama ugrožava sigurnost višemilionske publike Twittera. Ukinut mu je nalog i neko vrijeme od njega na društvenim mrežama nije bilo “ni traga ni glasa”.

U mnogim aspektima, digitalne tehnologije obećavaju proširenje sposobnosti i promicanje ljudske sigurnosti. Međutim, ispostavlja se da tehnološki napredak u kombinaciji sa novim izazovima i ljudskim neznanjem utiče na integritet individue čovjeka, koji je napadnut od strane brojnih uticaja koji dolaze iz cyber prostora. Kako digitalne tehnologije postaju sve šire prihvaćene, pristup ljudske sigurnosti skreće pažnju na to kako tehnologija može potkopati dobrobit, prava i sposobnosti ljudi. Primjetno je da je sigurnost digitalnih mreža kao i pohranjenog sadržaja ugrožena na različite načine (Reznik, 2013.). Korisnici stvaraju ogromne količine podataka koji su pohranjeni u digitalnom obliku, na disku ili na “mreži”, profilima i serverima, a koji se mogu zloupotrijebiti. Informacijsko-komunikacijske tehnologije nisu samo alat nego i sila novog ekosistema koja utiče na našu percepciju sebe, naše interakcije i međusobne odnose, kao i predstavu stvarnosti i sigurnosti (Floridi, 2015, prema Hibert, 2018.).

5.2. Cyber hibridno ratovanje

Razvoj cyber prostora i drugih elemenata digitalnog okruženja, te prelazak medija i informisanja u digitalni oblik, stvorili su prostor za još nekoliko rastućih prijetnji ljudskoj sigurnosti u digitalnom dobu, a to su cyber napadi i cyber hibridno ratovanje. Ubrzan društveni i tehnološki razvoj, te broj korisnika interneta, o kojem smo detaljno govorili u prethodnim poglavljima, kao logičan slijed, jasno upućuje na to da će u budućnosti doći do sve ozbiljnijih i sve učestalijih cyber napada i korištenja cyber hibridnog ratovanja u ostvarivanju nekih ciljeva. Ako cyber ratovanje namjerno posmatramo samo kao širenje dezinformacija, odnosno informaciju posmatramo kao oružje, onda možemo reći da se čovjek danas nalazi u konstantnom ratu. Takvi napadi uzrokuju ogromne materijalne i nematerijalne štete, te na više načina ugrožavaju humanu sigurnost čovjeka i njegova zagarantovana prava.

Način hibridnog ratovanja nije novi, kao što već znamo mnoge države i njihove obavještajne agencije su u bliskoj prošlosti koristile različite subverzivne načine i alate u širenju raznih dezinformacija i propaganda. Hibridni rat predstavlja vrlo opširan i popularan pojam koji se odnosi na savremeno ratovanje. Hibridne prijetnje predstavljaju koncept koji je ušao u mnoge službene dokumente i sigurnosne strategije. EU i NATO poduzeli su ozbiljne mjere za suzbijanje aktivnosti koje su povezane s hibridnim prijetnjama. Politički rat, aktivne mjere i tajne akcije vođene komunikacijom nisu novost, a propaganda se koristila kroz povijest u sukobima i situacijama sličnim ratu. Međutim danas, naše digitalno komunikacijsko okruženje i komunikacijski alati koje u legitimne svrhe koristimo također koriste i neprijateljski autoritarni akteri koji su se umiješali u mnoge demokratske procese. Uticanjem na takve procese, kao što su: izbori, polariziracija i podjela društva, te širenje animozita između društva, države i međunarodnih partnerskih zemalja, vrlo jednostavno uništavaju povjerenja u državne institucije i njihove sposobnosti da zaštite sebe i svoje stanovnike. Može se reći da digitalna transformacija, samo još jednom potvrđuje citat kojeg su iznijeli kineski vojni stratezi, a koji kaže da: „Sve što može koristiti čovječanstvu može mu i naškoditi.“ Ovime se želi reći da na svijetu danas ne postoji ništa što ne može postati oružje. (Liang, Q., Xiangsui, W., 1999, p. 25) Hibridni rat je „multidimenzionalni fenomen koji integrira nekoliko aspekata borbe –vojnu, informacijsku, ekonomsku, političku i društveno-kulturnu, u jednu domenu. Ono po čemu je karakterističan je kombinacija vojnih i nevojnih utjecaja koji su produženi istodobno preko

višestrukih bojnih polja i stoga zahtjevaju dobro organizirano mnogo-vektorsko odupiranje.“ (Kolobara, 2019;117).

Obilježja hibridnog ratovanja su:

1. Rat/Sukob koji egzistira ispod radara tradicionalnih sukoba/ratova (Stoga tradicionalne metode zaštite čovjeka i njegove sigurnosti, često ostaju bez mogućnosti za pravovremeno djelovanje)
2. Nema pravila ko u njemu sudjeluje (stoga se strah širi i izvan kruga napadač-žrtva)
3. Cilj napada može biti bilo šta, bilo kad i bilo gdje (pa samim time što su nepredvidivi i neselektivni, stvaraju rastući osjećaj potencijalne ugroženosti i nesigurnosti)
4. Jeftin za napadača, a potencijalno skup za napadnutog (puno jeftiniji i efikasniji način ratovanja od tradicionalnog, koji iziskuje ogromne troškove)
5. Nema državnih granica (pa se tako napadi mogu sprovesti vrlo brzo, sa neke udaljene ili “prikrivene” lokacije, u suradnji hakera iz cijelog svijeta, na bilo koje mjesto)
6. Odlučno utjecati/destabilizirati ciljanu(e) publiku(e) (Prosječan korisnik digitalnih platform, u moru informacija, ne može razaznati koja je istinita, provjerena i vjerodostojna, a koja obmanjujuća, lažna ili iskrivljena)
7. Iskoristiti slabosti sistema (Svaki sistem koji je čovjek projektovao ima ugrađenu opciju ili grešku koju neki haker, malo dubljom analizom može iskoristiti za upad u sistem ili njegovo onesposobljavanje)
8. Ranjivost koalicija (Ranjivost koalicija, zbog nedostatka edukacije, ima težnju da raste)
9. Ugrožena komunikacijska infrastruktura (Kolaps informacijske infrastrukture u današnjem digitalnom dobu može izazvati nesagledive štetne posljedice po čovjeka.) (Jacobs, A., Lasconjairas, G, 2017)

Karakteristike cyber ratovanja su:

1. Namjerna i organizovana aktivnost primjene sile prema protivniku u cilju nanošenja štete njegovim resursima, vrijednostima, stanju i interesima;

2. Ostvaruje se u cyber prostoru i iz cyber prostora, što znači primjenom informacionih sistema i informacija u njima, te dejstvom na informacione sisteme i informacije u njima;

3. Preduzima se od strane države ili organa u ime države;

4. Izvodi se u cilju ostvarivanja vojnih i političkih ciljeva (Mladenović, 2016.).

Hibridno ratovanje ili subverzija, ogleda se u nekoliko pojavnih oblika:

1. Kao psihološki rat, koji se koristi i u doba mira i u doba rata, radi podizanja vlastitog a smanjivanja neprijateljskog morala. Medijski ili informacijski rat je trenutno najpoznatiji oblik ovog rata. Vrši se između država ili protiv neke države kako bi se pridobilo javno mnijenje na vlastitu stranu. Njime se diskreditiraju protivnička postignuća, omalovažava nečija historija i ratne žrtve, obezvrjeđuje se, kleveće, stigmatizira, etiketira protivnika i tako dalje. U takva djelovanja se često ubrajaju i "lažne vijesti" (Tuđman, 2009).
2. Gospodarski rat u kojem jedna država svojim akcijama nanosi ekonomsku štetu drugoj državi bez objave rata. Naprimjer, gospodarska blokada Kube od strane SAD-a ili UN i druge međunarodne asocijacije koje su proglasile ekonomske sankcije protiv cijelog niza zemalja involviranih u podupiranje terorizma.. itd. (Thompson, C. 2018).
3. Paravojne akcije s ciljem rušenja vlade neke države; (Rusija, koja je poznata po svojim cyber-hibridnim kapacitetima, još 2014. godine, mnogo prije nedavnog zvaničnog oružanog napada na Ukrajinu, sprovodila je seriju cyber napada na teritoriji Ukrajine, koji su imali za cilj oslabiti komunikaciju, povjerenje, ubacivati određene medijske tekstove, doći u posjed informacija koje mogu koristiti za ucjenu ili degradiranje nekih državnih zvaničnika itd.)
4. Obavještajne akcije, pomoću kojih se u nekim slučajevima može organizirati i izvršiti državni udar;
5. Terorističke akcije koje poduzimaju grupe koje su posve neovisne o raznim državama, ili pak takve grupe koje su finansirane i na druge načine potpomagane od tajnih službi pojedinih država; 6. Protuterorističke djelatnosti koje provode tajne službe, policijske snage, ali i specijalne vojne snage (Hoffman F., 2010).

Hibridi rat u cyber prostoru postao je svakodnevna pojava koja izaziva opasne učinke i posljedice u stvarnom svijetu, stvaranjem afere i prijetnji tamo gdje ih objektivno nema, a sve s ciljem unošenja podjela, zaustavljanja razvoja, poticanja nereda i nepovjerenja u državni sistem i institucije... Mediji posjeduju ogromnu moć jer svojim sadržajem i načinom izvještavanja, oblikuju percepciju publike, tako što određene događaje i aktere mogu staviti u različite kontekste i predstaviti na različite načine, kako bi kod publike izazvali različite reakcije koje mogu voditi kao osudi ili odobravanju nekog čina, kao i glorifikaciji ili satanizaciji neke osobe. Usljed takvog djelovanja, stanovništvo počinje gubiti povjerenje u svoju administraciju, vlastitu državu naziva propalom, te konačno može početi iskazivati nezadovoljstvo koje dovodi i do sukoba. U društvu se tako stvara histerično nepovjerenje

prema izvještavanju etabliranih i profesionalnih medija kada se radi o kontroverznim političkim temama.

Nezaobilazan primjer cyber djelovanja ponovo je Rusija. Od aneksije Krima 2014. godine, hibridni rat postao je široko korišten, ali i dvosmislen izraz za opisivanje neprijateljskih aktivnosti Rusije. Ovaj poznati primjer hibridnog rata pokazuje ostvarivanje ruskih političkih ciljeva na Krimu, a da Rusija nije ispalila niti jedan metak. Ruske snage su nevojnim sredstvima, prvenstveno korištenjem informacija, postigle svoj cilj, ne koristeći taktiku „spaljene zemlje", kao što su ranije koristili u Čečeniji ili Gruziji. Zapadni vojni analitičari su tek poslije Krima zapravo uvidjeli koliko je Rusija uložila u hibridno ratovanje, što se sada smatra njenim najvećim dostignućem (Analiziraj.ba Mušić, 2019).

Kada je riječ o izolovanim napadima, cyber napade možemo definisati kao: „zlonamjeran uticaj na informatičke sisteme, kompjuterske mreže i ostale elektoničke resurse, koji se odvija u cyber prostoru s ciljem ugrožavanja povjerljivosti, cjelovitosti i dostupnosti podatka koji se na tim sistemima, mrežama i resursima stvaraju, obrađuju, pohranjuju i koji se putem njih prenose" (CERT, Hrvatska). Primjeri cyber napada su mnogobrojni, a u ovom poglavlju navesti ćemo samo nekoliko. Dobar primjer hakerski napada je onaj na važne infrastrukturne stranice bolnica u Alabami. Tako su u novembru 2019. godine hakeri lansirali virus u digitalne sisteme tri bolnica u Alabami, koji su onemogućili bolnicama da prime svoje pacijente.
(Elsa Blog, 2020.)

Kada su u pitanju akteri i motivi za cyber napade, potrebno je prvo istražiti ko napada i zašto napada. Motivi za napad su često isprepleteni i zapravo nevidljivi. Mladenović (2016.) smatra da cyber napade, državni akteri pokreću uglavnom zbog geopolitičkih interesa, dok organizovane kriminalne grupe to čine uglavnom zbog profita. Cyber napadi se koriste i za različite ideološke izražaje, bilo to ideološko nasilje i terorizam, ili napadi od strane hakera zbog odbrane svoje ili neslaganja sa drugom ideologijom. Također, veliki broj cyber napada izvodi se iz zabave, osvete ili dokazivanja.

Negrađansko civilno društvo sastoji se od raznih aktera, a pojava cyber prostora dovela je ovu vrstu aktivnosti na novi nivo. Jedan dugoročni uticaj mogao bi biti socijalno nezadovoljstvo i nemiri, uključujući gubitak povjerenja javnosti u vladu, čak i ako je stvarna šteta uzrokovana zlonamjernim cyber aktivnostima bila minimalna (Choo, 2011: 719). Napori hakerskih grupa, koje navodno rade u ime nekih vlada, da se upliću u izborne procese demokratskih država i da manipulišu javnim mnijenjem već su nekoliko godina svakodnevna vijest, formirajući na mnogo načina svojevrsnu sivu zonu (Schmitt, 2018). Uz to, korištenje društvenih medija od

strane ekstremističkih grupa za komunikaciju i regrutaciju je dobro poznat trik. (Castilla, Pursiainen 2019.)

Ljudi su uglavnom pogođeni cyber napadima koji ciljaju na njihove informacije i sisteme s kojima dolaze u dodir u svakodnevnom životu. Mjere za rješavanje cyber šteta koje krše ljudska prava i slobode umanjuju ljudsku sigurnost (Salminen, 2018). Slom globalnog tehnološkog lanca, velike masovne digitalne dezinformacije i krađe digitalnih informacija mogu imati katastrofalne posljedice na daljnje funkcionisanje globalnih komunikacija, proizvodnje i transporta, što utiče na opstanak i funkcionisanje jednog modernog društva. Ovakve pojave, koje utiču na svih 5 grana ljudske sigurnosti i direktno prijete čovjekovom opstanku i funkcionisanju, ugrožavaju temeljne postulate humane sigurnosti: slobodu od straha i slobodu od siromaštva.

Tradicionalni mehanizmi pravne odgovornosti prema sadašnjem međunarodnom pravu često ne funkcioniraju kada je riječ o potrebi zaštite digitalnih prava koja su povrijeđena. Za primjer se može uzeti prisutnost međunarodnih anonimnih korisničkih "udruženja" koja mogu oštetiti digitalnu telekomunikacijsku mrežu, što će zaustaviti mnoga javna i privatna tijela. Neke zemlje čak i otvoreno navode da njihove oružane snage imaju jedinice za posebne informacijske operacije u cyber prostoru. Međutim, zbog razmjera ovih operacija mogu stradati mnogi nevini ljudi iz drugih zemalja (Bodmer, 2012., prema Zhemerov, 2020). Što se tiće pravnih mehanizama za rješavanje cyber prijetnji, dobar osnov daje Tallinn priručnik o međunarodnom pravu primjenjivom na cyber ratovanje. Glavno načelo priručnika je da se cyber ratovanjem upravlja međunarodnim pravom koje je već na snazi, posebno pravilima koja regulišu početak oružanog napada (jus ad bellum, povelja UN-a, uglavnom na snazi od 1945.) i pravilima koja regulišu vođenje oružanih sukoba (jus in bello, uključujući, na primjer, Hašku konvenciju iz 1899. i Ženevsku konvenciju iz 1949., sa protokolima o izmjenama i dopunama iz 1977.) (Heinegg, 2013.) Priručnik ima veliki zbornik međunarodnog prava oružanih sukoba ili međunarodnog humanitarnog prava. Osmišljen je kao referentni alat za državne pravne savjetnike, kreatore politike i operativne planere, a i naučnicima i studentima također može biti od koristi. Priručnik iz Tallinna striktno je izraz mišljenja Međunarodne skupine stručnjaka i kao takav ne predstavlja službene stavove Centra ili NATO-a (Schmitt, 2013). Primjetan je intenzivan interes za razvojem jasnijih međunarodnih normi za reguliranje različitih aspekata cyber aktivnosti i pri tome se nailazi na dvije problemske činjenice. Prva je da se neke države, a posebno one sa sofisticiranim cyber kapacitetima, kao što su Sjedinjene Američke Države, zadovoljavaju izjavom da će primjenjivati postojeća, opća međunarodna pravila na cyber dejstva. Ali te države imaju ograničene poticaje da otkriju kako konkretno primjenjuju te norme.

A druga problemska činjenica je da glavni cyber igrači Rusija, Kina i Sjedinjene Američke Države ostaju na različitim konceptualnim stranicama o tome kako dalje (Deeks, 2015).

Kako bi se riješili ovakvi problemi, potrebno je usvojiti opću konvenciju o cyber sigurnosti na međuvladinom nivou, koja bi definisala glavna područja saradnje između zemalja i odredila mjere za uticaj na zemlje prekršiteljice. Distribuirana, decentralizovana priroda interneta, koja je prvobitno viđena kao karakteristika koja obezbjeđuje otpornost, ustvari je otežala sistematsko rješavanje ove složene globalne ranjivosti. Globalna ranjivost ogleda se u tome da su integritet i dostupnost digitalnih informacija i infrastrukture pod stalnom prijetnjom. Virusi, zlonamjerni softveri i šeme društvenog inženjeringa postali su sofisticiraniji, kriminalno hakovanje je postalo unosnije, a softver za otkupnine[8] se umnožio. Nemogućnost brzog i dosljednog otkrivanja infiltracije s povjerenjem, doprinosi rastućem osjećaju nelagode zbog oslanjanja na digitalnu infrastrukturu u cijelom društvu (Human rights watch, 2016.). Rizik od kaskadnog sistemskog cyber kolapsa iz dana u dan raste. „Koncept cyber-Armagedona više nije samo stvar loših naučno-fantastičnih filmova, već se trenutno igra u sobama za nacionalnu sigurnost širom svijeta. (Ibid.).

Možemo zaključiti da je u ovom međusobno povezanom digitalnom svijetu, široko rasprostranjena mogućnost korištenja digitalnih sredstava za nanošenje fizičke štete, i to predstavlja još jedan put ugrožavanja jednog od najosnovnijih ljudskih prava: prava na život, slobodu i sigurnost ličnosti (Human rights watch, 2016.). Također, masovni cyber-napadi mogu izazvati veliku pometnju u digitalnim komunikacijama, što bi moglo dovesti u pitanje opću globalnu sigurnost, kao i sigurnost pojedinca i skupine (World Economic Forum, Global Risks, 2012.). Ferrajoli, (2012) smatra da je danas stanje političke predvidivosti jedan je od značajnih segmenata poimanja sigurnosti, koji je najvidljiviji kroz prizmu mirne promjene vlasti, vladavine prava, tj. pravnu državu kao pretpostavku ustavne demokratije (Ferrajoli, 2012). Svi ti efekti u digitalnom okruženju ima nesagledive posljedice po čovjeka.

Najbolji način za suprotstavljanje negativnom utjecaju tehnologije na sigurnosti jeste kombinacijom podizanja javne svijesti o cyber sigurnosti, kroz bolje upoznavanje sa digitalnim informacijsko-komunikacijskim tehnologijama i shvatanje kompleksnosti tog sistema u kojem se treba krenuti od činjenice da prvenstveno sami sebe moramo zaštiti. Također je od velike važnosti jačanje sistema javne, gospodarske i energetske sigurnosti, kao i sistema zaštite kritične infrastrukture, te stvaranje učinkovitog sistema upravljanja krizama

[8] Maliciozni software koji enkriptuje i zaključa žrtvine podatke, te traži otkup ključa u nekoj od kriptovaluta.

5.3. Zaštita ljudskih prava u digitalnom okruženju

Nažalost, većina platformsko-digitalnog okruženja dizajnirana je s ciljem da izaziva što veću ovisnost svojih korisnika. To se, između ostalog, radi s ciljem okupljanja što većeg broja korisnika, prikupljanja još više korisničkih podataka na osnovu kojih se otkrivaju novi obrasaci ljudskog reagovanja itd. Na kraju priče o digitalnom okruženju i njegovim efektima, osvrnuti ćemo se na važan stub svakog društva a to je poštivanje ljudskih prava, te kako se postojeća ljudska prava uklapaju u digitalni ekosistem današnjice. Također, razmatrati će se konceptualni izazovi univerzalnom okviru ljudskih prava koje je donijela digitalna tehnologija.

U svakom demokratskom društvu svrha vlasti je da štiti ljudska prava. Ta svrha je postala znatno teže ostvariva pojavom internet i cyber prostora. Što se tiče ljudskih prava i pojave internet, za očekivati je bilo da će još bolja povezanost čovječanstva doprinijeti razvoju i zaštiti ljudskih prava, naročito prava na informisanje i slobodu izražavanja, međutim, niko nije ni slutio da će se digitalni prostor koristiti i za nagrizanje i ugrožavanje ljudskih prava.
Od formiranja UN-a prije više od 70 godina, smatra se da principi ljudskih prava igraju ključnu ulogu u pružanju međunarodnog mira i sigurnosti. Budući da se to pokazalo istinitim, velike države shvatile da je za očuvanje mira potrebno reformisati vjeru u osnovna ljudska prava, dostojanstvo i vrijednosti ljudske ličnosti. Vlade koje poštuju ljudska prava također su generalno shvatile da poštovanje ljudskih prava i vladavine prava jača njihovu snagu, a ne umanjuje je. U današnje digitalno povezanom ali i ranjivom kontekstu, u kojem se vrlo lahko širi globalni i domaći terorizam, mnoge su vlade bile u iskušenju da koriste nove digitalne tehnologije bez obzira na ljudska prava, pri tome i ne shvatajući posljedice zanemarivanja ovih vrijednosti za sigurnost (Human rights watch, 2016.).
Mnogi nisu ni svjesni da se nalazimo usred ogromne digitalne transformacije koja je uticala na svaki aspekt društva. Digitalna tehnologija je donijela mnoge izazove uživanju ljudskih prava, sigurnosti i upravljanju. Veliki test za vlade, aktere iz privatnog sektora, članove civilnog društva i tehnološku zajednicu je zadatak da kroz saradnju više dionika razviju prije svega proaktivne i holističke politike koje osiguravaju da se tehnologija koristi za povećanje i slobode i sigurnosti, te da se koristi od digitalnih tehnologija širi na sve ljude širom svijeta.

Do sada svjedočili smo raznim prekršajima u online sferi. Konkretni slučajevi kršenja online prava i sloboda koje je zabilježio ShareLab tim su: proizvoljno blokiranje ili filtriranje sadržaja,

cyber napadi na neovisne internetske i građanske medije, uhićenja i sudski postupci protiv korisnika društvenih mreža i blogera, manipulacija javnim mnijenjem korištenjem različitih tehnoloških alata, nadzor elektroničkih komunikacija, kršenje prava privatnosti i zaštite osobnih podataka, pritisak, prijetnje i smanjenje sigurnosti novinara, građana i pojedinaca na internetu (ShareLab, 2016).

Asocijacija za progresivne komunikacije (eng. Association for Progressive Communications - APC) navodi da je „sposobnost dijeljenja informacija i slobodne komunikacije korištenjem internet, od vitalnog značaja za ostvarivanje ljudskih prava koja su sadržana u Univerzalnoj deklaraciji o ljudskim pravima, Međunarodnom paktu o ekonomskim, socijalnim i kulturnim pravima, Međunarodnom paktu o građanskim i političkim pravia, Konvenciji o eliminaciji svih oblika diskriminacije žena, itd.." (APC, Povelja o internetskim pravima, 2006.). Ova povelja o pravima na internetu rani je primjer općeprihvaćene povelje o pravima na internetu, važnog elementa digitalnog konstitucionalizma.

Prema tome, digitalna ljudska prava posebna su vrsta subjektivnih prava, izražena u mogućnosti subjekta da ima pristup informacijama, elektroničkim uređajima, komunikacijskim mrežama i s njima obavlja različite radnje. Glavna svojstva digitalnih prava koja ih razlikuju od drugih vrsta subjektivnih prava su:

1. Predmet ovih prava su podaci dostavljeni u posebnom obrascu.
2. Digitalna prava provode se korištenjem digitalnih tehnologija i umjetne inteligencije.
3. Digitalna prava pripadaju samo posebnim subjektima (sudionicima digitalne komunikacije). (Ibid.)

Sljedeće vrste digitalnih prava odražavaju se u važećim međunarodnim i drugim pravnim aktima:

1. Pravo pristupa i korištenja telekomunikacijskih mreža.
2. Pravo na digitalne tehnologije i umjetnu inteligenciju (blockchain tehnologija, internet stvari, usluge u Cloud-u, dodatna stvarnost i sl.).
3. Pravo na stvaranje, objavljivanje i zaštitu digitalnih djela.
4. Pravo pružanja i korištenja digitalnih usluga (digitalne mobilne komunikacije i sl.).
5. Pravo na razmjenu informacija, slobodnu komunikaciju i izražavanje mišljenja u komunikacijskim mrežama.
6. Pravo na povjerljivost i anonimnost digitalnih osobnih podataka. (Ibid.)

BIRN i Share Foundation vrše praćenje povreda digitalnih prava u južnoj i istočnoj Evropi, te se u najčešćim povredama digitalnih prava nalazi:

- Činjenje sadržaja nedostupnim putem tehničkih metoda
- Kompjuterska prevara
- Uništavanje i krađa podataka i programa prevara
- Neovlašćeni pristup - neovlašćena izmena i postavljanje sadržaja
- Objavljivanje informacija o privatnom životu
- Curenje podataka o ličnosti građana
- Nedozvoljena obrada podataka o ličnosti
- Objavljivanje neistina i neproverenih informacija sa namerom ugrožavanja reputacije
- Uvrede i neosnovane optužbe
- Preteći sadržaji i ugrožavanje sigurnosti
- Govor mržnje i diskriminacija
- Pritisci zbog objavljivanja informacija
- Kreiranje lažnih naloga i plaćeno promovisanje lažnog sadržaja
- Manipulacije sadržajem i organizovano prijavljivanje na društvenim mrežama
- Izmena ili uklanjanje sadržaja od javnog značaja
- Plasiranje komercijalnog sadržaja kao informativnog
- Algoritamsko blokiranje ili suspenzija sadržaja
- Druge manipulacije u digitalnom okruženju (BIRN, Share Foundation, 2022.)

S pojavom novih tehnologija i interneta, očekivalo se da će javna debata o uticaju na ljudska prava biti mnogo otvorenija, dostupnija i u konačnici produktivnija, međutim, ona je imala tendenciju da bude reaktivna, parcijalna i često nepraktična. S obzirom na to da je digitalna tehnologija poremetila mnoge dimenzije društva, kreatorima politike je bilo teško da vide neke veće, svjetske trendove, da shvate različite odnose i adekvatno procijene glavne prioritete. Već odavno je vrijeme da kreatori politike budu proaktivniji i holističkiji, te da unaprijede praktična rješenja za nekoliko prioritetnih globalnih izazova ljudskih prava. (Human rights watch, 2016.) Može se zaključiti da sadržaj interneta ne predstavlja svakoga, te da ako internet zaista želi ostvariti svoj demokratski potencijal, mora bolje predstavljati i služiti ljudima koji su trenutno marginalizirani zbog svog spola ili boje kože, socijalnog statusa, pristupa internetu i savremenim tehnologijama, vjerskih ili bilo kojih drugih uvjerenja... itd.

Svijet koji se dinamički mijenja zahtijeva da osiguramo da digitalna revolucija služi društvu, a ne obrnuto. Zato je bitno saslušati osobe iz ranjivih skupina, poput starijih ili osoba s posebnim potrebama, kao i one osobe koje nemaju pristup internetu, a na koje digitalizacija i uvođenje novih tehnologija često negativno utiču (Edri, Trojánek, 2022.). Također, bilo bi zanimljivo čuti glas osoba koje nemaju pristup internetu, i zamisliti na trenutak, kakav bi svijet bio kada bi 2 biliona ljudi koji ne koriste internet (Kemp, Datareportal, 2020), u potpunosti iskorištavali njegove potencijale.

U svjetlu ovakvog razvoja, jedno od najosnovnijih pitanja koje se mora riješiti je: Kako možemo osigurati da se tehnologija koristi za poboljšanje slobode, a ne za olakšavanje represije ili drugih podlih ciljeva? Samo postizanje napretka po ovom pitanju bio bi veliki doprinos međunarodnim ljudskim pravima.

U najnovijem izvještaju UNDP-ija naglašena je važnost ulaganja u prevenciju i otpornost, zaštitu naše planete i ponovnu izgradnju jednakosti i povjerenja na globalnom nivou kroz solidarnost i obnovljeni društveni ugovor. Ujedinjeni narodi nude prirodnu platformu za unapređenje ovih ključnih ciljeva uz uključivanje svih relevantnih sudionika. „Naša zajednička agenda“ koristiti koncept ljudske sigurnosti kao alat za ubrzanje postizanja ciljeva održivog razvoja do 2030. godine. (UNDP, pregled specijalnog izvještaja, 2022.) Sve ovo nalaže da je svijetu potrebna jasna Povelja o ljudskim pravima za internet.

IV DATA EKSTRAKTIVIZAM I HUMANA SIGURNOST

Kroz prethodna poglavlja ovog rada objasnili smo principe i svrhu humane sigurnosti, opisali novo sigurnosno okruženje potpomognuto tehnološkom transformacijom i protokom informacija, te istražili njegov uticaj na ljudska prava i sigurnost društva... Ovo završno poglavlje objedinjuje sve prethodne komponente umreženog svijeta, posmatrajući čovjeka kao korisnika i puki resurs iz kojeg se izdvajaju informacija koje se zatim prikupljaji, obrađuju, svrstavaju i koriste u svrhu sticanja koristi, uticaja i moći. Neka pitanja na koja ćemo pokušati odgovoriti u ovom poglavlju su: Da li svijet vođen informacijama i tehnologijom, koja ima potencijal da oblikuje i manipuliše ljudskim životima, ugrožava humanu sigurnost čovjeka? Ako mašinerija za prikupljanje velikih podataka čovjeka posmatra kao korisnika besplatne usluge koju plaća svojim nematerijalnim radom, svojim satima i svojom privatnošću da li onda čovjek polahko gubi svoj lični integritet jer je zarobljen u jednom takvom sistemu? Da li se mijenja značenje ljudskog bića, pomijeranjem ljudskih granica i činjenicom da danas skoro svaki čovjek nosi pametni telefon sa sobom?

1. Digitalni otisak

Informacije igraju važnu ulogu u modernim društvenim odnosima, te su tehnološkim napretkom i digitalnom transformacijom postale glavna pokretačka snaga globalnog sistema. Njihov utjecaj na sve sfere društva generira promjene u moralnoj, kulturnoj i vrijednosnoj orijentaciji čovjeka. Kroz historiju osvajala se teritorija, resursi, zlato itd. a u 21. stoljeću moglo bi se reći da se osvajaju ljudi, uz pomoć i zbog informacija. To osvajanje odvija se uz pomoć digitalnih tehnologija i u digitalnom prostoru, stoga je sigurnost čovjeka u današnjem svijetu sve više vezana za digitalni informacijski prostor. U ovakvom vidu osvajanja čovjeka ne koristi se nasilje, niti prisila, jer korisnik usluge sam pristaje na uvjete i uslove o korištenju nekog produkta, jednostavnim klikom na dugme „slažem se“. Uslov korištenja produkta je saglasnost sa instaliranjem tzv. kolačića[9] i većina web stranica će od vas tražiti da prihvatite upotrebu kolačića prije nego što možete pristupiti web stranici, a da zapravo ni ne

[9] HTTP kolačić (cookies) je mali dio podataka poslat sa posjećenog sajta i smješten u korisnikov pretraživač. Svaki put kada korisnik otvori tu stranicu, pretraživač šalje kolačić natrag serveru i obaveštava web sajt o korisnikovim prethodnim aktivnostima (ShareLab, 2015)

znate što to znači. U prvom paragrafu teksta o uslovima korištenja i prikupljanja korisničkih podataka, se nalazi tekst koji kaže da se ovi uslovi mogu mijenjati u svakom trenutku od strane vlasnika, a bez znanja korisnika.

Iako je čovjek po svojoj prirodi nepredvidivo biće koje teži da mu svaki dan bude drugačiji, analizom njegovog digitalnog traga, njegovih obrazaca ponašanja i online aktivnosti moguće je vrlo precizno predvidjeti njegova buduća ponašanja. To se najčešće korist kako bi se prava reklama prikazala u pravom trenutku, pravom čovjeku koji će najvjerovatnije kupiti neki proizvod.

"Digitalni otisak je trag podataka koji kreirate dok koristite internet. To uključuje web stranice koje posjećujete, e-poruke koje šaljete i informacije koje šaljete online uslugama." (Christensson, P.,2014). Još na samom početku, važno bi bilo naglasiti da digitalni otisci ne znače digitalni identitet ili "pasoš", ali prikupljeni sadržaj i metapodaci utiču na internetsku privatnost, povjerenje, sigurnost, digitalnu reputaciju i preporuke. Kako se digitalni svijet širi i integrira s više aspekata života, vlasništvo i prava u vezi s podacima postaju sve važniji (Duncan, 2009, Family lives, 2022.).

Digitalni otisak, poznatiji još i kao digitalin dosije, raščlanjuje se na aktivne i pasivne tragove podataka. Aktivni tragovi podataka su oni koje korisnik namjerno ostavlja, a najčešće su to objave i interakcije na društvenim mrežama ili blogovima, postavljanje slika i video zapisa, elektornska pošta, telefonski pozivi itd. "Pasivne tragove podataka povezane s pojedincem ostavljaju drugi ili se prikupljaju kroz aktivnosti koje korisnik radi bez namjernog objavljivanja podataka. Posjete i radnje na web stranici, pretraživanja i online kupovine su među aktivnostima koje dodaju pasivne tragove podataka digitalnom otisku."(Whatls, Wingmore 2014).

Digitalni otisak je relativno trajan, te treba imati na umu da ono što ide na internet obično tamo i ostaje, čak i ako izbrišete postove, ostat će trag podataka koji ste ostavili za sobom (Family lives, 2022.). Vlasnik svojih informacija o sebi ustvari ima vrlo malo uvida i kontrole nad načinom na koji će ih drugi koristiti. Stoga bi glavni fokus upravljanja digitalnim otiskom (eng. Digital footprint management -DFM-) trebao biti oprez u vezi sa aktivnostima na mreži za kontrolu podataka koji se mogu prikupiti. (Whatls, Wingmore 2014).

Sistemi društvenih mreža mogu snimati aktivnosti pojedinaca, a onda te aktivnosti postaju podaci koji prikazuju „životni tok". Takva upotreba društvenih medija i senzora unutar uređaja omogućavaju digitalno praćenje podataka koji uključuju pojedinačne interese, društvene grupe, ponašanja, lokaciju, pažnju, doba dana, rezultate pretraživanja i ključne riječi, kreiran i konzumiran sadržaj, digitalnu aktivnost itd.Takvi podaci se uglavnom prikupljaju i analiziraju

bez svijesti korisnika (ICTEA, 2020). “Dok se digitalni otisak može koristiti za zaključivanje ličnih podataka, kao što su demografske osobine, seksualna orijentacija, rasa, religijski i politički stavovi, ličnost ili inteligencija bez znanja pojedinaca, on takođe izlaže privatnu psihološku sferu pojedinca u društvenu sferu” (Latour, 2007., prema ICTEA, 2020.)

Neki primjeri korištenja digitalnog otiska mogu se naći svuda oko nas. Primjer koji navodi Vladan Joler je u hotelijerstvu, kada algoritam stranice nekog hotela prepozna da je model uređaja koji se koristi za rezervaciju Iphone ili neki uređaj koji predstavlja određenu vrstu prestiža i socijalnog statusa, automatski nudi skuplje aranžmane. Uber predstavlja sličan primjer. U kolačićima, prihvatili ste da aplikacija ima uvid u vaš postotak baterije. Ukoliko imate 10% baterije, veća je vjerovatnoća da ćete pristati na skuplju vožnju. (Agilast, Joller, 2022.). Kompanija Tesla nije samo fabrika električnih automobile, nego je i “data factory”, koja mnoštvom senzora na svojim vozilima bilježi podatke svakog pređenog kilometra, svakog punjenja i destinacije. Primjeri se dodatno komplikuju ako smo svjesni količine naših podataka koji su se tokom godina prikupljali. Takve stvari direktno utiču na životni tok i oblikuju ga u smjeru u kojem neko od svega toga ima profit. Shodno tome, slični primjeri potvrđuju generalnu hipotezu koja glasi: Tehnologija, koja se uvukla u svakodnevni život čovjeka, sa svojim potencijalom da ga oblikuje i manipuliše, duboko zadire u humanu sigurnost i ljudska prava. U tom procesu milijarde onlajn aktivnosti ljudi se prikupljaju i pohranjuju. Ti podaci su toliko veliki da hard disk nijednog računara ne može sve pohraniti i mora im se pristupiti preko Cloud-a. Ogromne farme servera koje se nalaze širom svijeta održavaju i drže ove lične podatke (Blog UAB, 2019).

2. Veliki podaci (Big Data)

„Veliki podaci“ se odnose na prikupljanje i korištenje ogromnih količina podataka za proučavanje, razumijevanje i predviđanje ljudskog ponašanja.“ (Blog UAB, 2019). Definicija velikih podataka objašnjava da su to podaci koji sadrže veću raznolikost, koji stižu u sve većim količinama i sa sve većim brzinama. Ovi skupovi podataka su toliko obimni da tradicionalni softver za obradu podataka jednostavno ne može njima upravljati. Ove ogromne količine podataka mogu se koristiti i za rješavanje poslovnih, tržišnih ili projekcijskih problema s kojima se prije ne biste mogli pozabaviti (Oracle Cloud Infrastructure, 2022).

Tu se nameće jasna potreba za transparentnim tokovima informacija, gdje bi korisnik znao tačno gdje se nalaze njegovi podaci, kome idu i ko sve ima mogućnost uvida i analiziranja istih. U tom pogledu veliku prepreku predstavljaju „Treće strane“, odnosno kompanije koje su saradnici ili posrednici, a na koje se zakon o zaštiti podataka skoro pa i ne odnosi.

U početku svog razvoja, internet je bio neprofitno mjesto na kojem su korisnici postavljali različite sadržaje. Tokom daljeg širenja interneta, došlo je do nastanka velikog broja „sporednih“ korisničkih podataka koji nisu imali nikakvu vrijednost i smatrani su za bezvrijedani otpad. Tako je bilo sve dok korporacije nisu počele shvatati koliko podataka su korisnici generisali putem platformi kao što su Facebook, YouTube, Google i drugi povezani online servisi. Tada na scenu stupa prediktivna analitika, koja na osnovu algoritama analizira i obrađuje ove podatke. Na osnovu analize ogromnog broja podataka moguće je kreirati obrasce ponašanja korisnika, njegove navike, reakcije, preferencije itd., te u konačnici predvidjeti njegove naredne korake i potrošačke afinitete.

Da su veliki podaci postali kapital pokazuju nam neke od najvećih svjetskih tehnoloških kompanija. Veliki dio vrijednosti koju nude proizlaze iz njihovih podataka, koje stalno analiziraju kako bi proizveli veću efikasnost i razvili nove proizvode. (Oracle Cloud Infrastructure, 2022). Mnoge od najvećih svjetskih kompanija koje se bave tehnologijom i društvenim medijima, uključujući Google, Facebook, Messenger, Twitter, Amazon i Snapchat su na čelu ove industrije. Uzmemo li u obzir činjenice da su ove kompanije ujedno i najbogatije na svijetu, te da prema mišljenju brojnih autora (Joller, 2020, Zuboff, 2019 i dr.) trenutno živimo informacijski kolonijalizam ili kapitalizam, sa sigurnošću se može reći da informacije pokreću svijet današnjice. Zanimljivo je da ove platforme u suštini ne proizvode nikakav sadržaj, nego je sav posao kreiranja, distribucije i konzumacije sadržaja prepušten korisnicima. Ipak ove platforme oblikujući svoj prostor utiču na korisnika jer diktiraju pravila igre (npr. koliko duga tekstualna objava može biti, koliko dugačak video može biti, koje reakcije možete dobiti, itd.) U rukama tehnoloških giganta tako novac postaje uticaj i moć.

Ove kompanije savršeno su pozicionirane da iskoriste „Big Data“. Svaka od ovih kompanija ima pristup informacijama miliona svojih korisnika i kupaca, što im omogućava da ispune ogromnu količinu podataka potrebnih za istraživanje velikih podataka. Mnoge svjetske vlade se također uključuju u korištenje prediktivne analitike. Neki primjeri korištenja velikih podataka su: borba protiv terorizma, personalizirani oglasi, povećanje radne produktivnosti, predviđanje izbijanja virusa... (Blog UAB, 2019.). Veliki podaci obećavaju mnogo, ali nisu bez svojih izazova. Iako su razvijene nove tehnologije za pohranu podataka, količine podataka se udvostručuju otprilike svake dvije godine. Međutim, nije dovoljno samo pohraniti podatke,

potrebno ih je prije tog prečistiti kako bi mogli biti relevantni za klijenta, i organizovani na način koji omogućava smislenu analizu, a to zahtijeva mnogo rada. Naučnici za podatke troše 50 do 80 posto svog radnog vremena na klasifikaciju i pripremu podataka, prije nego što se stvarno mogu koristiti. (Oracle Cloud Infrastructure, 2022). Dok veliki podaci predstavljaju mnoge mogućnosti za dobro, ipak izazivaju mnoge moralne i etičke brige. Primarna briga je pravo pojedinca na privatnost na internetu.

U mnogim zemljama širom svijeta lična prava na privatnost u fizičkom svijetu su poprilično dobro uspostavljena. To podrazumijeva da organi za provođenje zakona ili bilo ko drugi, ne može pretraživati naše stvari, domove, automobile ili osobe bez pristanka (osim ako ne postoje zakonski razlozi i nalog za pretres). Međutim, većina ovih zakona i propisa ne proširuje se na prava privatnosti za online aktivnosti. Brzi uspon Interneta i brzi tempo tehnoloških inovacija ostavili su ove zakone iza sebe, tj. zastarjelim i neadekvatnim za moderno doba u kojem je internet svakodnevni zahtjev za stilove života mnogih ljudi. (Blog UAB, 2019.)

Trenutno, vlade i kompanije širom svijeta koriste naše informacije onako kako oni smatraju prikladnim uz vrlo malo ili u nekim slučajevima bez saglasnosti ili nadzora. Može se sa sigurnošću reći da su veliki podaci postali vrijedna roba koja se kupuje i prodaje između ovih entiteta. Gotovo svaki aspekt našeg života koji je moguće pratiti, prati se široko rasprostranjenom upotrebom nadzornih kamera, bilježenjem historije pretraživanja našeg pretraživača, našim navikama kupovine putem interneta, rezervacijama letova, finansijskim podacima, objavama na društvenim mrežama, fizičkim izgledom i sigurnosnim podacima. Brojne privatne kompanije, kao što su Facebook i Google „koriste ove podatke za kreiranje miliona detaljnih korisničkih profila. Ove kompanije zatim unovčavaju svoje informacije o klijentima tako što prodaju pristup drugim kompanijama, vladama i organizacijama koje pokušavaju da sprovedu istraživanje, ciljaju oglase ili na drugi način koriste ovu ogromnu količinu informacija.“ (Ibid.)

Sa ovolikom količinom ličnih podataka u nečijem vlasništvu, postoji i veliki rizik od zloupotrebe. Sve češće možemo svjedočiti primjerima koji otkrivaju skandalozne zloupotrebe ili curenja povjerljivih i ličnih podataka ili nezakonita online nadziranja koje koriste kompanije ili državne vlade.

Ovakvi i slični slučajevi su jasna kršenja osnovnih ljudskih prava na privatnost i dodatno naglašavaju potrebu za zakonima o privatnosti na mreži. (Blog UAB, 2019). Rizici se rapidno povećavaju kada prava na internet i online privatnost nisu zaštićena zakonima. Zakoni o pristupu internetu i privatnosti zaštitit će od toga da vlada krši prava građana (Ibid.).

3. Svijet ekstraktovanja podataka

U ovom trenutku u 21. stoljeću, upoznajemo novi oblik ekstraktivizma koji seže u najudaljenije uglove biosfere i najdublje slojeve ljudskog kognitivnog i afektivnog bića (Crawford, Joler, 2018.). U tom kontekstu, ne eksploatišu se samo podaci nego i ljudski životi, ne manipuliše se samo podacima i informacijama, nego i ljudskim bićem.

Države oduvijek vrše nadzor nad svojim stanovništvom, samo što u današnjem svijetu to mogu vršiti mnogo intenzivnije i dublje. Stoga Shoshana Zuboff u svojoj knjizi "Godine nadzornog kapitalizma" (2019.) tvrdi da trenutno živimo u svakodnevnom nadzoru ogromne intetnet infrastrukture, koja djeluje nevidljivo i bez znanja čovjeka. Potom države i njihove obavještajne službe koriste te informacije, kako bi lakše upravljali stanovništvom. Također objašnjava da se termin nadzorni koristi jer se kao i državni nadzor, uglavnom odvija bez znanja čovjeka. A takva upotreba tehnologije se odražava na sve aspekte funkcionisanja jednog savremenog društva. Svjetskim vladama i globalnim kompanijama ne odgovara društvo koje kritički razmišljaja i posmatra svijet oko sebe, stoga se i odlučuju na takve poteze, nadzora, korištenja medija, umjetne inteligencije i algoritama za postizanje još veće kontrole i uticaja na društvo. Kao što Zuboff ističe, kapitalizam nadzora prikazuje ljudsko ponašanje tako da se ono može analizirati kao vidljive, mjerljive jedinice. Ako uzmemo u obzir to da su naša tijela, um i ponašanje jedan od krajnjih resursa za novi ekstraktivizam, onda svaki segment našeg postojanja može se posmatrati kao oblik direktnog ili indirektnog rada koji proizvodi podatke. “Kada dišemo, hodamo ili spavamo, svaka pojedinačna emocija koju osjećamo, naša pažnja, naša tjelesna temperatura ili bolesti koje imamo - sve može proizvesti višak u ponašanju ako ga uhvati ovaj divovski nadzorni aparat. U tom smislu, čak i naše golo postojanje može se posmatrati kao rad.” (Zuboff, 2019, prema Joler, 2020.)

Sve ove tehnologije koriste obradu podataka za donošenje odluka te se razlikuju po svojim metodama, ali ne i po obimu (Mantelero, 2018.). Sve veća upotreba algoritama i umjetne inteligencije u donošenju odluka može pojačati diskriminaciju i potaknuti nesigurne radne uvjete (Salminen, 2018). Svaki klik, like, komentar ili slika postaju entiteti za sebe, u nekoj velikoj bazi podataka. Iz te baze podataka algoritmi analiziraju te entitete i dovode u određene veze sa drugim entitetima te im pridodaju značenja i određuju odnose između njih. Na osnovu tih informacija algoritmi kreiraju nove informacije koje nas klasifikuju, svrstavaju u neku socijalnu grupu, zatim te podatke neko prodaje oglašivačima koji će preciznije vršiti ciljanje

oglasa (Agilast, Joller, 2022.). Koristeći se našim podacima generisanim kroz digitalni trag, matematičari i statističari proučavaju potencijal naših želja, kretanja, potrošnje, te „predviđanje naše pouzdanosti i izračunavanje našeg potencijala kao učenika, radnika, ljubavnika, kriminalaca...“ (O'Neil, 2016: 10), ali i glasača kojima još uvijek niko nije rekao da su u novom društveno-političko-tehnološkom uređenju algoritamske demokratije.

Ove nove tehnologije, kao što su algoritmi i umjetna inteligencija, ponekad su dočekane sa strahom. Na primjer, iako su autopiloti automobila i sistemi autonomne vožnje blizu plodnosti, spremnost javnosti da se vozi u njima opada. A zabrinutost zbog utjecaja umjetne inteligencije na radna mjesta ljudi raste, iako ekonomisti kažu da će se zanimanja vjerojatno prilagoditi tehnološkim promjenama , a ne da će se potpuno izgubiti (Hodson, 2018). Ali umjetna inteligencija već je ušla u naš svakodnevni život uglavnom putem mobilnih uređaja i interneta. (Shnurenko, 2020.) Slično, vlade i kompanije sve više koriste te alate i tehnike za rješavanje poslovnih problema i poboljšanje mnogih poslovnih procesa, posebno onih na mreži. Umjetna inteligencija danas, sposobna je praviti nikad prije viđene slike na osnovu našeg unesenog teksta.[10] Zabrinutost mogu stvoriti sve kompleksnije grafike koje su danas ultra realisitične, uz koje posmatrač ne može vidjeti razliku između stvarnosti i simulacije. Također, u se dodaje i tehnologija za prepoznavanje lica, koja analizira bilione fotografija na društvenim mrežama i drugdje. Zatim se te slike koriste za kreiranje digitalnih identiteta i chatbotova koji su toliko uznapredovali i vjerodostojni da čovjek u nekim slučajevima ne može znati da li komunicira sa živim biće, čovjekom ili chatbotom (Murovana, 2020.). Ako tome pridodamo deep fake tehnologiju i lažno predstavljanje, uviđamo da se sigurnosni rizici samo povećavaju. Takva umjetna inteligencija još uvijek ne posjeduje svijest, ali posjeduje sve tekstove, komentare, i dostupne podatke na internetu. Nju uglavnom razvija Google i drugi tehnološki giganti. Elon Musk smatra da je veća prijetnja čovječanstu umjetna inteligencija nego nuklearne bombe. Shodno tome, pozvao je na jasno postojanje regulatornog tijela koje će nadzirati razvoj super inteligencije (CNBC, 2018.).

Vladan Joler, vođa Share lab fondacije i autor brojnih radova, mapirao je algoritam faceboka te novi ekstraktivizam i topografiju interneta objašnjava kroz skup koncepata i alegorija11. On svoj rad počinje uvodnim alegorijama gravitacije, sile i crnih rupa. Na samom početku, monopoli i konglomerati kao što su Google i Facebook predstavljeni su kao ogromne crne rupe

[10] Primjer porgrama dostupan na: https://www.craiyon.com/

[11] Alegorija predstavlja priču, pjesmu ili sliku poučnog karaktera koja može biti interpretirana tako da otkriva neko skriveno značenje, najčešće moralno ili političko (Joler, 2020).

koje svojom gravitacijom privlače i gutaju sadržaj i korisnike. Njihovoj gravitacionoj sili doprinose brojni potencijalni vektori i društvene sile kao što su strah od društvene izolacije i propuštanja, ekonomska i profesionalna nesigurnost, depresija i anksioznost, nerealna očekivanja efikasnosti i produktivnosti u okruženju koje surovo kaže prilagodi se ili umri. Sve te sile i vektori, sa ili bez naše želje, drže nas vezanim za te platofrme. Ustvari, "Društvena cijena odustajanja je postala toliko visoka da je odustajanje u suštini fantazija." (Brunton i Nissenbaum, 2015, prema Joller, 2020.). Takvi uslovi okruženja uzrokovali su promjenu uloge čovjeka jer je on, kao što Fuchs navodi, zatvorenik i radnik, jer obavlja svoju trostruku funkciju kao radnik, resurs i proizvod (Fuchs, 2014). Ovaj multidimenzionalni portret pojedinca, koji se sastoji od miliona tačaka podataka u stotinama dimenzija, može se posmatrati kao ono što će Deleuze nazvati individuom. A opisuje ju kao "Fizički utjelovljeni ljudski subjekt koji je beskonačno djeljiv i svodljiv na prikaze podataka putem modernih tehnologija kontrole". (Deluze, 1992, prema Joler, 2020)

Takav razvoj događaja donosi nove stvarnosti u društveni život koje možda prije nisu bile doživljene. Ove stvarnosti navode većinu nas da provedu dosta vremena u raznim medijskim okruženjima i platformama društvenih medija iz profesionalnih ili društvenih razloga. Većina ovih online interakcija osmišljena je i vođena novim tehnologijama.

Kristian Lukić u svome eseju "Kolonizacija s ljubavlju", ističe da korisnici društvenih platform, bili oni zaposleni ili ne, sada čine svijet rada, koji ih primorava da provode sve više sati održavajući svoje profile, nudeći izravno svoju stručnost, iskustvo, priče o uspjehu, mišljenja i dokumentaciju o poslovima i aktivnostima, a to rade na sličan način kao seksualni radnici u ulicama crvenih svjetiljki. (Lukić, 2016, prema Joler, 2020.) U tom kontekstu "rad na digitalnom identitetu je prisilni rad 21. stoljeća." Joler, 2020.). Potrebno je puno privilegija te financijske i psihološke stabilnosti da ne sudjelujete u sistemima ekonomije ugleda koje moderiraju te platforme. Utiču na naše živote jer odlučuju šta vidimo, šta nam se nudi, šta kupujemo, kako da komuniciramo, kako da mislimo. To više nije odnos između čovjeka i tehnologije, ili između čoveka i čovjeka, nego postaje trougao između prirode, tehnologije i čovjeka, odnosno nas kao ljudskih bića (Bozar, Joler, 2021.)

Prijetnja koju zapadnoj demokratiji predstavlja dijeljenje korisničkih podataka stavila je Facebook i druge platforme društvenih medija pod lupu državnih vlasti. To se moglo vidjeti u ispitivanjima Marka Zuckerberga pred američkim Kongresom i Evropskim parlamentom u aprilu 2018., ili Googla u 2019. Ti procesi doveli su do određenih promjena u pogledu privatnosti i zaštite korisnika, te izrodili regulative se kao što je Opća uredba o zaštiti podataka (GDPR) i dr. Ona može poslužiti kao pokretač ljudskog djelovanja osiguravajući da (a)

korisnici budu bolje informisani o tragovima koje ostavljaju u cyber prostoru i (b) da su njihovi podaci bolje zaštićeni od korištenje, od strane trećih lica (Castilla, Pursiainen, 2019.).
Uticaj podataka na svjetsku politiku i sigurnost očituje se i iz primjera o čuvanju podataka između EU i SAD. Skladištenje evropskih korisničkih podataka na serverima u SAD izazvalo je smetnje u Safe Harbor ugovoru između SAD-EU. Smatra se da Evropa ima strožije zakone o privatnosti od Sjedinjenih Država, jer kompanijama koje posluju u Evropi nije dozvoljeno da šalju lične podatke korisnika van Evrope osim ako ti podaci nisu adekvatno zaštićeni (Wordfence, 2015). Zbog tih zakonskih regulative Facebook i Instagram bi mogli biti ugašeni širom Evrope, saopštila je matična kompanija Meta. Pitanje se svodi na evropske propise o podacima koji sprečavaju Metu, da prenosi, pohranjuje i obrađuje podatke Evropljana na serverima u SAD-u (Euronews, 2022). Povlačenje iz Evrope, ostavilo bi značajne posljedice na ekonomiju, oglašavanje i trgovinu, što potvrđuje uticaj podataka na svjetska dešavanja i navodi na razmišljanje slična algoritamskoj transparentnost. To je ideja koja smatra da mi kao korisnici i potrosači bismo trebali znati te biznis modele za koje smo toliko vezani (Agilast, Joller, 2022.). Na kraju ovog poglavlja možemo zaključiti da je u današnjem digitalnom okruženju, u kojem informacije predstavljaju izuzetno vrijedan resurs, prednost, ali i potencijalni rizik, zanemaruju se sloboda, dobrobit i integritet individue, jer se u prvi plan nameće monetizacija i medijsko-platformska kontrola društva. Samozaštita i otpornost čovjeka u takvom okuženju može se graditi kroz razumijevanje važnosti informacija i opreza prilikom dijeljenja svojih podatka. U tom duhu, medijska i informacijske pismenosti (MIP) je odličan alat u borba protiv dezinformacija i netačnih informacija, a također i odličan navigator za bolje i sigurnije snalaženje u digitalnom okruženju. Svakodnevna povezanost sa brojnim uređajima sve više zahtijeva naglašavanje etičkog promišljanja tehnologije.

V ZAKLJUČNA RAZMATRANJA – Digitalna transformacija humane sigurnosti

Prethodna poglavlja ovog rada koja su za cilj imala analizu digitalne transformacije humane sigurnosti, dovela su do sljedečih zaključaka:
Digitalna transformacija humane sigurnosti je proces koji uveliko traje i neizvjesno je u kojem smjeru može otići. Pitanje je samo koliko spremno i odgovorno možemo očuvati humanu sigurnost budućim generacijama?

Sigurnost u 21. stoljeću se definiše nešto drugačije nego u prijašnjim epohama, jer ona sve više ovisi od ekonomskog razvoja, od vladavine prava, poštivanja ljudskih prava, funkcionirajuće privrede i državnih institucija, od sloboda i jakog civilnog društva. Kooperacija umjesto dominacije morat će zbog svega toga postajati sve više i više princip u sigurnosnoj politici, ako se želi postići uspjeh (Lasić, 2010).

Humana sigurnost nastala je nešto prije "eksplozije" interneta i digitalnog okruženja, pa se stoga u početku odnosila na zaštitu čovjeka od tradicionalnih prijetnji. Masovnija upotreba Interneta prihvaćena je kao slobodniji vid izražavanja, komunikacije i informisanja uz sjajnu priliku da ljudi učestvuju u demokratskim i drugim društvenim aktivnostima. Danas je čovjek sve vise vezan za svoj ekran, odnosno prozor u svijet kroz koji se prikazuje spektakl informacija različitog oblika. Međutim, iza tog ekrana, a naspram korisnika nalazi se globalna "nevidljiva" mašinerija infrastrukture internet. U radu se detaljno istražilo digitalno sigurnosno određenje, na osnovu kojeg se može zaključiti da je sigurnost savremenog čovjeka sve više vezana za cyber prostor. Nekoliko godina nakon prvog UNDP-ijevog izvještaja (UNDP 1994.), u kojem su navedene dotadašnje prijetnje ljudskom razvoju, u krugovima UN-a sve više se priča o digitalnim prijetnjama. Cyber prostor je značajno zakomplikovao ljudsku sigurnost jer je kreirao potpuno nove socijalne vrijednosti i prijetnje ličnom blagostanju. Primarna među njima je nevoljni rebalans relativnih prioriteta sigurnosti i ličnih sloboda. Postoji realniji stav prema elektronskom nadzoru i njegovoj spornoj, ali neizbježnoj ulozi u savremenoj borbi protiv terorizma, te prihvatanje činjenice da će 'sloboda' biti manja da bi drštvena sigurnost bila veća. Sekundarne prijetnje mogu se odnositi na protok informacija i uticaj digitalnih medija na čovjeka. Pa je tako u mnoštvu informacija sve teže prepoznati pravu, a proporcionalno tome sve lakše ne prepoznati zabludu, neistinu ili dezinformaciju.

Također, rastuće prijetnje odnose se i na planetarnu fabriku, koju uglavnom čine tehnološki giganti i socijalne platforme, za prikupljanje podataka o korisniku, o njegovim navika, zanimanjima, interesovanjima, kupovinama, kretanjima, reakcijama, raspoloženjima, trenutnim osjećanjima, do podataka o njegovom fizičkom i biološkom stanju. Sve te informacije mogu se koristiti protiv čovjeka i s ciljem da se što kvalitetnije eksploatiše. Humana sigurnost stoga mora osigurati da integracija tehnologije u svakodnevni život i sigurnost čovjeka, mora biti humana. Dosadašnje postavke humane sigurnosti u komparaciji sa složenošću cyberprostora jasno ukazuju na činjenicu da zvanična humana sigurnost, vrlo malo zna o dugoročnim efektima cyberprostora na čovjeka.

Smatram da etična upotreba tehnologije, s ciljem očuvanja dobrobiti čovjeka u njegovom digitalizovanom svakodnevnom životnom okruženju, treba biti integrisana u srce koncepta

humane sigurnosti. Takav pristup potaknuo bi pervenstveo korištenje tehnoloških potencijala današnjice za razvoj čovječanstva, a zatim sveobuhvatnije i detaljnije razumijevanje efekata digitalnog razvoja širom svijeta. Dobro kontekstualizovano ispitivanje digitalne transformacije i humane sigurnosti, koja tretira ljudska bića kao referentne objekte (i subjekte koji doprinose) sigurnosti, može pružiti uvid u drugačije perspektive i načine očuvanja humane sigurnosti.

Digitalna transformacija same humane sigurnosti tako postaje nezaobilazan alat u procesu zaštite čovjeka, odnosno njegove sigurnosti, ličnog integriteta i prava u digitalnom okruženju. Ona primorava sigurnosne strukture na promjenu percepcije izvora i oblika ugrožavanja čovjeka..

Sva ova priča dobija novu dimenziju ako uzmemo u obzir to da se u digitalnom okruženju nalazi i ogroman broj djece, koji se sada nazivaju Alpha generacija ili milenijumska djeca. Veliki problem predstavlja činjenica da djeca nemaju izgrađene stavove i samo kritičko mišljenje, pa vrlo lahko mogu biti zloupotrebljena ili izmanipulisana a da toga nisu ni svjesna. Digitalno okruženje koje konstantno proizvodi osjećaj neizvjesnosti i nesigurnosti, iskazuje potrebu za jednakim pristupom digitalnim pravima i pravom na život, jer sve više svog "života" vezujemo za internet. Digitalni svijet je postao socijalna potreba, a potpuno "isključivanje" iz tog svijeta vodilo bi socijalnoj isključenosti u realnom svijetu. Budući da od tehnologije umreženog svijeta ne možemo (i ne trebamo) pobjeći, ostaje samo pitanje pitanje koliko dobro i koliko dugo će se humana sigurnost boriti da tehnološki pravac kojim idemo bude human i dobar za čovjeka. Sigurnost individue i njenog ličnog integriteta, u takvom sistemu, dodatno se komplikuju ako smo svjesni količine naših podataka koji su se tokom godina prikupljali. Svi ti podaci se čuvaju negdje (na bezbroj lokacija), a koriste se na način da direktno utiču na naš život i oblikuju ga u smjeru u kojem neko od svega toga ima profit. Shodno tome, slični primjeri potvrđuju generalnu hipotezu koja glasi: Tehnologija, koja se uvukla u svakodnevni život čovjeka, sa svojim potencijalom da ga oblikuje i manipuliše, duboko zadire u humanu sigurnost i ljudska prava.

Savremena kontrola i manipulacija, uglavnom se odvijaju bez nasilja, korištenjem informacija i medija koji te informacije prosljeđuju. Uz takve mogućnosti, manipulacija tržištima, informacijama i ljudima je poprilično efikasna, maliciozna i neuhvatljiva.

Budući da se velike vlade svijeta najviše boje društva koje kritički posmatra i postavlja stvari u cilju im je da čovjeka ostave u neznanju, zabludama, teorijama itd. Za takve ciljeve najčešće koriste medije koji imaju veliki uticaj na percepciju čovjeka, svojim senzacionalističkim naslovima koji prikljupljaju najviše klikova, sa više slika mačaka ili sa više slika nasilja i krvi. Mediji tako mogu upravljati tržištem, politikom, javnim mnijenjem, izbornim tijelom itd Stoga

možemo zaključiti da je čovjek u suštini biće vrlo podložno manipulaciji. Stoga možemo zaključiti da edukacija i podizanje nivoa medijske i informacijske pismenosti postaje ključna kompetencija opstanka u digitalnom okruženju.

Ne mozemo pobjeci od činjenice da će tehnologija u budućnosti zasigurno još više ući u naše živote, stoga je od presudne važnosti osigurati da tehnologija radi za nas a ne protiv nas. Zakonske regulative i međunarodni propisi koji se tiću ljudskih prava, te međunarodnog i humanitarnog prava moraju biti adaptirane za djelovanje u digitalnom prostoru i prilagođene digitalnom kontekstu. Brojne su ideje i savjeti o usvajanju jasnih pripisa o etičnoj upotrebi podataka. Budući da je to je planetarni problem, za njegovo rješenje bilo bi potrebno da se cijeli svijet promijeni. Najbolji način da se čovjek oslobodi od modernog ropstva, jeste da se radi na izgradnji svijesti pojedinca da može promijeniti svijet i da ima potpunu kontrolu nad svojim životom.

VI POPIS INICIJALNE LITERATURE

Prilozi:

Literatura:

1. Amer, K., Jehane, N., "The Great Hack", Netflix dokumentarac, 2019. Dostupno na: https://www.netflix.com/ba-hr/title/80117542 Pristupljeno: 23.04.2022
2. Analiziraj.ba, Mušić, S. (2019) "MODERNI SIGURNOSNI IZAZOVI I MEDIJI: Kako ne upasti u hibridni rat?" Dostupno na: https://analiziraj.ba/moderni-sigurnosni-izazovi-i-mediji-kako-ne-upasti-u-hibridni-rat/ Pristupljeno 25.04.2021
3. APC "Povelja o internetskim pravima", (2006.), Dostupno na: https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter Pristupljeno: 27.02.2022
4. BBC, (2021.) "Twitter 'permanently suspends' Trump's account" Dostupno na: https://www.tr.com/news/world-us-canada-55597840 Pristupljeno: 26.07.2022
5. Beridan, I., (2008.) Politika i sigurnost. Sarajevo: Fakultet političkih nauka.
6. Beridan, I., Tomić., M, i Kreso, M, (2001), „Leksikon sigurnosti", DES, Sarajevo
7. BIRN, Share Foundation, (2022.) „Praćenje povreda digitalnih prava u južnoj i istočnoj Evropi." Dostupno na: https://monitoring.labs.rs Pristupljeno: 06.01.2022
8. Blog UAB, Institute for Human Rights Blog (2019.) "Why Big Data is a Human Rights Concern", Dostupno na: https://sites.uab.edu/humanrights/2019/01/25/why-big-data-is-a-human-rights-concern/?fbclid=IwAR2RbEnCH8PrG_-_tpwBGqBkPy4Z9n630AEL5gri6N-g1shgHvKTBZ9MFO4 Pristupljeno: 26.06.2022
9. Bodmer, Kilger, Carpenter, & Jones. (2012.) "Reverse Deception: Organized Cyber Threat Counter-Exploitation" New York: McGraw-Hill Osborne Media, Dostupno na: https://www.abebooks.co.uk/9780071772495/Reverse-Deception-Organized-Cyber-Threat-0071772499/plp Pristupljeno: 21.05.2022
10. Booth, K. (1991) "Security and Emancipation, International Affairs", (3): 527-545. Dostupno na: https://www.academia.edu/2766404/Critique_of_Ken_Booths_Security_and_Emancipation_ Pristupljeno: 28.06.2022
11. Castilla, M., Evelyn, J., Pursiainen, C. (2019) "Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not", Journal of Civil Society, 15: 4, 392-411, Dostupno na: https://www.tandfonline.com/doi/full/10.1080/17448689.2019.1672288 Pristupljeno: 20.06.2022.
12. CERT, Hrvatska "O incidentu" Dostupno na: https://www.cert.hr/oincidentu/ Pristupljeno: 22.06.2022.

13. Choo, K. (2011) “The Cyber Threat Landscape: Challenges and Future Research Directions" Computers and Security, 30, 719–731 Dostupno na: https://www.semanticscholar.org/paper/The-cyber-threat-landscape%3A-Challenges-and-future-Choo/7ae59771c7d9a3a346fb6374d21c31ca62c3618b Pristupljeno: 28.05.2022
14. Christensson, P., (2014.) “Digital Footprint Definition”. Dostupno na: https://techterms.com/definition/digital_footprint Preuzeto: 15.06. 2022.
15. CNBC, LIFE WITH A.I., Clifford, C. (2018) "Elon Musk: ‘Mark my words — A.I. is far more dangerous than nukes’ Dostupno na: https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html Pristupljeno: 23.02.2022.
16. Conference of Council of Europe Justice Ministers (2019.), “Justice in Europe facing the challenges of digital technology” Speech by Dunja Mijatović Council of Europe Commissioner for Human Rights Strasbourg, Dostupno na: https://www.coe.int/en/web/commissioner/-/justice-in-europe-facing-the-challenges-of-digital-technology Pristupljeno: 29.04.2022
17. Crawford, K., Joler, V. (2018.) “Anatomy of an AI System: The Amazon Echo As An Anatomical Map of Human Labor, Data and Planetary Resources,” AI Now Institute and Share Lab, Dostupno na: https://anatomyof.ai/ Pristupljeno: 23.05.2022.
18. DATAREPORTAL, izvještaji: Dostupno na: https://datareportal.com/library?utm_source=Global_Digital_Reports&utm_medium=Partner_Article&utm_campaign=Digital_2022 Pristupljeno: 21.06.2022.
19. Deeks, A. (2015) “Tallinn 2.0 i kineski pogled na Tallinn process”, Dostupno na: http://www.lawfareblog.com/2015/05/tallinn-2-0-and-a-chinese-view-on-the-tallinn-process/ Pristupljeno: 03.03.2022
20. Deleuze, G. (1992.) "Postscript on the Societies of Control" 59, 3-7 Dostupno na: https://www.jstor.org/stable/778828 Pristupljeno: 28.07.2022.
21. Dijanović, D. (2020.) “Nakon korona-krize – koji su rizici za međunarodnu sigurnost?” Dostupno na: https://www.aem.hr/wp-content/uploads/2020/08/03.-Nakon-korona-krize-koji-su-rizici.pdf Pristupljeno: 28.06.2022.
22. Duncan, G. (2009.) "Threat to privacy under data law, campaigners warn". Telegraph. London. Dostupno na: https://www.telegraph.co.uk/news/politics/4339771/Threat-to-privacy-under-data-law-campaigners-warn.html Pristupljeno: 03.04.2022.

23. Elsa Blog, Vladislav V. Zhemerov (2020.) "Digital human rights near future or not?" Dostupno na: https://lawreview.elsa.org/digital-human-rights-near-future-or-not Pristupljeno: 07.04.2022.
24. Euronews, Davies, P. (2022) "Meta warns it may shut Facebook in Europe but EU leaders say life would be 'very good' without it" Dostupno na: https://www.euronews.com/next/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe-over-data-transfer-issues?fbclid=IwAR2uGPwxoyTKcYS7rY-yldAnXRQ1uXRpAG-l4QVXfKubdxm_NiqDPUyS_D0 Pristupljeno: 13.08.2022
25. Europska Konvencija za zaštitu ljudskih prava i temeljnih sloboda, (1950.) Rim Dostupno na: https://www.zakon.hr/z/364/%28Europska%29-Konvencija-za-zaštitu-ljudskih-prava-i-temeljnih-sloboda Pristupljeno: 03.05.2022.
26. Evropska komisija (2018). "Final report of the High-Level Expert Group on Fake News and Online Disinformation" Dostupno na: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271Pristupljeno: 03.04.2022.
27. Evropska komisija, (2022.), „Evropska deklaracija o digitalnim pravima i principima za digitalnu deceniju„ Brisel Dostupno na: https://ec.europa.eu/newsroom/dae/redirection/document/82703 Pristupljeno: 03.05.2022.
28. Family lives, 2022. "Digital Footprints" Dostupno na: https://www.familylives.org.uk/advice/your-family/online-safety/digital-footprints „Digitalna transformacija humane sigurnosti"
29. Ferrajoli, L, (2012.) "Ustavna demokratija" p. 15-68 https://doi.org/10.4000/revus.2303 Dostupno na: https://journals.openedition.org/revus/2303 Pristupljeno: 08.06.2022
30. Francis Hoffman „Hybrid Threats: Neither Omnipotent nor Unbeatable", Orbis 54, no. 3 (2010): Dostupno na: https://www.academia.edu/31357112/Hybrid_Threats_Neither_Omnipotent_Nor_Unbeatable Pristupljeno: 27.04.2021
31. Freeman C. Elgar, E. (1990.) "Ekonomija inovacije" Dostupno na: https://econpapers.repec.org/bookchap/elgeebook/550.htm Pristupljeno 08.04.2022.

32. Fuchs, C. (2014) "Digital Labour and Karl Marx" Dostupno na: https://www.routledge.com/Digital-Labour-and-Karl-Marx/Fuchs/p/book/9780415716161 Pristupljeno: 22.06.2022
33. Gregoratti, C. (2018.) "*Human security"* Enciklopedija Britannica, Dostupno na: https://www.britannica.com/topic/human-security Pristupljeno: 26.06.2022
34. Hansel, M. (2010.) "New and old barriers. Dominance and Political Participation in Cyberspace" Journal of Foreign and Security Policy, 3 (3), 357–378.).
35. Hellmann, G., Herborth, B.. (2017) "Uses of the West. Security and the Politics of Order", Cambridge University Press, Cambridge, str. 231-254. Dostupno na: https://oa.mg/work/10.1017/9781316717448 Pristupljeno: 24.07.2022
36. Hilbert M., Darmon D. (2020.B) "How Complexity and Uncertainty Grew with Algorithmic Trading" Dostupno na: https://www.mdpi.com/1099-4300/22/5/499 Pristupljeno: 17.06.2022
37. Hilbert, M, (2021.) "Information Theory for Human and Social Processes" doi: 10.3390/e23010009 PMCID: Dostupno na: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7822471/ Pristupljeno: 20.05.2022
38. Hilbert, M., (2020.A) "Digital technology and social change: the digital transformation of society from a historical perspective", Dialogues in clinical neuroscience, 22(2), 189–194. Dostupno na:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7366943/?fbclid=IwAR3FEIk8i9kS7lq_csO2fyPbXY5j1LGX3s76l0dD47BJ0j3oXTYwNWxVziA Pristupljeno: 31.01.2022
39. Hodson, R. (2018),Nature "Digital revolution" doi: https://doi.org/10.1038/d41586-018-07500-z Dostupno na: https://www.nature.com/articles/d41586-018-07500-z Pristupljeno: 22.12. 2021
40. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx?ID=68025
41. Human Rights Watch, (2014.) "Human Rights in the Digital Age" https://www.hrw.org/news/2014/12/23/human-rights-digital-age Pristupljeno: 25.05.2022
42. Human rights watch, (2016), Only security, "Digital Disruption of Human Rights 2" Dostupno na: https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights Pristupljeno: 24.05.2022

43. ICTEA, (2020.) Knowledgebase, "What a digital footprint?" Dostupno na: https://www.ictea.com/cs/knowledgebase.php?action=displayarticle&id=2235&language=english Pristupljeno: 17.16.2022
44. IIHR (Inter-American Institute of Human Rights), (2010) "What is Human Security?" Dostupno na: https://www.iidh.ed.cr/multic/default_12.aspx?contenidoid=ea75e2b1-9265-4296-9d8c-3391de83fb42&Portal=IIDHSeguridadEN#doce, Pristupljen: 01.06.2022
45. IT Professionalism Europe "New declaration for a human centred digital transformation" (2022.) Dostupno na: https://itprofessionalism.org/new-declaration-for-a-human-centred-digital-transformation/?fbclid=IwAR0jpTyD3pxptmnb56kBmRiMsr9xVRHTDE2xDsCpNxNWdybI6Nme4w761t4 Pristupljeno: 25.12.2021
46. Izvještaj Evropske komisije za BiH (2020). Dostupno na: https://europa.ba/wp-content/uploads/2020/10/Izvjestaj_za_BiH_za_2020_godinu.pdf Pristupljeno: 25.12.2021
47. J. Martín Ramírez, Luis A. García-Segura 2017. " Cyberspace Risks and Benefits for Society, Security and Development" Dostupno na: https://www.amazon.com/Cyberspace-Benefits-Development-Technologies-Applications/dp/3319855344 Pristupljeno: 15.12.2021
48. Jacobs, A., Lasconjairas, G. (2017) "NATO's Hybrid Flanks: Handling Uncinventional Warfare in the South and the East;" NATO's Response to Hybrid Threats, NATO Defence College, Forum paper 24, 2017, p.260. Dostupno na : https://www.files.ethz.ch/isn/190786/rp_112.pdf (datum pristupa 30.04.2021.)
49. Joler Vladan (2020) "New Extractivism - An assemblage of concepts and allegories." Dostupno na: https://extractivism.online/?fbclid=IwAR1_vuVgPSljIA3A6BTg-0BEMHt2YYK0PwFrFtKlMowVV3O9ppJPTSR5Lkg Pristupljeno: 03.05.2022.
50. Jovović, D., Korajčević, Š. (2020), "Upotreba informaciono komunikacionih tehnologija u Bosni i Hercegovini", Agencija za statistiku Bosne i Hercegovine.
51. Karahmetović, M. Mujić, K., Đultur, V. (2020) "Cyber criminal and privacy protection in the cyber world", CEPS Dostupno na: https://www.ceps.edu.ba/Files/DIT/Godina%206%20Broj%201/11.pdf?ver=1 Pristupljeno: 19.05.2022
52. Kemp, S., Datareportal, (2022). "DIGITAL 2022: GLOBAL OVERVIEW REPORT" Dostupno na: https://datareportal.com/reports/digital-2022-global-overview-report

53. Kolobara Robert. (2019) Hibridne prijetnje u 21.stoljeću – teorija i istraživanje nazivlja u Bosni i Hercegovini. Dostupno na: https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=337151
54. Lhamo, Tshering, Kuensell - UNDP, (2022) "Overcoming human security challenges in the age of digital governance"https://kuenselonline.com/overcoming-human-security-challenges-in-the-age-of-digital-governance/
55. Lipovac, M. (2013.), "Doprinos konstruktivističke paradigme studijama bezbednosti", Sociološki pregled, vol. XLVII (no. 3, str. 439–460 UDK: 303.442.23; 005.934 Fakultet bezbednosti Univerzitet u Beogradu
56. Lipovac, M., Živojinović, D., (2014.) "Međunarodna bezbednost -teorijski pristupi-Uvod u studije bezbednosti", Beograd, Univerzitet u Beogradu Fakultet bezbednosti Inovacioni centar Fakulteta bezbednost Dostupno na: https://www.scribd.com/document/455051578/Međunarodna-bezbednost-teorijski-pristupi-Uvod-u-studije-bezbednosti
57. Mantelero, A., (2018.), "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment", Computer Law & Security Review, Volume 34, Issue 4, str. 754-772 Dostupno na: https://www.sciencedirect.com/science/article/pii/S0267364918302012?via%3Dihub
58. Matteo Mirigliano (2022) "Komisija iznosi deklaraciju o digitalnim pravima i načelima za sve u EU-u 2022" Dostupno na: https://digital-skills-jobs.europa.eu/en/latest/news/commission-puts-forward-declaration-digital-rights-and-principles-everyone-eu Pristupljeno: 14.06.2022
59. Meta Investor Relations, „Facebook Reports Second Quarter 2021 Results", 2021.,Dostupno na: https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Second-Quarter-2021-Results/default.aspx Pristupljeno 13.06. 2022.godine
60. Michael Wade, THE CONVERSATION, "Psychographics: the behavioural analysis that helped Cambridge Analytica know voters' minds" 2018 , dostupno na: https://theconversation.com/psychographics-the-behavioural-analysis-that-helped-cambridge-analytica-know-voters-minds-93675 Pristupljeno: 21.02.2022.
61. Mihalinčić, M. (2020) "Savremena sigurnost, novi rizici i razvoj preventivnih modela kriznog upravljanja u Republici Hrvatskoj" Sveučilište u Zagrebu, Fakultet političkih zanosti, Zagreb. (Zagreb) Dostupno na:

https://www.fpzg.unizg.hr/_download/repository/DR_MARTINA_MIHALINCIC.pdf Pristupljeno: 24.06.2022

62. Mikac, R. (2013) “Suvremena sigurnost i privatne sigurnosne kompanije”. Zagreb: Jesenski & Turk.”
63. Mingst, K. (2018.). “United Nations Development Programme. Encyclopedia Britannica. Dostupno na:https://www.britannica.com/topic/United-Nations-Development-Programme Pristupljeno: 21.05.2022
64. Mladenović, D. (2016) “Multidisciplinarni aspekti sajber ratovanja” doktorska disertacija Beograd, Dostupno na: https://nardus.mpn.gov.rs/handle/123456789/6880 Pristupljeno: 29.05.2022
65. NATURE, Andrew Urquhart & Brian Lucey “Kripto i digitalne valute” (2022.) Dostupno na: https://www.nature.com/articles/d41586-022-00927-5 Pristupljeno: 23.05.2022
66. O’Neil, C. (2016): “Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy”. New York, NY: Crown. Dostupno na: http://governance40.com/wp-content/uploads/2019/03/Weapons-of-Math-Destruction-Cathy-ONeil.pdf
67. Oracle Cloud Infrastructure (OCI) "What is Big Data?" (2022.) https://www.oracle.com/big-data/what-is-big-data/
68. PCPress, Gavrilov, M. “Šta je Dark Web, a šta Deep Web? “, (2017.) Dostupno na: https://pcpress.rs/sta-je-dark-web-a-sta-deep-web/
69. Perez C., Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages, Edward Elgar Pub, New York, 2003. Dostupno na: https://www.e-elgar.com/shop/gbp/technological-revolutions-and-financial-capital-9781840649222.html Pristupljeno: 20.06.2022
70. Povelja Europske unije o temeljnim pravima, 2007, EZR-Lex, 2007. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A12007P
71. Povelja Ujedinjenih nacija, 1945. Dostupno na: https://advokat-prnjavorac.com/zakoni/Povelja_Ujedinjenih_nacija.pdf
72. Reznik, M. (2013). Krađa identiteta na web lokacijama društvenih mreža: Razvoj pitanja internetske impersonacije. Touro Law Review. Volume 29 Number 2, Article 12.
73. RISJ (2018). Digital News Report 2018 (Izvještaj o digitalnim vijestima 2018). University of Oxford). http://media.digitalnewsreport.org/wp-

content/uploads/2018/06/digi-tal-news-report-2018.pdf?x89475 [pristupljeno 29.03.2018

74. Salminen, M., Hossain, K., (2018.) “Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North” Dostupno na: https://www.researchgate.net/publication/325983560_Digitalisation_and_human_security_dimensions_in_cybersecurity_An_appraisal_for_the_European_High_North
75. Schmitt, MN (2018) 'Virtuelno' lišenje prava: miješanje sajber izbora u sive zone međunarodno pravo.Chicago Journal of International Law, 19 (1), 30–67.
76. Schmitt, MN., (2013) “Tallinn Priručnik o međunarodnom pravu primjenjivom na cyber ratovanje” Cambridge University Press, 2013., loc 209 - 351 od 7915, Kindle Ed.
77. Schumpeter, J. A. (1942). “Socialism, Capitalism and Democracy”, New York: Harper and Brothers Dostupno na: https://www.cambridge.org/core/journals/american-political-science-review/article/abs/capitalism-socialism-and-democracy-by-joseph-a-schumpeter-new-york-harper-and-brothers-1942-pp-x-381-350/13A4BF9E884069B0C4144E266443B82F Pristupljeno: 29.06.2022
78. Schumpeter, J.A. (1939) “Business Cycles: A Theoretical, Historical, and Statistical Analysis of the Capitalist Process. McGraw-Hill”, New York. Dostupno na: https://www.researchgate.net/publication/319503069_Schumpeter_Joseph_Alois_1939_Business_Cycles_A_Theoretical_Historical_and_Statistical_Analysis_of_the_Capitalist_Process Pristupljeno: 26.06.2022
79. ShareLab, (2015) "Nevidljiva infrastruktura: Onlajn pratioci" Dostupno na: https://labs.rs/sr/nevidljiva-infrastruktura-onlajn-pratioci/ Pristupljeno: 14.08.2022
80. ShareLab, 2016. "Mapping and quantifying political information warfare", Part 1 : Propaganda, domination & attacks on online media Dostupno na: https://labs.rs/en/mapping-and-quantifying-political-information-warfare/#easy-footnote-bottom-5-1349 Pristupljeno: 28.07.2022
81. Shnurenko, I., Murovana, T., Kushchu, I. (2020) "Artificial intelligence: media and information literacy, human rights and freedom of expression" Moscow, UNESCO IITE and TheNextMinds Dostupno na: https://unesdoc.unesco.org/ark:/48223/pf0000375983 Pristupljeno: 02.02.2022
82. Smajić, M, (2012) „Evolucija koncepta Humane sigurnosti“, 2012., Sarajevski žurnal za društvena pitanja (jesen/zima 2012) Dostupno na: https://www.academia.edu/3621217/Evolucija_koncepta_ljudske_sigurnosti_u_savre

menim_sigurnosnim_studijama_Evolution_of_the_concept_of_human_security_in_contemporary_security_studies Pristupljeno: 24.05.2022

83. Smajić, M., Seizović, Z., Turčalo, S. (2017), „Humana sigurnost u postkonfliktnom kontekstu“, Sarajevo: Fakultet političkih nauka u Sarajevu
84. SPECIJALNI IZVJEŠTAJ UNDP OVERVIEW, 2022 “Nove prijetnje ljudska sigurnost u Antropocenu, zahtijevajući veću solidarnost” https://hdr.undp.org/system/files/documents//srhs2022overviewenpdf.pdf
85. SPECIJALNI IZVJEŠTAJ UNDP, 2022 “Nove prijetnje ljudska sigurnost u Antropocenu, zahtijevajući veću solidarnost” https://hs.hdr.undp.org/pdf/srhs2022.pdf
86. Strategija za Digitalna transformacija mirovnih snaga UN-a, United Nations Peacekeeping, NewYork (2021) Dostupno na: https://peacekeeping.un.org/sites/default/files/20210917_strategy-for-the-digital-transformation-of-un-peacekeeping_en_final-02_17-09-2021.pdf
87. Sushmita Chakraborty, (2022.) "Digitalna revolucija u 21. stoljeću" MCA Patna Women's College, ResearchGate, Dostupno na: https://www.researchgate.net/publication/358550489 Pristupljeno: 01.12.2022
88. Tačno. net, Bašić, N. (2022.) “Da li je čovječanstvo na novom raskršću?” Dostupno na: https://www.tacno.net/novosti/da-li-je-covjecanstvo-na-novom-raskrscu/ Pristupljeno: 01.04.2022
89. Termiz, Dž., (2009), “Metodologija društvenih nauka”, Lukavac: NIK, Grafit.
90. Termiz, Dž., (2014), “Specifičnost metodologije istraživanja u bezbjednosnoj djelatnosti”, Sarajevo: Fakultet političkih nauka
91. Thompson, Coburn LLP (SAD) (2018.). Checklists of Foreign Countries Subject to Sanctions, Dostupno na : https://www.thompsoncoburn.com/docs/default-source/publication-documents/country-chart.pdf?sfvrsn=63924cea_14 (datum pristupa 30.04.2021.)
92. Trojanek, H. (2022.) Edri, “Promoting human rights in the digital” Dostupno na: https://edri.org/our-work/promoting-human-rights-in-the-digital-era/ Pristupljeno: 05.07.2022.
93. Tuđman, M., (2009.) „Informacijske operacije i mediji ili kako osigurati informacijsku superiornost.“ National security and the future, Vol. 10 No. 3-4,. Dostupno na: https://hrcak.srce.hr/80565 Pristupljeno: (29.04.2021)

94. UN, (1966.) “Međunarodni pakt o građanskim i političkim pravima Dostupno na: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights Pristupljeno: 29.05.2022
95. UN, (2003.) "Resource Dio II: Ljudska prava u vrijeme izvanrednih situacija" . Ujedinjeni narodi. Preuzeto 31. februara 2022.godine. Dostupno na https://www.un.org/esa/socdev/enable/comp210.htm#10.2
96. UN, (1966.) “Međunarodni pakt o ekonomskim socijalnim i kulturnim pravima, 1966. Dostupno na: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights Pristupljeno: 29.05.2022
97. Univerzalnu deklaraciju o ljudskim pravima, (1948.) Dostupno na: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/cnr.pdf Pristupljeno: 14.02.2022
98. Vajzović E., Džihana A., Hibert M., Ibrahimbegović-Tihak V., Bakić S., Kulenović F. (2018). “Pregledna studija o politikama i strategijama medijske i informacijske pismenosti u Bosni i Hercegovini”, Sarajevo: Fakultet političkih nauka.
99. Vajzović, E. (2020), “Digitalna transformacija sigurnosti i algoritamska demokratija”, Sarajevo, Social Science Dostupno na: https://www.ceeol.com/search/article-detail?id=962456 Pristupljeno: 26.03.2022
100. Vajzović, E., Turčalo, S., Smajić, M., (2019), “Collective Cyber Security Defence – Prospects for Western Balkans” SECURITY FORUM Interpolis, Banská Bystrica, Slovakia.
101. Vajzović, Hibert, Turčilo i dr. (2021) "Medijska i informacijska pismenost Dizajn ucenja za digitalno" https://fpn.unsa.ba/b/wp-content/uploads/2021/04/MEDIJSKA-I-INFORMACIJSKA-PISMENOST-DIZAJN-UCENJA-ZA-DIGITALNO-DOBA_e-izdanje-1.pdf
102. WEF. (2016).”Digitalni mediji i društvo, implikacije u hiperpovezanoj eri” World Economic Izvještaj o projektu Forum Dostupo na: http://www3.weforum.org/ docs / WEFUSA_DigitalMediaAndSociety_Report2016.pdf
103. Whatls,(2014.) "What is digital footprint?" Dostupno na: https://www.techtarget.com/whatis/definition/digital-footprint
104. Williams, M. (2003) “Words, Images, Enemies: Securitization and International Polities”, International Studies Quarterly, 47: 511-531.

105. Wolfers, A. (1952) “National Security as an Ambiguous Symbol, Political Science Quarterly”, 67(4): 485.

106. Wolff Heinegg (2013) "The tallinn manual and international cyber security law" DOI:10.1007/978-90-6704-924-5-1 Dostupno na: https://www.researchgate.net/publication/291816775_Chapter_1_The_tallinn_manual_and_international_cyber_security_law Pristupljeno: 26.06.2022

107. Wordfance, Maunder, M. (2015.). “Storing European User Data on USA Servers?” Dostupno na: https://www.wordfence.com/blog/2015/10/european-data-on-usa-servers-safe-harbor/?fbclid=IwAR3_vGMEPUAwVjQpE4rHv03ACRTsiDrwC-gIUOyXVc4wqW-CUferk0hYbqs Pristupljeno: 13.05.2022.

108. World Economic Forum (WEF), (2016). „Digital media and society. Implications in a Hyperconnected Era", Dostupno na: https://www.weforum.org/reports/digital-media-and-society-implications-in-a-hyperconnected-era/ Pristupljeno: 23.04.2022

109. World Economic Forum, Global Risks, 2012. Dostupno na: https://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

110. Youtube, Agelast, (2021.) "Podcast 099: Vladan Joler i Filip Milošević (Share fondacija)", Dostupno na: https://www.youtube.com/watch?v=uSujabFEG0s&list=TLPQMTEwODIwMjKnrgSNSpJIJQ&index=3 Pristupljeno: 10.08.2022

111. Youtube, Bozar, Joler, V., (2021.) "The Future of Living – Panel 2 –" Dostupno na: https://www.youtube.com/watch?v=BnMHMHiP0aA&t=680s Pristupljeno: 21.08.2022

112. Zojer, G. (2019). “The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised through the Human Security Lens” The Yearbook of Polar Law Online https://doi.org/10.1163/22116427_010010014 Dostupno na: https://brill.com/view/journals/yplo/10/1/article-p297_14.xml?language=en Pristupljeno: 25.12.2022

113. Zuboff, S. (2019) “The age of surveillance capitalism – The Fight for a Human Future at the New Frontier of Power” Dostupno na: https://we.riseup.net/assets/533560/Zuboff%2C+Shoshana.The+Age+of+Surveillance+Capitalism.2019.pdf Pristupljeno: 13.06.2022