

# Lažno informiranje na internetu

---

**Željeznik, Barbara**

**Undergraduate thesis / Završni rad**

**2021**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Pula / Sveučilište Jurja Dobrile u Puli**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:137:265927>

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

*Download date / Datum preuzimanja:* **2024-09-18**



*Repository / Repozitorij:*

[Digital Repository Juraj Dobrila University of Pula](#)



Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

**Barbara Željeznik**

**LAŽNO INFORMIRANJE NA INTERNETU**

Završni rad

Pula, rujan 2021.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

**Barbara Željeznik**

## **LAŽNO INFORMIRANJE NA INTERNETU**

Završni rad

JMBAG: 0303075546, redoviti student

Studijski smjer: Informatika

Kolegij: Informacijska tehnologija i društvo

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacije znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: Doc. dr. sc. Snježana Babić

Pula, rujan 2021.



## IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani/a **Barbara Željeznik**, ovime izjavljujem da je ovaj seminarski rad rezultat isključivo mogega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio seminarskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

Barbara Ž

U Puli, rujan, 2021. godine



## IZJAVA

o korištenju autorskog djela

Ja, **Barbara Željeznik** dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom **Lažno informiranje na Internetu** koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu sa Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Student

Barbara Ž

U Puli, rujan, 2021. godine

# Sadržaj

1. Uvod .....	1
2. Lažno informiranje na Internetu .....	2
2.1. Misinformacija i dezinformacija .....	4
2.2. Načini prepoznavanja lažnih informacija kao korisnik .....	5
3. Načini širenja lažnih informacija na Internetu .....	8
3.1. Širenje putem društvenih mreža .....	8
3.2. Širenje putem digitalnog novinarstva .....	10
4. Primjena umjetne inteligencije u širenju i prevenciji lažnih informacija na Internetu .....	13
4.1. Umjetna inteligencija u borbi protiv širenja lažnih vijesti .....	14
4.2. Umjetna inteligencija kao alat za izradu i širenje lažnih vijesti .....	15
4.2.1. <i>Deepfake</i> .....	16
4.2.2. Izmjena konteksta originalnih fotografija .....	18
4.2.3. Društveni botovi .....	21
4.2.4. GPT-3 .....	24
5. Velike baze podataka ( <i>Big data</i> )- dohvaćanje i analiziranje istinitosti informacija .....	27
5.1. Primjeri korištenja <i>Big data</i> tehnologija sa svrhom dohvaćanja i analize istinitosti informacija .....	28
6. ZAKLJUČAK .....	31
LITERATURA .....	32
POPIS SLIKA .....	34
POPIS TABLICA .....	35
SAŽETAK .....	36
SUMMARY .....	37

## 1. Uvod

U današnje vrijeme informacije su postale lako dostupne svakom pojedincu. Veliki broj internetskih stranica, društvenih platformi i internetskih medija donose beskonačan broj informacija te je naizgled nemoguće ostati neinformiran. No, s tolikom količinom informacija uvijek postoji rizik da je dio tih informacija neispravan te bi ih korisnik trebao prepoznati i odbaciti, no nažalost korisnici često, svjesno ili ne, postaju žrtve lažnog informiranja te i sami prenose lažne sadržaje kao činjenice, pridonoseći tako razvoju lažnih informacija na Internetu.

Lažne informacije mogu biti dezinformacije odnosno informacije s lošom namjerom te misinformacije, točnije informacije koje se šire bez znanja o točnosti informacije. Dezinformacije su kreirane iz više različitih namjera kako štetnih tako i bezazlenih, u svrhu humora. Borba protiv dezinformacije je uvijek aktiva, ali nikada neće biti dovršena niti savršena budući da je tehnologija širenja dezinformacija svaki dan sve bolja te stoga zahtjeva i sustavni rad na napretku tehnologija za suzbijanje.

Umjetna inteligencija veliki je faktor u širenju i prevenciji lažnih informacija na Internetu, budući da je prisutna u botovima i tehnologijama za izradu i širenje dezinformacija, ali također i u tehnologijama koje te iste dezinformacije detektiraju i zaustavljaju.

Za dohvaćanje podataka i njihovu analizu može se koristiti i *Big data* tehnologija, budući da je u tome najefikasnija, najbrža i najkvalitetnija tehnologija za dobivanje sigurnih i točnih podataka koji će se koristiti u informiranju korisnika.

Cilj ovog rada je prikazivanje na koji način dolazi do lažnih informacija na Internetu i kako se od njih može obraniti. Rad se sastoji od šest poglavlja. U uvodnom poglavlju objašnjena je tema i svrha rada, zatim je u drugom poglavlju objašnjen pojam i vrste lažnih informacija, iza toga slijedi poglavlje u kojemu su objašnjena dva glavna načina na koja se šire lažne informacije - putem društvenih mreža i putem digitalnih medija. Nadalje, slijedi četvrto poglavlje gdje je objašnjena umjetna inteligencija i njene uloge u širenje lažnih informacija. U petom poglavlju objašnjena je tehnologija *Big data* koja dohvaća i analizira informacije te na kraju, kao zadnje poglavlje, stoji zaključak u kojemu je zaključen cijeli ishod završnog rada.

## 2. Lažno informiranje na Internetu

Ovo poglavlje obuhvaća pojam lažnih informacija koje se prenose Internetom. U današnje vrijeme su one česta pojava te mogu biti potpuno izmišljene ili poluistinite i bez konteksta te se često prezentiraju putem internetskih medija, a šire od korisnika internetskih platformi.

*„Posebnu važnost sloboda izražavanja dobiva u današnjem digitalnom okruženju gdje svatko ima mogućnost objavljivati bilo kakav sadržaj na Internetu. Uz mnoge pozitivne strane Interneta i društvenih mreža poput lakšeg širenja informacija i povezivanja ljudi, Internet postaje i pogodno sredstvo poduzimanja raznovrsnih nezakonitih radnji. Sve češća pojava, posebice u kriznim situacijama, postaje i širenje lažnih vijesti i govora mržnje za koje se još uvijek ne pronalazi odgovarajući univerzalni pravni okvir. Budući da ni zakonodavstvo Europske unije ne sadrži nikakvu regulaciju o suzbijanju lažnih vijesti, Europska komisija radi na provedbi širokog skupa akcija za borbu protiv širenja dezinformacija u Europi.“* (Pravna klinika - Pravni fakultet Zagreb, 2020.)

Glavno je usredotočenje na pronalaženju načina sprječavanja širenja te pravljenja razlike između istinitih i lažnih informacija za korisnike. S druge strane postoji pitanje zašto su korisnici i u kolikoj mjeri, podložni vjerovanju svim informacijama na koje nailaze na Internetu te kako ih se može zaštititi od loše medijske pismenosti i lažnih informacija.

Prepoznavanje i daljnje analiziranje uzroka, posljedica i karakteristika sadržaja na Interneta pomažu i razvoju algoritama za detektiranje i borbu protiv lažnog informiranja. Također, društvene platforme kao jedne od glavnih izvora lažnog informiranja trebaju educirati korisnike u prepoznavanju lažnih sadržaja, kao i označavati takve sadržaje kako bi svima bilo vidljivo kada je sadržaj djelomično istinit ili je potpuno izmišljen.

Gotovo svakodnevne promjene i razvoj na Internetu potiču i promjene u društvu te su za širenje informacija nekad postojali drugačiji kriteriji, primjerice kao što su kvaliteta informacija i prenošenje vijesti iz svijeta, no to je sada zamijenjeno s novijim kriterijima kao što su zabava, vlastita zatvorena mišljenja, površnost i najbitnije – zarada.

Lažne informacije mogu biti predstavljane na više načina. Uz sadržaje koji su namjerno potpuno izmišljeni i zlonamjerni, postoje i sadržaji koji su lažni u svrhu zabave i humora



te sadržaji koji zavaravaju. Stoga treba poznavati sve vrste informacija kako bi se bolje kontrolirala njihova izmjena. U tablici ispod prikazane su i objašnjene vrste lažnih informacija prema namjeri autora:

*Tablica 1 - Različite vrste lažnog informiranja na Internetu (Wardle i Derakhshan, 2017.)*

<b>Satirični/humoristični Sadržaji</b>	sadržaj nije zlonamjerman , no može prevariti svojim sadržajem
<b>Zavaravajući sadržaj</b>	sadržaj korišten za zavaravanje čitatelja s ciljem prevare korisnike o nekom pojedincu ili problemu
<b>Izmišljeni sadržaj</b>	potpuno izmišljen sadržaj dizajniran da prevari i naštetiti
<b>Lažna povezanost</b>	slučaj kada naslov, slike i predstavljanje sadržaja nisu povezani sa samim sadržajem
<b>Lažni kontekst</b>	korištenje istinitih sadržaja, ali s lažnim kontekstom
<b>Manipulirajući sadržaj</b>	nepotpuno korištenje točnih ili netočnih informacija, kako bi se manipuliralo s javnošću

## 2.1. Misinformacija i dezinformacija

Korisnicima pozornost uglavnom zaokuplja sadržaj koji je vizualno upečatljiv, podržava njihova već postojeća stajališta, naslovom potiče na iznenađenje i čuđenje ili potiče bilo kakve emocije. Upravo tako se kreiraju lažne informacije kako bi pridobile pažnju korisnika i kako bi svojim sadržajem poticale na širenje. Takvi štetni i lažni sadržaji izgledaju atraktivno i često djeluju vjerodostojno te ih korisnici nemaju potrebu provjeravati.

Problematičan dio lažnih sadržaja na Internetu je to što stvaraju informacijski poremećaj, što znači da je korisnicima teško razlikovati istinite od lažnih sadržaja. Takvi sadržaji, također, potiču nepovjerenje u institucije i medije te na društvenim mrežama, omogućuju nevjerodostojne i alternativne izvore. (Nenadić i Vučković, 2021.)

Pojam informacijskog poremećaja u kontekstu lažnog informiranja mnogo je veći od samog pojma lažnih vijesti. U nekim slučajevima vijesti i sadržaji znaju imati djelić istine, mogu biti istinite, ali bez konteksta, ili biti navedene, ali bez izvora ili neke potvrde činjenica.

Iz toga razloga lažne informacije dijelimo na dvije glavne podjele lažnog informiranja: misinformacija i dezinformacija. Ta dva, naizgled jednoznačna pojma, ustvari imaju jedno bitnu razliku, a to je u namjeri korisnika koji ih širi.

Dezinformacije su stvorene i proširene s namjerom da obmanu javnosti. Informacije su u tom slučaju netočne, zavaravajuće i prezentirane kao činjenice te namjerno distribuirane s ciljem nanošenja štete ili stvaranja vlastite koristi.

Dok se misinformacijom smatra nesvjesno širenje dezinformacije, što znači da korisnik nije svjestan da informacija koju širi drugima nije istinita. Takva vrsta širenja uglavnom se događa jer korisnici nisu informirani u području sadržaja ili krivo tumače sadržaj i žele prenijeti svoje shvaćanje istog. Dezinformacije su stvorene i distribuirane s motivom zavaravanja korisnika, dok su, misinformacije, iste dezinformacije prosljeđene dalje od korisnika, ali bez ikakvog motiva obmane ostalih korisnika. (Nenadić i Vučković, 2021.)

Društveni mediji i Internet omogućili su svim pojedincima s pristupom da iskažu svima svoje ideje, stavove i mišljenja. Ljudi su u mogućnosti primiti i saznati svakakve vrste informacija kroz par sekundi, što je najbrža i najveća razmjena informacija ikada dosad.

S druge strane, to daje pravo svakom korisniku da sudjeluje u raspravama, nameće svoje mišljenje drugima i prenosi informacije bez kakvih posljedica.

Dezinformacija može biti stvorena, no ne postiže ništa bez publike koja ju dijeli. U najvećem broju dijeljenje dezinformacija odvija se na društvenim mrežama. Kada je dezinformacija izrađena pravilno može se jako brzo proširiti pa i lagano preći s jedne društvene platforme na drugu, dopijevajući na taj način nekada i do novinarskih medija koji bez dobre provjere informacija također nastavljaju sa širenjem iste informacije, dopirući do još više ljudi i tako omogućujući skoro nemoguće uklanjanje te dezinformacije.

Dijeljenje dezinformacija u većini slučajeva nije samo na korisnicima, već postoje botovi ili roboti koji su stvoreni samo za tu svrhu ponavljanja zadanih mrežnih zadataka. Te softverske aplikacije šire informacije puno brže nego što to mogu ljudi te povećavaju doseg mnogih dezinformacija.

Facebook i Twitter glavne su društvene platforme te su isto tako glavne za širenje dezinformacija. Budući da im dezinformacije prave nezadovoljstvo kod korisnika, te su platforme razvile programe za detektiranje botova i njihovo uklanjanje, kao i uklanjanje korisnika koji su skloni širenju i poticanju dezinformacija. Također, postoje i programi koji korisnicima olakšavaju uočavanje lažnih informacija, označavajući informacije kao lažnim, kako ne bi došlo do nesvjesnog širenja dezinformacija. (Nenadić i Vučković, 2021.)

## **2.2. Načini prepoznavanja lažnih informacija kao korisnik**

*„Lažne vijesti odnose se na namjerne neistine ili priče koje sadrže neku istinu, ali nisu potpuno točne, slučajno ili smišljeno. Neki ljudi također tvrde da su istinite priče "lažne vijesti", samo zato što se s njima ne slažu. To može dovesti do opasnog zanemarivanja vitalnih savjeta.“* (Mind Tools, 2020.)

Jasno je kako korisnik kao pojedinac ne može puno promijeniti kada dođe do velike količine lažnih informacija na Internetu i njihovog širenja. No, kada bi korisnici bili više upućeni u načine kako i sami mogu detektirati i izbjeći lažne informacije, vrlo lagano bi se mogla stvoriti velika razlika u svijetu informacija koje se šire Internetom. Ovdje su navedeni neki od savjeta za bolje prepoznavanje lažnih informacija:

- **Citirani sadržaji**

Mnogi sadržaji koji su napisani od strane ozbiljnih medija uvijek se služe s mnogo citata. Ako je riječ o ozbiljnoj temi, uglavnom će biti velika količina citata, kako bi se pokazale točne i stručne informacije donesene od stručnjaka u određenim područjima.

- **Pregled izvora**

Nadovezujući se na prvi način – pregledanja citata, bitno pitanje koje se uz tu temu veže je također i odakle ili od koga su citirani ti tekstovi. Potrebno je za svaku primljenu informaciju putem Interneta, pronaći izvor i provjeriti je li taj izvor pouzdan.

- **Pregled domene i url-a stranice**

Organizacije i stranice koje su priznate i vjerodostojne uglavnom posjeduju svoje domene i standardni ozbiljni izgled stranice. Mnoge stranice koje nisu pouzdane često pokušavaju prikazati svoje sadržaje kao ozbiljne i kopirati legitimne novinarske stranice, no uz slična ili kopirana imena stranica često sadrže završetke kao com.co (npr. abcnews.com je legitimni izvor informacija, dok je abcnews.com.co nije, iako dijele naizgled isti naziv).

- **Razvoj kritičkog razmišljanja**

Potrebno je biti kritičan prema bilo kakvim informacijama koje su prisutne na Internetu. Najčešći način širenja lažnih informacija je u tome što su prikazane kao da su vjerodostojne i iz ozbiljnih izvora vijesti. Važan faktor u pridobivanje pažnje je i izazivanje emocionalne reakcije kod korisnika, kao što su šok, ljutnja ili iznenađenje. Stoga treba uvijek biti oprezan i prvo razmisliti je li pročitani sadržaj uistinu istinit i ne reagirati prvo emocijama.

- **Uređivanje fotografija**

U današnje vrijeme vrlo je lako manipulirati slikama pomoću različitih softvera jer takve fotografije uglavnom izgledaju realno te većina ljudi ne može vidjeti razliku između manipuliranih fotografija i originalnih. Postoji nekoliko jasnih znakova da je fotografija uređivana, kao neobične sjene koje nemaju smisla i nazubljeni rubovi oblika.

- **Obrnuto pretraživanje slika** (Google Reverse Image Search)

Fotografije su u današnje vrijeme često korištene bez konteksta, znači fotografije jednog događaja korištene su za primjer nekog nevezanog događaja. To je česta pojava u lažnom informiranju, budući da su slike prave, sadržaj se čini vjerodostojnim, no korištenje originalne slike bez konteksta iz kojega dolazi jedna je od najvećih vrsta obmana korisnika. Glavno rješenje za takvu vrstu lažnih vijesti je *Obrnuto pretraživanje slika*, gdje se može lako vidjeti prvi i originalni izvor navedene slike:

*“ Google obrnuto pretraživanje slika pomaže vam brzo otkriti vizualno slične slike sa cijelog weba. Prenesite fotografiju sa svoje radne površine na Google slike i ona će vam gotovo trenutno prikazati povezane slike korištene na drugim web stranicama, kao i različite veličine iste fotografije.”* (Digital inspiration, n.d.)

- **Pravopisna točnost**

Sadržaji koji potječu iz ozbiljnih izvora uglavnom su detaljno pregledani i bez ikakvih pravopisnih pogrešaka, pogotovo kada se radi o bitnim i svjetskim vijestima. Kontrola i višestruki pregledi ključni su za vjerodostojne informacije radi što boljeg prenošenja činjenica.

### 3. Načini širenja lažnih informacija na Internetu

U okviru ovog poglavlja bit će navedeni i objašnjeni glavni načini širenja lažnih i istinitih informacija na Internetu. Širenje putem društvenih mreža i putem digitalnih medija.

#### 3.1. Širenje putem društvenih mreža

Sa sve većim brojem društvenih mreža, promijenio se i način na koji se percipira i rukuje sa informacijama. Društvene mreže u današnje vrijeme pružaju konstantan protok informacija te se lažne informacije mogu stvarati i jednostavno širiti putem weba i društvenih mreža rezultirajući brzom i efikasnom proširenošću po cijelom svijetu. (Nagi, 2018.) Platforma društvenih mreža dizajnirana je da potiče korisnike na razmjenu informacija brzo i bez napora te često dolazi do pogrešnih ili „iskrivljenih“ informacija. Ipak, u velikoj većini slučajeva, za širenje informacija na društvenim mrežama su odgovorni botovi – programi koji automatski objavljuju i šire informacije.

Botovi koji objavljuju i šire informacije često su teški za identificirati, stoga su, također, teški za označiti i ukloniti sa društvenih mreža. Botovi su dizajnirani da se ponašaju kao ljudski korisnici te često prave manje pravopisne greške kako bi bili teži za pronaći i izdvojiti. Najveći problem je u tome što otkrivanje botova rezultira proizvodnjom boljih botova, stoga se zadatku pronalaska botova treba pristupiti jako oprezno.

Facebook i Twitter uvijek imaju postotak korisnika koji su botovi te se s tim problemom pokušavaju suočiti unapređivanjem softvera za detekciju botova. Programi za detekciju botova, često, ne namjerno, detektiraju prave korisnike kao botove, a uklanjanje pravih korisnika sa društvenih mreža šteti odnosima s javnošću. Facebook ozbiljnije shvaća znatni porast lažnih informacija na svojoj platformi, stoga rade na poboljšanju tehnologija.

*„Facebook je rekao da je do promjene došlo zbog boljih alata za praćenje nezakonitih aktivnosti, a ne zbog naglog porasta broja prijavljenih korisnika.*

*Za razliku od Twitter-ovog „sve prolazi“ pristupa, Facebook je poznat po tome da strogo provjerava identitet svakog korisnika u stvarnom životu. U nekim slučajevima čak ide dotle da se zahtijeva službena dokumentacija. Pa ipak, lažni se računi još uvijek uspjevaju razmnožiti na platformi - neki zbog nedužnih grešaka korisnika, a drugi stvoreni za širenje neželjene pošte ili rad kao dio sjenovitih mreža botova..“ (Kulp, 2017.)*

Botovi su automatizirani programi koji se maskiraju kao ljudi, no nasuprot tome postoje trolovi. Trolovi su ljudski korisnici koji koriste društvene platforme za uvjeravanje ljudi u istinitost lažnih sadržaja. Oni šire i potiču negativne reakcije na različite institucije ili osobe na platformama.

Nastavkom rasta lažnog informiranja riskira se sve veće smanjenje pouzdanosti i vjerodostojnosti vijesti koje su istinite i provjerene. Uz bolji poticaj prema obrazovanju i kritičkom razmišljanju korisnika, u budućnosti bi se moglo usporiti ili čak zaustaviti širenje lažnih informacija na društvenim mrežama. Sva odgovornosti za širenje lažnih vijesti, naravno, ne može biti samo na korisnicima, već bi veću odgovornost trebale imati i platforme društvenih mreža.

Postoji više načina zaustavljanja širenja lažnih vijesti, kao što su onemogućavanja izrade više računa te poticanje na pažnju u slijepom širenju informacija. Neke platforme kao WhatsApp ograničavaju svojim korisnicima prosljeđivanje poruka prema više od pet drugih korisnika odjednom. Na taj se način uvelike smanjuje brzina širenje informacija i olakšava se detekcija lažnih vijesti i njihovo brzo uklanjanje.

Kako se botovi sve više razvijaju i šire, platforme društvenih mreža su počele koristiti algoritme za kontrolu i odlučivanje koje informacije ne treba širiti većoj javnosti. Algoritmi su dizajnirani da prema interesu korisnika, odlučuju koje informacije treba više prikazivati korisniku. Ovakav način rada stvara filtre putem preporuke, točnije, korisnicima se prikazuju informacije koje se slažu s već iznesenim mišljenjima koje su prikazali na platformi. Ovaj je algoritam osmišljen za bolje zadovoljstvo korisnika, no u isto vrijeme taj algoritam ograničava izloženost svih vijesti korisnicima različitih mišljenja, što bi moglo pomoći boljem, uravnoteženom mišljenju u globalnom pogledu.

Platforme za društvene mreže takvim promjenama i restrikcijama mogu donijeti negativni utjecaj na prihod i odlazak korisnika s platforme, stoga je i dalje najveći dio borbe protiv lažnih informacija na samim korisnicima.

Širenje lažnih vijesti na društvenim mrežama često je uspoređivano s virusima koji stvaraju bolesti. „ *Znanstvenici su prilagodili model za razumijevanje bolesti koje mogu zaraziti osobu više puta. Gleda se koliko je ljudi "osjetljivo" na bolest - ili u ovom slučaju*

*vjerojatno će vjerovati lažnoj vijesti. Također se gleda koliko ih je bilo izloženo, a koliko je zapravo "zaraženo" i vjeruju u priču te koliko će ljudi vjerojatno širiti lažne vijesti.*

*Slično poput virusa, istraživači kažu da s vremenom izloženost više vrsta lažnih vijesti može oslabiti otpor osobe i učiniti je sve osjetljivijom. Što je osoba više puta izložena lažnoj vijesti, osobito ako dolazi iz utjecajnog izvora, veća je vjerojatnost da će biti uvjerena ili zaražena.., (Andrews, 2017.)*

### **3.2. Širenje putem digitalnog novinarstva**

U današnje vrijeme novinarstvo je znatno izmijenjeno, nasuprot tomu kakvo je bilo prije nekoliko godina. Novinarstvo je bilo izvor vijesti s vjerodostojnim izvorima, temeljeno na činjenicama. Iako se neki digitalni mediji i dalje drže tih istih načela, povećan pristup tehnologijama dovodi do povećanog broja korisnika koji sami bez provjere izvora i činjenica plasiraju informacije te se nazivaju novinari građani ili aktivisti. Na taj način se u vijesti unose vlastita stajališta i pristranost, a to prikazuju kao činjenice. Tehnologije su također korištene i kao propagande pod krinkom vijesti. Naravno, Internet je svim svojim korisnicima omogućio da budu autori vijesti, bez ikakvih posljedica ako informacije nisu istinite. Digitalno novinarstvo u današnje doba mora djelovati jednako brzo kao i ostale tehnologije kako bi bilo u koraku s vremenom i kako bi moglo dostaviti prave informacije u pravo vrijeme, točnije, kako bi postiglo ravnotežu između pravovremenog i detaljnog i točnog izvještavanja. (Maryville University, n.d.)

Sve češće se spominju problemi medijske manipulacije javnosti, najčešće vezani uz širenje lažnih informacija putem Interneta. Poznato je da se novinari i tradicionalne internetske stranice pridržavaju novinarskih normi objektivnosti te na taj način stječu uvijek visoku razinu vjerodostojnosti i povjerenja. Mediji na Internetu su potaknuti ne unositi vlastita mišljenja u svoje članke te se trebaju pridržavati informacija koje su u interesu publike.

No, na društvenim mrežama te se iste norme često ne poštuju ili namjerno zanemaruju. Korisnici na društvenim mrežama, uglavnom dijele informacije bez ikakve provjere činjenica, posebno ako je slučaj osobne emocionalne privrženosti sadržaju. Izazivanje emocionalnih reakcija kod korisnika doprinose bržem širenju istih informacija te to uvelike otežava procjenu istinitosti informacija.



No, manipulacija javnosti putem medija nije uvijek napravljena kao pritisak na medije. Mediji su često i sami uključeni u manipulaciju svoje publike. Jedan od načina koji se koristi od strane medija za manipulaciju je da se publici nudi znatno više zabavnoga, nego informativnoga, obrazovnog ili znanstvenoga sadržaja. Mediji zbog svoje proširenosti mogu manipulirati potrebama svih svojih pratitelja, neovisno o dobi.

Najveća opasnost digitalnog novinarstva jest neispravno odrađivanje posla, u smislu provjere izvora i konteksta sadržaja. Na taj je način lažne informacije još teže dokazati, jer su objavljene putem novinara te se time čine vjerodostojnije. (Nenadić i Vučković, 2021.)

Međutim, problem nije samo u lažnim informacijama prenesenim putem medija, već i općem nezadovoljstvu javnosti tradicionalnim medijima, najviše iz razloga prenošenja ideologija i mišljenja velikih organizacija i političkih stranki. Iz pogleda javnosti koja prati medije, problem lažnih vijesti nije samo u lažnim informacijama, već se tiče nekvalitetnog obavljanja posla u novinarstvu, korištenja političke propagande i manipulacije putem oglašavanja i općeg ne povjerenja u medije.

Najnovija tehnika širenja vijesti nije u objavljivanju potpuno neistinitih informacija, već se koriste naprednije i profinjenije tehnike koje rade na način da se miješaju istinite i lažne informacije pa se ne mogu koristiti uobičajeni načini otkrivanja lažnih vijesti putem mehanizama zabrane i uklanjanja lažnih informacija s Interneta. Suzbijanje dezinformacija može se temeljiti i na tehnološkim (računalnim) algoritmima i na kvalitativnoj analizi. Naravno, uvijek treba biti naglašeno da se također edukacijom javnosti putem medija može znatno pridonijeti razvoju medijske kompetencije i analitičkog razmišljanja korisnika Interneta.

Algoritmi za provjeru činjenica u digitalnom novinarstvu koriste sustav provjere činjenica i osiguravanja da je sam izvor pouzdan. Društvene mreže uglavnom prate istu logiku u korištenju takvog algoritma. (*prikaz slika 1.*)

Primjer algoritma za provjeru činjenica:

---

```
1. candidateTopics:: {List of sources that contain messages about these topics}
2. text = retrieveMessageText(source, postId)
3. Who = extract(People + Institutions + Organizations, text)
4. Where = extract(Places + Regions, text)
5. When = extract(PeriodsOfTime, text)
6. Topic = TopicDetection(text)
7. Fact ← combine(Topic, Who, Where, When)
8. Foreach x in candidateTopics
9.   If x.Topic == Fact.Topic Then
10.     result = CrossCheck(x,Fact)
11.     if result == True Then return Validated
12.     else return notValidated
```

---

*Slika 1. Primjer algoritma za provjeru činjenica (Figueiraa i Oliveirab, 2017.)*

Mediji često nisu potpuno odgovorni za širenje lažnih vijesti, budući da su tekstovi često napisani na način da se mogu interpretirati na više načina, što daje prostora korisnicima da uzimaju informacije po osobnom stajalištu. Stoga se mediji trebaju usredotočiti na pravilno prenošenje informacija sa izvorima koji podupiru iznesene tvrdnje i bez sadržaja koji nemaju konteksta uz sebe. Također je važna medijska pismenost koja se mijenja sa napretkom tehnologija, no glavne sposobnosti su uvijek iste, a to su znanje o sustavu rada medija te kreativne, motivacijske, obrazovne i moralne vještine.

Tehnologije se razvijaju velikom brzinom stoga i mediji moraju pratiti taj razvoj te biti u korak s potrebama publike. Znanje je veoma pristupačno u današnje vrijeme, dok se ranije oduvijek smatralo privilegijom i nečim nedostupnim svakom čovjeku. Trenutno je Internet zasićen prevelikim brojem informacija i mediji su skloni zasipavanju korisnika sa mnoštvom poruka i informacija koje je potrebno provjeravati i proučiti prije prihvatanja. Potrebno je pametno postupati i primati informacije te zaštititi sigurnost informacija na Internetu.

## **4. Primjena umjetne inteligencije u širenju i prevenciji lažnih informacija na Internetu**

Umjetna inteligencija ima veliku ulogu u širenju i prevenciji lažnih vijesti, stoga će biti detaljnije objašnjena u ovom poglavlju.

*„Umjetna inteligencija je sposobnost nekog uređaja da oponaša ljudske aktivnosti poput zaključivanja, učenja, planiranja i kreativnosti.*

*Umjetna inteligencija omogućuje tehničkim sustavima percipiranje okruženja, uzimanje u obzir onog što vide i rješavanje problema kako bi postigli neki cilj. Računalo prima podatke (koji su već pripremljeni ili prikupljeni s pomoću vlastitih senzora, npr. fotoaparata), obrađuje ih i daje odgovore.*

*Sustavi umjetne inteligencije mogu u određenoj mjeri prilagoditi svoje ponašanje analiziranjem prethodnih situacija i samostalnim radom.“*

(Europski parlament, 2020.)

Umjetna inteligencija već je i sad prisutna na svakom koraku, služi nam za čuvanje osobnih podataka na Internetu, poboljšavanje svakodnevnih radnji, kao što je pregled prometa i vremenskih uvjeta te za čišći zrak i prirodne izvore energije. U budućnosti će se život potpuno promijeniti uvođenjem sve veće količine uređaja s umjetnom inteligencijom.

Postoje tri vrste umjetne inteligencije zavisno o nivou ugrađene inteligencije:

### **1. Umjetna sužena inteligencija (ANI- Artificial narrow intelligence )**

Umjetna sužena inteligencija slaba je vrsta umjetne inteligencije, ona je uglavnom usmjerena na samo jedan zadatak te je slabog raspona sposobnosti. Primjeri ove vrste umjetne inteligencije je uključena u svakodnevni život čovjeka, kao na primjer, Google prevoditelj, Siri ili Alexa, google asistent i razni chatbotovi. (Fourtané, 2019.)

### **2. Umjetna opća inteligencija (AGI-Artificial General Intelligence)**

Ova vrste umjetne inteligencije sa svojim je sposobnostima često uspoređivana s sposobnostima ljudi. Ovo je novo polje stoga još nije potpuno funkcionalno u razmjeru u kojemu je zamišljeno. Tehnologija značajno napreduje svaki dan stoga nije nemoguće da

će i umjetna inteligencija, kao ljudski mozak, moći stvarati i razrađivati sveobuhvatna znanja i imati opću inteligenciju. No, takva vrsta inteligencije donosi svakakve vrste promjena stoga će se društvo morati prilagoditi. (Fourtané, 2019.)

### **3. Umjetna super inteligencija (ASI- arifical super intelligence)**

Vjeruje se da će ova razina umjetne inteligencije donijeti budućnost. Ova vrsta umjetne inteligencije moći će nadmašiti ljude u svim pogledima. Od ove vrste umjetne inteligencije očekuje se odlično snalaženje u donošenju odluka i emocionalnim odnosima, no zasad se te mogućnosti smatraju strogo ljudskima. Umjetna će inteligencija imati mogućnosti savršenog odlučivanja i kontrole emocija što ljudi nikad nisu bili u mogućnosti stoga se smatra da će umjetna inteligencija moći ispraviti stvari u kojima su ljudi loši. (Fourtané, 2019.)

#### **4.1. Umjetna inteligencija u borbi protiv širenja lažnih vijesti**

Umjetna inteligencija se dokazala veoma korisnom u borbi protiv lažnog informiranja na Internetu jer ima mogućnost analizirati velike količine informacija svakodnevno, što je inače nemoguće od strane samih ljudi. Iako ima mogućnosti veće od ljudskih, umjetna inteligencija postiže najbolje rezultate ako su u proces uključeni i ljudi. Uz zajednički rad ljudi s umjetnom inteligencijom, korisnicima Interneta olakšano je razlikovanje istine od laži i fikcija.

Internet je donio mogućnost da svaki korisnik iznosi svoja mišljenja i ima slobodu izražavanja, no za točno informiranje, korisnicima su potrebne provjerene činjenice.

Jedan primjer rješenja koje kombinira umjetnu inteligenciju s radom ljudi za uspješnu borbu protiv lažnih informacija razvijen je 2017. godine od Lyric Jaina i nazvano je Logically koji se predstavlja na ovaj način:

*„Mi smo tehnološka tvrtka koja kombinira naprednu umjetnu inteligenciju i strojno učenje s jednim od najvećih svjetskih timova za provjeru činjenica kako bi svima, od pojedinačnih građana do nacionalnih vlada, pružila alate koji su im potrebni za identifikacija i razoružavanje štetnih i zavaravajućih informacija koje se dijele na internetu.“* (Logically, n.d.)

Logically se koristi naprednim tehnologijama obrade prirodnog jezika ili NLP-om i također tehnikama inženjeringa znanja za identificiranje i označavanje sadržaja s ocjenom „niska“, „srednja“ ili „visoka“ uz uspoređivanje sličnih informacija s mnogobrojnim izborima, korištenjem ne samo sadržaja već i metapodataka i fotografija. Na taj način omogućuje korisnicima kako bi uvidom u istinitost informacija, sami odlučili što s tim informacijama žele učiniti.

Drugi primjer umjetne inteligencije korištene u borbi s lažnim informacijama je AdVerif.ai, kojoj je glavni cilj zaštita korisnika od zavaravajućih ili neprikladnih sadržaja i lažnih vijesti. Tvrtka koristi algoritam nazvan FakeRank te služi za osiguravanje praćenja pravila tvrtki i zaštite samih korisnika od neispravnih informacija. FakeRank se također koristi tehnologijama obrade prirodnih jezika i dubokog učenja kako bi pokazao je li sadržaj neistinit ili zavaravajući, provjerom sadržaja po činjenicama iz baze.

*„Naš tim koristi cijeli niz AI tehnologija. S našim vlasničkim algoritmom FakeRank na vrhu smo otkrivanja lažnih vijesti. Korištenjem ove tehnologije osnažujemo ljudske recenzente da prošire proces moderiranja i poboljšaju njegovu točnost, čuvajući korisnike sigurnima.“* (AdVerif.ai, n.d.).

Uz to postoje i alati koji mogu pomoći korisnicima u uočavanju lažnih informacija. Na primjer mrežni alat *Hoaxy* koji je svima lako dostupan omogućava korisnicima da vizualiziraju širenja i pretraživanja činjenica putem mreže. Također, *Google Chrome* isto ima proširenja koja mogu pomoći filtrirati lažne informacije, čak i *Snopes* i *FactCheck.org*, popularne web stranice, mogu pomagati u identificiranju lažnih informacija koje su na Internetu. (Marr, 2017.)

## **4.2. Umjetna inteligencija kao alat za izradu i širenje lažnih vijesti**

Umjetna inteligencija, iako korištena za svrhe obrane protiv lažnih informacija, često se koristi i u svrhu izrade i širenja lažnih informacija, stoga su ti sadržaji često teški za detektirati i ukloniti. Razvojem tehnologije za borbu protiv lažnih informacija, uspijeva se detektirati lažni sadržaj stoga se radi i na boljim načinima kako prezentirati lažne sadržaje kao istinite. Iz tog razloga konstantnog napretka tehnologije, smatra se da Internet nikada neće biti potpuno siguran od lažnih informacija.

### 4.2.1. Deepfake

Ljudski mozak u pravilu je treniran vjerovati onome što može vidjeti, točnije onome što je vizualno prikazano u obliku fotografije, videozapisa ili audio zvuka. Stoga se najvećom prijetnjom smatra upravo manipulacija tih sadržaja.

Jedan od načina manipulacije fotografijama, audio zvukom i videozapisima je *deepfake*. *Deepfake* se koristi umjetnom inteligencijom i strojnim učenjem za izmjenu sadržaja kao što su fotografija, zvuk ili videozapis u svrhu nanošenja štete i lažnog predstavljanja neke osobe. *Deepfake* se uglavnom služi *Autoencoder* umjetnom inteligencijom koja služi za prepoznavanja lica i otkrivanja detalja lica.

Generativna kontradiktorna mreža (GAN - *generative adversarial network*) omogućuje izradu fotografija ljudi koji ne postoje te lažnih sadržaja s pravim osoba u situacijama koje se nisu dogodile. Također, izradom fotografija osoba koje ustvari ne postoje, olakšava se izrada lažnih profila na društvenim mrežama. (*prikaz slika 2.*)



Slika 2. Fotografije ljudi koji ne postoje, izrađene tehnologijom GAN (Karras. 2019.)

Mnogi korisnici smatraju manipulaciju slikama i videozapisima pomoću umjetne inteligencije kao oblikom zabave ili vrstom humora, a ne prijetnjom za Internet i medije. Tako se prvobitno razvio i *deepfake*, korisnici su se njime koristili kako bi izrađivali

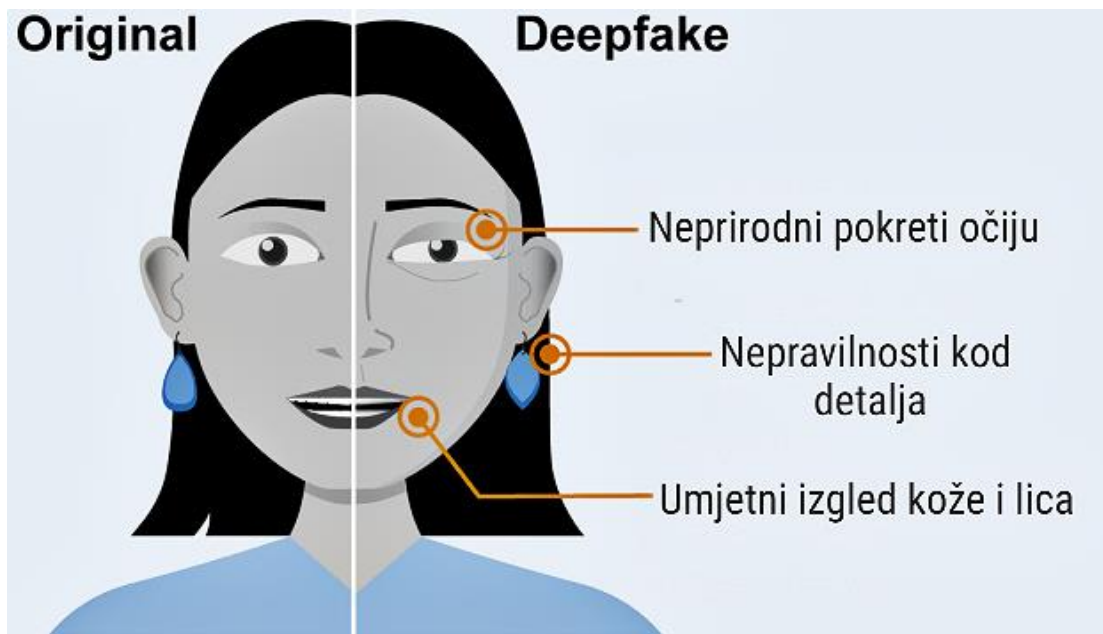
zabavne sadržaje, no s vremenom, ova vrsta manipulacije videa počinje biti korištena u više različitih svrha.

Nažalost dolaskom ovakvih programa na Internet, znatno se povećao broj lažnih vijesti i dezinformacija. Ubrzanim napretkom tehnologije, manipulacija tehnologijom postaje sve češća pojava stoga u današnje vrijeme ljudi nisu u mogućnosti vjerovati ničemu što vide na Internetu, uključujući fotografije i videozapise.

Sve je veći broj aplikacija koje su lako dostupne i besplatne te služe za zamjenu ili dodavanje lica na videozapise, jedan od primjera takve aplikacije je *FakeApp*.

*“Najpoznatija aplikacija je FakeApp, javno je dostupna, iako posve sigurno nije jedina. Radi na bilo kojem Windows računalu s jačom grafičkom karticom i većom količinom diskovnog prostora. Rezultati rada ove aplikacije uglavnom su lako prepoznatljivi jer nedostaje ručni dio retuširanja videozapisa kako bi se uklonili artefakti, ali ponekad na prvu loptu mogu djelovati uvjerljivo.”* (Dejanović, 2020.)

Iako neizbježan, *deepfake* je u dosta slučajeva izrađen amaterski, u svrhu prevare, stoga pri pregledu sumnjivih videozapisa, treba pripaziti na pokrete lica osobe koji znaju izgledati umjetno kod *deepfake* sadržaja, kao na primjer treptanje oka koje izgleda neprirodno ili nepostojeće. Promatranje videa, u nekim slučajevima, biti će moguće prepoznati lažni videozapis te zaustaviti njegovo širenje. (*Prikaz na slici 3.*)



Slika 3. Mogući znakovi deepfake sadržaja (WatchBlog, 2020.)

*„Videozapise moguće je mijenjati na nekoliko načina, a ovisno o izabranoj metodi bit će lakše ili teže otkriti izmjene. [...] Dobro montiranom radu teško će se pronaći mana ako ne znate što točno gledati, no isplati se provjeriti (Dejanović, 2020.):*

- pravilno usmjerene sjene, sve u jednom smjeru
- boja sjene treba biti jedne boje (sunce ili reflektor)
- jeli odjeća osobe s videozapisa prilagođena vremenskim uvjetima
- postojanje anomalije kod odjeće od osobe, ako je odjeća boje pozadine
- postojanje anomalije kod detalja, kao kosa
- postojanje anomalije na reflektirajućim objektima, kao staklo ili ogledalo
- nedostaje li osjećaj dubine kod pomicanja kamere

Tehnologije kod montiranja scena je toliko usavršena da je moguće napraviti scene jednake stvarnom životu, koje su korisnicima nemoguće za prepoznati kao lažne, pogotovo kad se radi o brzim scenama. (Dejanović, 2020.)

#### **4.2.2. Izmjena konteksta originalnih fotografija**

Uz *deepfake*, postoji još različitih vrsti vizualnih dezinformacija. Većina takvih vrsta dezinformacija prisutna je svakodnevno svakom korisniku na Internetu. Najčešće



korištene tehnike su recikliranje starih pravih videozapisa i fotografija te njihova obrada kako bi izgledale dramatičnije ili postigle bilo kakvu vrstu reakcije od korisnika s kojima će biti u kontaktu.

Primjeri ove vrste dezinformacija bila je veoma česta tokom početka pandemije 2020. godine, gdje su Internetom, pogotovo društvenim platformama, kružile fotografije praznih polica u trgovinama mješovite robe koje su poticale strah i ljutnju od strane korisnika koji su susreli s tim fotografijama. No, fotografije korištene kao primjer su dokazano, ustvari fotografije slikane od fotografa Marka Bakera u trgovinama u Japanu. Japan je te godine bio pogođen sa potresom magnitude 9 i sa tsunamijem u kojemu je smrtno stradalo tisuće ljudi i uništeno mnogo gradova. Fotografije su slikane nakon nestanka hrane i ostalih zaliha u trgovinama u Japanu, te su korištene kao vizualna manipulacija publike u 2020. godini.

Različiti stručnjaci proučavaju na koji način ljudi uočavaju točne, odnosno, netočne informacije s kojima se susreću. Stoga se ovakva vrsta manipulacije, bez konteksta fotografije, smatra izuzetno jakom vrstom lažnog informiranja.

Opasnost ove vrste dezinformiranja je osobito izražena u promicanjima lažnih uvjerenja i popularnih mišljenja. Ljudski mozak lakše prima i prihvaća informacije ako su prikazane uz fotografije. Fotografije također lakše privlače pažnju korisnika. Ta tehnika je često korištena i u informiranju od strane medija za lakše izazivanje emocija kod korisnika, stoga korisnici često uz događaje u povijesti vežu slike ozlijeđenih ljudi ili uništenih gradova.



Slika 4. Fotografija uslikana u Japanu 15.3.2011, no korištena na internetu kao primjer panike tokom pandemije 2020.-2021. (Evon, 2019.)

*„Gore prikazana slika nema mnogo veze sa "socijalizmom" ili važnošću slobodnih tržišta. Ova slika zapravo prikazuje trgovački prolaz koji je nakon prirodne katastrofe gotovo očišćen od zaliha. Ovu je fotografiju 15. ožujka 2011. snimio fotograf Associated Press Mark Baker u supermarketu u Moriyami u Japanu. Zemlja je upravo doživjela potres magnitude 9 i razorni tsunami u kojem su tisuće ljudi poginule i uništeno više od 100.000 zgrada. Nakon katastrofe Japan je pretrpio nestašicu hrane, benzina, lijekova i drugih zaliha, što je dovelo do dugih redova i praznih polica u trgovinama.“ (Evon, 2019.)*

Postoji mnogo razloga zbog čega fotografije povećavaju korisnikovo vjerovanje u informacije. Jedan od razloga je da fotografija uglavnom u objavama služi kao dokaz da se neki događaj uistinu dogodio. Sljedeća stvar je da fotografije pomažu za lakše pamćenje informacija, također je događaje lakše zamisliti i stoga se i lakše razvijaju emocije kod korisnika.

Društvene platforme kao što su Facebook i Twitter su potaknute od korisnika na omogućavanje označavanja fotografija s informacijom kada je prvi puta objavljena, radi lakše prevencije korištenja starih fotografija u svrhu manipulacije javnosti.

No, dok se takve inovacije ne ostvare od strane društvenih platformi, korisnici se mogu poslužiti tehnikom obrnutog pretraživanja slika. Takva tehnika bi mogla smanjiti utjecaj dezinformacija na korisnike. Na primjer korištenje te tehnike vrlo je jednostavno na

pregledniku *Google Chrome*. *Google obrnuto pretraživanje* korisniku omogućava pretraživanje sličnih slika kroz cijeli web. Slika se jednostavno prenese s računala na *Google slike* te se trenutno prikazuju sve slične slike koje su korištene na različitim web stranicama, kao i slučaj različitih veličina iste slike. Novinari se u digitalnom novinarstvu služe ovom opcijom pretraživanja kako bi pronalazili izvornu sliku i kontekst u kojemu je navedena te vrijeme kada je prvi put bila objavljena. (Digital inspiration, n.d.)

#### **4.2.3. Društveni botovi**

*„Botovi na društvenim mrežama su algoritmi dizajnirani za razgovore sa ljudskim korisnikom. Algoritmi su osmišljeni tako da oponašaju ljudsko ponašanje koje bi se podudaralo sa obrascima sličnim onima ljudskog korisnika.“* (Mušanović, 2020.)

Drugo ime za botove s društvenih mreža je društveni botovi. Oni služe kako bi svojim oponašanjem korisnika izvršavali zadani zadatak. Fenomen botova na društvenim mrežama stekao je veliko zanimanje, ali i zabrinutost na platformama društvenih mreža zbog sve većeg broja zlonamjernih botova.

Botovi se mogu koristiti u korisne svrhe kao što je objavljivanje vijesti, automatsko ažuriranje vremenske prognoze. No, nažalost, velika većina botova nastala je i korištena je za zlonamjerne svrhe kao što su: širenje lažnih i štetnih informacija te neželjenih sadržaja i virusa.

Postoji mnogo izazova u otkrivanju botova, no jedan od najvećih baš na društvenim medijima je razumijevanje što sve u današnje vrijeme društveni botovi mogu učiniti. Ranije vrste botova su uglavnom obavljale po jednu vrstu aktivnosti, a to je automatsko objaviti neki sadržaj. Ti su botovi bili jednostavni i lako ih je uočiti sa algoritmima za otkrivanje botova, poput fokusiranja na veliku količinu generiranja sadržaja. (Ferrara et.al, 2016.)

U posljednjih nekoliko godina, vidljivo je da su botovi na *Tweeter-u* postali mnogo bolji te je njihovo otkrivanje otežano. Granica u otkrivanju razlike između ponašanja ljudskog korisnika i botova sada postaje jako nejasna. Na primjer, botovi sada mogu pretraživati web u potrazi za podacima s kojima mogu ispuniti svoje profile te brzo i efikasno objavljivati materijale koje pronađu, oponašajući tako rad ljudskog korisnika na način ujednačenog i redovnog objavljivanja. Botovi se mogu uključivati i u složenije interakcije

s ostalim korisnicima, kao na primjer, zabavni razgovori, komentiranja slika i postova i odgovaranja na pitanja ostalih korisnika. Kako bi bili što vidljiviji, botovi mogu infiltrirati popularne rasprave i generirati tematski prikladne, zanimljive sadržaje. Korištenjem tehnikom pretraživanja po ključnim riječima u nabavljanu informacijama za razgovore. (Ferrara et.al, 2016.)

Društveni botovi se razlikuju po svojoj programiranoj svrsi. Neki primjeri svrhe botova su korištenje u političkim izborima, uglavnom za brže širenje informacija o kandidatima, uglavnom se šire negativne informacije. Također, jedna od često korištenih svrha je povećavanje broja pratitelja putem botova.

Botovi su pristupačni, jeftini i laki za izradu, stoga su gotovo nemogući za prepoznavanje i uklanjanje od strane društvenih platformi. Njihova izrada može se odvijati na besplatnim i pristupačnim softverima te uglavnom imaju jednostavne svrhe kao što su:

- pregledavanje objava prema određenoj riječi,
- prenošenje već unaprijed određenih i napisanih tekstova prema drugim korisnicima putem komentara i objava te
- vođenje jednostavnih razgovora s korisnicima.

Prvobitna namjena botova na društvenim mrežama bila je pomoć ostalim korisnicima te za brže širenje vijesti. No, brzo je otkriveno da se mogu upotrijebiti i za propagande te u svrhe opasne za ostale korisnike, namećući vijesti koje su polu istinite ili potpuno lažne kao činjenice. Mnogim korisnicima nije bitno odakle potječe vijest, već koliko ju drugih korisnika podržava. Stoga, svaki korisnik, u današnje vrijeme, na društvenim mrežama treba obratiti pažnju na informacije koje dijeli jer često podrijetlo takvih vijesti nije poznato.

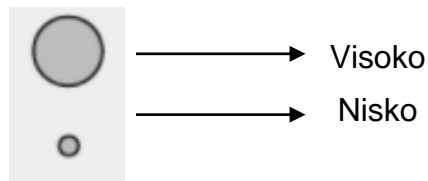
### **„Zagađenje od strane botova**

*Botovi ili automatizirani računi koji se lažno predstavljaju kao korisnici, uvelike smanjuju kvalitetu informacija na društvenoj mreži. U jednoj računalnoj simulaciji, istraživači OSoMe-a uključili su u društvenu mrežu botove (modelirane kao agenti koji tvitaju samo meme nulte kvalitete i retvetiraju samo jedan drugog).*

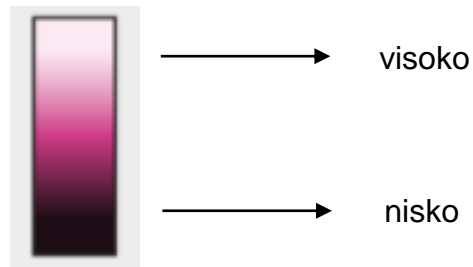
Otkrili su da kada manje od 1 posto ljudskih korisnika prati botove, kvaliteta je informacija visoka (lijevo). No, kada postotak infiltracije botova premaši 1, nekvalitetna informacija se širi cijelom mrežom (desno). Na stvarnim društvenim mrežama samo nekoliko ranih glasova botova može učiniti da lažna vijest postane viralna.“

(Menczer i Hills, 2020.) (dolje naveden prikaz stimulacije)

- **Prikaz računalne stimulacije:**

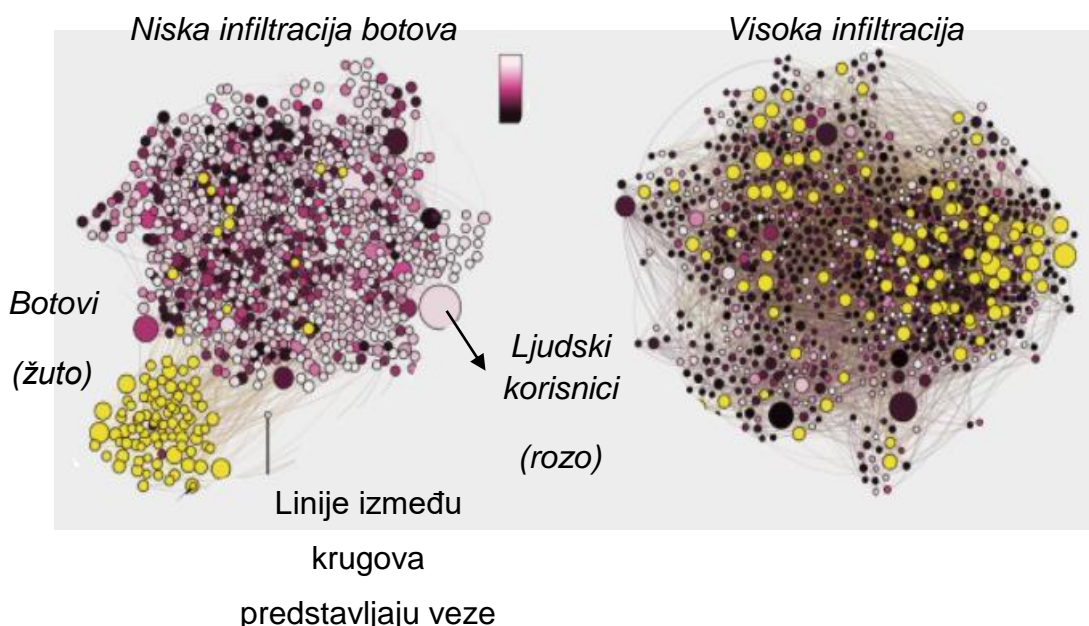


*Veličina krugova predstavlja utjecaj (na autentične korisnike)*



*Boja krugova predstavlja kvalitetu dijeljenih informacija*

- **Svaki krug predstavlja zasebni račun na društvenim mrežama**



Slika 5. Prikaz računalne simulacije proširenosti botova (Menczer i Hills, 2020.)

#### 4.2.4. GPT-3

„GPT-3, ili generacijski unaprijed obučeni transformator treće generacije, model je strojnog učenja neuronske mreže koji se trenira pomoću internetskih podataka za generiranje bilo koje vrste teksta. Razvio ga je OpenAI, potrebna je mala količina ulaznog teksta za generiranje velikih količina relevantnog i sofisticiranog strojno generiranog teksta.,, (Schmelzer, 2021.)

GPT-3 je testiran od strane znanstvenika kroz šest različitih scenarija u pogledu dezinformacija. Ovaj je softver predviđen za pravljenje različitih tekstualnih objava koje trebaju izgledati kao da su napisane od različitih korisnika, ali da istodobno potiču razgovor o istoj temi.

Pisanje poruka s određenom namjerom je jedna od stvari koja je previše napredna i složena i za ovu verziju GPT-a, no ljudi mogu raščlaniti te zadatke na jednostavnije i manje zadatke, što omogućuje sustavu da daje važne izjave u obliku teksta.

GPT-3 je poznat po svojoj strogoj ograničenosti korisnika. Ova umjetna inteligencija je podijeljena samo nekolicini partnera s odobrenim pristupom, što bi se moglo promijeniti u

budućnosti te bi to moglo ubrzati širenje različitih informacija pa tako i lažnih informacija. Naravno, svi uključeni u GPT-3 su svjesni tog rizika i posljedica.

Korištenje softvera kao GPT-3 i ostalih ima mogućnost preplavlivanja društvenih platformi i cijelog Interneta sa dezinformacijama u tolikih količinama da će većina informacija biti beznačajne i beskorisne. Ovaj scenarij naravno potiče znanstvenike da razvijaju jednako jake alate za detekciju i obranu od dezinformacija. Jedan od načina koji se najčešće koristi za prepoznavanje GPT-3 i ostalih sličnih softvera, je traženje tako zvanih „otisaka prstiju“. Pod tim nazivom se nalaze često korištene fraze i riječi iz rječnika koji su programirani tim softverima za korištenje. Proizvođači softvera za širenje informacija pokušavaju izraditi softvere sa što manje „otisaka prstiju“, kako bi bili što manje prepoznatljivi u detekciji i imali što prirodnije i ljudskije odgovore.

Jedna od značajki GPT-3 je generiranje izvornog koda. Obučen je za sav postojeći tekst koji je na Internetu, a veliki dio tog istog teksta je dokumentacija računalnih kodova. GPT-3 stoga ima mogućnost automatiziranja lažnog predstavljanja te generiranja izvornih kodova. Također može biti korišten od strane sigurnosnih operacija za otkivanje i obranu od napada i krađe podataka.

Iako je GPT-3 vrlo velik i uspješan, i dalje posjeduje nekakva ograničenja i moguće rizike pri uporabi. Jedan od najvećih trenutnih problema GPT-3 je to što ne uči stalno, već je prethodno obučen te nema sposobnost učenja iz svakih novih interakcija. Ostali problemi s kojima se suočava GPT-3 su nedostatak sposobnosti za objašnjavanje i tumačenjem iz kojeg razloga određen ulaz rezultira određenim izlazom, sljedeće je njegova pristranost strojnog učenja budući da je taj model treniran na tekstovima s interneta, on ima pristranost kao i autori teksta. Na primjer, istraživači s Middlebury instituta za međunarodne studije dolaze do otkrića da GPT-3 ima nevjerovatnu vještinu u stvaranju radikalnih tekstova, kao na primjer diskursa koji se ponašaju kao teoretičari zavjere ili rasisti. Ovo se ukazalo kao prilika za te skupine da automatiziraju svoje govore mržnje. Osim toga, javnost je veoma zabrinuta zbog velikih mogućnosti GPT-3, iz razloga što bi takva tehnologija bila vrlo uspješna u širenju lažnih informacija automatski i velikom brzinom. (Schmelzer, 2021.)

Već postoje lažne kopije GPT-3 koje se koriste za napade te u budućnosti treba očekivati da će te pojave biti sve češće. Te se od GPT-a očekuje da će moći imati bolje moralne okvire i smjernice prema boljem načinu rada jezičnih modela.

Kampanje misinformacija i dezinformacija su veoma pristupačne, jeftine, teško uočljive, ali i učinkovite. No, granice i dalje postoje, budući da je dobro osmišljenu dezinformaciju moguće proširiti samo brzinom kojom ju korisnik može fizički napisati, no u budućnosti se očekuje da će i softveri za generiranje teksta biti sposobni napraviti i proširiti smislene dezinformacije, na taj način proširujući opseg napada.

Budući da je GPT-3 trenutno pri samom vrhu među softverima za generiranje automatiziranog teksta, također je ujedno i jedan od najboljih opcija za dezinformacijske napade. Poznato je da se u većini slučajeva ne poznaje razlika između teksta napisanog od strane čovjeka i GPT-3, stoga se lagano koristi na društvenim platformama u kampanjama lažnog informiranja, najveći problem u takvoj vrsti zlonamjernog korištenja ovog softvera je u tome što GPT-3 ima čestu tendenciju skretanja sa zadanih tema.



## 5. Velike baze podataka (*Big data*)- dohvaćanje i analiziranje istinitosti informacija

*Big data* tehnologija je još jedan bitan pojam koji donosi još mogućnosti suzbijanja lažnih informacija, što će biti detaljno objašnjeno u ovom poglavlju.

*„Velike baze podatka ili Big data opisuju tehnologije koje ispunjavaju temeljno načelo istraživanja u informacijskim sustavima, a to je pružiti prave informacije pravom primatelju u pravoj količini i kvaliteti u pravo vrijeme.“* (Schermann et.al., 2014.)

Postoje mnoge mogućnosti koje donosi korištenje *Big data*, kao što su značajno povećanje stjecanja znanja, podržavanje znanstvenih napredaka te korištenje u pronalasku informacija za inovativne vijesti i članke na Internetu. U zadnjih nekoliko godina enormni rast podataka i potrebe za mjestom pohrane tih podataka omogućava sve veću potrebu za *Big data* tehnologijom. Svi korisnici su naučeni na dobivanje samo informacija koji ih zanimaju, na oglase i reklame koje prate i na razgovore i medijske sadržaje koje iznose na Internet, to sve nam omogućava upravo ova tehnologija.

Velike količine podataka na Internetu zahtijevaju i tehnologije za njihovo pohranjivanje, analiziranje i na kraju upravljanje. Sve te tehnologije u jednom daju *Big data*, ljudska snaga i znanja su zamijenjena tehnologijom te je pristup podacima sada znatno olakšan i beskonačne količine podataka mogu biti spremljene i spremne za korištenje u kratkom roku. Prednosti koje dolaze s *Big data* tehnologijom treba iskoristiti, no oprezno i uz puno znanje načina korištenja takve tehnologije.

*Big data* ima jedan bitni nedostatak, a to je nedostatak vještina za analiziranje i obrađivanje podataka. Ulaganje u radnu snagu koja će analizirati i obrađivati informacije, kako bi bile istinite i pravilne, veliki je trošak te i sama edukacija radnika u tom području traje duži period vremena. Stoga je jasno da se u današnje vrijeme svugdje traži način za obradu i analizu podataka brzo i jeftino. Kako bi se korisnicima pružile pouzdane, originalne i točne informacije, nastaje potreba za kvalitetnom pripremom informacija koje se iznose. Informacije prije same uporabe od korisnika, moraju biti analizirane te moraju imati osiguranu točnost, pravilnost oblika i relevantnost.

Nepravilno spremanje i iznošenje informacija može neku platformu jako ugroziti te onemogućiti njenu vjerodostojnost. Budući da su prostor za pohranu podataka i sustavi za analiziranje vrlo skupi za održavanje, sve više se koriste alati za obradu *Big data* podataka koji se koriste tehnologijama otvorenog koda koji znatno smanjuju troškove za softvere.

## 5.1. Primjeri korištenja *Big data* tehnologija sa svrhom dohvaćanja i analize istinitosti informacija

- **Facebook**

Facebook je najpoznatija društvena platforma te se na njoj izmjenjuju ogromne količine podatka, iako je Facebook-ova glavna funkcija komunikacija između korisnika, također je korišten od velikih kompanija za prodaju proizvoda ili usluga, za objavljivanje vijesti i izmijene mišljenja te na taj način korisnici ostaju informirani. Korištenje Facebook-a za navedene stvari i je puno jeftinije i jednostavnije nego na primjer, televizija ili neki drugi oblik medija. No, već nam je poznato da takav način informiranja nije potpuno siguran od strane korisnika zbog mogućnosti lažnog informiranja, što je veliki problem Facebook-a koji stvara probleme s povjerenjem od strane korisnika. Stoga je Facebook započeo s ozbiljnim koracima u pokušaju sprečavanja prikaza lažnih vijesti na svojoj platformi na način da analizira podatke koje dohvaća kako ne bi bili ne točni, bez izvora ili u zastari.

### **Tehnologije:**

*„Njegovi podatkovni centri puni su prilagođenih poslužitelja, izrađenih od Intel i AMD čipova, te tehnologije za uštedu energije koja pomaže u smanjivanju ogromnih troškova održavanja tolikog broja strojeva koji rade 24 sata dnevno. Dizajni za poslužiteljske sustave, dostupni su kao dokumentacija otvorenog koda. Facebook se također oslanja na tehnologiju otvorenog koda za svoj softver, koji je napisan na PHP-u i pokreće MySQL baze podataka.*

*Njegovi programeri stvorili su HipHop for MySQL kompajler, koji prevodi PHP kôd u C ++ za vrijeme izvođenja, dopuštajući brže izvršavanje koda i smanjujući opterećenje CPU -a. Za upravljanje pohranom koristi vlastiti distribuirani sustav za*

*pohranu temeljen na Hadoopovoj HBase platformi. Također je poznato da Facebook koristi Apache Hive za analizu korisničkih podataka u stvarnom vremenu.*, ([http://www.bdbanalytics.ir/media/1169/bernard-marr-big-data-in-practice\\_-how-45-successful-companies-used-big-data-analytics-to-deliver-extraordinary-results-wiley-2016.pdf](http://www.bdbanalytics.ir/media/1169/bernard-marr-big-data-in-practice_-how-45-successful-companies-used-big-data-analytics-to-deliver-extraordinary-results-wiley-2016.pdf), Marr, 2016.)

HBase je namijenjen za pohranjivanje ogromnih količina podataka te omogućava bolji i lakši pristup podacima koji omogućava lakšu analizu za točnost i pravovremenost informacija, te sigurnije informacije za korisnike Facebook-a.

- **LinkedIn**

*„Osnovan 2003. godine, LinkedIn povezuje svjetske stručnjake kako bi bili produktivniji i uspješniji. S više od 756 milijuna članova diljem svijeta, uključujući rukovoditelje iz svake tvrtke Fortune 500, LinkedIn je najveća svjetska profesionalna mreža.“* (LinkedIn, n.d.).

LinkedIn uspješno osigurava da njihova web platforma ostane alat za zapošljavanje u kompanijama i sigurno mjesto za korisnike. Kako bi se to i ostvarilo ključno je korištenje *Big data* tehnologija, za davanje najbržih i najkvalitetnijih informacija korisnicima.

LinkedIn se koristi tehnologijama za osiguravanje najtočnijih informacija, koje su uvijek ažurirane, stoga prikupljanjem i prikazivanje informacija uvijek pružaju samo najbolju kvalitetu informacija za svoje korisnike. Uobičajena praksa je dohvaćanje podataka te naknadna analiza, no LinkedIn se koristi tehnologijom koja podatke skuplja i analizira u stvarnom vremenu, točnije dohvaća podatke i analizira ih u vremenu prijenosa na korisnika, tako korisnik dobiva točne informacije u najbržem mogućem roku bez mogućnosti zastare informacija i prikaza nepravilnih informacija.

## **Tehnologije:**

*„Hadoop čine jezgru LinkedInove infrastrukture velikih podataka i koriste se za ad hoc i paketne upite. Tvrtka ima velika ulaganja u Hadoop, s tisućama strojeva koji rade na mapi/smanjuju broj radnih mjesta. Ostali ključni dijelovi LinkedIn slagalice za velike podatke uključuju Oracle, Pig, Hive, Kafka, Java i MySQL. Više podatkovnih centara iznimno je važno za LinkedIn kako bi se osigurala visoka dostupnost i izbjegao jedan jedini kvar.*

*Danas LinkedIn nema više od tri glavna podatkovna centra. LinkedIn je također razvio vlastite alate otvorenog koda za pristup i analizu velikih podataka. Kafka je na ovaj način započeo život, a drugi razvoj uključuje Voldemort i Espresso (za pohranu podataka) i Pinot (za analitiku). Ovako otvorena tehnologija važna je za LinkedIn jer smatraju da dugoročno stvara bolji kod (i bolji proizvod). Osim toga, tvrtka ima impresivan tim internih znanstvenika za podatke-oko 150 prema trenutnim procjenama. Tim ne samo da radi na poboljšanju LinkedIn proizvoda i rješavanju problema za članove, već objavljuje i na velikim konferencijama i doprinosi zajednici otvorenog koda. Zapravo, tim se potiče na aktivno bavljenje istraživanjem u brojnim područjima, uključujući računalno oglašavanje, strojno učenje i infrastrukturu, pronalaženje teksta i analizu osjećaja, sigurnost i neželjenu poštu.“ (Marr, 2016.)*

## 6. Zaključak

Korisnici koji prate sadržaje medija na Internetu često su uključeni u različita društvena zbivanja i imaju češći kontakt s drugim korisnicima, stoga lakše prihvaćaju razlike u stajalištima između korisnika, no nažalost, ti mediji također omogućavaju i lažne informacije te manipulacije javnošću.

Svrha internetskih medija je u suštini trebala biti prijenos važnih činjeničnih informacija, prenošenje otkrića i novih znanja te zabavljanje publike, no ta svrha je zamijenjena željom za zaradom, stoga Internet nikada neće biti potpuno sigurno mjesto za učenje.

Učenje i informiranje putem medija i interneta važan je dio obrazovanja svakog čovjeka. Budući da je Internet mjesto beskrajnog broja informacija, korisnici su potaknuti na medijsko obrazovanje i ono postaje neophodno za današnje društvo.

Napredak tehnologije nam donosi mnoge promjene u načinima dobivanja informacija te se za pomoć od lažnih informacija koriste različiti alati kao umjetna inteligencija i *Big data* tehnologija, no te tehnologije su još uvijek upravljane od strane ljudi stoga se mogu koristiti i u svrhu izrade i plasiranja lažnih informacija. U budućnosti se očekuje da će tehnologije biti i same sposobne prepoznavati i uklanjati lažne ili poluistinite informacije, kao i informacije koje služe za poticanje na mržnju i nasilje.

Sigurno je da Internet sa svojim sadržajima nije sigurno mjesto za informiranje korisnika te će tehnologija s vremenom imati sve veći utjecaj na prenošenje informacija, no i sve veću kontrolu nad time jesu li informacije istinite i pravilne.

## LITERATURA

1. AdVerif.ai, (n.d.), About us, dostupno na: <https://adverifai.com/about/> [pristupljeno: 15.09.2021.]
2. Andrews E., (2017.), How fake news spreads like a real virus, dostupno na: <https://engineering.stanford.edu/magazine/article/how-fake-news-spreads-real-virus> [pristupljeno: 15.09.2021.]
3. Dejanović R., (2020.), Priručnik za provjeru informacije iz medija, dostupno na: <https://dznep.hr/wp-content/uploads/2020/03/PRIRUCNIK-ZA-PROVJERU-INFORMACIJA-IZ-MEDIJA.pdf>, [pristupljeno: 15.09.2021.]
4. Digital inspiration, (n.d.), Know more about any photograph with Google Reverse Image Search, dostupno na: <https://www.labnol.org/reverse/> [pristupljeno: 15.09.2021.]
5. Europski parlament, (2020.), Što je umjetna inteligencija i kako se upotrebljava?, dostupno na: <https://www.europarl.europa.eu/news/hr/headlines/society/20200827STO85804/sto-je-umjetna-inteligencija-i-kako-se-upotrebljava> [pristupljeno: 15.09.2021.]
6. Evon D., (2019.), Is This Shopping Aisle Empty Due to Socialism?, dostupno na: <https://www.snopes.com/fact-check/shopping-aisle-empty-socialism/> [pristupljeno: 15.09.2021.]
7. Ferrara E., et.al, (2016.), The Rise of Social Bots, dostupno na: <https://dl.acm.org/doi/abs/10.1145/2818717> [pristupljeno 15.09.2021.]
8. Fourtané S., (2019.), The Three Types of Artificial Intelligence: Understanding AI, dostupno na: <https://interestingengineering.com/the-three-types-of-artificial-intelligence-understanding-ai> [pristupljeno: 15.09.2021.]
9. Kulp P., (2017.), Facebook admits to nearly as many fake or clone accounts as the U.S. population, dostupno na: <https://mashable.com/article/facebook-phony-accounts-admission> [pristupljeno: 15.09.2021.]
10. LinkedIn (n.d.), About us, dostupno na: [https://www.linkedin.com/company/linkedin/?src=li-other&veh=www.linkedin.com&trk=homepage-basic\\_directory\\_aboutUrl](https://www.linkedin.com/company/linkedin/?src=li-other&veh=www.linkedin.com&trk=homepage-basic_directory_aboutUrl) [pristupljeno: 15.09.2021.]
11. Logically, (n.d.), About us, dostupno na: <https://www.logically.ai/about> [pristupljeno: 15.09.2021.]

12. Marr B. (2016.), Big data in practice, dostupno na: <http://www.bdbanalytics.ir/media/1169/bernard-marr-big-data-in-practice-how-45-successful-companies-used-big-data-analytics-to-deliver-extraordinary-results-wiley-2016.pdf> [pristupljeno: 15.09.2021.]
13. Marr, B., (2017.), Fake News: How Big Data And AI Can Help, dostupno na: <https://www.forbes.com/sites/bernardmarr/2017/03/01/fake-news-how-big-data-and-ai-can-help/?sh=26b116e770d5> [pristupljeno: 15.09.2021.]
14. Maryville University, (n.d.), The Rise of Digital Journalism: Past, Present, and Future, dostupno na: <https://online.maryville.edu/blog/digital-journalism/> [pristupljeno: 15.09.2021.]
15. Menczer F. & Hills T., (2020.), Information Overload Helps Fake News Spread, and Social Media Knows It, dostupno na: <https://www.scientificamerican.com/article/information-overload-helps-fake-news-spread-and-social-media-knows-it/> [pristupljeno: 15.09.2021.]
16. Mušanović M., (2020.), Šta su zapravo internet botovi?, dostupno na: <https://novine.ba/2020/07/31/sta-su-zapravo-internet-botovi/> [pristupljeno: 15.09.2021.]
17. Nagi K., (2018.), New Social Media and Impact of Fake News on Society, dostupno na: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3258350](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3258350) [pristupljeno 15.09.2021.]
18. Nenadić I., Vučković M., (2021.), Dezinformacije, dostupno na: <https://www.medijskapismenost.hr/wp-content/uploads/2021/04/brosura-Dezinformacije.pdf> [pristupljeno: 15.09.]
19. Pravna klinika, Pravni fakultet Zagreb, (2020.), Širenje lažnih vijesti i posljedice, dostupno na: <http://klinika.pravo.unizg.hr/content/sirenje-laznih-vijesti-i-posljedice> [pristupljeno: 15.09.2021.]
20. Schermann M., et.al. (2014.), Big Data, dostupno na: <https://link.springer.com/content/pdf/10.1007/s12599-014-0345-1.pdf> [pristupljeno: 15.09.2021.]
21. Schmelzer R., (2021.), GPT-3, dostupno na: <https://searchenterpriseai.techtarget.com/definition/GPT-3> [pristupljeno: 15.09.2021.]

## POPIS SLIKA

Slika 1. Primjer algoritma za provjeru činjenica, Figueiraa A., Oliveirab L., (2017.), dostupno na: <https://www.sciencedirect.com/science/article/pii/S1877050917323086> [pristupljeno: 15.09.2021.]

Slika 2. Fotografije ljudi koji ne postoje, izrađene tehnologijom GAN, Karras T., (2019.), dostupno na: <https://thispersondoesnotexist.com/> [pristupljeno: 15.09.2021.]

Slika 3. Mogući znakovi deepfake sadržaja, WatchBlog, (2020.), dostupno na: <https://blog.gao.gov/2020/10/20/deconstructing-deepfakes-how-do-they-work-and-what-are-the-risks/> [pristupljeno: 15.09.2021.]

Slika 4. Fotografija uslikana u Japanu 15.3.2011, no korištena na internetu kao primjer panike tokom pandemije 2020.-2021., Evon D., (2019.), dostupno na: (<https://www.snopes.com/fact-check/shopping-aisle-empty-socialism/>) [pristupljeno: 15.09.2021.]

Slika 5. Prikaz računalne stimulacije proširenosti botova, Menczer F. & Hills T., (2020.), dostupno na: <https://www.scientificamerican.com/article/information-overload-helps-fake-news-spread-and-social-media-knows-it/> [pristupljeno: 15.09.2021.]



## POPIS TABLICA

Tablica 1 - Različite vrste lažnog informiranja na Internetu, Wardle C., Derakhshan H., (2017.), dostupno na: <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html> [pristupljeno 15.09.2021.]

## SAŽETAK

U ovom radu će biti prikazano što su lažne informacije na Internetu te na koji način se mogu širiti, ali i prevenirati. Internet je ispunjen beskonačnim brojem informacija koje su stalno dostupne korisnicima. Lažne informacije se dijele na dvije podjele po namjeri korisnika koji ih širi, a to su misinformacija i dezinformacija. U izradi i širenju lažnih informacija uglavnom se koristi umjetna inteligencija, kao što su botovi i automatizirane UI za generiranje tekstova te za videozapise - deepfake. Umjetna inteligencija se ne koristi samo u izradi i širenju lažnih informacija, već i u obrani od istih, uz analiziranje i označavanje lažnih informacija kako bi korisnicima olakšali informiranje na Internetu. U radu se također govori i od *Big data* tehnologijama, koje se također koriste za dohvaćanje i analizu informacija, za olakšan rad s informacijama i njihovu najbolju kvalitetu i točnost. Najveću ulogu u izradi i širenju dezinformacija imaju društvene mreže, gdje se najlakše šire i najmanje mogu kontrolirati, stoga se najveći oprez i pažnja preporuča baš na korištenje društvenih mreža.

Cilj rada je približiti pojam lažnih informacija korisnicima Interneta, kako bi lakše prepoznavali različite vrste lažnih informacija i načine njihova širenja. Također ukazuje na veliku važnost i utjecaj tehnologija kao što je umjetna inteligencija i *Big data* u izradi i širenju lažnih informacija, no i kako s tim tehnologijama, zaustaviti širenje istih lažnih informacija.

**Ključne riječi:** lažno informiranje, umjetna inteligencija, dezinformacije, misinformacije, botovi, društvene mreže, Internet, *Big data*

## SUMMARY

This paper will show what is false information on the Internet and how it can be spread, but also prevented. The Internet is filled with an infinite amount of information that is constantly available to users. False information is divided into two divisions according to the intention of the user who spreads it, namely misinformation and disinformation. Artificial intelligence is mainly used in the creation and dissemination of false information, such as bots and automated AIs for generating texts and for videos - deepfake technology. Artificial intelligence is used not only to create and disseminate false information, but also to defend against it, with the analysis and labeling of false information to make it easier for users to get information on the Internet. The paper also talks about Big data technologies, which are also used to retrieve and analyze information, to facilitate the work with information and its best quality and accuracy. Social networks have the biggest role in creating and spreading disinformation, where they are the easiest to spread and the least can be controlled, so the greatest caution and attention is recommended to the use of social networks.

The aim of this paper is to bring the concept of false information closer to Internet users, in order to more easily identify different types of false information and ways of spreading it. It also points to the great importance and influence of technologies such as artificial intelligence and Big data in the creation and dissemination of false information, but also use of these technologies, to stop the spread of the same false information.

**Keywords:** false information, artificial intelligence, misinformation, disinformation, bots, social networks, Internet, Big data