

# Utjecaj društvenih mreža na socijalnu stvarnost

---

**Miloknoja, Karlo**

**Undergraduate thesis / Završni rad**

**2024**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, Faculty of Croatian Studies / Sveučilište u Zagrebu, Fakultet hrvatskih studija**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:111:724261>

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

*Download date / Datum preuzimanja:* **2025-01-20**



*Repository / Repozitorij:*

[Repository of University of Zagreb, Centre for Croatian Studies](#)





SVEUČILIŠTE U ZAGREBU  
FAKULTET HRVATSKIH STUDIJA

Karlo Miloknoja

**UTJECAJ DRUŠTVENIH MREŽA  
NA SOCIJALNU STVARNOST**

ZAVRŠNI RAD

Zagreb, 2024.



SVEUČILIŠTE U ZAGREBU FAKULTET

HRVATSKIH STUDIJA

Odsjek za sociologiju

Karlo Miloknoja

# UTJECAJ DRUŠTVENIH MREŽA NA SOCIJALNU STVARNOST

ZAVRŠNI RAD

Mentor: doc. dr. sc. Ivan Perkov

Zagreb, 2024.

## SADRŽAJ

<b>1.</b>	<b>UVOD .....</b>	<b>1</b>
<b>2.</b>	<b>TEMELJNE ODREDNICE DIGITALNOG OKRUŽENJA .....</b>	<b>2</b>
<b>2.1.</b>	<b>Komunikacija na društvenim mrežama .....</b>	<b>4</b>
<b>3.</b>	<b>ETIČKA PITANJA KOD KORIŠTENJA DRUŠTVENIH MREŽA .....</b>	<b>6</b>
<b>3.1.</b>	<b>Pitanje privatnosti društvenih mreža .....</b>	<b>6</b>
<b>3.2.</b>	<b>Sloboda govora na društvenim mrežama .....</b>	<b>7</b>
<b>3.3.</b>	<b>Zaštita identiteta na društvenim mrežama.....</b>	<b>9</b>
<b>3.4.</b>	<b>Anonimnost i online nasilje.....</b>	<b>12</b>
<b>3.5.</b>	<b>Ciljano oglašavanje i manipulacija korisnicima.....</b>	<b>13</b>
<b>4.</b>	<b>UTJECAJ DRUŠTVENIH MREŽA NA SOCIJALNU STVARNOST .....</b>	<b>15</b>
<b>4.1.</b>	<b>Utjecaj društvenih mreža na zdravlje .....</b>	<b>15</b>
<b>4.2.</b>	<b>Utjecaj društvenih mreža na socijalnu anksioznost .....</b>	<b>18</b>
<b>4.3.</b>	<b>Manipulacija algoritmom.....</b>	<b>18</b>
<b>4.4.</b>	<b>Uloga influencera i njihov utjecaj na korisnike društvenih mreža .....</b>	<b>20</b>
<b>5.</b>	<b>ZAKLJUČAK .....</b>	<b>21</b>
	<b>Literatura.....</b>	<b>22</b>

## 1. UVOD

Uvodno poglavlje seminarskog rada usmjereno je na definiranje glavnih postavki rada, a to su predmet i cilj pisanja rada, izvori i metode prikupljanja podataka i sadržaj i struktura rada. Evolucija društvenih medija stvorila je novu paradigmu komunikacije i interakcije. Društvene mreže postale su dio našeg društvenog života koji nam pomaže da se povežemo s prijateljima, obitelji i kolegama, ali i nepoznatim osobama. Pojava platformi društvenih medija poput Facebooka, Twittera i What's Appa donijela je revolucionarnu promjenu u načinu na koji se koristi Internet u osobne i profesionalne svrhe. Društvene mreže utječu i na socijalnu interakciju s ljudima budući da se većinski dio komunikacije obavlja putem Interneta i društvenih mreža. Mnogi ljudi nisu svjesni negativnih strana koje donose društvene mreže, kao i činjenica da se prevelikom konzumacijom društvenih mreža narušava čovjekovo zdravlje, fizičko i psihičko. Cilj rada je ukazati na privatnost, sigurnost i posljedice pretjerane konzumacije društvenih mreža. Za potrebe izrade seminarskog rada, podaci su prikupljeni sekundarnim putem i to kroz knjige, članke te relevantne internetske izvore. Prilikom analize prikupljenih sekundarnih podataka korištene su metoda analiza i sinteze te metoda deskripcije.

Seminarski rad strukturiran je u tri poglavlja. U uvodnom poglavlju objašnjavaju se predmet i cilj rada, sadržaj i struktura rada te izvori i metode prikupljanja podataka. U drugom poglavlju naglasak je na definiranju društvenih mreža te privatnosti i sigurnosti na njima. Treće poglavlje usmjereno je na utjecaj društvenih mreža na socijalnu stvarnost.

## 2. TEMELJNE ODREDNICE DIGITALNOG OKRUŽENJA

Suvremeno doba je doba sveprisutnih digitalnih medija. Ti se mediji istražuju u različitim teorijskim konceptualizacijama i na različite načine (Paska, 2019:2348). Za razliku od prethodnih razdoblja razvoja medija, suvremena digitalna medijska okruženja postala su sveprisutna zahvaljujući novoj informacijsko-komunikacijskoj tehnologiji. Jedan od razloga zašto ljudi dijele informacije jest taj što je to neizbježan dio pridruživanja „informacijskoj autocesti“.

Danas postoji više od 4,6 milijardi aktivnih korisnika interneta, a još milijarde će se priključiti. Platforme društvenih medija i tražilice okupljaju milijarde korisnika dnevno koji dobrovoljno odaju svoje privatne podatke s očekivanjem da će to "optimizirati" njihovo iskustvo. Izraz "društveni mediji" prvi je put upotrijebljen 1994. godine u tokijskom online medijskom okruženju pod nazivom Matisse (Aichner i sur., 2021:215). U tim ranim danima komercijalnog interneta razvijene su i lansirane prve društvene mreže. „Društvene mreže mogu se definirati kao digitalna okruženja u kojima sadržaje u potpunosti ili djelomično kreiraju njihovi korisnici korištenjem tehnološke platforme koja omogućuje komunikaciju s drugim korisnicima. Društvene mreže dio su prožimajućih društvenih digitalnih okruženja za koje se može tvrditi da su potaknule širenje ovih mreža, s obzirom na učestalost njihove uporabe.“ (Paska, 2019:2351).

Društvene mreže postale su globalni komunikacijski fenomen, počevši od skromnih početaka sa SixDegrees.com društvenom mrežom, pa sve do Friendster, MySpace, Facebook, Twitter i svih onih koji su se između navedenih pojavljivale i nestajale s globalne komunikacijske scene i društvenog prostora. Friendster je društvena mreža osnovana od strane bivšeg zaposlenika Netscape-a Jonathana Abramsa 2002. godine, a Web stranica dizajnirana jetako da korisnici stvaraju profile koji uključuju osobne informacije i mogućnosti povezivanja s prijateljima s kojima nije tako jednostavno stupiti u kontakt. Ubrzo nakon Friendstera pojavljuje se nova društvena mreža nazvana MySpace, koja je zamišljena drugačije od Friendstera s ciljem pretvaranja društveno mrežnog komunikacijskog fenomena u multimedijски (Grbavac, 2014:206).

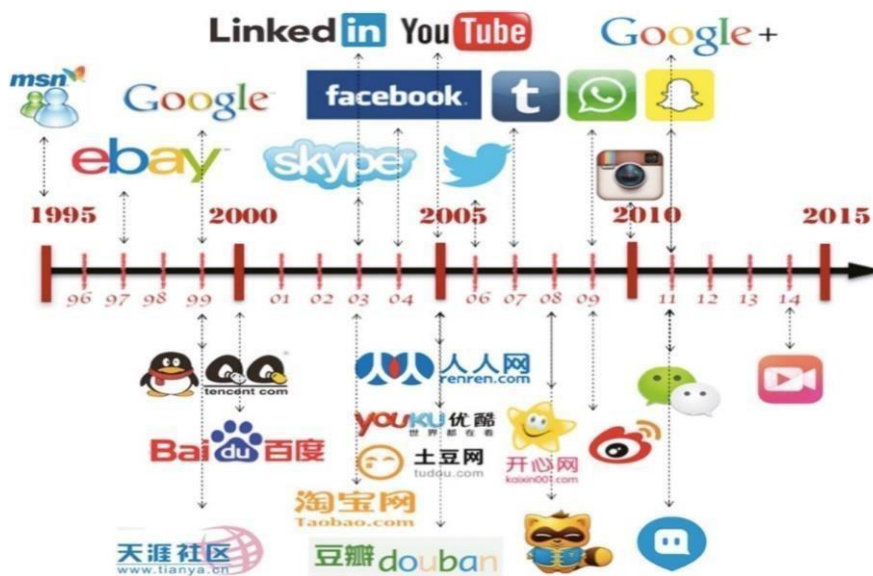
U današnje doba najpoznatije društvene mreže su Facebook i Instagram. Facebook je osnovao

Mark Zuckerberg i nije mogao ni zamisliti da će se kratkom vremenu tisuće i tisuće ljudi pojaviti na društvenoj mreži, a broj korisnika i dalje raste. Na slici 1 vidljiv je vremenski slijed pojavljivanja nekih društvenih mreža. Društvene mreže čine veliki dio digitalnog okruženja kada je riječ o privatnoj upotrebi, ali i sve većoj upotrebi u poslovne svrhe. Kao što je je vidljivo na slici, radi se o velikom broju društvenih mreža, a mnoge od njih više nisu upotrebi.

Slika 1. Vremenski slijed pojavljivanja nekih društvenih stranica

Izvor: *Timeline of social media,*

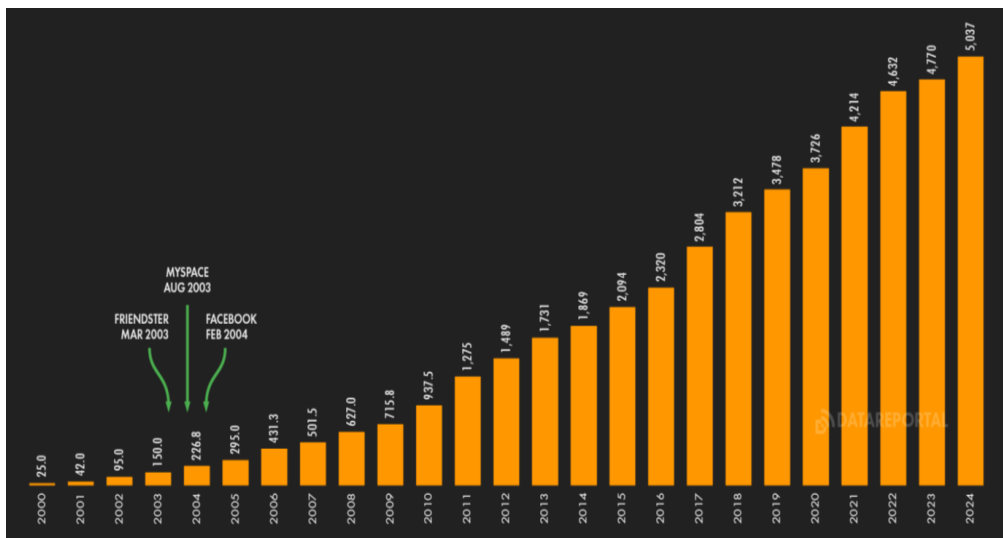
<https://socialoutside.blogspot.com/2017/10/timeline-of-social-media.html>



Društvene mreže koriste sve dobne skupine za komunikaciju i stvaranje veza s ljudima diljem svijeta. Iz godine u godinu raste broj novih korisnika društvenih mreža, pa tako grafikon 1 prikazuje broj identificiranih korisnika društvenih medija (u milijunima) tijekom vremena. Naime, 2000. godine broj korisnika je bio mali budući da nije svako kućanstvo posjedovalo kompjutere ili pristup Internetu. Iz godine u godinu broj korisnika je rastao i od tada pa sve do danas vidi se uzlazna putanja koja će vjerojatno i dalje rasti narednih godina. Budući da postoje razne društvene mreže ova uzlazna putanja ne iznenađuje jer se mnogi korisnici služe jednom ili nekoliko društvenih mreža.

Grafikon 1. Broj identificiranih korisnika društvenih medija (u milijunima) tijekom vremena

Izvor: Datareportal, <https://datareportal.com/reports/digital-2024-global-overview-report>



Jasno je da se moderna digitalna okruženja sve više fokusiraju na vizualni sadržaj. Instagram je društvena mreža u kojoj je vizualni princip temelj funkcioniranja, a pojavio se 2010. godine. Naglasak je na vizualnim elementima, odnosno objavljivanju fotografija na korisničkim profilima koje objavljuju sami korisnici. Oni također „prate“ druge profile i time zapravo na vlastitim profilima određuju tko ih može pratiti ili ne ovisno da li im je profil privatn ili javan. Objavljivanjem fotografija korisnici drugim osobama omogućuju da komentiraju ili označe da im se sviđa navedena fotografija.

## 2.1. Komunikacija na društvenim mrežama

„Razvoj računala i interneta omogućio je nastanak društvenih mreža, koje su postale globalni fenomen i dio svakodnevice. Ljudi putem društvenih mreža predstavljaju sebe kreiranjem profila, u skladu sa slikom koju žele prikazati. Ovaj proces samopredstavljanja analizira se kroz Goffmanov dramaturški pristup, uz prilagodbu Hogana i njegov koncept izložbene stranice. Razmatraju se razlike između klasičnog i virtualnog samopredstavljanja, uključujući asinkronu komunikaciju. Goffmanov koncept samopredstavljanja temelji se na upravljanju dojmovima koje pojedinac želi ostaviti na svoju publiku, gdje pojedinac naglašava ili potiskuje



određene aktivnosti kako bi ostavio željenu sliku o sebi. Također, važan je kontekst informacijske tehnologije i Castellsova teorija o "prostoru tokova" i "bezvremenskom vremenu" interneta, što radikalno mijenja društvene procese i komunikaciju. McLuhanova teorija medija, uključujući tetradu, također pomaže razumjeti utjecaj novih medija na društvo.“ (Perkov, Šarić, 2021:628-630). Jedan od ključnih aspekata komunikacije na društvenim mrežama jest bezvremenski okvir, koncept koji je definirao sociolog Manuel Castells u svojoj teoriji o informacijskom društvu. Castells tvrdi da su digitalne mreže transformirale poimanje prostora i vremena, što omogućuje da se komunikacija odvija izvan tradicionalnih granica. Internet omogućuje prijenos informacija neovisno o prostornoj udaljenosti između sudionika, što mijenja tradicionalni koncept prostora (Castells, 1996). Na društvenim mrežama, korisnici mogu komunicirati iz bilo kojeg dijela svijeta u realnom vremenu ili asinkrono, bez obzira na fizičku udaljenost.

Društvene mreže omogućuju pohranu i dostupnost informacija i sadržaja u bilo kojem trenutku. Na primjer, Instagram ili Twitter postovi ostaju trajno pohranjeni, dostupni za pregled i reakcije dugo nakon što su izvorno objavljeni. Glavna karakteristika društvenih mreža bi svakako bila asinkrona komunikacija koja označava vrstu komunikacije u kojoj sudionici ne moraju biti prisutni istovremeno. U ovoj vrsti komunikacije, poruke se šalju i primaju s vremenskim razmakom između njih, što omogućuje primatelju da odgovori kada mu to odgovara, bez potrebe za trenutnim odgovorom. Ovaj oblik komunikacije razlikuje se od sinkrone komunikacije, gdje su svi sudionici prisutni u isto vrijeme, poput u telefonskim razgovorima ili video pozivima. Sudionici mogu odgovarati na poruke u svom vlastitom tempu, što omogućuje veću fleksibilnost i prilagodbu u odnosu na njihove rasporede. Pošiljatelji mogu pažljivo oblikovati svoje poruke prije nego što ih pošalju, dok primatelji mogu razmišljati o odgovorima prije nego što reagiraju. Poruke ostaju pohranjene, što omogućuje korisnicima da se vrate na prethodne razgovore i referiraju se na njih u budućnosti. Jedan od ključnih radova o asinkronoj komunikaciji dolazi od Johna B. Walthera (1996) koji je istraživao kako asinkroni oblici komunikacije mogu utjecati na percepciju i interakciju među korisnicima. Walther opisuje kako asinkrona komunikacija omogućava "hiperpersonalnu komunikaciju", gdje pojedinci mogu upravljati svojim slikama na način koji nije uvijek moguć u sinkronim komunikacijama (Walther, 1996:28).

### **3. ETIČKA PITANJA KOD KORIŠTENJA DRUŠTVENIH MREŽA**

Budući da iz dana u dan raste broj korisnika Interneta pa tako i društvenih mreža, često se postavlja pitanje sigurnosti i privatnosti na društvenim mrežama. Česti su primjeri neetičnih radnji izvršenih preko Interneta, stoga se raznim strategijama nastoji zaštititi korisnike društvenih mreža. Pitanja koju su najčešće vezana uz etično ponašanje na društvenim mrežama opisana su u nastavku poglavlja.

#### **3.1. Pitanje privatnosti društvenih mreža**

Nije tajna da su životi ljudi postali sve više digitalizirani. Od načina komunikacije s prijateljima i obitelji, do načina na koji se radi i kupuje, jasno je da je tehnologija promijenila način na koji se živi. Zajedno s ovim prelaskom na digitalniji svijet, razmatranja privatnosti su također evoluirala. Dok su u prošlosti osobni podaci bili uglavnom sadržani u fizičkim oblicima poput papirnatih dokumenata ili kućnih filmova, sada se prvenstveno pohranjuju na mreži. Ova promjena je olakšala drugima pristup našim podacima bez dopuštenja“. Bez obzira radi li se o hakeru koji provaljuje u račune e-pošte ili tvrtki koja prikuplja podatke u marketinške svrhe, privatnost ljudi je pod stalnim napadom u digitalnom dobu. Tehnološki napredak omogućio je da se osobni podaci prikupljaju, pohranjuju, analiziraju, kopiraju i distribuiraju s lakoćom i razinom sofisticiranosti koji bi bili nezamislivi kada su doneseni zakoni o zaštiti podataka i privatnosti.“ (Dorraj i Barcy, 2014).

Privatnost je složena kategorija koja se mijenjala kroz povijest i ovisno o stupnju društvenog razvoja i demokratskih procesa unutar zemalja. Pravo na privatnost međunarodno je priznato Općom deklaracijom o ljudskim pravima iz 1948. godine. Ona sadrži odredbe kojim se zabranjuju ropstvo, tortura, diskriminacija, ali i pravo na zaštitu privatnosti. Boban (2012:582) navodi da je pravo na privatnost „elementarno čovjekovo pravo, kako međunarodno, tako i ustavno pravo javno- pravnog značaja te osobno pravo civilno-pravnog značaja kao jedan od nezamjenjivih elemenata čovjekovog postojanja koji štiti čovjeka od prekomjernog posezanja državne vlasti, javnosti i drugih pojedinaca u pojedinačevu odlučujuću duševnu, prostornu i informacijsku privatnost.“ Općenito, privatnost se može podijeliti na više aspekata ovisno o nekoliko čimbenika kao što su vrijeme, okruženje i kontekst.

Privatnost i zaštita podataka tiču se svih i pitanja su od velike važnosti diljem svijeta. Privatnost je predstavljena kao "sastavni dio naše ljudskosti", "srce naše slobode" i "početak svih sloboda

(Dorraj, Barcy, 2014:307). Privatnost je zahtjev pojedinaca, grupa ili institucija da sami određuju kada, kako i u kojoj mjeri se informacije o njima prenose drugima. Katulić i sur. (2022) razlikuju devet tipova privatnosti, a to su tjelesna, intelektualna, prostorna, odlučujuća, komunikacijska, asocijacijska, vlasnička, bihevioralna privatnost kojima pridodaju devetu, a to je informacijska privatnost koja se preklapa sa svih osam tipova.

„Informacijska privatnost zauzima posebno mjesto i predstavlja dodirnu točku s ostalim vrstama privatnosti iz razloga što se odnosi na prikupljanje i diseminaciju podataka, te uključuje pravila upravljanja, prikupljanja i korištenja osobnih podataka. Informacijska privatnost općenito uključuje kontrolu nad širenjem osobnih podataka i nadzor nad pristupom osobnim podacima. Tijekom posjećivanja internetskih stranica korisnike se upozorava na odgovornost, pri čemu je važno spomenuti pojam cyber etika. Cyber etika daje orijentaciju o dobrom i lošem, dobrom i lošem, vezano uz cyber prostor. Pokušava primijeniti i modificirati temeljne vrijednosti i vrline na specifične nove izazove i situacije koje proizlaze iz cyber tehnologija i cyber društva. Kako cyber prostor utječe na sve dijelove društva, cyber etika uključuje gotovo sve etičke domene.“ (Stückelberger, Duggal, 2018).

Korištenjem stranica društvenih mreža ljudi se otvaraju različitim vrstama opasnosti koje redovito utječu na kršenje njihove privatnosti. Privatnost može biti napadnuta na nekoliko načina ako se osobni podaci ne koriste razumno i pouzdano. Kreatori sadržaja na društvenim mrežama preporučuju ograničenje u kojem zaštita može biti napadnuta neodobrenim pristupom društvenim korisničkim informacijama zbog narušavanja privatnosti ili onesposobljavanja loših strategija. Uz to, procijenili su da se zadiranje u privatnost može dogoditi i kao opcijsko korištenje gdje se informacije prikupljene za jedan dizajn koriste za ispunjavanje različitih zatvaranja, bez učenja ili pristanka vlasnika podataka. Unatoč tome, ako odgovarajuće informacijske strategije i prakse daju ljudima kontrolu nad otkrivanjem i korištenjem vlastitih podataka, brige o zaštiti mogu se riješiti (Kumar, 2016). U vezi s internetskom interpersonalnom komunikacijom društvenog raspona, takva regulacija ograničenja može se postići korištenjem postavki privatnosti.

### **3.2. Sloboda govora na društvenim mrežama**

Pravo na slobodu izražavanja je jedno od temeljnih ljudskih prava. Konvencija za zaštitu ljudskih prava navodi da svi ljudi imaju pravo na slobodu izražavanja, a to pravo obuhvaća slobodu mišljenja i slobodu primanja i širenja informacija i ideja bez uplitanja javne vlasti

(Roksandić Vidlička, Mamić, 2018:331). Pojedinci imaju mogućnost slobodnog izražavanja i dijeljenja mišljenja s ostatkom svijeta zahvaljujući internetu i društvenim medijima. Odbor za ljudska prava Ujedinjenih naroda također je nastojao provesti ideju slobode izražavanja u praksi u modernom medijskom okruženju, kojim dominiraju internet i mobilni uređaji, ali je naišao na poteškoće (Bansal, Rani, 2021:862). Uzimajući u obzir da se Internet pojavio kao međunarodna mreža za razmjenu ideja i perspektiva koja ne ovisi o tradicionalnim masovnim medijima, Odbor je preporučio da vlade ulože sve potrebne napore kako bi osigurale da ti novi mediji ostanu neovisni, a istovremeno osiguravaju da njihovi građani imaju pristup njima.

Graciyal i Viswan (2018:110) navode da „za razliku od stvarnog svijeta, gdje se društvena etiketa i maniri ponekad mogu činiti restriktivnim i ograničavajućim, ljudi osjećaju da imaju veći osjećaj slobode izražavanja i/ili govora kada koriste internetske mreže.“ Naravno, sadržaj se nadzire i može se ukloniti, ali s milijunima korisnika na stranicama kao što su Facebook i Twitter, čak i YouTube, ne može se svaki pojedinačni status, fotografija ili komentar pogledati, ocijeniti i potpuno kontrolirati. Ove informacije koje se dijele na stranicama društvenih medija nedvojbeno su dovele do porasta izraza, osjećaja i ideja ljudi kojima bi inače bilo teško prikazati sebe onakvima kakvima bi željeli uživo i licem u lice s drugima.

Facebook mreža uglavnom se oslanja na samokontrolu svojih korisnika. Twitter ima politiku slobode govora što znači da se ne miješa u sporove niti ograničava ono što opisuje kao „kontroverzni sadržaj.“ Štoviše, sama priroda komunikacija temeljenih na internetu neizbježno postavlja izazove za pravne sustave u smislu primjenjivog zakona i povezanosti s teritorijalno ograničenim jurisdikcijama. Jedno od najvažnijih pitanja privatnosti je dijeljenje osobnih podataka. Platforme društvenih medija često zahtijevaju od korisnika dijeljenje osobnih podataka, kao što su ime, adresa e- pošte i lokacija, kako bi stvorili profil. Platforma može koristiti te podatke za personalizaciju korisničkog iskustva i ciljanje oglašavanja. Međutim, može se koristiti i za opasnije svrhe, poput krađe identiteta ili uhođenja. Korisnici moraju biti svjesni rizika uključenih u dijeljenje svojih osobnih podataka na internetu i trebaju poduzeti korake za zaštitu svoje privatnosti. Drugo razmatranje privatnosti je prikupljanje podataka od strane platformi društvenih medija Graciyal i Viswan (2018:110-115). Ove platforme prikupljaju ogromne količine korisničkih podataka, uključujući povijest pregledavanja, upite pretraživanja i interakcije s drugim korisnicima. Ti se podaci mogu koristiti za izradu detaljnih profila pojedinaca i ciljano oglašavanje. Korisnici moraju biti svjesni opsega u kojem

se njihovi podaci prikupljaju i koriste te trebaju poduzeti korake za ograničavanje podataka koji se prikupljaju o njima.

### **3.3.    Zaštita identiteta na društvenim mrežama**

Zaštita temeljnih ljudskih prava jedno je od temeljnih načela prava Europske unije. Usvajanje Lisabonskog ugovora krajem 2009. godine pružilo je snažnu pravnu osnovu za razvoj „jasnog i učinkovitog” sustava zaštite podataka. Kroz brojne izmjene i dopune Ugovora, Povelja o temeljnim pravima Europske unije postala je pravno obvezujuća, Unija je pristupila Europskoj konvenciji o ljudskim pravima, a temeljna prava zajamčena Europskom konvencijom o ljudskim pravima postala su obvezujuća načela prava Unije. Još jedna važna promjena je da je zaštita osobnih podataka priznata kao temeljno pravo prema članku 16. stavku 1. Ugovora o funkcioniranju Europske unije (TFEU). Temeljno sekundarno zakonodavstvo EU-a o zaštiti osobnih podataka je Direktiva 95/46/EZ, koja propisuje da države članice štite temeljna prava i slobode fizičkih osoba, a posebno njihovo pravo na privatnost, u pogledu obrade osobnih podataka (Europska komisija, 2023). Direktiva se primjenjuje na podatke koji se obrađuju automatiziranim sredstvima i podatke sadržane u neautomatiziranim sustavima arhiviranja ili namijenjene da budu dio tih sustava.

Opća uredba o zaštiti podataka (GDPR) europski je zakon koji uspostavlja zaštitu privatnosti i sigurnosti osobnih podataka o pojedincima u operacijama koje se temelje na Europskom gospodarskom prostoru ("EGP") i određenim organizacijama izvan EGP-a koje obrađuju osobne podatke pojedinaca u EGP. Primjenjuje se za prikupljanje i korištenje osobnih podataka. Zemlje koje su usvojile GDPR vidljive su u tablici u nastavku. Prema GDPR-u, "osobni podaci" odnose se na sve informacije koje se odnose na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (tj. pojedinca, ne tvrtku ili drugu pravnu osobu), inače poznatu kao "osoba podataka". Primjeri "osobnih podataka" uključuju ime osobe, adresu e-pošte, identifikaciju koju je izdala vlada ili drugi jedinstveni identifikator kao što je IP adresa ili broj kolačića, te osobne karakteristike, uključujući fotografije.

Tablica 1. Zemlje Europske unije koje su usvojile GDPR

Austrija	Belgija	Bugarska	Hrvatska
Cipar	Češka	Estonija	Finska
Francuska	Njemačka	Grčka	Mađarska
Irska	Italija	Latvija	Litva
Malta	Nizozemska	Poljska	Portugal
Slovačka	Slovenija	Španjolska	Ujedinjeno Kraljevstvo
Norveška	Island	Lihtenštajn	

Izvor: Human Research Protection Office (n.d.), dostupno na: <https://www.hipo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr>

GDPR koji je usvojila EU poboljšat će privatnost i trebao bi potaknuti druge zemlje da poboljšaju zaštitu osobnih podataka ljudi. Nova uredba koja je 25. svibnja 2018. postala pravno obvezujuća u 28 država članica EU-a, jedan je od najopsežnijih i najjačih pokušaja na globalnoj razini da se regulira prikupljanje i korištenje osobnih podataka od strane vlade i privatnog sektora. Unatoč činjenici da je GDPR potaknuo mnoge druge nacije da ojačaju svoje cyber zakone, nijedna ne nudi građanima pravo na privatnost podataka (UNESCO Series on Internet Freedom, 2016).

Kod zaštite osobnih podataka bitno je spomenuti i etičko testiranje sigurnosti, koje je vrlo čest pojam. Hartley (2015:96) navodi da se etičko testiranje može definirati kao "metodologija koju koriste stručnjaci za sigurnost kako bi otkrili ranjivosti u radnim okruženjima informacijskih sustava." Istraživanje sigurnosnih sustava kao slobodna istraživačka aktivnost odgovorno je za mnoge od najnaprednijih razvoja u razvoju softvera. Etički stručnjak za sigurnost također je etički i ugovorno obvezan poštivati zahtjeve klijenta; stoga su im potrebne vještine kako bi osigurali da ne pružaju lažan osjećaj sigurnosti (Thomas, 2020). Etičko testiranje sigurnosti je legitimno i provodi se uz autorizaciju cilja. Cilj tog procesa je pronaći ranjivosti iz perspektive napadača kako bi sustavi bili bolje osigurani. To je dio općeg programa za upravljanje podacima koji uzima u obzir napredna sigurnosna poboljšanja.

„Phishing je oblik socijalnog inženjeringa koji se koristi kako bi se prevarila osoba i navela da izvrši određeni zadatak ili hakeru pruži osjetljive informacije, poput korisničkog imena, lozinke ili financijskih podataka.“ (Vukelić i sur., 2023:306). Ovaj proces najčešće se odvija putem lažnih poruka e-pošte, dizajniranih tako da izgledaju kao legitimna komunikacija od poznatih ili pouzdanih izvora, poput banaka, tehnoloških tvrtki ili čak prijatelja i kolega. Napadi ove vrste obično su oportunistički, šalju se velikom broju ljudi odjednom, uz nadu da će barem neki od primatelja nasjesti na prevaru. Standardni phishing napadi obično uključuju e-poštu s hitnim porukama, u kojima se od primatelja traži da klikne na poveznicu, preuzme datoteku ili unese svoje vjerodajnice. Često su popraćeni zastrašujućim porukama, poput obavijesti da je korisnički račun kompromitiran ili da je potrebna hitna akcija kako bi se izbjegao problem.

„Ciljani phishing napadi poznati su kao spear phishing. Ovi napadi su pažljivo osmišljeni za određene pojedince ili organizacije, koristeći informacije o njihovim navikama, interesima i poslovnim aktivnostima kako bi napad izgledao vjerodostojnije. Napadači koriste podatke dostupne putem društvenih mreža, javnih baza podataka ili iz prošlih incidenata s curenjem podataka, kako bi personalizirali napade. Kitolov (whaling) je još sofisticiranija varijanta spear phishinga, usmjerena na visoko pozicionirane rukovoditelje, direktore ili druge osobe na odgovornim pozicijama unutar tvrtke. Ove osobe često imaju pristup osjetljivim informacijama ili mogu odobriti velike financijske transakcije, što ih čini primamljivim metama. Manje uobičajene varijacije phishinga uključuju napade putem mobilnih uređaja. Smishing (SMS phishing) koristi tekstualne poruke poslane na mobilne telefone, koje sadrže poveznice ili zahtjeve za unos podataka. Ovi napadi često izgledaju kao poruke od banaka, dostavnih službi ili drugih usluga. S obzirom na sveprisutnost mobilnih uređaja, ova metoda postaje sve popularnija. S druge strane, vishing (voice phishing) koristi telefonske pozive. Napadači se predstavljaju kao službenici banke, tehnička podrška ili čak policijski službenici kako bi izvukli osjetljive podatke ili uvjerali žrtvu da izvrši neku radnju, poput prijenosa novca ili otkrivanja osobnih podataka. Broj phishing napada se stalno povećava, a napadači usavršavaju svoje tehnike kako bi bili što uvjerljiviji i teže otkriveni. Statistike pokazuju da su navedeni napadi uzrokovali značajne financijske gubitke, a mnoge organizacije koriste napredne sustave za prepoznavanje i filtriranje zavaravajućih poruka, kao i edukaciju zaposlenika o prepoznavanju ovakvih prijetnji.“ (Thomas, 2020).

### 3.4. Anonimnost i online nasilje

Cyberbullying i govor mržnje na društvenim mrežama predstavljaju ozbiljne etičke i društvene probleme zbog mogućnosti anonimnog sudjelovanja i širenja nasilnog ponašanja. Ove aktivnosti mogu imati dalekosežne posljedice, od emocionalnih trauma do stvarnih fizičkih prijetnji i društvenih podjela. Ferrara i suradnici (2018:1) navode da je cyberbulling ili virtualno zlostavljanje svako ponašanje koje putem elektroničkih ili digitalnih medija izvode pojedinci ili skupine koje opetovano komunicira neprijateljske ili agresivne poruke s namjerom nanošenja štete ili neugode drugima.

„Online nasilje se odnosi na upotrebu tehnologije, posebice društvenih mreža, za uznemiravanje, vrijeđanje i prijetnje. Anonimnost na društvenim mrežama često omogućuje korisnicima da se skrivaju iza lažnih identiteta i provode agresivne aktivnosti bez straha od sankcija. Jedan od najpoznatijih slučajeva cyberbullyinga dogodio se 2012. godine, kada je Amanda Todd, tinejdžerica iz Kanade, počinila samoubojstvo nakon dugotrajnog cyberbullyinga na društvenim mrežama. Todd je postala žrtva ucjene i uznemiravanja nakon što je anonimni korisnik objavio njene intimne fotografije, a zatim proširio uvredljive poruke među njezinim školskim kolegama. Iako je prijavila incident, izostanak adekvatne pravne reakcije doveo je do daljnjeg zlostavljanja. Društvene mreže često nemaju dovoljno učinkovite mjere za prepoznavanje i sankcioniranje cyberbullyinga. Iako su mnoge platforme implementirale opcije za prijavljivanje uvredljivih sadržaja, reakcija često dolazi prekasno ili se zlostavljanje nastavlja putem novih anonimnih računa. Etika dolazi u pitanje jer platforme ne provode dovoljno stroge mjere da zaštite ranjive skupine, posebice djecu i tinejdžere. Nedostatak odgovornosti na ovim platformama otvara pitanje o nužnim promjenama u regulaciji i transparentnosti online ponašanja.“ (Marwick, Lewis, 2017). Trolanje se odnosi na namjerno provociranje i stvaranje sukoba putem društvenih mreža, dok govor mržnje uključuje upotrebu uvreda, dehumanizirajućeg jezika i poticanja nasilja prema pojedincima ili skupinama na temelju rase, vjere, spola, seksualne orijentacije i drugih karakteristika. Ovi oblici nasilnog ponašanja mogu potaknuti stvarnu fizičku štetu i pogoršati društvene podjele. Trolanje i govor mržnje predstavljaju etičke probleme jer društvene mreže često nisu u stanju učinkovito ukloniti ovaj sadržaj ili spriječiti njegovu eskalaciju. Anonimnost i lažni računi omogućuju korisnicima da šire mržnju bez straha od posljedica, a platforme ponekad favoriziraju "slobodu govora" u odnosu na sigurnost korisnika. To otvara etička pitanja o ravnoteži između slobode izražavanja i odgovornosti platformi da osiguraju sigurno okruženje



za sve korisnike. Iako su mnoge društvene mreže implementirale politike za borbu protiv govora mržnje i online nasilja, te mjere često nisu dovoljno efikasne. Primjerice, Twitter je u više navrata bio kritiziran zbog sporog reagiranja na prijave uznemiravanja, što je dovelo do bojkotiranja platforme od strane poznatih osoba. Facebook je bio pod pritiskom 2020. godine zbog širenja govora mržnje tijekom američkih izbora i prosvjeda Black Lives Matter. Unatoč uvođenju novih politika, mnogi kritičari tvrde da platforma nije učinila dovoljno kako bi spriječila širenje mržnje i dezinformacija. Platforma YouTube često je korištena za širenje ekstremističkog sadržaja, a unatoč politici za sprječavanje govora mržnje, mnogi kanali koji promiču radikalne ideje nastavljaju rasti. Nedovoljna moderacija dovela je do problema poput radikalizacije mladih korisnika koji konzumiraju takav sadržaj (Marwick, Lewis, 2017).

### **3.5. Ciljano oglašavanje i manipulacija korisnicima**

Personalizirano oglašavanje koristi prikupljanje velikih količina podataka kako bi se oglasi prilagodili individualnim korisnicima na temelju njihovih interesa, ponašanja i demografskih informacija. Društvene mreže kao što su Facebook i Instagram koriste sofisticirane algoritme kako bi analizirale korisničke podatke, uključujući povijest pretraživanja, lajkanje sadržaja i interakcije s postovima. Iako ova praksa omogućava učinkovitije oglašavanje, otvara ozbiljna etička pitanja kada se oglasi ciljaju prema ranjivim skupinama ili se manipulira osobnim podacima korisnika.

Personalizirani oglasi često ciljaju ranjive korisnike, uključujući mlade ljude, starije osobe ili osobe s mentalnim zdravstvenim problemima. Primjerice, studija koju su proveli Andrews i suradnici 2020. godine pokazala je kako društvene mreže koriste algoritme koji ciljaju mlade s problemima samopouzdanja o glase koji promoviraju nezdrave dijete ili plastičnu kirurgiju, što može imati ozbiljne posljedice za njihovo mentalno zdravlje. Poznati slučaj Cambridge Analytica skandal iz 2018. godine otkrio je kako su podaci milijuna Facebook korisnika bili nelegalno prikupljeni i korišteni za ciljano političko oglašavanje tijekom predsjedničkih izbora u Sjedinjenim Američkim Državama 2016. godine. Cambridge Analytica koristila je psihografske profile korisnika kako bi personalizirala političke poruke i manipulirala glasačkim ponašanjem. Ovaj slučaj otvorio je pitanja o pravednosti i transparentnosti u prikupljanju i korištenju podataka za oglašavanje.

Društvene mreže omogućuju političkim organizacijama da koriste sofisticirane alate za ciljano oglašavanje i manipulaciju glasačkog ponašanja. Ove platforme omogućuju političarima i strankama da identificiraju specifične demografske skupine na temelju njihovih stavova, interesa i ponašanja te ih ciljaju personaliziranim političkim porukama. Iako ove tehnike mogu povećati angažman, one također mogu potkopati demokratske procese jer omogućuju manipulaciju informacija, širenje lažnih vijesti i dezinformacija. Tijekom referenduma o izlasku Velike Britanije iz Europske unije, političke organizacije koristile su društvene mreže, posebno Facebook, kako bi ciljale specifične skupine glasača s dezinformacijama i propagandom. Istraživanje koje je proveo Howard 2017. godine pokazalo je kako su personalizirane poruke tijekom Brexit kampanje često uključivale lažne informacije o migraciji i ekonomskim posljedicama, čime su manipulirali stavovima glasača. Osim Cambridge Analytica slučaja, istraživanja su pokazala kako su ruske organizacije koristile društvene mreže za širenje lažnih vijesti i utjecaj na političke preferencije američkih glasača. Ove kampanje ciljale su specifične demografske skupine, kao što su Afroamerikanci i bijeli radnici, kako bi potkopale povjerenje u izborne procese i polarizirale biračko tijelo. Ciljano političko oglašavanje može potkopati osnovne demokratske vrijednosti, jer omogućuje političkim organizacijama da manipuliraju informacijama i usmjeravaju birače prema određenim odlukama, često kroz lažne ili iskrivljene poruke. Političke kampanje često nisu transparentne u vezi s načinom na koji koriste podatke i ciljanje korisnika, što dovodi do pitanja o etičnosti takvog ponašanja. Platforme poput Facebooka i Twittera često su kritizirane zbog sporog reagiranja na širenje dezinformacija i neuspjeha da pruže dovoljnu zaštitu demokratskih procesa.

## **4. UTJECAJ DRUŠTVENIH MREŽA NA SOCIJALNU STVARNOST**

Interakcija i razgovori povezuju ljude, osiguravaju koheziju i stvaraju osjećaj zajedništva. Društveni mediji omogućuju pojedincima da izgrade i upravljaju svojim društvenim identitetom. Korisnici mogu odabrati što žele prikazati o sebi putem postova, fotografija ili osobnih podataka. Međutim, identitet formiran na društvenim mrežama ne odražava uvijek pravi identitet. Društveni mediji često su mjesto za predstavljanje idealizirane verzije sebe, što može dovesti do neautentičnosti i neusklađenosti s nečijim pravim identitetom. To može utjecati na način na koji ljudi komuniciraju i stvoriti jaz između slike projicirane na Internetu i društvenih interakcija u stvarnom svijetu. Društvene mreže mogu se definirati kao digitalna okruženja u kojima sadržaje u potpunosti ili djelomično kreiraju njihovi korisnici korištenjem tehnološke platforme koja omogućuje komunikaciju s drugim korisnicima. Društvene mreže dio su prožimajućih društvenih digitalnih okruženja za koje se može tvrditi da su potaknule širenje ovih mreža, s obzirom na učestalost njihove uporabe (Paska, 2019:2351). Društveni mediji također mogu predstavljati rizike kao što su:

- učitavanje neprikladnog sadržaja, poput neugodnih ili provokativnih fotografija ili videozapisa sebe ili drugih,
- dijeljenje osobnih podataka sa strancima – na primjer, slike, datum rođenja, lokacija ili adresa,
- internetsko zlostavljanje,
- izloženost povredama podataka, kao što je prodaja njihovih podataka drugim organizacijama itd.

### **4.1. Utjecaj društvenih mreža na zdravlje**

Korištenje Interneta uobičajen je aspekt svakodnevnog života. Međutim, pretjerano korištenje Interneta klasificira se kao bihevioralna ovisnost koja se naziva "ovisnost o Internetu" ili "online ovisnost." Društvene mreže postaju ovisnost kada počnu ometati čovjekove odnose ili kada predstavljaju kočnicu u ciljevima kojima teže, poput dobrih ocjena ili doprinosa sportskoj aktivnosti. Na temelju toga, ovisnost o društvenim mrežama definira se kao primarna, kronična bolest koju karakterizira poremećaj kontrole ponašanja (Kostovska, 2024:82). Pretjerano korištenje Interneta povezano je s psihijatrijskim poremećajima kao što su depresija i anksioznost i drugim povezanim psihološkim pokazateljima, kao što je nisko samopoštovanje (Ueno, Ito, Mural, Fujiwara, 2020:1). Poremećaj ovisnosti o Internetu ima mnogo sličnih

značajki u usporedbi s drugim oblicima ovisnosti, kao što su simptomi odvikavanja kada je onemogućen pristup Internetu. Dok Internet može biti sredstvo za dobro u smislu obrazovanja i jačanja međuljudskih odnosa, ovisnost o Internetu može biti problematična jer može negativno utjecati na akademski uspjeh i nečiju sposobnost učinkovite osobne komunikacije.

Unatoč negativnim situacijama ili rizicima, mnogi ljudi nastavljaju koristiti društvene medije čak i kada je to loše za njih, a ti se razlozi razlikuju od pojedinca do pojedinca i od okolnosti. Jedan značajan razlog zašto ljudi nastavljaju koristiti društvene medije iako oni negativno utječu na njih jest to što jednostavno nisu svjesni njihovog štetnog utjecaja. Nadalje, u nekim slučajevima ljudi su svjesni štetnog utjecaja društvenih mreža na njih, ali ne mare dovoljno za te opasnosti da bi željeli promijeniti svoje ponašanje. Naposljetku, postoje i mnogi situacijski čimbenici koji mogu navesti ljude da koriste društvene medije unatoč njihovoj volji ili želji. Primjerice, ako svi prijatelji neke osobe koriste određenu mrežu društvenih medija, ta bi je osoba također mogla koristiti, jednostavno kako bi bila svjesna što se događa u njezinim društvenim krugovima.

Arya (2021:2) navodi da su potreba za virtualnim zadovoljenjem u obliku lajkova, komentara i pratitelja, usporedba društvenog života na Internetu i pritisak vršnjaka ključni razlozi koji dovode do poremećaja percepcije tijela i prehrambenih navika uz depresiju, anksioznost, poremećaje sna, promjene raspoloženja, manje zadovoljstva životom i ovisnosti o društvenim mrežama. Društvene mreže, iako omogućuju povezivanje, često dovode do negativnih psiholoških učinaka zbog društvenog pritiska i uspoređivanja s drugima. Istraživanja su pokazala da prekomjerno korištenje društvenih mreža može biti povezano s porastom simptoma anksioznosti, depresije i niskog samopouzdanja. Studija Twengea i suradnika (2017) je ukazala na porast simptoma depresije i anksioznosti kod adolescenata koji provode više vremena na društvenim mrežama. Zabilježeno je da su mladi koji su bili više online imali 71% veći rizik od depresije u odnosu na one koji su manje koristili društvene mreže. Ova pojava često se povezuje s "fear of missing out" (FOMO) – strahom da će korisnici propustiti nešto važno ako nisu stalno online. Eksperiment iz 2014. godine koji su proveli Kramer i suradnici pokazao je da Facebook može utjecati na emocionalno stanje korisnika manipulacijom njihovog *news feeda*. Korisnici koji su vidjeli više negativnih postova također su počeli objavljivati negativniji sadržaj, što ukazuje na utjecaj društvenih mreža na emocionalno stanje.

Dizajnerske tehnike društvenih mreža često su osmišljene tako da potiču ovisničko ponašanje. Platforme koriste mehanizme poput beskonačnog skrolanja, "lajkova" i notifikacija, što kod korisnika stvara stalnu potrebu za provjerom novog sadržaja i reakcija na vlastite objave. Ove tehnike ciljaju na dopaminski sustav u mozgu, stvarajući kratkoročni osjećaj nagrade koji korisnika motivira na nastavak korištenja platforme. Aplikacije poput Instagrama osmišljene su da kontinuirano pružaju nove podražaje putem lajkova, komentara i notifikacija. Ova stalna interakcija potiče oslobađanje dopamina, kemikalije u mozgu povezane s osjećajem ugone, zbog čega korisnici postaju ovisni o ponovnom provjeravanju svojih profila. Takav način interakcije može dugoročno izazvati anksioznost i depresiju, jer korisnici postaju opsjednuti vlastitom popularnošću i prihvaćanjem na platformi. Dizajn Facebooka, Twittera i drugih platformi koristi beskonačno gledanje sadržaja kako bi osigurao da korisnici provode što više vremena na platformi. Godine 2017. Alter je proveo istraživanje koje je pokazalo da ovakve dizajnerske metode mogu dovesti do ovisničkog ponašanja, slično kao kod korištenja videoigara. Etika ovih dizajnerskih tehnika dolazi u pitanje jer su platforme osmišljene s ciljem maksimiziranja angažmana, čak i kada je jasno da to može negativno utjecati na mentalno zdravlje korisnika (Alter, 2017). Dizajneri i programeri svjesno koriste podatke o ljudskom ponašanju kako bi stvorili proizvode koji povećavaju ovisnost, čime se postavlja pitanje njihove odgovornosti za mentalno zdravlje korisnika.

Korištenje društvenih mreža često dovodi do nerealnih usporedbi, jer korisnici obično prikazuju idealizirane verzije svojih života. Ova praksa može uzrokovati osjećaj manje vrijednosti kod drugih korisnika, posebno kod mladih ljudi. Istraživanja su pokazala da Instagram, s naglaskom na savršene slike, može izazvati nezadovoljstvo vlastitim tijelom, osobito kod tinejdžerica. Facebookova interna istraživanja iz 2021. godine pokazala su da je Instagram negativno utjecao na mentalno zdravlje oko 32% tinejdžerki, koje su rekle da se osjećaju loše zbog svog izgleda nakon što su pregledavale objave na platformi. Upotreba društvenih mreža i njihovi dizajnerski elementi imaju dubok utjecaj na mentalno zdravlje korisnika. Ovisničko ponašanje, pritisak za stalno povezivanje i negativne usporedbe s drugima dovode do ozbiljnih problema, osobito kod mladih. Platforme bi trebale preuzeti odgovornost za ove probleme i prilagoditi svoje dizajne kako bi minimizirale negativne učinke na korisnike.

## **4.2. Utjecaj društvenih mreža na socijalnu anksioznost**

Društveni mediji imaju snažan utjecaj na ljudske osjećaje i emocije. Kada društveno umrežavanje utječe na emocionalno zdravlje, emocionalno zdravlje trpi. Mnogi korisnici bit će prisiljeni isključiti se iz stvarnog svijeta jer smatraju da je virtualni svijet pun mašte i uživanja. Što više ljudi međusobno komunicira, to je veza jača, a što je više platformi društvenih medija, to je veza jača. Socijalnu anksioznost karakteriziraju osjećaji strepnje, emocionalne boli i suzdržano ili izbjegavajuće ponašanje u stvarnim ili zamišljenim društvenim interakcijama (Puklek Levpušček, Berce, 2012:406). Osobe koje pate od socijalne anksioznosti najčešće pomoć traže tek nakon godina borbi s anksioznošću, nemaju adekvatnu podršku, usamljeni su, javljaju se depresivni simptomi, moguća zlorporaba alkohola i psihoaktivnih tvari te imaju narušene odnose i sliku o sebi (Biglbauer, Lauri Korajlija, 2020:416). Iako ne postoji izravna korelacija između društvenih medija i socijalnog anksioznog poremećaja, korištenje društvenih medija može pridonijeti socijalnoj anksioznosti i pogoršati simptome osobe. Ljudi sa socijalnom anksioznošću često će koristiti društvene medije kao način izbjegavanja interakcije licem u lice koja inače može izazvati simptome anksioznosti i nelagode, poput onih koje smo gore spomenuli. Glavna poveznica između socijalnog anksioznog poremećaja i društvenih medija je nedostatak osobnih interakcija. Dok interakcija s drugima iza ekrana nudi utjehu nekome sa socijalnom anksioznošću, ona također može spriječiti njegovu sposobnost da osobno komunicira s drugima. Drugim riječima, korištenje društvenih medija i Interneta, u kombinaciji sa strahom od društvenog umrežavanja i motivacijom da se izbjegne interakcija licem u lice, povezuje se s većom socijalnom anksioznošću.

## **4.3. Manipulacija algoritmom**

Manipulacija korisnicima na društvenim mrežama putem algoritama i stvaranje tzv. eho-komora fenomen je koji se u posljednjem desetljeću sve više proučava. Društvene mreže poput Facebooka, YouTubea, Twittera i Instagrama koriste složene algoritme kako bi personalizirale sadržaj koji se prikazuje korisnicima, što rezultira dubokim utjecajem na način na koji korisnici doživljavaju informacije i donose odluke. Ovi algoritmi nisu neutralni – oni su dizajnirani tako da maksimiziraju angažman korisnika, što često dovodi do manipulacije njihovim uvjerenjima i ponašanjima. Facebookov algoritam koristi podatke o korisnikovom ponašanju kako bi predložio sadržaj koji je osmišljen da privuče što više njihove pažnje. Tijekom predsjedničkih izbora u Sjedinjenim Američkim Državama 2016. godine, otkriveno je da je Facebookov algoritam favorizirao politički sadržaj koji izaziva snažne emocionalne

reakcije, posebno sadržaj s dezinformacijama i teorijama zavjere. Kampanje lažnih vijesti, kao što su tvrdnje da papa podržava Donalda Trumpa ili da Hillary Clinton vodi tajnu pedofilsku mrežu, postale su viralne upravo zahvaljujući algoritamskom promicanju.

Prema studiji Allcotta i Gentzkowa (2017), lažne vijesti bile su mnogo češće dijeljene na Facebooku nego stvarne vijesti tijekom izbora 2016. godine. Algoritmi su neprestano favorizirali sadržaj koji izaziva veći angažman, što je doprinijelo širenju netočnih informacija među korisnicima. Jedan od najjasnijih primjera algoritamske manipulacije je YouTube. Algoritam preporuka na YouTubeu osmišljen je tako da zadrži korisnike što duže na platformi, često ih uvodeći u sve ekstremniji sadržaj. Istraživanje Zeynep Tufekci (2018) pokazuje kako korisnici koji gledaju bezazlene videozapise o zdravoj prehrani mogu završiti gledajući teorije zavjere ili ekstremističke političke videozapise nakon samo nekoliko preporuka. Algoritam teži preporučivanju sadržaja koji izaziva intenzivne emocionalne reakcije, što često uključuje šokantne ili kontroverzne teme. U slučaju političkog sadržaja, to može voditi ka desničarskom ili lijevičarskom ekstremizmu. Brazil je posebno pogođen ovim fenomenom. Studija koja se bavila brazilskom političkom situacijom tijekom 2018. godine otkrila je da su korisnici često vođeni putem algoritama prema sve radikalnijim desničarskim političkim sadržajima. Ovo je posebno značajno u kontekstu rasta popularnosti ekstremno desničarskog kandidata Jaira Bolsonaroa.

Eho-komore se javljaju kada korisnici postanu zatvoreni u svojim informacijskim balonima, izloženi samo sadržaju koji potvrđuje njihove prethodne stavove i uvjerenja. Na primjer, na platformama kao što je Facebook, algoritmi prate korisničke sklonosti, kao što su interakcije s određenim objavama ili profilima, i zatim preporučuju sličan sadržaj. To dovodi do situacije u kojoj korisnici nisu izloženi različitim gledištima i postaju sve više uvjereni u svoje stavove. Studija Bakshyja, Messinga i Adamica (2015) pokazala je da korisnici Facebooka uglavnom vide sadržaj koji je u skladu s njihovim političkim stavovima, jer algoritmi filtriraju suprotna mišljenja. Ova studija otkriva da su korisnici često izloženi vrlo ograničenom spektru mišljenja, što doprinosi polarizaciji u društvu i smanjuje šanse za konstruktivan dijalog.

Jedan od najozbiljnijih problema vezanih za algoritamsku manipulaciju je širenje lažnih vijesti. Tijekom pandemije COVID-19, lažne informacije o virusu, cjepivima i mjerama zaštite širile su se društvenim mrežama brže od točnih znanstvenih informacija. Facebook, Twitter i Instagram bili su posebno kritizirani zbog svog doprinosa širenju dezinformacija, jer su

algoritmi nagrađivali sadržaj koji je izazivao najviše angažmana, bez obzira na njegovu točnost. Studija koju je proveo MIT pokazala je da lažne vijesti imaju 70% veće šanse da budu dijeljene na Twitteru nego istinite informacije.

#### **4.4. Uloga influencera i njihov utjecaj na korisnike društvenih mreža**

Influenceri na društvenim mrežama predstavljaju podskup kreatora digitalnog sadržaja definiran njihovim značajnim brojem sljedbenika na mreži, karakterističnom osobnošću robne marke i uzorkovanim odnosima s komercijalnim sponzorima (Erin Duff, 2020:1). Kako bi zaradili prihod, reklamiraju robne marke i usluge svojim zajednicama sljedbenika, a takva promotivna komunikacija ima oblik informacija, savjeta i inspiracije. Budući da je podrška brandu utjecajnih osoba integrirana u njihove postojeće arsenale vizualnog, tekstualnog i/ili narativnog sadržaja, njihova se uvjerljiva komunikacija općenito shvaća kao "autentičnija" od tradicionalnog plaćenog oglašavanja. Lugonja (2013:68) navodi da snaga influencera ovisi o vjerodostojnosti i sposobnosti prenošenja svog stručnog znanja putem određenog kanala društvenih medija. Fenomen influencera proširio se društvenim medijima i teško je otkriti tajne širenja ovog fenomena. Nije tajna da su influenceri postali atrakcija kojima se pribjegava na većini polja, bilo da se radi o humanitarnim pitanjima, modi, oglašavanju, marketingu itd. Influenceri su novi igrači u javnom medijskom prostoru koji pridonose marketingu roba i usluga, posebice na društvenim mrežama, kao što je Instagram. Među influencerima su grupe poznatih umjetnika ili zvijezda sportaša. Sve veća rasprostranjenost oglašavanja na društvenim mrežama dovela je do nepovjerenja ljudi prema utjecajnim osobama na društvenim mrežama. Iako većina pratitelja preferira točan, profesionalan i iskren oglas, imidž influencera utječe na njihove stavove. Utjecaji snažno utječu na publiku propagirajući specifične koncepte (ideologija, konzumerizam itd.), koji zauzvrat utječu na norme, vrijednosti i stavove primatelja.



## 5. ZAKLJUČAK

Digitalne tehnologije duboko su promijenile djetinjstvo i adolescenciju. Internet i sredstva za pristup njemu, poput tableta i pametnih telefona, zajedno s platformama društvenih medija i aplikacijama za razmjenu poruka, postali su sastavni dio života ljudi diljem svijeta. Mnoge generacije ljudi aktivne su na društvenim mrežama jer im one omogućuju da lakše komuniciraju, iskazuju svoje osjećaje, stavove, navike i sve što im društvene mreže omogućuju. Korištenje društvenih medija pomaže mladima u dijeljenju informacija o novom razvoju društva i vanjskog svijeta. Pružanje informacija o bilo čemu poput knjiga, e-knjiga, digitalnih izvora, novina, dokumentarnih filmova, različitih rezača, povijesnih informacija itd. dostupno je svugdje ili svugdje putem internetske veze. Društveni mediji golemo su područje pružanja informacija i u njega su uključene sve vrste informacija. Neke informacije su korisne, a ponekad daju negativne ili pozitivne informacije. Ali sve vrste informacija uključuju mlade u nezdrave aktivnosti koje gube vrijeme. Uključivanje u mnoge aktivnosti uključuje mnoge navike i tjeskobe koje se razvijaju u osobnosti mladih. Internetska komunikacija s drugima razvija socijalnu anksioznost i osjećaj usamljenosti. Mladi se angažiraju na komunikaciji s drugima, ali u ovoj bezizražajnoj komunikaciji sprječavaju zablude. Zabluda je poznata kao nerazumijevanje tuđih pogleda.

Uz značajne prilike koje donose društvene mreže, dolazi i niz različitih rizika i šteta. Društvene mreže povećale su razmjere seksualnog zlostavljanja i iskorištavanja djece. Počinitelji seksualnih prijestupnika nad djecom povećali su pristup djeci putem nezaštićenih profila na društvenim mrežama i foruma za online igrice. Tehnološki napredak omogućio je pojedinačnim počiniteljima i lancima trgovaca ljudima da izbjegnu otkrivanje putem šifriranih platformi i stvaranja lažnih identiteta te im je omogućio da progone više žrtava u isto vrijeme. Društvene mreže mogu utjecati i na samu osobu ukoliko je previše isključena iz vanjskog svijeta i učestalo koristi društvene mreže. Društvene mreže olakšavaju komunikaciju i stvaraju zajedništvo među ljudima, samo je potrebno znati razlikovati virtualnost i stvarnost i biti duhom i tijelom prisutan u onome što se radi.

## Literatura

1. Aichner, T., Grunfelder, M., Maurer, O., Jegeni, D. Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019, *Cyberpsychology, behavior, and social networking*, Vol. 24, No. 4, 2021., str. 215-222
2. Alter, A. *Irresistible: The rise of addictive technology and the business of keeping us hooked*. Penguin Press., 2017.
3. Andreassen, C. S. Online social network site addiction: A comprehensive review. *Current Addiction Reports*, 2(2), 2015., 175-184.
4. Andrews, K. J., Bale, C., & Hickman, A. Online advertising: Ethics, manipulation, and autonomy. *Journal of Business Ethics*, 165(2), 2020., 333-351.
5. Arya, S. (2021). The Influence of Social Networks on Human Society, dostupno na: <https://arxiv.org/pdf/2103.13187> (pristupljeno: 25.8.2024.)
6. Bakshy, E., Messing, S., & Adamic, L. A. Exposure to Ideologically Diverse News and Opinion on Facebook. *Science*, 348(6239), 2015., 1130-1132.
7. Bansal, A., Rani, A. Freedom of speech and expression vs social media violations, Vol. 12 No. 1, 2021., str. 862-872
8. Biglbauer, S., Laura Korajlija, A. Društvene mreže, depresivnost i anksioznost, *Socijalna psihijatrija*, Vol. 48 No. 4, 2020., str. 404-425
9. Boban, M. Pravo na privatnosti i pravo na pristup informacijama u suvremenom, *Zbornik radova Pravnog fakulteta u Splitu*, god. 49, 3/2012., str. 575- 598
10. Castlls, M. *The Rise of the Network Society*. Wiley-Blackwell, 1996.
11. Chou, H. T. G., & Edge, N. "They are happier and having better lives than I am": The impact of using Facebook on perceptions of others' lives. *Cyberpsychology, Behavior, and Social Networking*, 15(2), 2012., 117-121.
12. Datareportal, <https://datareportal.com/reports/digital-2024-global-overview-report> (pristupljeno: 15.8.2024.)
13. Dorraji, S.E., Barcy, M. Privacy in digital age: dead or alive?! Regarding the new eu data protection regulations, *Social technologies*. 2014, 4(2): 306–317
14. Europska komisija, (2023). Danta protection in EU, dostupno na: [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu\\_en](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en) (pristupljeno: 15.8.2024.)
15. Erin Duff, B. Social Media Influencers, "e International Encyclopedia of Gender, Media, and Communication. Karen Ross (Editor-in-Chief), John Wiley & Sons, Inc., 2020.

16. Facebook internal research, 2021 (Wall Street Journal report). Facebook knows Instagram is toxic for teen girls, company documents show
17. Ferrara, P., Ianniello, F., Villani, A., Corsello, G. Cyberbullying a modern form of bullying: let's talk about this health and social problem, Ferrara et al. Italian Journal of Pediatrics (2018) 44:14
18. Graciyal, G., Viswam, D. Freedom of Expression in Social Media: A Political Perspective. International Journal of Multidisciplinary, 3(1), 2018., str. 110-113
19. Grbavac, J., Grbavac, V. Pojava društvenih mreža kao globalnog komunikacijskog fenomena, Mediji, kultura i odnosi s javnostima, Vol. 5 No. 2, 2014. str, 206-219
20. Howard, P. N. (2017). Lie machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives. Yale University Press.
21. Hartley, R.D. Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack, Journal of International Technology and Information Management, Vol. 24 No. 4, 2015., str. 95-104
22. Human Research Protection Office (n.d.), dostupno na: <https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr> (pristupljeno: 15.8.2024.)
23. Katulić, A., Katulić, T., Hebrang Grgić, I. Application of the principle of transparency in processing of European national libraries patrons' personal data, Digital Library Perspectives, Vol. 38 No. 2., 2022., str. 1-14
24. Kostovska, K. The Influence of Social Networks on the Social Development of Children, The Eurasia Proceedings of Educational & Social Sciences (EPESS), Vol. 24, 2024., str. 81-90
25. Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences, 111(24), 2014., 8788–8790.
26. Kumar, S., Deepa, S. On Privacy and Security in Social Media – A Comprehensive Study, Procedia Computer Science, Volume 78, 2016, Pages 114-119
27. Lugonja, D. Social Network Influence to Society Development through the viewpoint of Social presence theory, Faculty of Organization and Informatics University of Zagreb, 2013., dostupno na: <file:///D:/Downloads/ceciis2013.pdf> (pristupljeno: 20.8.2024.)
28. Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. Data & Society Research Institute.
29. Paska, I. Digital Media Environments and their Implications: Instagram, In Medias Res, Vol. 8 No. 15, 2019., str. 2347-2364

30. Phillips, W. (2015). This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture. MIT Press.
31. Perkov, I., i Šarić, P. (2021). 'Samopredstavljanje na društvenim mrežama', Filozofska istraživanja, 41(3), str. 627-638.
32. Puklek Levpušček, M., Berce, J. Socijalna anksioznost, socijalna prihvaćenost i akademsko samoopažanje učenika gimnazija, Društvena istraživanja: časopis za opća društvena pitanja, Vol. 21 No. 2 (116), 2012., str. 405-419
33. Roksandić Vidlička, S., Mamić, K. Zloupotreba društvenih mreža u javnom poticanju na nasilje i mržnju i širenju lažnih vijesti: potreba transplantiranja njemačkog Zakona o jačanju provedbe zakona na društvenim mrežama?, Hrvatski ljetopis za kaznene znanosti i praksu, Vol. 25 No. 2, 2018., str. 329-357
34. Stükelberger, C., Duggal, P. Cyber Ethics 4.0, Geneva: Globethics.net, 2018.
35. Thomas, G.A. Issues of professionalism concerning the ethical hacking of law firms, Technology at Charles Sturt University, 2010.
36. Timeline of social media, <https://socialoutside.blogspot.com/2017/10/timeline-of-social-media.html> (pristupljeno: 15.8.2024.)
37. Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. From liberation to turmoil: Social media and democracy. Journal of Democracy, 28(4), 2017., 46-59.
38. Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. Increases in depressive symptoms, suicide-related outcomes, and suicide rates among U.S. adolescents after 2010 and links to increased new media screen time. Clinical Psychological Science, 6(1), 2017., 3-17.
39. Ueno, T., Ito, K., Mural, T., Fujiwara, H. Mental Health Problems and Their Association With Internet Use in Medical Resident, Froniter Public Health, Vol. 8, 2020., str. 1-8
40. Vosoughi, S., Roy, D., Aral, S. The spread of true and false news online. Science, 359(6380), 2018., 1146-115
41. Vukelić, B., Zvonarić, A.D., Protrka, N. The Recognition of an E-Mail Phishing Cyberattack in Business Organizations, Policija i sigurnost, Vol. 32 No. 3, 2023., str. 304-316
42. Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power
43. Walther, J. B. Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction, 1996.