

DIGITALNA BEZBJEDNOST NIJE LUKSUZ, VEĆ GRAĐANSKA DUŽNOST

Piše: Branko Džakula, ekspert za sajber bezbjednosti

U današnjem digitalnom dobu, gotovo cjelokupno stanovništvo Crne Gore ima pristup internetu, a procjenjuje se da oko 472 hiljade građana aktivno koristi društvene mreže. Digitalni prostor danas o nama čuva više podataka nego bilo koja institucija u stvarnom životu. Iako ovakva povezanost donosi nesumnjive prednosti, ona sa sobom nosi i sofisticirane prijetnje po privatnost i kvalitet informacija.

U eri u kojoj vještačka inteligencija (AI) postaje glavni alat i za kreiranje i za zloupotrebu sadržaja, spoj sajber bezbjednosti i medijske pismenosti postaje temelj stabilnog društva. To više nisu odvojene oblasti, već jedinstvena vještina neophodna u savremenom svijetu.

Privatnost na udaru algoritama

Svaki naš klik, pretraga ili „lajk“ ostavlja digitalni trag. Istraživanja pokazuju da je svega nekoliko desetina interakcija na mreži dovoljno da algoritmi precizno procijene naše navike, potrošačke sklonosti i politička uvjerenja. Skandal *Cambridge Analytica*, gdje su podaci miliona korisnika zloupotrijebljeni u političke svrhe bez njihovog pristanka, najbolji je dokaz da smo pod stalnim nadzorom.

Ovi podaci se prvenstveno koriste za personalizaciju sadržaja i reklama, ali isti mehanizmi mogu biti iskorišćeni za manipulaciju javnim mnjenjem. Kada se privatne fotografije, lokacije i kontakti nađu u pogrešnim rukama, rizikujemo sve, od ciljanog marketinga do krađe identiteta.

Kako platforme oblikuju našu stvarnost

Društvene mreže imaju ogroman uticaj na formiranje stavova gdje za preko 60% građana Crne Gore one predstavljaju glavni izvor vijesti. Međutim, algoritmi koji pokreću ove platforme optimizovani su za zadržavanje pažnje, a ne za istinitost.

Sadržaj koji izaziva snažne emocije (bilo pozitivne ili negativne) najbrže se širi. Ako algoritam prepozna da reagujemo na senzacionalizam, serviraće nam još ekstremnije naslove. To stvara tzv. „**echo komore**“ (eho sobe) u kojima nam se neprestano potvrđuju sopstveni stavovi, dok se drugačija mišljenja filtriraju. Interna analiza Facebooka pokazala je da je čak 64% pridruživanja ekstremističkim grupama bilo direktna posljedica preporuka algoritma. U takvom okruženju, korisnici postaju ranjiviji na dezinformacije jer im one djeluju kao potvrda „njihove istine“.

Deepfake i AI: Nova era prevara

Pojavom napredne vještačke inteligencije, manipulacija je ušla u novu fazu. **Deepfake** tehnologija omogućava kreiranje hiperrealističnih video i audio zapisa u kojima stvarne osobe govore ili rade stvari koje se nikada nisu desile.

Opasnosti su višestruke, od **političke destabilizacije** sa lažnim videom ukrajinskog predsjednika Zelenskog iz 2022. godine, u kojem navodno poziva vojsku na predaju, pokazao je kako deepfake može uticati na geopolitičke krize. Zatim preko **finansijske prevare** zabilježeni su slučajevi gdje je AI-klonirani glas direktora kompanije ubijedio zaposlenog da izvrši lažnu uplatu od 243.000 dolara. Ni mladi nisu pošteđeni, čak su posebno ugroženi jer se njihove fotografije mogu koristiti za digitalno nasilje i ucjene.

Crna Gora na meti digitalnih manipulacija

Ni crnogorski digitalni prostor nije pošteđen. Pored kampanja širenja lažnih vijesti koje podrivaju povjerenje u institucije, svjedočimo i sofisticiranim prevarama. Konkretno i opasan primjer je nedavna zloupotreba identiteta ljekara. Prevaranti su pomoću AI alata izmijenili TV intervju poznatog crnogorskog doktora tako da izgleda i zvuči kao da on reklamira sumnjivi medicinski proizvod. Ta lažna vijest plasirana je na sajtu koji je vizuelno kopirao portal RTCG-a, zbog čega su mnogi građani povjerovali i postali žrtve prevare.

Linija odbrane: Kritičko razmišljanje i tehnička zaštita

Tehnička zaštita je važna, ali prva linija odbrane je **kritičko razmišljanje**. U svijetu vještačke inteligencije, princip „ne vjeruj svojim očima“ postaje pravilo.

Kako prepoznati AI manipulaciju?

- **Video:** Obratite pažnju na neprirodno treptanje, pokrete usana koji se ne poklapaju savršeno sa govorom, ili čudne refleksije svjetla.
- **Audio:** Slušajte da li postoje nagli prelazi, robotska monotonija ili potpun nedostatak pozadinskog šuma.
- **Emocija:** Budite sumnjičavi prema sadržaju koji izaziva naglu ljutnju ili strah jer to je često znak manipulacije.

Praktične mjere zaštite:

1. **Zaštita naloga:** Koristite jake, jedinstvene lozinke i obavezno uključite dvostepenu verifikaciju (2FA). To je najefikasnija brana od krađe naloga.

2. **Diskrecija:** Ograničite ko može da vidi vaše objave i profil. Što manje ličnih podataka (datum rođenja, adresa) dijelite javno, to je teže napraviti vaš profil za prevaru.
3. **Provjera izvora:** Ne klikćite na linkove iz sumnjivih poruka („phishing“). Ako dobijete hitan zahtjev za novac od „prijatelja“ ili „direktora“, uvijek provjerite pozivom na broj koji znate.

Zaključak

Digitalna bezbjednost nije luksuz, već građanska dužnost. Vještačka inteligencija donosi revoluciju, ali razumijevanje načina na koji ona funkcioniše daje nam prednost. Udruženim naporima i kroz tehničku zaštitu svojih naloga i kritičku provjeru informacija koje konzumiramo stvaramo bezbjednije okruženje za sebe, svoju porodicu i cijelo društvo.

Ovaj tekst je pisan za sajt medijskapismenost.me u okviru programa Agencije za audiovizuelne medijske usluge. Tekst je moguće preuzimati i dijeliti uz obavezno navođenje izvora.