



**FAKULTET
POLITIČKIH
NAUKA**

UNIVERZITET U SARAJEVU
MCMXLIX

ODSJEK Sigurnosne i mirovne studije

**ALGORITAMSKA PISMENOST
NA UNIVERZITETU U SARAJEVU:
ZAŠTITA PODATAKA I INFOMACIJSKA SIGURNOST
- magistarski rad -**

Kandidatkinja:
Adilović Emina
Broj indeksa: 9-IS/22

Mentor:
prof. dr. Hibert Mario

Sarajevo, oktobar 2023. godine

Sadržaj

Uvod	4
1. Medijska, informacijska i algoritamska pismenost	6
1.1. Medijska i informacijska pismenost na Univerzitetu u Sarajevu	9
1.1.1. Naučnoistraživačka platforma i holistički pristup.....	10
1.1.2. MOOC budućnosti – algoritmi, umjetna inteligencija i sigurnost	13
1.2. Od cyberpismenosti do algoritamske pismenosti	14
1.2.1. Konvergencija algoritamske pismenosti i informacijske sigurnosti	16
2. Informacijska sigurnost	18
2.1. Informacijska sigurnost na Univerzitetu u Sarajevu	21
2.2. Propisi i standardi informacijske sigurnosti	23
2.2.1. Standard ISO 27001 – tranzicija upravljanja sigurnosti informacija	25
2.3. Mjere informacijske sigurnosti u algoritamskom okruženju	28
2.3.1. Mjerenje i primjeri dobre prakse.....	29
3. Metodološki okvir	30
3.1. Ciljevi istraživanja	31
3.2. Način istraživanja	31
3.2.1. Odabir uzorka.....	32
3.2.2. Priprema i instrumenti istraživanja	34
3.2.3. Vremensko i prostorno određenje istraživanja.....	36
4. Kvalitativne analize istraživanja	37
4.1. Algoritamska pismenost u MIP kontekstu	40
4.1.1. Mediji i informacije u odnosu konvergencije i divergencije.....	40
4.1.2. Predodžbe algoritamske pismenosti	42
4.2. Obrazovanje i iskustvo	43
4.2.1. Edukacije i kursevi.....	44
4.2.2. MOOC i moduli IX i X.....	45
4.3. Utjecaj platformi i društvenih mreža	47
4.3.1. Rezičnacija i indignacija.....	48
4.3.2. Generacijski i digitalni jaz	49
4.4. Personalizacija sadržaja	50
4.4.1. Prikupljanje zvučnih podataka	52
4.4.2. Tehnokapital i manipulacije.....	53
4.5. Privatnost i sigurnost	54
4.5.1. Zaštita podataka i povjerljivost informacija.....	55
4.5.2. Algoritamska pismenost za informacijsku sigurnost	56

4.6. Krićka svijest i (samo)regulacije	58
4.6.1. Ogranićavanje personalizacije i mjere zaštite	58
4.6.2. Regulacije i usklaćenost.....	60
5. Diskusija rezultata	62
5.1. Predodžbe pismenosti i algoritamska iskustva.....	62
5.2. Odnosi i uslovljenosti.....	63
5.3. Algoritamska budućnost i sigurnosne mogućnosti.....	64
Zaključak	66
Literatura.....	67
IZJAVA O AUTENTIĆNOSTI RADOVA.....	75

Algoritamska pismenost na Univerzitetu u Sarajevu: zaštita podataka i informacijska sigurnost

Emina Adilović

Sažetak:

Umjesto jednostranog stjecanja vještina za sudjelovanje u automatiziranim procesima, algoritamska pismenost obuhvata skup znanja, vještina i vrijednosti, omogućavajući pojedincima prepoznavanje algoritamskih procesa i upotrebu tehnologija umjetne inteligencije, njihove primjene i kritičku procjenu nevidljive infrastrukture. Ovo istraživanje ima za cilj ispitati razinu algoritamske pismenosti među studentima i osobljem Fakulteta političkih nauka i Filozofskog fakulteta Univerziteta u Sarajevu, analizirati kako studenti, nastavno i nenastavno osoblje vide odnos informacijske sigurnosti, zaštite podataka i algoritamske pismenosti, te procijeniti mogućnosti unapređenja dosadašnjih praksi algoritamske pismenosti na Univerzitetu u Sarajevu. Analiza rezultata dobivenih kroz intervjuje sa ciljnim skupinama pruža dublji uvid u percepciju automatiziranog donošenja odluka, iskustva personalizacije informacija i zaštite podataka te perspektive kako umjetna inteligencija utječe na podučavanje i učenje studenata, rad akademskog osoblja i obrazovne procese općenito. Rezultati istraživanja pružaju uvide u potencijal razvijanja postojećih obrazovnih resursa za podršku algoritamskoj pismenosti.

Ključne riječi: Univerzitet u Sarajevu, medijska i informacijska pismenost, algoritmi, sigurnosne mjere, personalizacija sadržaja, prikupljanje podataka, predodžbe i iskustva

Uvod

Imajući u vidu relevantnost medijske i informacijske pismenosti u kontekstu digitalnog učenja i potencijalnih sigurnosnih rizika vezanih za uticaj algoritama na procese donošenja odluka u podatkovnom društvu, ova master tema istražuje važnost algoritamske pismenosti, zaštite podataka i informacijske sigurnosti na Univerzitetu u Sarajevu. Činjenica da sigurnosne specifičnosti algoritamskih implikacija u postdigitalnom dobu nisu nova idejna okosnica, stavlja akcent na potrebu za kontinuiranim praćenjem društvenih, kulturoloških i komunikoloških aspekata u promjenjivom tehnološkom okruženju, a predstavljajući neizostavnu granu digitalne pismenosti, ovakav pristup ne želi skrenuti pažnju samo na tehničke sposobnosti koje nisu dovoljne za kretanje i snalaženje u umreženom prostoru. Umjesto jednostranog sticanja sposobnosti sudjelovanja u automatiziranim procesima, algoritamska pismenost obuhvata složeniji skup znanja, vještina i vrijednosti prepoznavanja algoritamskih procesa u svakodnevnom korištenju tehnologija umjetne inteligencije, njihove primjene i kritičkog vrednovanja nevidljive infrastrukture kroz procjenu objektivnosti, pravednosti i pouzdanosti mašinskog upravljanja i kreiranja podataka.

Nakon uvida u temu istraživanja, razloge za njen odabir i idejna polazišta, način na koji će biti obrađena i strukturu rada, slijedi teorijski okvir koji obuhvata relevantnu literaturu – istraživanja i primjere dobre prakse iz područja medijske, informacijske i algoritamske pismenosti, te zaštite podataka i propisa koji se odnose na informacijsku sigurnost. Prvo poglavlje posvećeno je medijskoj i informacijskoj pismenosti te algoritamskoj pismenosti kao posebnoj podkategoriji. Zatim će biti obrađena informacijska sigurnost, s naglaskom na zaštitu podataka i algoritme. Ova tema će biti obrađena kroz teorijski okvir koji obuhvata različite aspekte medijske i informacijske pismenosti, s posebnim osvrtom na primjere dobre prakse u kontekstu Univerziteta u Sarajevu i razmatranje integracije algoritamske pismenosti u obrazovni proces s fokusom na informacijsku sigurnost.

Informacijska sigurnost u kontekstu algoritamske pismenosti odnosi se na zaštitu podataka i osiguranje da se algoritamski procesi primjenjuju tako da podržavaju sigurnost informacija uključujući mjere i prakse koje su usmjerene na sprečavanje neovlaštenog pristupa, otkrivanje i sprečavanje sigurnosnih prijetnji te osiguravanje povjerljivosti, integriteta i dostupnosti podataka. Integracija i razvoj algoritamske pismenosti za informacijsku sigurnost omogućava razumijevanje kompleksnog mašinskog učenja, a algoritamski pismene osobe imaju sposobnost prepoznati potencijalne sigurnosne rizike i razumjeti mehanizme zaštite

podataka u tim procesima. Nadalje, bit će analizirani propisi i norme koji se odnose na informacijsku sigurnost, posebno uzimajući u obzir ISO 27001 standard, kao i mjere informacijske sigurnosti u algoritamskom okruženju.

Nakon pregleda relevantne literature koja nudi teorijski okvir i kontekst integracije algoritamske pismenosti za razvoj informacijske sigurnosti na Univerzitetu u Sarajevu, slijedi poglavlje o metodologiji istraživanja koje obuhvata odabir uzorka, instrumente prikupljanja podataka i proceduru ispitivanja. Metodologija se zasniva se na uvidima, istraživačkom okviru i strukturi grupnih diskusija sa studentima u okviru Projekta informacijske pismenosti (PIL) te prema istraživanju algoritamske pismenosti provedenom na Harvard Graduate School of Education. U fokusu dijela rada koji se bavi analizom izazova, prepreka i potreba studenata, biće ispitani studenti organizacione jedinice Univerziteta u Sarajevu – Fakulteta političkih nauka kao reprezentativni uzorak u pilot ispitivanju. Uzimajući u obzir da su područja političkih, komunikoloških, socioloških, sigurnosnih i mirovnih nauka koje se izučavaju na Fakultetu političkih nauka u uskoj vezi sa algoritamskim amplifikacijama jer se umjetna inteligencija koristi u političkom odlučivanju, komunikacijskim platformama, analizi društvenih mreža, sigurnosnim sistemima drugim područjima relevantnim za pomenute discipline, u istraživanju se koristi tehnika fokus grupa sa studentima Fakulteta političkih nauka kako bi se procijenila njihova razinu algoritamske pismenosti, svijest o zaštiti podataka i informacijskoj sigurnosti.

Potom slijedi analiza izazova, prepreka i potreba studenata u vezi s informacijskom sigurnošću i algoritamskom pismošću te diskusija koja će raspravljati o dobivenim rezultatima istraživanja, prednostima, nedostacima i mogućnostima unapređenja. Rezultati rada nastojat će ukazati na važnost upravljanja rizicima i usklađenosti s propisima u području informacijske sigurnosti – razvijanje algoritamske pismenosti među studentima otvara prostor za bolje razumijevanje tehnoloških alata i procesa koji se koriste u obradi podataka i znanja o potencijalnim rizicima i mjerama zaštite, te pruža osnovu za implementaciju efikasnih obrazovnih programa i politika za zaštitu podataka i informacijsku sigurnost na univerzitetima i drugim obrazovnim institucijama. Integracija algoritamske pismenosti u obrazovni proces može pružiti studentima neophodne vještine i znanja koja će im pomoći u njihovoj budućoj karijeri, bilo da se bave istraživanjem, upravljanjem informacijskom sigurnošću ili razvojem tehnoloških rješenja. Kroz kritički osvrt na postojeće prakse i analizu rezultata, uvidi mogu biti korišteni i na drugim obrazovnim institucijama i organizacijama koje se bave zaštitom

podataka i informacijskom sigurnošću, te poslužiti kao polazište za opširniju evaluaciju i istraživačku analizu na nivou drugih organizacionih jedinica Univerziteta u Sarajevu.

1. Medijska, informacijska i algoritamska pismenost

Ako se vratimo na primarne razloge za promišljanje objedinjenog koncepta medijske i informacijske pismenosti, uočavamo da je nastao iz potrebe da se tradicionalni model medijske pismenosti koji se razvijao kao odgovor na rastući utjecaj medija u društvu, objedini sa zahtjevima digitalne sfere. Područja medijskih studija dolaze u dodir sa informacijskim naukama – razumijevanje informacijskih izvora, istraživanje, analiza podataka, razlikovanje relevantnih informacija te razvijanje kritičke informacijske pismenosti prožima se sa razumijevanjem i analizom medijskih poruka, prepoznavanjem tehnika manipulacije i razvijanjem kritičkog razmišljanja u kontekstu medijske kulture.

Objašnjavajući genezu pojedinačnih pojmova i nastanak objedinjenog koncepta, autori (Carlsson 2019; Wilson et al. 2011) izdvajaju UNESCO inicijativu iz 2007. godine, preporuku korištenja termina „medijska i informacijska pismenost“ i utjecaj dva faktora na uvođenje nove terminologije: temeljne promjene u razumijevanju medija kao rezultat digitalizacije, i proširenje UNESCO-ovog rada u oblasti društava znanja i slobode. Ovakve postavke posredovanja digitalnih platformi u razmjeni informacija, usluga i resursa pokazuju odlike „platformskog društva“ (Castells 1996; Van Dijck, Poell i De Wall 2018) koje zahtjeva primjenu modela razvoja medijske i informacijske pismenosti u odnosima između građana, država i tehnoloških kompanija. Iako novo digitalno okruženje teži platformskoj objedinjenosti ljudskih aktivnosti i djelovanja, potrebno je u nastavku promišljanja medijske i informacijske pristupiti suprotno – težiti razumijevanju pojedinačnih pojmova, različitih područja i koncepta unutar šireg okvira kako bi se kasnije sagledao značaj algoritamske pismenosti ne zanemarujući pritom kritički uklon algoritamskog društva koje donosi objedinjeni MIP koncept.

Standardiziranje objedinjenog koncepta za daljnji razvoj i primjenu u praksi implicira potrebu za njihovim detaljnijim objašnjenjem. Pojedina nastojanja za određivanjem razlika idu u oba pravca konvergencije, kada je medijska pismenost shvaćena kao širi okvir, ili kada je informacijska pismenost glavno polje istraživanja (Silajdžić 2021). Drugi tipovi razlikovanja polaze od područja istraživanja (Terra 2023; Lee i So 2014) fokusirajući se na to da je informacijska pismenost inherentna bibliotekskim i informacijskim znanostima, dok je medijska pismenost dio komunikoloških studija. Autori knjige *Medijska i informacijska pismenost:*

dizajn učenja za digitalno doba (2021) jedinstvenost također baziraju primarno na usmjerenosti: „razlika je prvenstveno u tome da se informacijska pismenost najčešće upotrebljava u kontekstu obrazovanja (istraživanja, nauke), dok je medijska pismenost upućena na šire građanske kompetencije“ (14).

Daljnje raščlanjivanje prema namjeni nije svrha samo sebi, već služi identificiranju postojećih pismenosti koje strateški razvoj treba uključiti i konsolidirati. Tako UNESCO (2013) navodi različite termine: „medijska pismenost, informacijska pismenost, pismenost za slobodu izražavanja i informacije, bibliotečka pismenost, žurnalistička pismenost, računarska pismenost, internetska pismenost, filmska pismenost, pismenost za računalne igre, televizijska pismenost, reklamna pismenost, digitalna pismenost i metapismenost“ (13). Među različitim oblicima srodnih i pripadajućih oblika pismenosti, digitalna pismenost se „pogrešno (sinonimno) koristi za medijsku i informacijsku (pismenost)“ (Vajzović et al 2021, 115). Nastojanja za ovladavanjem tehničkim i tehnološkim vještinama i alatima – dostatnim metodama za snalaženje u digitalnom okruženju – izvedena su iz gledišta *tehnološkogolucionizma*. Predstavljajući naizgled alternativu za društvena previranja, tehnologija djeluje na dva nivoa – utječe na sposobnost *dubokog* razmišljanja (Carr 2010) svakog pojedinca i istovremeno djeluje masovno jer oblikuje javno mnijenje u digitalnoj javnoj sferi (Tufekci 2017), ne proizvodeći pritom često značajan angažman koji bi vodio ka pozitivnom ishodu.

Ukoliko je shvatanje medijske i informacijske pismenosti naglašeno fokusirano na digitalne kompetencije, zanemaruje se širi spektar vještina i znanja koji je potreban za razumijevanje, interpretaciju i kritičko promišljanje. Sinonimna upotreba digitalne pismenosti je redukcionistička ako se ima u vidu da zanemaruje dvije dimenzije koncepta medijske i informacijske pismenosti koji „obuhvata tri često jasno razdvojene dimenzije: informacijsku pismenost, medijsku pismenost i IKT/digitalnu pismenost.“ (Vijeće Evrope 2023). Konsolidirana upotreba ovih dimenzija fokusira na kritičko razmišljanje, etičke dileme, snalaženje u medijskim i informacijskim sistemima i utjecaj platformskog okruženja na pojedince i društvo i tako prevazilazi tehničke vještine naglašavajući razvoj kritičkih i analitičkih sposobnosti. Razmatranje i objašnjavanje pojedinih aspekata medijske i informacijske pismenosti može pomoći u boljem razumijevanju i valoriziranju pojma algoritamske pismenosti koji zahtijeva detaljnije razmatranje i definiranje.

Drugim riječima, iako se radi o povezanim konceptima, podjednako je pogrešno izjednačavati digitalnu i algoritamsku pismenost – potonja je usmjerena ka kritičkom

razmišljanju o načinima na koje algoritmi oblikuju i filtriraju informacije te kako nevidljiva struktura savremenih informacijsko-komunikacijskih tehnologija utječe na donošenje odluka, dok se digitalna pismenost odnosi uglavnom na skup vještina korištenja digitalnih tehnologija i alata. Ukoliko se algoritamska pismenost posmatra kao posebna oblast medijske i informacijske pismenosti, integrira cijeli niz kompetencija poput kritičkog mišljenja, usmjerenosti na društvo i dubinskog istraživanja, a “one su utoliko ključne, ne samo za pojedinca nego i društvo i zajednicu u cjelini, čiji je interes da se sastoji od mislećih individua koje su sposobne da kreiraju bolje medijsko i društveno okruženje“ (Turčilo 2020, 32).

Ukoliko interakciju sa algoritmima ne svedemo na praktikovanje u privatnoj sferi kroz njihovo *prilagodavanje* kako bismo suzili rezultate svakodnevne pretrage pojmova na Google-u, ovom fenomenu moguće je pristupiti masovnije i sistemski. Razlikovanje digitalne i algoritamske pismenosti može imati šire implikacije ukoliko se primijeni u procesu kreiranja obrazovnih politika koje ne odbacuju konkretniji aspekt utjecaja algoritama na privatnost, sigurnost podataka i slobodu izražavanja. Takav pristup razvijanja integriranog modela medijske i informacijske pismenosti pojavljuje se u UNESCO kurikulumu za nastavnike (2011) koji je odigrao značajnu ulogu u promociji medijskog i informacijskog obrazovanja i njegovom integriranju u nacionalne obrazovne programe (Mansoor 2023).

U ovom kontekstu, prilikom razvijanja obrazovnih politika i programa za medijsku, informacijsku i algoritamsku pismenost, ključno je premjestiti fokus s usmjerenosti na sadržaj na polaznike. (Turčilo 2020). Odnosno, treba postaviti pojedinca u središte pažnje, razmatrajući ga kao jedinstvenu osobu s posebnim potrebama i prirodnom sklonosti prema informacijama, koje je potrebno prepoznati i poboljšati, te sagledati ga kao aktivnog člana društvene zajednice čije sposobnosti treba jačati u različitim aspektima društvene komunikacije. Upravo je ova promjena perspektive na individualne potrebe i kompetencije postala ključna u oblikovanju obrazovnih programa za medijsku, informacijsku i algoritamsku pismenost diljem svijeta. Nakon 2011. godine, UNESCO-ov kurikulum za ove oblike pismenosti postao je izuzetno važan smjernica posluživši kao temelj za razvoj obrazovnih politika koje promiču razumijevanje medija, informacija i algoritama na individualnoj razini, pridonoseći tako boljem obrazovanju i informiranju građana u digitalnom dobu.

1.1. Medijska i informacijska pismenost na Univerzitetu u Sarajevu

Prepoznavši značaj UNESCO kurikuluma za nastavnike (2011) u kontekstu razvoja obrazovnih politika usmjerenih na digitalnu transformaciju društva, te potrebu za njegovim prilagođavanjem bosanskohercegovačkom kontekstu i osavremenjivanjem shodno promjenama nastalim tokom decenijskog vremenskog otklona, Institut za društvena istraživanja Fakulteta političkih nauka Univerziteta u Sarajevu od 2017. godine radi na strateškom naučnoistraživački zasnovanom razvoju i unapređenju medijske i informacijske pismenosti. U partnerstvu sa drugim javnim univerzitetima u Bosni i Hercegovini, Univerzitet u Sarajevu na ovaj način razvija naučnoistraživačku platformu (Vajzović, Hibert i Adilović 2023) s ciljem definiranja procesa, unapređenja koncepta i kreiranje rezultata koji daju izvodljiv i održiv koncept za inovacije u široj multidimenzionalnoj i specifičnoj antidisciplinarnoj oblasti funkcionalne pismenosti.

Iako u Bosni i Hercegovini nije uveden sistemski pristup i dugoročna strategija za integraciju medijske i informacijske pismenosti u obrazovni sistem (Hodžić 2019, 15), u posljednjih pet godina primijećen je pomak na nivou pojedinih kantona i manjih organizacionih jedinica. Uopće razmatranju prilagođavanja obrazovnih politika zahtjevima digitalnog okruženja doprinijela su višegodišnja istraživanja, analize stanja te preporuke u knjigama, zbornicima, izvještajima i studijama¹, pružajući pionirske uvide u trenutno stanje, te pomažu donositeljima politika i obrazovnim institucijama da razvijaju strategije koje će bolje odgovoriti na izazove digitalnog doba. Naslanjajući se na publikacije koje ovom konceptu pristupaju iz šire

¹ U knjizi "Medijska i informacijska pismenost: istraživanje i razvoj" (2020), izdvojene su i pobrojane do sada najznačajnije publikacije koje se tiču stanja i perspektiva medijske i informacijske pismenosti u Bosni i Hercegovini: zbornik „Medijska pismenost i civilno društvo“ (Zgrabljić-Rotar 2006), udžbenik „Informacijska pismenost: smjernice za razvoj inovativnih mrežnih modula“ (Dizdar et al. 2012), „Medijska kultura i medijska pismenost“ (Rašević 2014), zbornik „Medijska pismenost – preduvjet za odgovorne medije“ (Car et al. 2015), studija „Mladi, politika i mediji: priručnik za razvijanje političke i medijske pismenosti mladih“ (Turčilo et al. 2017), „Media Literacy and Education: needs of journalists and the public in Bosnia and Herzegovina“ (Halilović et al 2017), „Mediji ishrinking space: utišani alternativni Medijska i informacijska pismenost: Istraživanje i razvoj 48 glasovi“ (Turčilo i Buljubašić 2017), „Konceptualni okvir medijske pismenosti“ (Trninić, 2017), priručnik „Prevenција vršnjačkog i rodno zasnovanog nasilja u školi: Jačanje partnerstva nastavnika i roditelja“ (Šuta-Hibert 2017), „Informacijsko društvo i demokratija: građanska pismenost za digitalno doba“ (Vajzović 2017), „Pregledna studija o politikama i strategijama medijske i informacijske pismenosti u Bosni i Hercegovini“ (Vajzović et al. 2018; 2020), knjiga „Medijska pismenost vs. političke manipulacije“ (Hadžialić 2018), „Priručnik za trenere iz oblasti medijske i informacijske pismenosti“ (Janjić i Dekić 2019), „Medijska i informacijska pismenost u Bosni i Hercegovini: brojne inicijative civilnog sektora i nedostatak javnih politika“ (Hodžić, Petković i Bašić 2019), „Medijsko opismenjavanje u porodici i preporuke za implementaciju projekata unapređenja medijske pismenosti u okviru porodice u Bosni i Hercegovini“ (Čengić 2019); „Medijska i informacijska pismenost u sistemu cyber sigurnosti“ (Vajzović 2019); „Uvođenje medijske i informacijske pismenosti u obrazovni sistem – procjena kompetencija nastavnika za podučavanje medijske i informacijske pismenosti u Kantonu Sarajevo.“ (Vajzović et al. 2019); „Digitalni odrast i postdigitalna dobra“ (Hibert 2019).

perspektive, značajno je izdvojiti i naučnoistraživačke napore u području integracije MIP koncepta u obrazovni sistem.

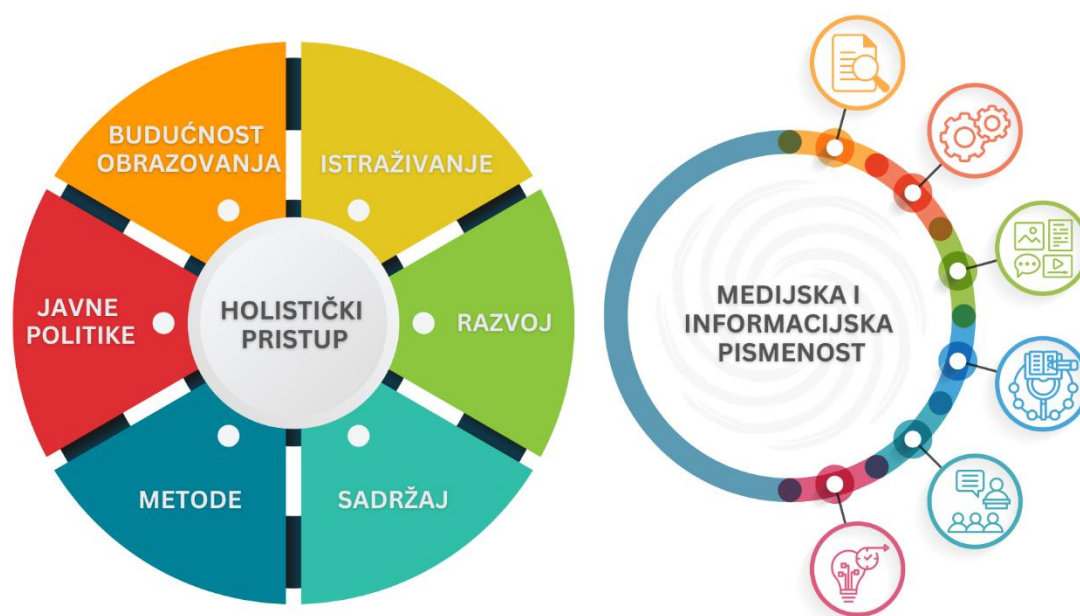
Dvije godine nakon izdavanja UNESCO kurikulomom za nastavnike, Lea Tajić 2013. godine analizira prikaz postojećeg stanja koncepta medijske pismenosti u kontekstu Bosne i Hercegovine, a Dizdar i Hajdarpašić (2014) ističu važnost promjene modela učenja u digitalnom dobu i razvoj informacijske pismenosti na Univerzitetu u Sarajevu. Potom Dizdar, Khattab i Grebović-Lendo (2016) ukazuju na ulogu bibliotekara u razvoju informacijske pismenosti i tako fokusiraju priču o razvoju na konkretne uloge koje učesnici obrazovnog procesa trebaju preuzeti kako bi MIP koncept *zaživio* u učionici. Rašidović (2016) nastavlja promišljati način integracije u obrazovni sistem, s akcentom na analizu izbornog predmeta informacijske pismenosti na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu.

Fokusirajući se također na položaj i funkciju medijske i informacijske pismenosti na visokoškolskim ustanovama, Hajdarpašić i Khattab (2019) istražuju kompetencije informacijske pismenosti studenata na Odsjeku za komparativnu književnost i bibliotekarstvo Filozofskog fakulteta Univerziteta u Sarajevu. S druge strane, Silajdžić (2020) proučava vještine medijske i informacijske pismenosti studenata Odsjeka za komunikologiju Fakulteta političkih nauka Univerziteta u Sarajevu. Zapravo, prepoznavši zajedničko interesno polje, sistemski pristup započinje suradnjom dvije organizacione jedinice Univerziteta u Sarajevu, Filozofskog fakulteta i Fakulteta političkih nauka (Vajzović, Hibert i Adilović 2023). Uspostavljanje radnih timova koje su činili istraživači sa Katedre za informacijske nauke i različitih odsjeka Fakulteta političkih nauka rezultiralo je omogućavanjem uslova za prikaz sveobuhvatnijeg uvida kroz holistički pristup.

1.1.1. Naučnoistraživačka platforma i holistički pristup

S obzirom da su početni naučno-akademski naponi propitivanja prakse integralnog koncepta medijske i informacijske pismenosti na Univerzitetu u Sarajevu ukazali na nedostatak detaljne i koherentne istraživačke baze, manjak literature na regionalnim jezicima te pedagoško-metodičke nejasnoće na polju metoda neophodnih za primjenu MIP-a, prvi naredni korak podrazumijevao je osmišljavanje holističkog pristupa za uspostavljanje

naučnoistraživačke platforme. Shvaćen kao PDCA ciklus², ovaj holistički pristup obuhvata šest ključnih koraka koji se kontinuirano ponavljaju u procesu. Počevši s istraživanjem trenutnog stanja, ovaj model dalje objedinjava 2. razvoj strategija, 3. kreiranje relevantnih sadržaja, 4. primjenu odgovarajućih metoda, 5. usklađivanje s javnim politikama i 6. promišljanje o budućnosti obrazovanja i medijske informacijske pismenosti.



Ilustracija 1: Shema holističkog pristupa medijskoj i informacijskoj pismenosti Instituta za društvena istraživanja Fakulteta političkih nauka Univerziteta u Sarajevu

Primjena hibridnog modela višekomponentne integracije³ koji podržava provođenje svih elemenata ciklusa na horizontalnoj i vertikalnoj razini⁴ zamišljena je s ciljem provođenja holističkog pristupa koji se oslikava u tri komponente: (1) Hibridni model višekomponentne integracije MIP-a; (2) Razvoj javnih politika i strateškog okvira MIP-a; (3) Istraživanje i razvoj MIP-a. (Vajzović 2021, 32). Ovako postavljen holistički pristup ne samo da omogućava provođenje svih ključnih koraka u razvoju i integraciji medijske i informacijske pismenosti, već istovremeno osigurava da se komponente međusobno dopunjuju i naglašavaju. Istraživački

² PDCA ciklus, također poznat kao Demingov ciklus ili ciklus kontinuiranog poboljšanja, je konceptualni model koji se koristi za postizanje kontinuiranog unapređenja u organizacijama. Ovaj ciklus se sastoji od četiri faze: 1. Planiranje (engl. Plan), 2. Izvršavanje (engl. Do), 3. Provjera (engl. Check) i 4. Djelovanje (engl. Act).

³ Jedinstveni inkluzivni model koji razvija Institut za društvena istraživanja Fakulteta političkih nauka Univerziteta u Sarajevu od 2017. godine (Vajzović 2020, 13).

⁴ Vertikalna integracija podrazumijeva razvoj istraživanja, nauke i cjeloživotno obrazovanje nastavnika, te Horizontalna integracija podrazumijeva kroskurikularnu saradnju nastavnika i bibliotekara u okviru nastavnih programa i planova, te ishoda učenja (Vajzović 2021).

element iznjedrio je niz strateških dokumenata poput preglednih i pozicijskih studija⁵, te Deklaraciju o značaju medijske i informacijske pismenosti (2019), dok sadržaj uključuje publikacije⁶ i programe obuka nastavnika, bibliotekara i učenika.

Sljedeći element holističkog pristupa čine javne politike: na temelju postojećih studija i strateških dokumenata Radna grupa izradila je Strategiju razvoja medijske i informacijske pismenosti u oblasti obrazovanja u Kantonu Sarajevu koja je 2022. godine usvojena na sjednici Vlade Kantona Sarajeva. Prepoznavajući specifičnosti umreženog okruženja, Strategija uzima u obzir „izazov primjene, kako metoda digitalnog učenja, tako i upoznavanja sa gorućim pitanjima koja se tiču algoritamskih društvenih interakcija o kojima malo ili nedovoljno znamo“ (Vlada Kantona Sarajeva 2022, 8). Nadovezujući se na prethodnu kariku holističkog pristupa, šesti element pokušava osvijetliti *malo ili nedovoljno*. Drugim riječima, element *budućnost obrazovanja*, usmjerava se prema kritičkoj medijskoj i informacijskoj pismenosti ne samo zbog toga što se „sakupljanje podataka dešava nevidljivo i neprestano“ (Head, Fister i MacMillan 2020, 5), već i zbog toga što interakcije bazirane na algoritmima zahtijevaju aktualiziranje informacijskih zajedničkih dobara (engl. information commons). Elementi holističkog modela proizlaze iz ideje zajedničkog dobra ako je primarna svrha univerzitetske naučnoistraživačke platforme olakšavanje istraživanja i generiranja znanja putem raznolikog i dijeljenog znanja (Huskić, Vajzović i Hibert 2022). Tako se narativ o budućnosti obrazovanja nadovezuje na četvrti element, *metode*, odnosno, moduse potrebnog djelovanja. Govoreći o metodama, značajno je izdvojiti masovni otvoreni online kurs⁷ (engl. MOOC – Massive Open Online Course) medijske i informacijske pismenosti koji je razvio Fakultet političkih nauka Univerziteta u Sarajevu uz podršku UNESCO-a i Evropske unije.

⁵ Okupivši različite sektore u Bosni i Hercegovini, zaključci nacionalnih konsultacija ukazali su na potrebu za strateškim pristupom koji je započeo s Preglednom i Pozicijskom studijom koje su analizirale politike i strategije vezane za medijsku i informacijsku pismenost. Pregledna studija prikazala je postojeće politike, dok se Pozicijska studija temeljila na prikupljenim podacima te konsultacijama, radionicama i literaturi kako bi ponudila pet ključnih preporuka: „kreiranje nacionalne strategije za razvoj medijske i informacijske pismenosti, određivanje javnog tijela za koordinaciju implementacije politika u ovoj oblasti, usklađivanje formalnog obrazovanja s ciljevima medijske i informacijske pismenosti, razvoj u kontekstu neformalnog i cjeloživotnog učenja te jačanje uloge biblioteka“ (2018).

⁶ Edicija Medijska i informacijska pismenost sastoji se od četiri publikacije: „Medijska i informacijska pismenost: istraživanje i razvoj“ (2020), Medijska i informacijska pismenost: dizajn učenja za digitalno doba“ (2021), „Regionalni osvrt na razvoj i integraciju medijske i informacijske pismenosti“ (2021), „Odrastanje učenja: društvo, kultura, religija u digitalnom dobu“ (2021).

⁷ Masivno otvoreni online kurs medijske i informacijske pismenosti. 2023. Univerzitet u Sarajevu – Fakultet političkih nauka. www.mip.unsa.ba. Pristupljeno 12. septembra. 2023.

1.1.2. MOOC budućnosti – algoritmi, umjetna inteligencija i sigurnost

Neke od ključnih karakteristika MOOC-ova čine njihova skalabilnost zbog mogućnosti da istovremeno prime veliki broj polaznika kursa, čime obrazovanje postaje dostupno globalnoj publici; podržavaju načela pokreta za „otvoreno obrazovanje“ i promoviraju cjeloživotno učenje podržavajući kontinuirano obrazovanje i razvijanje profesionalnih vještina (Sinclair et al. 2015). Stoga MOOC medijske i informacijske pismenosti, omogućava dva načina pohađanja kursa, *self-paced* i *fixed-paced*⁸. Dvanaest modula sadržaja MOOC-a⁹ nastali su na osnovu prilagođenog materijala UNESCO kurikuluma za nastavnike (2011). Prožimanje uslovljava gradaciju kompleksnosti tema, pa tako IX modul tematizira ishodišta umjetne inteligencije te utjecaj i posljedice djelovanja algoritama, a X modul sigurnosni aspekt informacijske, medijske i algoritamske pismenosti.

Činjenica da nakon algoritamske pismenosti i informacijske sigurnosti slijedi modul *Pismenost budućnosti*, ukazuje na zrcaljenje međusobno prožimajućih elemenata makrostrukture holističkog pristupa u specifičnim metodama, u ovome slučaju, mikrostrukтури informacijskog zajedničkog dobra, masivno otvorenom online kursu. Pri tome, IX i X moduli prizivaju u fokus istraživanja detaljnije objašnjenje – prakse praćenja u algoritamskom društvu „postale sve češće i naprednije, postalo je hitno razumjeti kako ovi računarski programi funkcionišu i imaju širok uticaj. Kako studenti razumiju skrivene filtere koji utječu na ono što vide i uče, te oblikuju njihovo razmišljanje i identitet“ (Head, Fister i MacMillan, 13). Stoga će kasnija analiza rezultata posebno tematizirati mogućnosti modula IX i X u kontekstu integracije detaljnijih pristupa i reorganizaciji odgovarajućih sadržaja.

Algoritamska pismenost nije dovoljno složena oblast i nužno fokusirana perspektiva unutar šireg okvira medijske i informacijske pismenosti zbog aktualnosti razgovornih modela umjetne inteligencije¹⁰, već iz potrebe da se postojeće metode poput MOOC-a nastave razvijati

⁸ *Self-paced* način pohađanja MOOC-a je pristup koji omogućava polaznicima da sami određuju tempo učenja. U ovom režimu, polaznici MOOC-a imaju fleksibilnost da pristupe materijalima kada im to odgovara i da napreduju prema vlastitom rasporedu bez unaprijed postavljenih rokova. S druge strane, *fixed-paced* u kontekstu ovog MOOC-a podrazumijeva pohađanje u sklopu nastavnih i grupnih aktivnosti ujednačenim i unaprijed postavljenim rasporedom i zajedno sa predavačima.

⁹ 1. Razumijevanje medijske i informacijske pismenosti; 2. Informacijsko društvo, ljudska prava i demokratski diskurs; 3. Informacijska pismenost i etika; 4. Društvena uloga medija; 5. Kreiranje medijskih poruka; 6. Korisnička interakcija sa medijima; 7. Internet, izazovi i prilike; 8. Digitalna ekologija i “pametno” selo; 9. Podaci, algoritmi i umjetna inteligencija: pismenost za 21. vijek; 10. Medijska i informacijska pismenost u kontekstu sigurnosti; 11. Kritičko mišljenje; 12. Pismenost budućnosti

¹⁰ Razgovorni modeli umjetne inteligencije su programi ili softveri dizajnirani za komunikaciju s ljudima ili drugim računarima koristeći se tehnikama obrade prirodnog jezika (engl. Natural Language Processing - NLP)

kako bi unaprijedili sposobnost pojedinca za razumijevanje, analiziranje i kritičku procjenu u svakodnevnim aktivnostima, učenju i istraživanju – kako zapravo algoritmi funkcionišu, utječu na informacije koje konzumiraju i kako oblikuju njihovo digitalno iskustvo. Ovako shvaćena, ovaj oblik pismenosti (treba da) ide dalje od jednostavnog razumijevanja tehničkih aspekata algoritama i istražuje njihov društveni, kulturni i politički uticaj.

1.2. Od cyberpismenosti do algoritamske pismenosti

U pokušajima da se odredi spram MIP koncepta, lako se zanemaruje drugi ugao posmatranja algoritamske pismenosti – onaj koji polazi od koncepta metapismenosti.¹¹ Razvijajući teorijski okvir razumijevanja i praktičnom primjenom vještina pismenosti u digitalnom dobu, Tom Mackey i Trudi E. Jacobson u modelu metapismenosti preformulisali su pismenost informacija kao metapismenost, „proširujući model kako bi obuhvatio proizvodnju i dijeljenje znanja putem društvenih medija i online zajednica“ (Magnuson 2015). Metapismenost se razlikuje od tradicionalnih pedagoških pristupa naglašavanjem saradničke proizvodnje i dijeljenjem informacija jer se učenici potiču da aktivno učestvuju u stvaranju sadržaja, razmjene ideja i komuniciraju sa drugima u online zajednicama s ciljem razvijanja kritičkog razmišljanja, analitičkih vještina i sposobnosti evaluacije.

U članku „Reframing Information Literacy as a Metaliteracy“ (2010), Jacobson i Mackey ističu važnost razumijevanja utjecaja tehnologije na način pristupanja informacijama te podsjećajući na pojedine oblike pismenosti¹², ističu i *cyberpismenost*. Premda dijeli etička stajališta sa informacijskom pismenošću kada je riječ o prevazilaženju dosega tradicionalne računalne/tehničke pismenosti, cyberpismenost je specifičnije povezana s participativnom internet kulturom (Jacobson i Mackey 2010). Počevši od „edukativnih cybersfera“ (Kenway i Nixon 1999), pa do 2011. i *prelaznih godina*¹³ tehnološkog razvoja, konceptualni okvir *cyberpismenosti* pojavljuje se kao preteča algoritamske pismenosti danas.

kako bi razumjeli i generirali ljudski jezik. Najpoznatiji primjeri razgovornih modela su *chatbotovi* ili virtualni asistenti koji se koriste za korisničku podršku, automatizaciju zadataka i personalizaciju iskustva.

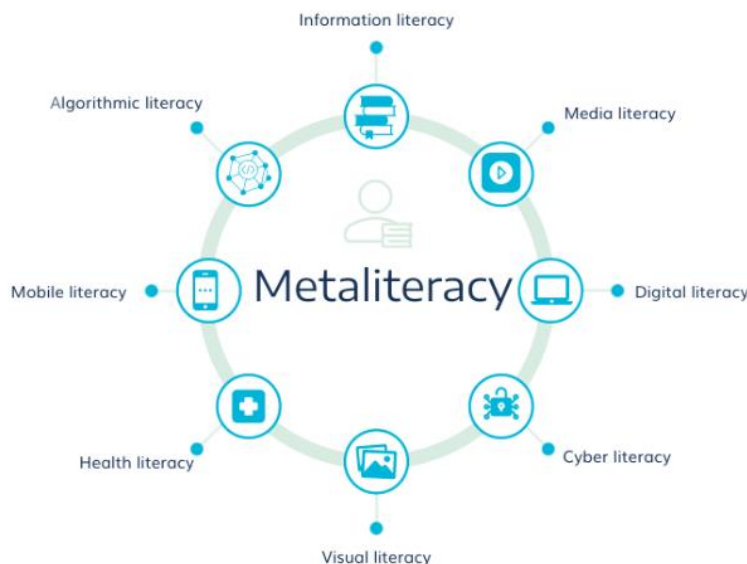
¹¹ Detaljima modela metapismenosti moguće je pristupiti putem mrežne prezentacije Metaliteracy.org

¹² Jacobson i Mackey (2011) nabrajaju informacijsku, medijsku, digitalnu, vizualnu i cyberpismenost.

¹³ *Prelaznim godinama* označava se period značajnog tehnološkog razvoja koji još uvijek nije dosegnoo razmjere i promjene koje vidimo danas: etabrirani početci iOS-a i Androida, rast društvenih medija (Facebook, Twitter i YouTube) i e-trgovine, razvoj cloud servisa i popularizacija *streaming* usluga. Govoreći o stepenu razvoja algoritama i njihovog utjecaja, desetljeće prije predstavlja znatno drugačije vrijeme u pogledu primjene u odnosu na danas. Iako su algoritmi bili prisutni i koristili su se u različitim sektorima, razina njihove sofisticiranosti i rasprostranjenosti znatno se povećavala tijekom proteklih deset godina kada su se koristili u pretraživanju Interneta, preporukama proizvoda, analizi podataka i sličnim područjima, ali nisu bili duboko integrirani u

Pružajući teorijsku osnovu za koncept i daju primjere njegove primjene u obrazovnoj praksi, model metapismenosti osavremenjuje koncept cyberpismenosti pristupom kontinuirane refleksije učenika na vlastiti proces razmišljanja i prakse učenja kako bi se definirale efikasne strategije stjecanja znanja. U članku „The Role of Algorithmic Literacy in Academia and Beyond: Some Considerations“ (2022), Marta Samokishyn propituje poziciju algoritamske pismenosti u kontekstu drugih pismenosti iznoseći primijećenu praksu:

„Mnogi autori se slažu da je potrebno ponovno zamisliti algoritamsku pismenost kao dio metapismenosti, budući da su različite vrste pismenosti, kao što su digitalna i cyber pismenost, medijska pismenost i vizualna pismenost, postale neodvojivi dio obrazovanja o informacionoj pismenosti (Gersch i sar., 2016; Mackey i Jacobson, 2014).“



Ilustracija 2: Vizualni prikaz Marte Samokishyn predstavlja model metapismenosti, djelimično baziran na Mackey i Jacobson (2014).

Vizualni prikaz modela metapismenosti pokazuje da integracija pojedinih elemenata pismenosti poput cyberpismenosti, digitalne pismenosti, algoritamske, informacijske i medijske pismenosti, dolazi kao posljedica procesa indukcije srodnih oblika koji konsolidirani u provođenju jedinstvenog modela osnažuju učenike „da efikasno primjenjuju participativne tehnologije za kreiranje sadržaja istovremeno vodeći računa o ličnoj privatnosti i informacijskoj sigurnosti“ (Jacobson, Mackey i O'Brien 2021, 144). Stavljanjem akcenta na

svakodnevnog života i komercijalne usluge. Stoga je termin *cyberpismenost* bila dostatna terminološka odrednica u smislu praćenja razvojnog trenutka, ali je u kontekstu sveobuhvatnosti područja počela pokazivati odlike nedostatnosti, a prepoznata *anomalija* vodila je, između ostalog, ka razvoju modela metapismenosti. Danas, deset godina poslije, metapismenost se ponovo javlja kao odgovarajući model koji teži da pripremi pojedince da budu informirani potrošači i odgovorni proizvođači informacija u različitim društvenim zajednicama, uključujući one koje su posredovane tehnologijom.

objedinjene kompetencije prije nego na pojedinačne elemente modela, metapismenost prepoznaje da informacijska sigurnost nije izolirani koncept, već se integrira u širi okvir algoritamske i inih pismenosti kao usvajanje znanja o važnosti zaštite (ličnih) podataka, povjerljivosti, cjelovitosti i dostupnosti informacija u digitalnom okruženju.

1.2.1. Konvergencija algoritamske pismenosti i informacijske sigurnosti

Imajući u vidu da se informacijska sigurnost¹⁴ često izučava i shvata kroz primarno tehničku perspektivu, a algoritamska pismenost biva svedena pod matematičke i računalne vještine (Astambayeva et al. 2021), postavlja se imperativ proširivanja teorijskih polazišta i praktičnih aktivnosti koje se odmiču od koncepcije digitalne pismenosti. Algoritamske kompetencije obuhvataju dijeljene sa izazovima drugačijim od usvajanja digitalnih i vještina kodiranja jer se u biti usredotočuju na razumijevanje mehanizama putem kojih se informacije pružaju korisnicima na *frontend-u* web stranica. (Hill 2022, 50). Na sličan način koncept informacijske sigurnosti nije samo pitanje tehničkih i tehnoloških znanja – ljudski, pravni, etički i društveni aspekti¹⁵ čine značajni dio fokusa ako se ljudski faktor shvati kao „najslabija karika“ i postavi pitanje zašto pojedinci obično barataju sa slabim sigurnosnim odlukama (Gubta i Sharman 2008).

Postojanje ljudskog faktora kao najslabije karike ne znači *apriori* potpuno odbacivanje tehničke paradigme, ali zato počiva na temeljima njenog proširivanja sa humanocentričnim pristupom (Tsuji 2006; Komatsu, Takagi i Takemura 2013) društvenih nauka. Podjednako kao i šira oblast kritičkih sigurnosnih i mirovih studija, koncept ljudske sigurnosti nastaje iz potrebe za društvenim razvojem u posthladnoratovskom periodu. Bez obzira na promicanje humanocentrične sigurnosti u izvještaju Ujedinjenih naroda (1994), kasniji slučajevi iz prakse pokazuju da se fokus idalje stavlja na rješavanje sukoba namjesto sprječavanja njihovog uzroka. Drugim riječima, izvodivost koncepta ljudske sigurnosti postaje sporna iz sličnih razloga kao i sam koncept ljudskih prava koja postaju instrument “nametanja Zapada ostatku svijeta i poticat će sukobe civilizacija” (Mouffe 2016, 136-137).

¹⁴ Jedna od definicija koja oslikava tehničke aspekte: “informacijska sigurnost niz mjera i postupaka u cilju zaštite informacije od širokog spektra prijetnji sigurnosti da bi smo osigurali kontinuitet rada, minimizovali rizike i imali najbolji omjer uložene i dobijene sigurnosti.” (Puharić i Budimlić 2008).

¹⁵ Ljudske aktivnosti često su najslabija karika u lancu sigurnosti i pogreške poput slabih lozinki, odgovaranja na na *phishing* e-mailove ili nesvjesnog dijeljenja osjetljivih informacija i tako predstavljaju ozbiljnu prijetnju informacijskoj sigurnosti. Psihološki pristup poput socijalnog inženjeringa ne može biti shvaćen i zaustavljen isključivo putem tehničkih mjera. Pravni aspekt podrazumijeva poštivanje zakona i propisa, poput GDPR-a koji postavljaju zahtjeve zaštite privatnosti korisnika, a etički i društveni aspekti zadiru u polja privatnosti ličnih podataka, povjerenja, pravednosti i jednakosti i transparentnosti.

S druge strane, informacijske nauke 90-ih godina započinju ubrzan proces redefiniranja koncepta, oblasti i praksi podstredstvom razvoja informacijsko-komunikacijskih tehnologija (IKT). Nakon nepunog desetljeća tehnoutopističke faze vođene idejom da će prelazak u digitalno okruženje riješiti postojeća neslaganja, konflikte i ratove, teroristički napad 11. septembra uslovio je dodatni nivo sekuritizacije¹⁶ u svim dijelovima međunarodnog sistema (D'Appollonia 2012, 77) postavivši se, između ostalog, kao moguće polazište informacijsko-komunikacijskih nauka za ispitivanje promjena procesa upravljanja, prikupljanja i diseminacije informacija. Opseg ovakvih kritičkih informacijskih teorija u postdigitalnom dobu omogućava da se sigurnosne i mirovne studije dovedu u blisku vezu sa informacijskim naukama, ali i procese međusobnog uslovljavanja – diseminacija informacija putem mrežnih tehnologija osvjetljava spregu „nasilja i vidljivosti“ (Della Ratta 2021).

Poredeći konvergentni put sigurnosnih studija i informacijskih nauka zadnjih desetljeća XX vijeka, informacijsko-komunikacijske tehnologije ujedinile su dvije discipline ispočetka kroz uočavanje zajedničke potrebe za redefiniranjem teorijskih i praktičkih kretanja, a potom uz pomoć institucionalnih, državnih i multidisciplinarnih akademskih inicijativa. Na početku dvadeset i prvog stoljeća većina zemalja ubrzano radi na razvoju vlastite „informacijske politike“ (Duff 2004; Bramen 2006) kako bi se ustoličile kao društva znanja koja svoj razvoj temelje na iskorištavanju potencijala informacijsko-komunikacijskih tehnologija. Područja poput privatnosti, upravljanja rizikom, odgovornosti i etike, obrazovanja i zakonskih regulacija u digitalnom dobu, otvorila su zajednička polja promatranja sigurnosti informacija.¹⁷

Interdisciplinarna oblast zaštite podataka dio je područja informacijskih nauka i sigurnosnih studija. Dok se informacijske nauke bave prikupljanjem, obradom i distribucijom informacija, informacijska sigurnost fokusira se na zaštitu tih informacija od prijetnji i zloupotreba. Tim slijedom, oba polja prepoznaju da je zaštita podataka ključna komponenta u osiguravanju integriteta, povjerljivosti i dostupnosti informacija¹⁸. Danas se algoritamska pismenost dovodi u vezu sa prikupljanjem i obradom ličnih podataka, dok informacijska

¹⁶ Sekuritizacija označava proces koji određeni problem podiže iz razine svakodnevne politike i prepoznaje kao sigurnosnu prijetnju te stoga zahtijeva posebnu pažnju i sigurnosne mjere.

¹⁷ U mrežna globalna kretanja podcrtavaju promjenu tradicionalnog pristupa gdje se pojam informacije uglavnom vezao za područje komunikoloških nauka te informacijske i baštinske ustanove poput arhiva, muzeja i biblioteka. Ubrzan razvoj informacijskih politika početkom XXI vijeka potvrdio je zanemareni odnos između ove discipline i sektora za koje bi se u ovom historijskom kontekstu moglo reći kako nemaju previše dodirnih tački sa informacijskim razvojem: „Što se tiče neinformacijskih sektora, doseg informacijske politike bio je još širi: sve od energetske planiranja do sigurnosti tankera, do korištenja bolničara, do estetike arhitekture, do regulacije domaće zrakoplovne industrije, do nacionalne sigurnosti (Duff 2004, 74).

¹⁸ Saltzer i Schroeder u radu „The Protection of Information in Computer Systems“ (1975), definirali su tri osnovna principa informacijske sigurnosti: povjerljivost, integritet i dostupnost.

sigurnost poima prijetnje privatnosti¹⁹ i obratno. Stoga „znanje o potencijalnim regulatornim i prilagodbenim mjerama koje se odnose na donošenje odluka pomoću algoritama u internetskim aplikacijama – kao što su pravilnici i prava korisnika, npr. u vezi s automatiziranim obradama podataka i zaštitom privatnosti“ (Dogruel 2021, 80), trebaju biti uključeni u kognitivnu dimenziju stvarnog znanja o algoritmima.

2. Informacijska sigurnost

Nasuprot realističkom pristupu koji stavljanjem državne autonomije i suvereniteta, fizičke sigurnosti, te unutrašnje politike u centar sigurnosnih značajki, ostaje ograničen unutar tradicionalnih sigurnosnih studija, kritički pristupi predstavljaju odgovarajući teorijski fokus ukoliko se ovoj disciplini teži pristupiti sa stanovišta mapiranja „naučnih revolucija“ (Kuhn 2012). Tako autori u zborniku „Kritičke sigurnosne studije: Koncepti i slučajevi“ (1997) u periodu netom nakon Hladnog rata otkrivaju „anomalije“ u matrici proučavanja i fokusa sigurnosnih studija. Poteškoće u procesu propitivanja određenja referentnog objekta²⁰ ne proizlaze toliko iz naklonosti (post)modernističkih teorija ka praznom označitelju, koliko iz potrebe da se, u poraću tenzija ponovo pristupi pitanju „ko ili šta treba biti osigurano“ (Krause i Williams 1997, 68). Promjena fokusa ogleda se ponajbolje u rezultatima sukcesivnih kretanja ka humanocentričnoj i umreženoj perspektivi:

Ako usredotočenost na državu kao referentni objekt nije dovoljna, što ako naš fokus postavimo na pojedino ljudsko biće, ili možda na zajednicu u kojoj ljudi žive? Zaista, što ako se zapitamo o sigurnosti čovječanstva kao cjeline, iznad umjesto unutar država u kojima se većina nas nalazi? (Collins 2010, 77).

Period propitivanja polazišta sigurnosnih studija pretpostavio je njihova daljnja kretanja u interdisciplinarnom, multidisciplinarnom i transdisciplinarnom pravcu. Odustajući od pretpostavke da je država središnji referentni objekt, savremene sigurnosne studije ukazuju na tendencije ka povezivanju sa drugim disciplinama. Postavljajući pitanje o tome *ko* i *šta* treba biti sigurno u savremenom društvu, kritičke sigurnosne studije proširuju pojam sigurnosti, a kao jedan od novih koncepata pojavljuje se i ljudska sigurnost: „Ova duga filozofska i politička tradicija usmjerena na čovjeka tek odnedavno uključuje koncept nazvan 'ljudska sigurnost'“ (Collins 2010, 115). Ukoliko se humani pristup posmatra iz deskriptivne perspektive, može se

¹⁹ Prijetnja na nivou svakog pojedinca, ne zanemarujući ljudski faktor i humani pristup.

²⁰ Referentni objekat u slučaju područja sigurnosnih studija podrazumijeva stvarni objekat koji je u središtu proučavanja discipline, a može biti fokusiran na državu, međunarodne odnose, okoliš, cyber sigurnost, terorizam, sigurnosne politike te ljudski faktor i pojedince.

uočiti njegova usmjerenost na „potrebe i prava pojedinaca u kontekstu čovječanstva kao cjeline, a ne kao građana pojedinih država ili članova isključivih političkih zajednica“ (Atack 2005). Suočavajući se sa tehnološkim razvojem, ljudska sigurnost dolazi pred seriju izazova koja će iznova propitati čvrstinu stajališta humanocentričnog pristupa.²¹

Humana sigurnost u doticaju sa informacijsko-komunikacijskim tehnologijama usmjerava se u pravcu digitalne transformacije sigurnosti koja odgovara na složenost modernog sigurnosnog okruženja i nove izvore nesigurnosti, posebno u cyber prostoru i uticaj algoritama, te popunjava praznine u tradicionalnom, državocentričnom pristupu. Suočavajući se s destabilizacijom u informacijskom prostoru i iskrivljivanjem u političkom i tržišnom kontekstu, ovaj pristup shvata da sigurnosne prijetnje i izazovi više nisu ograničeni na tradicionalne oblike međunarodno definiranih konflikata, već se šire na područje „hibridnih asimetričnih sigurnosnih izazova i ratova“ (Vajzović 2020, 6). Pri tome, zauzimanje novog, nevidljivog prostora nije jedini proces koji se dešava posredstvom digitalne transformacije sigurnosti. Umjesto toga, prožimanje ide u oba pravca – „snimak kamere i pucanj iz oružja potpuno se spajaju i konvergiraju u doba društvenog weba“ (Della Ratta 2021)²².

Vajzović (2020) podsjeća da bez obzira na raznolikost oblika sigurnosti²³ svaki tip „podložan je informacijskoj i medijskoj interpretaciji stvarnosti, i zavisno od stepena razvoja naših kompetencija medijske i informacijske pismenosti (MIP), sposobni smo donositi informisane, obrazovane i kritički promišljene odluke“ (7). Imajući u vidu da na interpretaciju

²¹ Dok se informacijske i bibliotečke nauke nalaze u prijelomu između paradigme okrenute ka sistemima i korisnicima, polazišta principa ljudske sigurnosti bivaju iznova razmotrena uvođenjem informacijsko-komunikacijskih tehnologija i nalazi se na razmeđu informacijskih sistema i korisnika tih sistema. Principi ljudske sigurnosti postaju kritični jer se ne radi samo o tehničkim pitanjima, već i o tome kako korisnici percipiraju sigurnost i privatnost u digitalnom okruženju. S obzirom da korisnici sve više ovise o IKT-u u svakodnevnim aktivnostima, postavlja se pitanje kako osiguravanja osjećaja sigurnosti i zaštite.

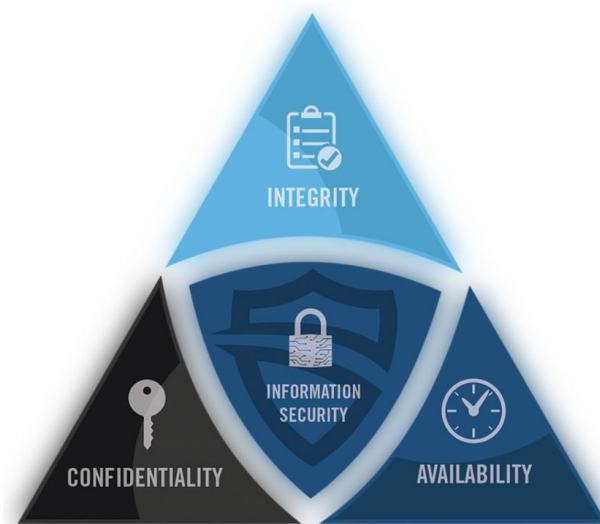
²² Odnosi se na konkretnu pojavu "dvostrukog snimanja", gdje jedna osoba snima događaje dok druga *otvara vatru*, simbol Arapskog proljeća. Della Ratta u članku „Violence, Visibility, and Contemporary Digital Culture in Post-Uprising and Pandemic Times“ (2021) istražuje utjecaj na ratne sukobe tvrdeći da ovo preusmjeravanje utječe na način kako se nasilje i vidljivost percipiraju i imaju implikacije na digitalnu kulturu XXI vijeka. Teza autorice odnosi se na transformaciju ove dinamike kroz upliv društvenih medija i participativne kulture istražujući kako suvremena mrežna kultura omogućava širenje ovih snimaka i slika putem društvenih mreža i drugih online platformi. Ova promjena transformira nasilje i vidljivost u "mrežnu sliku", gdje su viralnost i širenje postali važniji od samog sadržaja ili značenja slika. Digitalni pomak zamagljuje granice između reprezentacije i stvarnosti, a mrežna slika okarakterisana je viralnošću i sposobnošću širenja, gdje je naglasak na cirkulaciji, a ne na semantičkom značenju

²³ U članku „Digitalna transformacija sigurnosti i algoritamska demokratija“ (2020) Vajzović navodi neke od oblika sigurnosti poput društvene, političke, ekonomske, ekološke i zdravstvene. Sigurnost nije jednostavno definisana kao fizička zaštita ili odbrana od prijetnji, već obuhvata širok spektar aspekata vezanih za transformaciju humane sigurnosti. To uključuje fizičku sigurnost, ekonomsku sigurnost, informacijsku sigurnost, političku stabilnost, sigurnost hrane i mnoge druge oblasti pri čemu svaka posjeduje specifične karakteristike i zahtjeve, a promjene u tehnologiji, kontinuirano dovode do pojave novih vrsta prijetnji i potrebe za prilagođavanjem postojećih sistema sigurnosti.

stvarnosti utječe stepen medijske i informacijske pismenosti, tvrdnja se može staviti i u kontekst algoritamskih znanja, vještina i kritičkog sagledavanja njihovog vrednosnog aspekta. Podjednako kao što medijska, informacijska i algoritamska pismenost pokazuju odlike prilagodbe svakom sistemu, informacijska sigurnost pronalazi sfere utjecaja u društvenoj, ličnoj, ekološkoj, ekonomskoj, nuklearnoj i drugim oblicima sigurnosti čija je multidisciplinarnost primijećena počevši sa novim vijekom i digitalnim izazovima (Wood 2004), kao i potreba da na institucionalnom nivou uvođenja principa informacijske sigurnosti sudjeluje više odjela i stručnjaka iz različitih oblasti.

Jasnost i univerzalnost principa informacijske sigurnosti usko su vezani sa prilagodljivošću referenciranog CIA modela (engl. Confidentiality – povjerljivost, Integrity – cjelovitost i Availability – dostupnost)²⁴, koji može poslužiti kao jedinstven okvir za primjenu informacijske sigurnosti u drugim oblicima sigurnosti. Naprimjer, autori (Oliveira, Rosado da Cruz i Faria 2020) koji tematiziraju specifično područje i raspravljaju o implementaciji sistema mreže kioska za praćenje ribljih proizvoda u trgovinama s ciljem pružanja informacija o praćenju proizvoda kupcima, polaze od CIA modela kao i Gladden (2017) koji istražuje informacijsku sigurnost u kontekstu tehnološkog posthumanizma predlažući da područje aksiologije u svojstvu polazišta za učinkovitije identificiranje, analiziranje različitih vrsta vrijednosti i dobara koja se mogu ostvariti putem praksi informacijske sigurnosti.

Ilustracija 3: Vizualni prikaz tri CIA principa informacijske sigurnosti



²⁴ Informacijska sigurnost omogućava da se se poverljive informacije o sigurnosnim procedurama ili postupcima čuvaju tajnim (Confidentiality). Očuvanje integriteta (Integrity) podrazumijeva fizičke sisteme, sprečavanje neovlaštenog pristupa ili manipulaciju podacima o sigurnosti. Naposljetku, garantovanjem dostupnosti osigurava se protok informacija i komunikacijskih sistema.

Tri temeljna principa poslužila su kasnije kao temelj za razvoj raznih modela informacijske sigurnosti, poput Parkerian Hexad i International Organization for Standardization Model (ISO).²⁵

2.1. Informacijska sigurnost na Univerzitetu u Sarajevu

Nedovoljno razvijena disciplina informacijske sigurnosti u Bosni i Hercegovini čini iznimno ranjivim institucije, organizacije i pojedince u svim oblastima. Različiti nivoi vlasti nemaju ujednačene načine pripremljenosti niti sveobuhvatni strateški pristup za praćenje, evaluaciju i usavršavanja informacijske sigurnosti. Nedostatak zakonskih okvira, javnih politika, strategija i akcionih planova koji bi povećali otpornost društva i institucija te zaštitili informacijske sisteme i imovinu²⁶, uslovio je početak naučnoistraživačkog upliva akademske zajednice. U istraživanju Instituta za društvena istraživanja Fakulteta političkih nauka u okviru projekta Informacijska sigurnost (2017) sa ciljnom grupom organa vlasti i uprave u Kantonu Sarajevo, zabilježen je relativno nizak nivo informacijske sigurnosti i da nedostaje adekvatnih propisa u ovoj oblasti.

Prepoznavši značaj i utjecaj digitalne transformacije sigurnosti, Odsjek sigurnosnih i mirovnih studija Fakulteta političkih nauka Univerziteta u Sarajevu posljednjih deset godina radi na uspostavljanju teorijskih i praktičnih osnova za uvođenje discipline informacijske sigurnosti u bosanskohercegovački visokoškolski obrazovni sistem. Od akademske 2021/2022. godine u partnerstvu sa kompanijom CyberGate²⁷, uveden je novi interdisciplinarni master program iz informacijske sigurnosti²⁸. U Elaboratu interdisciplinarnog studijskog programa informacijske sigurnosti (2021) stoji da je Odlukom o usvajanju politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017 - 2022. godine

²⁵ Koristeći principe povjerljivosti, integriteta i dostupnosti, Clark i Wilson 1987. godine predstavili su takozvani Confidentiality, Integrity and Availability (CIA) model. Ovaj model osnova je koncepta informacijske sigurnosti, pomaže pri razvoju sigurnosnih politika za organizacije. Pri razvijanju novog proizvoda ili tehnologije model pomaže sigurnosnim timovima za vođenje politika informacijske sigurnosti (Moghaddasi, Sajjadi i Kamkarhaghghi 2016). Prvi nedostatak CIA modela jest taj da je određivanje ponekad preširoko ili preusko, odnosno, da definiira sigurna stanja kao sigurna i sigurna kao nesigurna (Lundgren i Möller 2019).

²⁶ Vijeće ministara Bosne i Hercegovine, na 95. sjednici, održanoj 22. marta 2017. godine, donijelo je Odluku o usvajanju politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017 - 2022. godine (Službeni glasnik BiH, broj 38/17). Potom je na prijedlog Ministarstva komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine na 54. sjednici, održanoj 28. jula 2022. godine, donijelo Odluku o usvajanju Smjernica iz politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period od 2017 - 2022. godine.

²⁷ CyberGate je organizacija sa sjedištem u Ujedinjenim Arapskim Emiratom osnovana s ciljem pružanja usluga cyber sigurnosti. CyberGate godinama surađuje sa različitim institucijama na globalnom nivou nudeći spektar usluga i rješenja cyber sigurnosti.

²⁸ Studijski program usklađen je sa potrebama i ciljevima Smjernica za strateški okvir cyber sigurnosti u Bosni i Hercegovini (2019), direktno sa ciljem C: „Podizanje nivoa svijesti i znanja o cyber sigurnosti“.

„otvoren prostor za provođenje principa i standarda, dana obaveza ali ne i rješenje za problem ljudskih resursa za njeno provođenje, što ovaj studijski program upotpunjava.“ (14).

Pokretanjem naučnoistraživački utemeljenog i praktičnog interdisciplinarnog programa informacijske sigurnosti težilo se dugoročno odgovoriti izazovima za stvaranje otpornosti i sposobnosti proaktivnog djelovanja u oblasti zaštite informacijskih sistema i imovine, kritične infrastrukture, te stabilne političke zajednice kao preduslova društvenoj sigurnosti. Provođeci nastavu kroz vođeno istraživačko učenje sa profesorima iz interdisciplinarnih oblasti, stručnjacima iz prakse i uz podršku informacijskih stručnjaka Instituta za društvena istraživanja Fakulteta političkih nauka Univerziteta u Sarajevu, studij informacijskoj sigurnosti ne pristupa isključivo kao tehničkoj i tehnološkoj kompetenciji, već je „orijentisan na netehničke aspekte informacijske sigurnosti koji uključuju strategije, liderstvo (upravljanje), prilagođavanje organizacijske strukture, politike, procedure i mehanizme za provođenje standarda informacijske sigurnosti.“ (Fakultet političkih nauka 2021, 11).

Koncipiran kao slijed disciplina, oblasti i različitih nauka koje se nadopunjuju i međusobno integriraju kako bi stvorile sveobuhvatnu sliku o informacijskoj sigurnosti unutar šireg konteksta organizacije i društva, te usklađujući nastavni plan i program sa Strategijom razvoja Univerziteta u Sarajevu 2019-2023²⁹, master studij omogućava studentima, istraživačima, nastavnicima i ostalim akterima da kritički promišljaju dinamiku društvenih, ekonomskih, tehničko-tehnoloških i političkih procesa kroz šest interdisciplinarnih nastavnih modula:



Ilustracija 4: Vizualni prikaz modula interdisciplinarnog master programa informacijske sigurnosti na Fakultetu političkih nauka Univerziteta u Sarajevu

Predstavljani moduli u Ilustraciji 4: I Savremene sigurnosne studije, II Sistemi upravljanja organizacijom, III Poslovni kontinuitet, IV Menadžment informacijske sigurnosti, V Zaštita

²⁹ Interdisciplinarni master studij informacijske sigurnosti usklađen je sa Strateškim ciljem 1: Promocija i podrška izvrsnosti u nastavnom procesu“ (Strategija razvoja Univerziteta u Sarajevu 2019, 28), te navedenim Aktivnostima ciljeva: N 1.1.1. Povećati broj interdisciplinarnih studijskih programa, N 1.1.2. Internacionalizirati studijske programe te formirati zajedničke studijske programe i studijske programe na stranim jezicima; N 1.1.3. Uskladiti studijske programe sa tržištem rada kroz jasno definiranje ishoda učenja za sve studijske programe koji se izvode na UNSA; N 1.3.1 Efikasno korištenje ICT u nastavi; N 1.3.3 Razviti široku mrežu nastavnih baza odnosno organizacija u kojima se povezuju praksa, znanost, umjetnost i visoko obrazovanje (31-33).

podataka i VI Profesionalna certifikacija čine temeljni okvir studija informacijske sigurnosti, pružajući holistički pregled ključnih aspekata ove discipline. Polazeći od petog modula, Zaštita podataka, koji je u direktnoj vezi sa algoritamskom pismenošću, profesionalna certifikacija tokom šestog modula omogućava agregaciju znanja stečenog u toku studija za dobijanje međunarodnog industrijskog ISO sertifikata³⁰ i sticanje šire perspektive informacijske sigurnosti, pripremajući se za zahtjeve savremenih propisa i normi.

2.2. Propisi i standardi informacijske sigurnosti

Područje informacijske sigurnosti definira niz relevantnih međunarodnih propisa, normi i standarda³¹ za osiguravanje integriteta, povjerljivosti i dostupnosti informacija. Pronalazeći razloge za spor razvoj informacijskih sistema u organizacijama i državnim dijelima u Bosni i Hercegovini, Mijić (2019) objašnjava složene društvene, ekonomske i političke okolnosti³² i ističe kako su po pitanju informacijske sigurnosti u Bosni i Hercegovini doneseni okvirni zakoni³³ koji pokrivaju ovu oblast, ali zakon o informacijskoj sigurnosti nije usvojen. Mahmutović i Trepanić (2022) naglašavaju da uprkos porastu učestalih cyber napada na globalnom nivou, Bosna i Hercegovina nije napravila značajan pomak i idalje ostaje jedina

³⁰ Informaciona tehnologija – Sigurnosne tehnike – Sistemi za upravljanje sigurnošću informacija – Zahtjevi (engl. ISO 27001:2013 Lead Implementer (Information technology — Security techniques — Information security management systems — Requirements) i/ili Bezbjednost i otpornost - Sistemi upravljanja kontinuitetom poslovanja - Zahtjevi. (engl. ISO 22301:2019 Lead Implementer (Security and resilience — Business continuity management systems — Requirements).

³¹ ISO 27001: međunarodni standard za upravljanje informacijskom sigurnošću koji definira okvir za uspostavljanje, implementaciju, održavanje i unapređenje sistema upravljanja informacijskom sigurnošću; GDPR (Opšta uredba o zaštiti podataka) - uvedena u Evropskoj uniji, uredba reguliše prikupljanje i obradu ličnih podataka te postavlja zahtjeve zaštite privatnosti građana; NIS Direktiva (Direktiva o mrežnoj i informacijskoj sigurnosti - usmjerena na poboljšanje sigurnosti kritičnih infrastruktura i pružalaca ključnih usluga u vezi sa informacijskom sigurnošću; eIDAS (Uredba EU o elektronskom identifikovanju i uslugama pouzdanog elektronskog potpisa) - reguliše upotrebu elektronskih identiteta potpisa u EU, uključujući pitanja bezbjednosti; Directive 2002/58/EC (e-Privacy Direktiva) – odnosi se na privatnost u elektronskim komunikacijama i pruža smjernice za upotrebu kolačića (engl. cookies); PSD2 (II Direktiva o plaćanjima usmjerena na potrošače): Reguliše elektronske transakcije i zahteva stroge sigurnosne mjere za online plaćanja).

³² “Bosna i Hercegovina je zemlja koja je ne tako davno izašla iz ratnog perioda, a i složenog je državnog ustroja sa dva entiteta (Entitet Federacije BiH i Entitet Republike Srpske) i Brčko Distrikt. Ekonomski i socijalni uvjeti u Bosni i Hercegovini su loši, što je i rezultat sporijeg razvoja informacijskih sustava kako u organizacijama tako i u državnim tijelima, tj. danas su na dosta nižoj razini nego u ostalim razvijenim zemljama u okruženju“ (Mijić 2019, 96).

³³ Tematizirajući zakonsku regulativu o informacijskoj sigurnosti u Bosni i Hercegovini, Mijić (2019) navodi: Zakon o zaštiti tajnih podataka (Službeni glasnik BiH br. 54/05. i 12/09.); Zakon o zaštiti osobnih/ličnih podataka (Službeni glasnik BiH br.32/01, 49/06, 76/11. i prečišćeni 89/11.); Zakon o centralnoj evidenciji i razmjenu podataka (Službeni glasnik br.32/01, 16/02, 32/07. i prečišćeni 44/07); Zakon o komunikacijama (Službeni glasnik BiH br. 31/03, 75/06, 32/10 i 98/12.); i Odluku o usvajanju Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period od 2017 - 2022. godine (Službeni glasnik BiH br.38/17.) (96). U julu 2022. godine Vijeće ministara donijelo je Odluku o usvajanju smjernica iz politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period od 2017 - 2022. godine (Službeni glasnik BiH, broj 62/22).

zemlja Zapadnog Balkana bez državne strategije cyber sigurnosti i „operativne mreže CERT-ova i CIRT-ova na državnom i regionalnom nivou“ (2).

Nacionalni timovi za hitne računarske intervencije (CERT) odgovorni su za zaštitu kritične informacijske infrastruktura (CIIP), obrazovanje i edukaciju o prevenciji incidenata, uspostavu protokola i procedura, te razvoj strateških dokumenata u domenu cyber sigurnosti. Prema repozitoriju nacionalnih strategija cyber sigurnosti Međunarodne telekomunikacijske unije (ITU), 123 zemlje posjeduju nacionalnu strategiju cyber sigurnosti³⁴ i 118 nacionalne timove za odgovor na računarske incidente (CIRT)³⁵. U Bosni i Hercegovini postoji Nacionalni CERT Republike Srpske³⁶ i Cyber Security Excellence Centre (CSEC)³⁷, ali ne i državni CERT³⁸. Ljubčić (2023) izdvaja obaveze Vijeće ministara BiH koje je 2017. godine usvojilo odluku o uspostavljanju Tima za odgovor na računarske incidente (CERT) u institucijama Bosne i Hercegovine³⁹.

S obzirom na nedostatak nacionalnih centara i strategija za cyber sigurnost u Bosni i Hercegovini te generalno razlike između pojmovnih i teorijskih aspekata cyber i informacijske sigurnosti⁴⁰, postoji mogućnost prilagodbe međunarodnih relevantnih standarda, strategija, regulativa i konvencija za područje informacijske sigurnosti. Naprimjer, u procesu pridruživanja Europskoj uniji, Bosna i Hercegovina obavezna je izmijeniti zakonski okvir prema Sporazumu o stabilizaciji i pridruživanju potpisanim sa EZ-om 2008. godine (Mahmutović i Trepanić 2022) koji implicira i usvajanje te provedbu Konvencije Vijeća Evrope

³⁴ Repozitorij uključuje nacionalne strategije cyber sigurnosti, bilo da se radi o jednom ili više dokumenata ili kao sastavnom dijelu šire strategije za informacijske i komunikacijske tehnologije (ICT) ili nacionalne sigurnosti (International Telecommunication Union 2023)

³⁵ National CIRT. 2023. International Telecommunication Union

<https://www.itu.int/en/ITUDE/Cybersecurity/Pages/national-CIRT.aspx> Pristupljeno 4. septembra 2023.

³⁶ CERT RS. 2023. Nacionalni CERT Republike Srpske. <https://certrs.org/>. Pristupljeno 4. septembra 2023.

³⁷ CSEC. 2023. Cyber Security Excellence Centre. <https://www.csec.ba/about?lang=bs>. Pristupljeno 4. septembra 2023.

³⁸ Mahmutović i Trepanić (2022) navode podatak da je u toku 2017. godine Ministarstvo sigurnosti BiH (MS) zaduženo za izradu nacrtu državne strategije cyber sigurnosti, te da su zbog zbog neusklađenosti podzakonskih akata do sada usvojene samo smjernice za strategiju cyber sigurnosti (3).

³⁹ Prema ovoj odluci, Ministarstvo sigurnosti zaduženo je za izradu izmjena i dopune Pravilnika o unutrašnjoj organizaciji i sistematizaciji radnih mjesta s ciljem uspostavljanja CERT tijela za institucije Bosne i Hercegovine kao posebne organizacione jedinice u okviru ministarstva.

⁴⁰ Informacijska sigurnost predstavlja širi koncept koji se odnosi na zaštitu informacija, podataka i resursa od svih vrsta prijetnji, uključujući zaštitu podataka na svim nivoima, od fizičke sigurnosti prostora do upravljanja pravilima i postupcima za pristup informacijama. Cyber sigurnost čini područje informacijske sigurnosti koje je specifično usmjereno na zaštitu informacija i podataka od cyber prijetnji i napada baveći se pritom zaštitom računarskih sistema, mreža i digitalnih podataka. Drugim riječima, informacijska sigurnost obuhvata sve aspekte zaštite informacija, dok se cyber sigurnost posebno bavi digitalnim aspektima sigurnosti, kao što su online napadi i zaštita digitalnih resursa.

(Konvencija iz Budimpešte)⁴¹ i Opšte uredbe Evrope unije o zaštiti podataka (GDPR). Nadalje, poželjna i nužna praksa jeste provođenje ISO 27000 porodice standarda⁴² zbog njihove međunarodne usklađenosti i univerzalne primjenjivosti, osiguravanju kvaliteta, pouzdanosti i transparentnosti, ujednačenog jezika, te podrške kontinuiranom poboljšanju pri čemu će u nastavku rada posebna pažnja biti posvećena ISO 27001:2013 standardu.

2.2.1. Standard ISO 27001 – tranzicija upravljanja sigurnosti informacija

Posmatrajući široko rasprostranjene, međunarodno priznate i često korištene standarde kvalitete⁴³ koji su pretrpjeli izmjene u procesu prilagodbe digitalnoj transformaciji društva (Simić i Marković 2020), izdvaja se sistem upravljanja zaštitom i sigurnosti informacija ISO/IEC 27001:2013 (engl. Information Security Management Systems). Ustoličivši se kao najpoznatiji standard informacijske sigurnosti ISO serije 27000⁴⁴, različite kompanije, organizacije i institucije uskladile su svoje poslovanje i poslovne procese prema principima⁴⁵ ISO 27001:2013 standarda koji omogućava efikasno upravljanje sistemima informacijske sigurnosti. U skladu sa digitalnog transformacijom, revidirano izdanje standarda iz 2013.

⁴¹ Mahmutović i Trepanić (2022) Konvencija iz Budimpešte nudi opšti obrazac za zemlje koje razvijaju svoje nacionalno zakonodavstvo i saradnju u borbi protiv cyber kriminala. S obzirom na znatne nedostatke koji postoje u nacionalnom zakonodavstvu i sporost u usklađivanju zakonodavstva, kao i ograničene kapacitete za rješavanje širih pitanja povezanih sa cyber sigurnošću i posebno pitanja povezanih sa ljudskim pravima, provođenje konvencije predstavljao bi značajan korak naprijed za BiH.

⁴² Standardi porodice ISO/IEC 27000 nude smjernice za kreiranje i provođenje procedura informacijske sigurnosti s ciljem ispunjavanja povjerljivosti, cjelovitosti i dostupnosti informacija.

⁴³ Jedno od gorućih pitanja EU regulativa tiče se prilagođavanja pravnog okvira digitalne ekonomije i stanardna informacijske sigurnosti. Simić i Marković (2020) navode neke od međunarodnih standarda koji su prošli proces redefiniciranja u skladu sa okvirom GDPR-a, e-Privacy, Digital Copyright Act/NB-Internet of Things : ISO 9001:2015; ISO 14001:2015; ISO/IEC 27001:2013; ISO 20000-1:2018; ISO 22301:2019; ISO/TC 16949:2009, IATF 16949:2016; ISO 10218-1:2011; PAS 181:2014 (82).

⁴⁴ Pored osnovnog standarda informacijske sigurnosti ISO/IEC 27001:2013 u ISO 2700 seriju standarda spadaju: ISO/IEC 27002:2013 (engl. Information Technology — Security Techniques — Code of Practice for Information Security Controls); ISO/IEC 27003:2017 (engl. Information Technology — Security Techniques — Information security management systems — Guidance); ISO/IEC 27004:2016 (engl. Information Technology — Security Techniques — Information security management — Monitoring, measurement, analysis and evaluation); ISO/IEC 27005:2018 (engl. Information technology — Security techniques — Information security risk management); ISO/IEC 27011:2016 (engl. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27001 for telecommunications organizations); ISO/IEC 27033-1:2015 (engl. Information technology — Security techniques — Network security — Part 1: Overview and concepts); ISO/IEC 27031:2011 (engl. Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity); ISO/IEC 27799:2016 (engl. Health informatics — Information security management in health using ISO/IEC 27002); ISO/IEC 27001:2022 (engl. Information security, cybersecurity and privacy protection — Information security management systems — Requirements) (ISO 2023).

⁴⁵ Principi ISO 27001 standarda posebno značajni za implementaciju ISMS-a u organizacijama polaze i od netehničkih aspekta i zalaze u područje upravljanja i ljudskih resursa poput razvijanja svijesti o potrebi za informacijskom sigurnošću, jasnom opredjeljenju o podjeli odgovornosti te uključivanje zainteresovanih strana na ovom polju, unapređenje ljudskih, društvenih i etičkih vrijednosti, potvrđivanje i praktikovanje sigurnosti kao primarnog elementa i svojstva informacija i podataka (Simić i Marković 2020, 104).

godine adresira rastuće globalne izazove u području cyber i informacijske sigurnosti i teži unaprijediti koncept digitalnog povjerenja (Harper 2022).

Posljednje izdanje standarda 27001, ISO/IEC 27001:2022 (engl. Information security, cybersecurity and privacy protection — Information security management systems — Requirements), razlikuje se od prethodnog iz 2013. godine najviše u Prilogu A, jer struktura islistanih kontrola ne slijedi raspored četrnaest područja ISO 27001:2013 standarda, već je konsolidovana u četiri područja⁴⁶, broj navedenih kontrola smanjen je sa 114 na 93, te je uveden koncept atributa (The British Standards Institution 2023)⁴⁷. Osim Priloga A, ostale promjene tiču se: 1. konteksta i obima, 2. planiranja, 3. podrške i 4. procesnih operacija – potrebno je identifikovati „relevantne“ zahtjeve zainteresovanih strana, pratiti ciljeve informacijske sigurnosti koji moraju biti „dostupni kao dokumentovane informacije“ (IT Governance 2022), te zahtjeve za definisanje ko će komunicirati zamijeniti zahtjevom za definisanjem "kako komunicirati“ (ISO 2022)⁴⁸. Bez obzira na dugu listu pojedinačnih revizija, ISO 27001:2022 ne razlikuje se bitno od ISO 27001:2013 jer se većina ovih promjena odnos na Prilog SL, strukturu visokog nivoa⁴⁹ ISO standarda za upravljanje sistemima, a ne na informacijsku sigurnost *per se*.

Fokusirajući se na strukturalne odlike, sadržaj standarda ISO 27001:2013 podijeljen je u jedanaest poglavlja⁵⁰ i Prilog A koji sadrži 35 kontrolnih ciljeva i 114 sigurnosnih kontrola u četrnaest sekcija⁵¹. Postavljajući uslov ljuskih potencijala informacijske sigurnosti za vrijeme zaposlenja, kontrolni cilj *A.7.2.2. Svjesnost o informacijskoj sigurnosti, obrazovanje i treninzi*, moguće je, između ostalog, razumijevati i kao proces usvajanja znanja o algoritmima, a iako

⁴⁶ 1. organizacija, 2. ljudi, 3. fizički i 4. tehnološki aspekt

⁴⁷ Pojedine kontrole su spojene, uklonjene, uvedene ili ažurirane. Atributi su usklađeni sa standardiziranim terminima i predstavljeni su kao: Vrsta kontrole, Atributi sigurnosti informacija, Koncepti cyber sigurnosti, Operativne sposobnosti i Sigurnosne domene.

⁴⁸ Kusotić (2022) navodi kako su prema dokumentu "Zahtjevi za tranziciju na ISO/IEC 27001:2022" Međunarodnog foruma za akreditaciju kompanije koje su već certifikovane prema ISO 27001:2013, obavezne završiti tranziciju na ISO 27001:2022 do 31. oktobra 2025. godine.

⁴⁹ U slučaju ISO standarda, *struktura visokog nivoa* odnosi se na zajednički okvir za organizaciju i strukturu standarda koji se primjenjuju na različite oblasti i discipline. Struktura visokog nivoa, poznata i kao "Prilog SL" (engl. Annex SL), ima za cilj da obezbijedi jedinstven okvir za upravljanje sistemima, nezavisno od toga da li je riječ o standardima za upravljanje kvalitetom, informacijskom sigurnošću, okolinom ili nekom drugom aspektu, što je uvjetovano univerzalnošću karakteristika poput jedinstvenosti okvira, zajedničkog jezika, jednostavnosti implementacije, primjenjivosti i fleksibilnosti.

⁵⁰ Jedanaest poglavlja ISO 27001:2013 standarda čine: Poglavlje 0: Uvod; 1: Predmet i područja primjene; 2: Upućivanje na druge norme; 3: Pojmovi i definicije; 4: Kontekst organizacije; 5: Rukovođenje; 6: Planiranje; 7: Podrška; 8: Djelovanje; 9: Procjena učinaka i Poglavlje 10: Poboljšanja, uz napomenu da da prva tri uvodna poglavlja nisu obavezna za primjenu.

⁵¹ Kontrole od A.5 do A.18.

se u tekstu ne spominje, kontrola vezana uz ovaj cilj, tiče se izravno algoritamske pismenosti (ISO 27001:2013, 11). Nepostojanje detaljnih uputa za pružanje obuke i razvoj algoritamske pismenosti, ukazuje na strukturu i svrhu ISO standarda čiji fokus nije usmjeren na precizno definiranih metoda, alata ili strategija za provođenje kontrolnih ciljeva. Umjesto toga, ISO 27001 postavlja širi okvir koji organizacijama i omogućava razvijanje vlastitih strategija programe obuke kako bi ispunile kontrolne ciljeve u skladu sa vlastitim potrebama i kontekstom.⁵² Informacijska sigurnost potiče se kroz ovaj standard općenito u poglavljima i aneksu, a precizni strateški i tehnički izvedbeni oblici i metode poput algoritamske pismenosti, ostaju odgovornost organizacije da ih razviju i primijene unutar svog okruženja.

S obzirom da ISO 27001:2013 indirektno pretpostavlja provođenje programa obuke o algoritamskoj pismenosti i zaštiti podataka, uvođenje Opšte uredbe o zaštiti podataka (GDPR)⁵³ u raspravu o tranziciji i prilagođavanju ISO 27001 standarda specifičnim potrebama ciljnih skupina, doprinosi jasnijem metodološkom određenju predloženog pristupa. Premda predstavljaju temeljno različite okvire (Secure Privacy 2020) kada je riječ o fokusu, svrsishodnosti i oblasti regulacije⁵⁴, ISO 27001 i GDPR dijele zajedničke principe zaštite podataka. Standard se usmjerava na ljude, procese i tehnologiju organizacije kako bi se spriječili incidenti i „osigurao pravilan mehanizam za prijavljivanje, vođenje evidencije o incidentima i održavanje okoline informacijske sigurnosti organizacije“ (Gemser 2019). Prema GDPR-u, lični podaci su ključne informacije koje organizacije trebaju štiti, a ISO 27001 pruža sredstva kako bi se osigurala zaštita i šira usklađenost s ovom regulativom.

Autori (Gemser 2019, 1) naglašavaju da ISO 27001 promovira kulturu i svijest o sigurnosnim incidentima u organizacijama, te da značajni dio područja informacijske sigurnosti

⁵² Kontrolni cilj ISO standarda 27001:2013 A.7.2.2. - *Svjesnost o informacijskoj sigurnosti, obrazovanje i treninzi*, dovodi se u vezu sa algoritamskom pismošću u smislu osiguravanja da zaposlenici budu svjesni važnosti informacijske sigurnosti i razumiju osnovne principe zaštite podataka. Međutim, standard ne pruža detaljan okvir ili alate za pružanje obuke ili razvoj algoritamske pismenosti.

⁵³ Autori Gemser analize (2019) navode nekoliko kontrola iz Priloga A standarda ISO 27001 koje se mogu koristiti kako bi se podržala usklađenost s GDPR-om kada je u pitanju zaštita ličnih podataka: A.10.1 specificira zahtjeve za enkripciju u organizaciji, a korištenje enkripcije pretpostavlja očuvanje povjerljivosti ličnih podataka, bilo da se radi o onima na mreži, u prenosu ili na mobilnim uređajima. A.9. obrađuje kontrolu pristupa koja, ako je pravilno implementirana, osigurava da samo osobe s legitimnim pravom mogu pristupiti informacijama u skladu sa njihovim stepenom privilegija, odnosno da način i doseg pristupa odgovara stepenu autorizacije. 18.2.3 kontrola zahtijeva izvođenje testiranja ranjivosti i penetracije kako bi se osigurala nekompromitiranost testiranih sistema. Zahtjev za upravljanje tehničkim ranjivostima prema ISO 27001 podrazumijeva od organizacija da ažuriraju sisteme i vode evidenciju zapisa. Nadalje, i ISO 27001 i GDPR zahtijevaju redovno testiranje sigurnosnih mjera i obnovu podataka u slučaju sigurnosnog incidenta.

⁵⁴ S jedne strane, ISO 27001 pojavljuje se kao širi okvir za zaštitu informacija i upravljanje informacijskom sigurnošću, dok GDPR predstavlja zakonodavni okvir za zaštitu ličnih podataka građana Europske unije. ISO obuhvata tehničke, organizacijske i ljudske aspekte, dok je GDPR usmjeren na zaštitu privatnosti pojedinaca i regulira kako organizacije prikupljaju, obrađuju i čuvaju podatke.

čine i ljudska djelovanja, a ne samo tehnološka rješenja. Stoga iako nekoliko sigurnosnih ciljeva i kontrola iz Priloga A otvara prostor za usklađenost sa GDPR odredbama, kontrolni cilj A.7.2.2. izdvaja se u kontekstu homanocentričnog pristupa jer promovira svijest o potencijalnim prijetnjama sigurnosti podataka ostavljajući prostor za isticanje algoritamske pismenosti, što je ključno za razumijevanje i zaštitu informacija u suvremenom digitalnom okruženju. Ova kontrola pomaže organizacijama da educiraju svoje zaposlenike i kontraktore o važnosti informacijske sigurnosti, uključujući i razumijevanje algoritama i njihovu ulogu u zaštiti podataka. Time se stvara snažna kultura svijesti o sigurnosnim rizicima, što je ključno za očuvanje integriteta, povjerljivosti i dostupnosti informacija u organizaciji.

2.3. Mjere informacijske sigurnosti u algoritamskom okruženju

Govoreći o specifičnim defanzivnim mjerama za zaštitu podataka i osiguravanje povjerljivosti informacija, autori i stručnjaci iz područja informacijske sigurnosti predlažu nekoliko sigurnosnih kontrola koje pojedincu omogućavaju da utječe na povećanje nivoa zaštite podataka:

- a) Enkripcija podataka koristi se za šifriranje osjetljivih podataka kako bi se osiguralo njihovo ograničeno čitanje ili zloupotrebljavanje u slučaju krivog posjeda, što je posebno važno kada se podaci prenose ili pohranjuju u oblaku (Stallings 2017).
- b) Autentikacija i autorizacija služe za provjeru identitet korisnika i osiguravanje da samo ovlašteni korisnici imaju pristup određenim podacima, što uključuje upotrebu lozinki, dvofaktorske autentikacije i kontrolu pristupa (Stallings 2016).
- c) Sigurnosne zakrpe i ažuriranja softverskih komponenti kako bi se ispravile poznate sigurnosne ranjivosti.
- d) Pouzdanost i dostupnost tiče se osiguravanja dostupnosti informacija što podrazumijeva praksu smanjivanje redundancije, klasifikacije, pohranu podataka i planiranje za oporavak od katastrofe.
- e) Programi obuka i sistematizacija znanja s ciljem podizanja svijesti o algoritamskoj pismenosti i zaštiti podataka.
- f) Politike i procedure tiču se uspostavljanja standardiziranih sistema informacijske sigurnosti unutar organizacija, kompanija i institucija.

Navedene mjere informacijske sigurnosti u algoritamskom okruženju moguće je primijeniti na raznolike kontekste privatnih organizacija i javnih institucija, a kako bi se ispitalo njihovo provođenje u kontekstu Univerziteta u Sarajevu, daljnja razrada i detaljno razvijanje

instrumenata istraživanja zahtijeva određivanje načina na koji će se provođenje i razumijevanje sigurnosnih mjera analizirati u ovom radu. Stoga je nakon postavljanja teorijskog okvira algoritamske pismenosti i informacijske sigurnosti razrađen sistem evaluacije i mjerenja dosadašnjih praksi baziran na postojećim studijama i istraživanjima.

2.3.1. Mjerenje i primjeri dobre prakse

Algoritamska studija (Head, Fister i MacMillan 2020), nastala kao rezultat desetogodišnjeg istraživanja u okviru aktivnosti projekta Information Literacy (PIL)⁵⁵, predstavlja značajan doprinos istraživanju informacijske pismenosti u kontekstu algoritamskog okruženja uzimajući u obzir da obuhvata širok spektar obrazovnih ciljeva fokusirajući se na razumijevanje kompleksnog odnosa između algoritama i informacijske pismenosti u digitalnom dobu. Razrađena uz podršku John S. i James L. Knight Fondacije, Harvard Graduate School of Education i Univerziteta u Južnoj Karolini, neke od ključnih značajki ove studije jesu duboka analiza utjecaja algoritama na svakodnevne informacijske navike i pristup informacijama; pružanje uvida u načine na koje algoritmi oblikuju način pretraživanja, evaluiranja i korištenja informacije na internetu; istraživanje percepcija korisnika o ulozi algoritama u filtriranju i dostavi informacija; te analiziranje strategija koje ljudi razvijaju kako bi se nosili s posljedicama algoritamskog upravljanja.

Prvi dio Studije (Head, Fister i MacMillan 2020), istražuje algoritamske faktore koji su doveli do dubokih promjena u informacijskom društvu, uključujući velike količine podataka, automatizirano donošenje odluka i umjetnu inteligenciju, dok drugo poglavlje donosi nalaze iz fokus grupa sa studentima i intervju s fakultetskim osobljem o automatiziranom donošenju odluka, personalizaciji informacija i vijesti, te zabrinutostima o njihovom utjecaju. Na kraju, treći dio izlistava četiri preporuke za nastavnike, bibliotekare i novinare, razmatrajući mogućnosti za ponovno definiranje informacijske pismenosti.

Budući da PIL Studija kroz istraživanje izazova i prilika u algoritamskom društvu pomaže identificirati ključna područja koja zahtijevaju posebnu pažnju u obrazovanju i obuci kako bi

⁵⁵ Projekt Informacijska pismenost (PIL) je neprofitni istraživački institut u San Franciscu koji proučava pozicije i iskustva studenata u digitalnom dobu. U nizu od 11 znanstvenih istraživanja, PIL je istraživao kako američki studenti i alumni koriste istraživačke vještine, informacijske kompetencije i strategije za izvršavanje akademskih zadataka, interakciju s vijestima i rješavanje informacijskih problema u svakodnevnom životu i na radnom mjestu. Istraživački nalazi i preporuke iz PIL-ovih studija informirali su i utjecali na razmišljanje i prakse različitih dionika iz cijelog svijeta, uključujući one u visokom obrazovanju, javnim bibliotekama i medijima.

se disciplina informacijske pismenosti prilagodila trenutnim zahtjevima algoritamskog oblikovanja društvenih procesa, korištena metodologija služi kao dragocjena polazna tačka za razvoj istraživačkih metoda u ovom radu.

3. Metodološki okvir

Rasprava u prethodnom odjeljku predstavila je teorijski pregled i rezime dosadašnjih praksi na Univerzitetu u Sarajevu kao uvod u određivanje istraživačkih pitanja unutar metodološkog okvira istraživanja. Stoga se istraživačka pitanja razlikuju u vrsti s obzirom da uključuju identifikaciju sličnosti i razlika između pojmova medijske, informacijske i algoritamske pismenosti, deskriptivno opisuju značaj elemenata informacijske sigurnosti poput standardizacije i zaštite podataka. Postavljajući predmetno određenje istraživanja na algoritamsku pismenost na Univerzitetu u Sarajevu te problem istraživanja dosadašnjih iskustva algoritamske pismenosti studenata, nastavnog i nenastavnog osoblja, njihove percepcije odnosa između informacijske sigurnosti i zaštite podataka te potreba za unapređenjem postojećih modela pristupa na Univerzitetu u Sarajevu, izvedena su tri istraživačka pitanja:

IP1: ispitati dosadašnje predodžbe i iskustva algoritamske pismenosti studenata, nastavnog i nenastavnog osoblja.

IP2: analizirati kako studenati, nastavno i nenastavno osoblje vide odnos informacijske sigurnosti, zaštite podataka i algoritamske pismenosti.

IP3: koje su mogućnosti unapređenja dosadašnjih praksi algoritamske pismenosti na Univerzitetu u Sarajevu.

Kako bi se odgovorilo na istraživačka pitanja, ovaj rad koristi se metodama kvalitativne analize sadržaja (Mayring 2010) i tematske analize (Braun i Clarke, 2006) koje omogućavaju dublje razumijevanje iskustava, stavova i percepcija sudionika u istraživanju te sistematizaciju i interpretaciju kvalitativnih podataka.⁵⁶ Problem istraživanja proizlazi iz nedostatka informacija o razini algoritamske pismenosti studenata na Univerzitetu u Sarajevu, a predmet istraživanja razina algoritamske pismenosti studenata, nastavnog i nenastavnog osoblja fokusirajući se na Fakultet političkih nauka i Katedru za informacijske nauke Filozofskog fakulteta Univerziteta u Sarajevu. Rezultati kvalitativnih analiza nastojat će dati nove uvide u

⁵⁶ Kvalitativna analiza sadržaja koristi se za analizu intervjua kako bi se identificirali centralni elementi u odgovorima sudionika na istraživačka pitanja, dok tematska analiza služi za identificiranje i analizu ključnih tema i motiva koji se pojavljuju u ovim kvalitativnim podacima

stanje i perspektive medijske, informacijske i algoritamske pismenosti u kontekstu informacijske sigurnosti i zaštite podataka.

3.1. Ciljevi istraživanja

Na temelju dosadašnje metodologije i postavljenih istraživačkih pitanja, možemo definirati kako se ostvaruju naučni i društveni ciljevi ovog master rada i istraživanja. Prvo, kroz dublje razumijevanje trenutnih stanja i izazova u vezi s algoritamskom pismošću, društveni cilj rada jeste prvenstveno identifikacija mogućih poboljšanja u praksama algoritamske pismenosti koja potom ispunjava prvi uslov za unapređenje obrazovanja na ovom polju, poput kreiranja smjernica i preporuka za unapređenje obrazovnih programa i metoda na Univerzitetu u Sarajevu kada je riječ o boljoj pripremi studenata i osoblja za izazove informacijske sigurnosti i zaštite podataka. Osim toga, ovaj društveni cilj doprinosi stvaranju svijesti o važnosti algoritamske pismenosti u savremenom informacijskom društvu, potičući raspravu o njenom značaju ne samo unutar obrazovnih institucija već i u širem kontekstu društvene odgovornosti.

Nadalje, naučni ciljevi fokusiraju se na ispitivanje dosadašnjih predodžbi i iskustava kroz pregled razine algoritamske pismenosti među studentima, nastavnim i nenastavnim osobljem na Univerzitetu u Sarajevu. Percepcija algoritama i (ne)postojanja potrebe za zaštitom podataka otkriva kako sudionici istraživanja djeluju u akademskim, stručnim i ličnim aktivnostima vezanim za procese zaštite podataka i informacijske sigurnosti. Postavljajući prikaz trenutnog stanja u specifičnom kontekstu već razvijene naučno-istraživačke platforme medijske i informacijske pismenosti i holističkog modela, ciljno usmjerenje čini i prilika za istraživanja koji bi obuhvatila veći korpus i sličan tematski fokus. Na taj način, uključivanje većeg broja studenata i osoblja Univerziteta u Sarajevu olakšalo bi identifikaciju potencijalnih problema i nedostataka u trenutnim pristupima te predlaganje konkretnih poboljšanja iskustva svih ciljnih skupina istraživanja.

3.2. Način istraživanja

Kako bismo dublje razumjeli temu algoritamske pismenosti kroz uvid u iskustava studenata i osoblja Univerziteta u Sarajevu, koristeći kvalitativni pristup, provedeni su polustrukturirane intervju, koji su pomogli pri prikupljanju podataka i informacija za istraživačka pitanja IP1, IP2 i IP3. Cilj tehnike intervjua bio je identificirati obrasce percipiranja i ponašanja studenata prvog, drugog i trećeg ciklusa te nastavnog i nenastavnog osoblja prilikom participiranja u algoritamskim procesima. Zajednički elementi u pojedinačnim tačkama gledišta ispitanika biće

korišteni u kasnijoj diskusiji za utvrđivanje specifičnih, jedinstvenih i klasificiranih izazova digitalne transformacije na razini sistemskih rješenja. Različiti stupnjevi pismenost i načini percipiranja svakog pojedinačnog ispitanika omogućavaju sagledavanje šireg kritičkog uklona razine znanja, vještina, vrijednosti specifičnih kategorija unutar ciljane skupine.

3.2.1. Odabir uzorka

Općenito posmatrajući odabir ciljne skupina učesnika istraživanja može biti vođen različitim kriterijima, a u slučaju kvalitativne analize studenata i osoblja Univerziteta u Sarajevu, odabran je neprobabilistički uzorak koji se ne bazira na temelju proračuna vjerovatnosti – umjesto toga, postavljen je u skladu sa određenim kriterijima istraživača. Niz kriterija odabira inicira namjerno uzorkovanje koje se za potrebe ovog rada bazira na pet kriterija:

- studenti koji su na prvoj godini prvog ciklusa studija na Odsjeku sigurnosnih i mirovnih studija Fakulteta političkih nauka i Katedre za informacijske nauke Filozofskog fakulteta Univerziteta u Sarajevu pohađali predmet medijske i informacijske pismenosti;
- nastavno i nenastavno osoblje Fakulteta političkih nauka Univerziteta u Sarajevu koje je aktivno učestvovalo u aktivnostima razvoja i integracija medijske i informacijske pismenosti u visokoškolski obrazovni sistem;
- studenti, nastavno i nenastavno osoblje Fakulteta političkih nauka Univerziteta u Sarajevu koje nije imalo direktnog, kontinuiranog i sistemskog učešća u informacijskom, medijskom i algoritamskom opismenjavanju;
- studenti Fakulteta političkih nauka te studenti Filozofskog fakulteta Univerziteta u Sarajevu koji su aktivno učestvovali u lokalnim, regionalnim i globalnim naučnoistraživačkim projektnim aktivnostima promicanja medijske i informacijske pismenosti;
- studenti interdisciplinarnog master studija Informacijska sigurnost na Odsjeku sigurnosnih i mirovnih studija Fakulteta političkih nauka Univerziteta u Sarajevu.

Među relevantnim faktorima za odabir uzorka ciljne skupine studenata ubraja se: 1. relevantnost za temu istraživanja – studenti pohađaju predmete medijske i informacijske pismenosti, zaštite podataka, digitalne kulture i organizacije informacija, što ih čini relevantnima za procjenu dosadašnje razine algoritamske pismenosti; 2. raznolikost iskustava – ciljna skupina studenata sadrži profile sa određenim predznanjem o umjetnoj inteligenciji, dok drugi nemaju značajnog

iskustva u tom području što omogućuje analizu razlika u percepcijama i iskustvima među studentima s različitim razinama predznanja; 3. perspektiva studenata i budućih stručnjaka iz oblasti informacijske sigurnosti i zaštite podataka; 4. specifični istraživački interesi i projektni angažman u promicanju medijske, informacijske i algoritamske pismenosti.

Ciljna grupa uključuje nastavno i nenastavno osoblje zbog nekoliko faktora: 1. različite uloge u obrazovnom procesu vezane za iskustva integracije medijske i informacijske pismenosti od 2017. godine, trenutne nastavno-naučne aktivnosti i procese planiranja budućnosti obrazovanja uslovljavaju niz raznolikih perspektiva algoritamske pismenosti; 2. nastavno osoblje može prepoznati unutarne prepreke i mogućnosti za implementaciju algoritamske pismenosti; 3. nastavno osoblje može prepoznati unutarne prepreke i mogućnosti za njenu implementaciju 4. praktična iskustva i stručni uvidi nenastavnog osoblja u primjeni informacijske sigurnosti i zaštite podataka u stvarnom radnom okruženju, kako u operativnom funkcionisanju i održavanju institucionalne „digitalne higijene“, tako i u razvoju algoritamske pismenosti kroz procese oblikovanja strategija za unapređenje nastavnih planova i programa.

CILJNA SKUPINA	KRITERIJI ZA ODABIR CILJNE SKUPINE			
	MIP NPP	InfoSec NPP	Aktivno učešće	Pasivno učešće
Studenti FPN UNSA	2	3	3	7
Studenti FF UNSA	2		2	
Nastavno osoblje FPN UNSA			1	1
Nenastavno osoblje FPN UNSA		1	1	2

Tabela 1: Prikaz kriterija za odabir ciljne skupine

Tabela 1 nudi numerički prikaz karakteristika ispitanika istraživanja prema specifičnim kriterijima odabira. Od ukupnog broja od osamnaest (N=18) ispitanika koji su izabrani za učestvovanje u istraživanju, četiri (n=4) ispitanika pohađala su predmet medijske i informacijske pismenosti i javni otvoreni online kurs (MOOC) na prvoj godini studija Odsjeka sigurnosnih i mirovnih studija Fakulteta političkih nauka i Odsjeka za komparativnu književnost i informacijske nauke Filozofskog fakulteta Univerziteta u Sarajevu; četiri (n=4) interdisciplinarni master studij informacijske sigurnosti na Fakultetu političkih nauka Univerziteta u Sarajevu. Od ukupnog broja odabranih studenata, četiri (n=4) ispitanika učestvovala su aktivno u istraživanjima i projektnim aktivnostima medijske i informacijske

pismenosti, dok preostalih osam (n=8) nije uključeno u kontinuirani proces na sistemskom nivou. Kada je riječ o učešću nastavnog i nenastavnog osoblja, troje (n=3) ispitanika učestvovalo je aktivno, a dvoje (n=2) pasivno u razvoju medijske, informacijske i algoritamske pismenosti, kroz povremeno prisustvo seminarima i predavanjima različitih međunarodnih i lokalnih nevladinih organizacija.

Razlog za neujednačen broj studenata na prvoj godini prvog ciklusa studija na Odsjeku sigurnosnih i mirovnih studija FPN UNSA i Katedri za informacijske nauke FF UNSA te nastavnog i nenastavnog osoblja koji su izabrani kao učesnici istraživanja proizlazi iz strukturne organizacije pojedinih odsjeka i katedri na ova dva fakulteta⁵⁷ kao i iz nemogućnosti intervjuiranja pojedinih lica kako bi se smanjio rizik sukoba interesa i posljedica prigodnog uzorka⁵⁸. Međutim, zabilježeno je da se studenti Filozofskog fakulteta uključeni u istraživanje pojavljuju istovremeno u ulozi učesnika aktivnog promicanja medijske i informacijske pismenosti zbog čega su mogli ponuditi dodatnu perspektivu vannastavnih aktivnosti. Studenti koji nisu bili aktivno uključeni, birani su kombinirajući namjerno uzorkovanje⁵⁹ te uzorak dobrovoljaca i snježne grudve.

3.2.2. Priprema i instrumenti istraživanja

Prije početka procesa uključivanja sudionika, urađen je pregled dostupne literature o algoritamskoj pismenosti, specifično u području ispitivanja studentske populacije i akademskog osoblja, a shodno prethodnim uvidima Studije (2020) u okviru projekta Informacijska pismenost. Polazišta o algoritamskom dobu u prvom i percepcije studenata u drugom poglavlju te opisane tehnike i načini provedbe u metodama na kraju konsolidiranog dokumenta, bile su polazna tačka prilagođenog okvira za izradu upitnika prema postavljenim istraživačkim pitanjima ovog magistarskog rada. Jedan od aneksa, Skripta održanih fokus grupa⁶⁰ i pitanja za intervju u sklopu objedinjenog teksta Studije o algoritmima, poslužili su za

⁵⁷ Filozofski fakultet broji trinaest odsjeka i dvije katedre, a Fakultet političkih nauka pet odsjeka zbog čega je od samog početka u procese razvoja medijske i informacijske pismenosti u drugom slučaju bilo olakšano integrirati veći broj nastavnog i nenastavnog osoblja zbog smanjene disperzivnosti disciplina i područja. Nadalje, Odsjek za sigurnosne i mirovne studije kao i Fakultet političkih nauka općenito bilježi veći broj studenata koji se u okviru vlastitih disciplina bave pojedinim aspektima medijske i/ili informacijske pismenosti.

⁵⁸ Jedan od oblika neprobabilističkih uzoraka, prigodni uzorak nosi rizik velikog broja pristrasnih ispitanika jer se temelji na praktičnosti ili dostupnosti, a ne na strogo utvrđenim statističkim metodama.

⁵⁹ Namjerno uzorkovanje ove kategorija zasniva se na izboru onih studenata koji zbog svoje uključenosti u druge aktivnosti Univerziteta i Fakulteta mogu dati uvid u mogućnosti sistemskih rješenja algoritamske pismenosti.

⁶⁰ Objavljena pod Creative Commons licencom CC BY-NC SA. (Imenuj autora-Nekomercijalno-Dijeli pod istim uvjetima), Skripta fokus grupa ne može se koristiti u komercijalne svrhe i ako je sadržaj izmijenjen ili prilagođavan mora biti diseminiran pod istom licencom.

kreiranje dijelova pojedinačnih setova pitanja⁶¹ i etičkih aspekata forme informiranog pristanka. Razrada etičkih aspekata istraživanja prethodila je standardiziranom postupanju sa ispitanicima prije, tokom i nakon provođenja intervjua, te tekstualnim i audio materijalom nakon njihovog održavanja: 1. svi sudionici bili su obaviješteni o svrsi istraživanja, da imaju mogućnost odbiti sudjelovanje i povući svoj pristanak u bilo kojem trenutku; 2. osigurana je anonimnost sudionika i povjerljivost njihovih odgovora; 3. uklonjena su imena i/ili bilo kakve osobne identifikacijske karakteristike iz bilješki i dodijeljeni kodni brojevi svakom ispitaniku kako biste osigurali anonimnost; 4. dopunjeni su nedostajući podaci; 5. poslan je e-mail zahvale studentima i osoblju; 5. uništene su istraživačke bilješke, obrisani audio snimci i osiguran kontinuitet povjerljivosti podataka.

Proces validiranja kreiranih etičkih vodilja istraživanja vezuje se uz zahtjeve koje postavlja Etički kodeks Univerziteta u Sarajevu. Nalažući dostavljanje dokumentacije za ocjenu etičnosti određenog postupka/istraživanja organizacionoj jedinici⁶² postavljeni su standardi postupanja sa ispitanicama i materijalima nastalim tokom istraživanja koji osiguravaju da su intervjui provedeni u skladu s etičkim normama i standardima koji promiču sigurnost i dobrobit ispitanika te integritet istraživanja. Nakon zaprimljene saglasnosti, stvoreni su zakonski uslovi za vremensko i prostorno planiranje detalja održavanja intervjua sa ciljnim skupinama.

⁶¹ Pitanja za fokus grupe projekta Informacijska pismenost prilagođena su srodnoj tehnici provođenja intervjua sa ciljanim skupinama u sekcijama: 1. iskustva osobe u vezi s načinima na koje je pristupala online informacijama u proteklim sedmicama, tražeći od ispitanika da pruže nedavni primjer pronalaženja informacija putem interneta na platformama poput Googlea, YouTube-a, Instagrama ili Facebooka kako bi istraživač dobio uvid u navike i iskustva studenata i osoblja u korištenju popularnih online platformi kao izvora informacija u njihovom svakodnevnom životu; 2. istraživanje svijesti ispitanika o tome da popularne platforme poput Googlea, YouTube-a, Instagrama i Facebooka koriste algoritme za personalizaciju informacija i vijesti koje im dostavljaju, postavljajući pitanje o korištenju algoritama, nizova programskog koda koje obično ne vide, kako bi se informacije prilagodile njihovim preferencijama i interesima s ciljem da istraživanje obuhvati i aspekt stupnja upoznatosti s konceptom personalizacije sadržaja putem algoritama i načina percipiranja ove prakse na spomenutim platformama; 3. zabrinutost ispitanika u vezi sa sve većom personalizacijom rezultata koje dobivaju putem online platformi, pitajući ih za detalje ličnih bojazni, obrazloženje razloga za strah, brigu i anksioznost uzrokovanu prikupljanja velike količine podataka i načina na koji se ti podaci koriste kako bi se izdvojile predodžbe o sve većoj personalizaciji i prikupljanju podataka na internetu; 4. utjecaj kurseva koje su ispitanici pohađali na njihovo razmišljanje o tome kako se informacije koje primaju stvaraju i oblikuju na različitim online platformama koje koriste s ciljem razumijevanja u kojoj mjeri su kursevi utjecali na svijest ispitanika o procesima oblikovanja informacija na internetu te načinima na koje su razvili kritičko promišljanje.

⁶²Zahtjev, biografiju sa bibliografijom glavnog istraživača, projekt i kratki rezime projekta, prijedlog formulara informiranog pristanka za učesnike u istraživanju, upitnike i druge istraživačke dokumente, potpisan obrazac za Etičku saglasnost organizacione jedinice.

3.2.3. Vremensko i prostorno određenje istraživanja

Kako bi okupili ispitanike istraživanja, poduzeti su naredni koraci:

- a) Slanje inicijalnog e-maila kontaktima nastavnog osoblja Fakulteta političkih nauka Univerziteta u Sarajevu kako bi predložili studente za ispitivanje prema unaprijed postavljenim kriterijima;
- b) Slanje inicijalnog e-maila studentima Filozofskog fakulteta Univerziteta u Sarajevu sa uvodnim informacijama o istraživanju;
- c) Slanje inicijalnog e-maila nastavnom i nenastavnom osoblju Filozofskog fakulteta Univerziteta u Sarajevu sa uvodnim informacijama o istraživanju;
- d) Dostavljanje detaljnog informativnog e-mail sa prilogom informativnog pisma i rasporeda mogućih termina za održavanje intervjua.

Detaljni informativni e-mail dostavljen je na preko 30 e-mail adresa kako bi se otvorio prostor za dobrovoljno javljanje studenata koji nisu učestvovali u dosadašnjim aktivnostima razvoja medijske i informacijske pismenosti. Postavljen je dovoljno fleksibilan vremenski okvir imajući u vidu da se planirani intervjui poklapaju sa terminima održavanja pojedinih septembarskih ispita te je također prosljeđen poziv za Zoom sastanak u slučaju nemogućnosti fizičkog prisustva studenata i osoblja. Glede osiguravanja mjesta održavanja intervjua, pripremljen je prostor Multimedijalne sale Instituta za društvena istraživanja na Fakultetu političkih nauka UNSA. Pri dolasku, svim učesnicima priložen je obrazac informiranog pristanka zajedno sa Prilogom 1 – Objašnjenjem istraživanja, etičkim standardima i okvirnim pitanjima zajedno sa ponuđenim tekstom za čitanje.

Godina/ciklus	UTORAK 12. septembar 2023.	SRIJEDA 13. septembar 2023.	ČETVRTAK 14. septembar
I godina I ciklus FPN UNSA	11:00 - 12:00		
II godina I ciklus FPN UNSA	12:00 - 13:00		
III godina I ciklus FPN UNSA	13:00 - 14:00		
I godina II ciklus FPN UNSA	14:00 – 15:00		
II godina II ciklus FPN UNSA	15:00 – 16:00		
III ciklus i nastavno osoblje FPN UNSA		11:00 – 13:00	
Nenastavno osoblje FPN UNSA		13:00 – 16:00	
Studenti FF UNSA			11:00 – 13:00
dotatni termin za sve godine, cikluse i fakultete			14:00- 16:00

Tabela 2: Datumi prikupljanja podataka s intervjuisanim ispitanicima

Tabela 2 prikazuje detaljan raspored planiranih intervjua za istraživanje o algoritamskoj pismenosti na Univerzitetu u Sarajevu koji je osmišljen je s ciljem efikasnog provođenja intervjua ispitanika i dostavljen svim kategorijama kao prilog informativnom e-mailu. Organiziran prema godinama studija, ciklusima i ulogama učesnika, raspored prikazuje intervjue planirane za tri uzastopna dana, počevši od utorka, 12. septembra 2023. godine i završavajući u četvrtak, 14. septembra 2023. godine. Nakon utorka i intervjua sa studentima prvog i drugog ciklusa Fakulteta političkih nauka Univerziteta u Sarajevu, srijeda je bila predviđena za intervjue sa studentima trećeg ciklusa i nastavnim osobljem, a četvrtak za intervjue s nenastavnim osobljem FPN UNSA i studentima Filozofskog fakulteta Univerziteta u Sarajevu (FF UNSA). Planiran je također i dodatni termin za sve godine, cikluse i fakultete kako bi se osigurala potpuna pokrivenost ciljnih grupa, ali koji nije iskorišten.

Polustrukturirani intervjui izvršeni su uz iduće kriterije: svaki intervju trajao je otprilike 45 do 60 minuta na bosanskom/hrvatskom/srpskom jeziku; vođene su bilješke tokom održavanja; svi intervjui snimljeni su mobilnim diktafonom čiji je manualni transkript urađen po njihovom kompletiranju. Od ukupno osamnaest provedenih intervjua, četiri su održana online putem Zoom platforme, a preostalih četrnaest u Multimedijalnoj sali i Institutu za društvena istraživanja na Fakultetu političkih nauka Univerziteta u Sarajevu. Svi učesnici ostali su anonimni i prikupljeni su jedino njihovi demografski podaci poput oblasti studiranja, zemlje, starosti i uloge (student, nastavnik, saradnik). Uočeni izazovi prilikom intervjuiranja odabranih ispitanika ticali su se ponajviše povremenih tehničkih smetnji online intervjua putem Zoom platforme koje su utjecale na kraće trajanje i sažetije odgovore učesnika istraživanja.

4. Kvalitativne analize istraživanja

Nakon što je dovršen transkript svih intervjua, urađena je njihova analiza uz pomoć NVivo softvera koji je olakšao kategorizaciju i organizaciju transkriptiranih intervjua, čime je omogućeno dublje razumijevanje stavova, iskustava i percepcija sudionika istraživanja. Proces analize podataka započeo je stvaranjem tematskog okvira koji je omogućio identifikaciju ključnih tema i kategorija. Svaki intervju detaljno je pregledan, a relevantni dijelovi teksta označeni su i grupirani u određene tematske kategorije. Kroz ovaj korak, cilj je bio identificirati uzorke i obrasce u odgovorima ispitanika kako bi se odgovorilo na postavljena istraživačka pitanja. Nakon kreiranja tematskog okvira, uslijedila je dublja analiza svake teme ili kategorije. To uključuje usporedbu i kontrastiranje odgovora različitih sudionika, identifikaciju izuzetaka ili konzistentnosti u njihovim odgovorima te traženje dubljih nijansi u interpretaciji. Ovaj korak

omogućio je bolje razumijevanje različitih perspektiva i složenosti tema koje su bile predmet istraživanja. Po završenoj analizi, rezultati su sistematično organizirani i interpretirani kako bi se odgovorilo na istraživačka pitanja IP1, IP2 I IP3 te prezentirani u tekućim poglavljima rada, prateći strukturu istraživačkih pitanja.

U slučaju ove kvalitativne analize, nije bilo potrebno razdvajati grupe odgovora jer se neki odgovori odnose na više od jednog pitanja, kao i na sva tri istraživačka pitanja (IP1, IP1 I IP3). Ipak, u ovom istraživanju imamo dva tipa ispitanika: studente i osoblje pri čemu možemo nastaviti grananje prema različitim kategorijama i svaku od njih podijeliti u nekoliko dodatnih grupa. Prva kategorija grupira studente na one koji su 1. bili sistemski uključeni u podučavanje nekih od aspekata bitnih za odgovaranje na istraživačko pitanje (pohađanje predmeta medijske i informacijske pismenosti te master studija informacijske sigurnosti) 2. one studente koji su sporadično upoznati sa temom; 3. studente oba fakulteta uključene u dodatne i vannastavne aktivnosti, ljetne škole i kurseve medijske i informacijske pismenosti. Sličan način klasificiranja može se primijeniti na nastavno i nenastavno osoblje, pa stoga prva kategorija obuhvata nastavnike, saradnike i stručne saradnike Fakulteta političkih nauka Univerziteta u Sarajevu koji su do sada 1: imali značajnog iskustva i ulogu u razvoju medijske i informacijske pismenosti u visokoškolskom obrazovnom sistemu te 2. nastavnike, saradnike i stručne saradnike bez primijećenog kontinuiranog doprinosa ovoj oblasti funkcionalne pismenosti.

Za potrebe analize intervjua korištena je kombinacija dvije metode. Izrada kodova kako bi se grupirali u podteme i teme provedena je pomoću analize sadržaja (Mayring 2010, poglavlje 5), a potom je uvedena metoda tematske analize u kvalitativnoj analizi (Braun i Clarke 2006). Ovaj kombinirani pristup omogućio nam je detaljnu analizu intervjua s više perspektiva i dublje razumijevanje iskustava i stavova ispitanika u vezi s istraživačkim pitanjima. Metoda analize sadržaja ponudila je početni skup od 118 kodova koji su se filtriranjem i sažimanjem sveli na pregledniji broj od 53 koda⁶³. Filtriranje i sažimanje kodova pomoglo je identificirati ključne tematske elemente intervjua, čime je postignuta fokusiranost analize sadržaja. Kasnija tematska analize u okviru kvalitativne analize, prema Braunu i Clarkeu (2006), pružila je kontekstualni pregled intervjua, omogućujući bolji uvid razmatranih teme i bolje razumijevanje složenosti iskustava i stavova ispitanika.

Tabela 3: Prikaz tema, podtema i kodova sadržajne analize intervjua

BR.	TEMA	PODTEMA	KOD
-----	------	---------	-----

⁶³ Zbog neujednačenog pristupa označavanju dijelova teksta, u procesu revizije kodova, bilo je potrebno smanjiti redundaciju sažimanje sličnih ili istih skupova kodova.

I	Algoritamska pismenost u MIP kontekstu	<ol style="list-style-type: none"> 1. Mediji i informacije 2. Konvergencija 3. Algoritamska pismenost 4. Predodžbe algoritma 	<ol style="list-style-type: none"> 1. Algoritamska pismenost kao olakšavanje rada 2. Važnost algoritamske pismenosti 3. Nedostatak edukacije o algoritamskoj pismenosti: 4. Definicija Koncepta Pismenosti 5. Medijska pismenost 6. Informacijska pismenost 7. Algoritamska pismenost 8. Veza između medija i informacijske pismenosti 9. Odnos prema algoritamskoj pismenosti
II	Obrazovanje i iskustvo	<ol style="list-style-type: none"> 1. Kursevi 2. Javni otvoreni online kurs 3. Moduli 9 i 10 	<ol style="list-style-type: none"> 10. Potreba za praktičnim znanjem: 11. Prepoznavanje pouzdanih informacija i vijesti 12. Obrazovna pozadina 13. Individualna i kolektivna edukacija 14. Edukacija o medijskoj pismenosti 15. Utjecaj kurseva na razumijevanje informacija
III	Utjecaj platformi i društvenih mreža	<ol style="list-style-type: none"> 1. Reznacija 2. Indignacija 3. Potreba za akcijom 4. Generacijski jaz 5. Digitalni jaz 6. Opći dojam 7. Stavovi javnosti i okoline 	<ol style="list-style-type: none"> 16. Utjecaj medija na političke stavove 17. Izazovi starijih osoba u razumijevanju tehnoloških koncepata 18. Pristup pronalasku pouzdanih informacija 19. Utjecaj na stariju populaciju 20. Utjecaj na mlađu populaciju 21. Potreba za akcijom
IV	Algoritmi i personalizacija	<ol style="list-style-type: none"> 1. Prikupljanje zvučnih podataka 2. Tehnokapital 3. Političke manipulacije 4. Medijske manipulacije 	<ol style="list-style-type: none"> 22. Personalizacija sadržaja i utjecaj algoritama 23. Zabrinutost zbog personalizacije i privatnosti 24. Odnos prema personaliziranim pretragama i preporukama: 25. Razmišljanje o personalizaciji sadržaja 26. Iskustvo s personalizacijom sadržaja 27. Utjecaj algoritama na prikazivanje informacija 28. Motivi platformi za personalizaciju sadržaja 29. Razmišljanje o utjecaju personalizacije na raznolikost informacija 30. Iskustvo s personaliziranim pretragama 31. Utjecaj personalizacije na online iskustvo 32. Različiti doživljaji personalizacije 33. Razumijevanje razloga za personalizaciju 34. Stav prema personalizaciji i privatnosti 35. Razmišljanje o utjecaju personalizacije na raznolikost informacija

			36. Utjecaj personalizacije na online iskustvo 37. Filter mjehuri i eho komore
V	Privatnost i sigurnost podataka	1. Zaštita podataka 2. Povjerljivost informacija 3. Informacijska sigurnost	38. Povezanost algoritamske pismenosti, informacijske sigurnosti i zaštite podataka: 39. Razumijevanje informacijske sigurnosti: 40. Svjesnost o privatnosti i zaštiti podataka: 41. Mjere zaštite privatnosti na internetu: 42. Briga o privatnosti 43. Razumijevanje rizika u vezi sa zloupotrebom podataka 44. Utjecaj informacijske sigurnosti na zaštitu privatnih informacija 45. Razumijevanje algoritama za bolju digitalnu sigurnost 46. Povezanost algoritamske pismenosti s informacijskom sigurnošću
VI	Kritička svijest i (samo)regulacija	1. Mjere zaštite 2. Odgovornost pojedinca 3. Odgovornost države 4. Standardizacija	47. Zakonodavstvo, regulacija i usklađenost 48. Odgovornost korisnika 49. Poslovni modeli i porezi 50. Transparentnost i osvještavanje korisnika 51. Evaluacija koristi zaštite privatnosti 52. Alati za Zaštitu Privatnosti 53. Defanzivne prakse

4.1. Algoritamska pismenost u MIP kontekstu

U prvoj koloni Tabele 3 predstavljeno je šest krovnih tema koje obuhvataju četrnaest fokusiranih tema/podtema u drugoj i njima pripadajućih kodova u trećoj koloni. Prva tema, *algoritamska pismenost u MIP kontekstu* pokazala je razumijevanja koncepta algoritamske pismenosti u odnosu sa predodžbama medijske i informacijske pismenosti. Ispitanici su uglavnom odvojeno posmatrali pojmove medijske, informacijske i algoritamske pismenosti pri tome pokazujući različita poimanja.

4.1.1. Mediji i informacije u odnosu konvergencije i divergencije

Studenti odnos između medijske i informacijske pismenosti uglavnom čitaju preko njihovih osnovnih pojmova i područja proučavanja – medija i informacije:

„Ako imamo tačku A u kojoj nastaje informacija i ona treba preći do tačke B, medij je staza kojom informacija gazi. Percipiramo informacije kroz medije i zato mislim da su povezani“ (student, II godina, I ciklus FPN UNSA).

Raščlanjivanje na medijsku i informacijsku pismenost prema područjima proučavanja ima za posljedicu da se pri tumačenju pojmova koji ga čine, integrirani koncept razumijeva kao konvergenijska posljedica već postojećih odvojenih i samodostatnih područja izučavanja. Prvenstveno, studenti medijsku pismenost uglavnom vide kao vještinu i kritičku sposobnost analiziranja sadržaja koje mediji plasiraju, bilo da se radi o fizičkom formatu ili online portalima: „Medijska pismenost je šiti pojam, sve što nam dolazi kroz razne medije“ (student FPN, I godina, II ciklus). Dok nastavno i nenastavno osoblje također pokazuje ujednačeno shvatanje medijske pismenosti, uočena su rijetka odstupanja pojedinih studenata. Takvi izuzeci tiču se izjednačavanja sa drugim srodnim pojmovima poput digitalne pismenosti:

„Medijska pismenost je za mene sinonim za digitalnu pismenost, odnosno, određene tehnike upotrebe određenih medija.“ (student FPN, I godina, II ciklus)

Nenastavno osoblje obratilo je više pozornosti drugom dijelu integriranog MIP koncepta tematizirajući informacijsku pismenost kroz akademski rad, dosadašnja iskustva studiranja i profesije koje su pomogle u razvijanju vještina akademskog pisanja:

„Informacijsku pismenost najlakše mi je objasniti kroz rad na akademiji, podrazumijeva se da znamo tražiti i vrednovati informacije, koje su informacije provjerljive i znamo da se ima i mnogo neutemeljenih teza, tako da ima istraživanja koja su *fake* istraživanja, ali su strašno velike opasnosti u toj nekoj odluci da napravite odluke i da se napravi jedan dobro argumentiran rad.“ (viši stručni saradnik za nastavu FPN UNSA)

Navodeći etičke kodekse i poredeći prijašnju praksu plagijarizma u neumreženom informacijskom okruženju, nenastavno osoblje istaklo je poseban značaj informacijske pismenosti za istraživače jer se odnosi na vrednovanje informacija, načine preuzimanja i intepretacije tekstova, dokumenata i materijala općenito.

Viši stručni saradnici naglasili su i potrebu za objedinjenim MIP konceptom s obzirom da podrazumijeva set različitih kompetencija, čini osnovnu funkcionalnu komponentu bilo kojeg društva i „šesto čulo koje svi pojedinci trebaju imati kako bi mogli učestvovati produktivno u današnjem društvu“ (viši stručni saradnik FPN UNSA). Analizirajući općenito stavove i prododžbe o razlozima zbog kojih bi se medijska i informacijska pismenost trebale posmatrati, razvijati i provoditi integrisano, uočen je sličan stav svih ispitanika koji je zasnovan na jednom od dva kriterija: 1. stavovi bazirani na uslovljenosti dva područja proučavanja (mediji + informacije) i 2. stavovi temeljeni na dosadašnjim nastavnim praksama:

„Uvijek kombinujem kada kažem šta je medijska i informacijska pismenost jer mi je tako ostalo u glavi tokom učenja o korištenju medija i informacija u smislu opismenjavanja ljudi i društva općenito“ (student FF UNSA, I godina, II ciklus).

Pored prednosti objedinjenog koncepta, manji broj ispitanika naveo je dopunjeni ili drugačiji tip odgovora. Potvrđujući da je medijsku i informacijsku pismenost kao integrirani model predložio UNESCO, nekoliko učesnika ispitivanja osvrnulo se na potrebnu za dodatnim promišljanjem i dekonstrukcijom strukture koncepta kako bi se njegovi pojedinačni elementi mogli sagledati detaljnije. Zatim, osim nužnosti komplementarnog pristupa naglašena je i potreba za detaljnijim izučavanjem informacijske pismenosti.

„Potrebno je obratiti više pažnje na informacijsku pismenost jer smo izloženi puno većem broju informacija koje nisu direktno iz medija i ne možemo govoriti samo o medijskoj pismenosti.“ (docent FPN UNSA)

Slično gledište o potrebi za redefiniranjem objedinjenog koncepta naveo je i student koji je na prvoj godini ciklusa pohađao predmet Medijska i informacijska pismenost:

„Medijska pismenost koristi se za svakodnevne stvari, a informacijska pismenost ima nivo stručnijeg okruženja, može se primijeniti na razne stvari. Kako bi medijska i informacijska pismenost bila dobro integrisana u idealno digitalno okruženje, ne mislim da se medijska odvoji od informacijske, već da se umjesto akcenta na medijski sadržaj naglašava da svako proizvodi medijski sadržaj.“ (student FF UNSA, III godina I ciklus)

Sugestije sudionika o potrebi za kritičkim sagledavanjem koncepta medijske i informacijske pismenosti ističu potrebu za ispitivanjem nijansi i komponenti unutar ovog šireg konteksta koja uključuje razumijevanje složenosti algoritama, podataka i njihovih implikacija. Odgovori studenata i osoblja u vezi s algoritamskom pismenošću pokazuju kako ispitanici percipiraju njenu ulogu u širem kontekstu medijske i informacijske pismenosti, kao i njihove uvide u specifične izazove i prilike.

4.1.2. Predodžbe algoritamske pismenosti

Za razliku od medijske i informacijske pismenosti koju su svi ispitanici percipirali i objasnili naglašavajući odvojeno medijsku, informacijsku i/ili objedinjeni koncept, predožba ispitanika o pojmu algoritamske pismenosti vezuje se isključivo za objedinjeni koncept. Drugim riječima, učesnici istraživanja algoritamsku pismenost vide u svojstvu posljednje karike postojećeg MIP niza:

„Algoritamska pismenost ide korak dalje, istražujući što se krije iza kulisa, kako informacije dolaze na ekran i kako se prikazuju u medijima.“ (student FPN UNSA, III godina)

„Ako su MIP riječi i slova, algoritamska pismenost bi bila gramatika toga, po mom nekom viđenju.“ (viši asistent FPN UNSA)

„Algoritamska pismenost je dublji koncept koji se odnosi na razumijevanje algoritama koji utječu na to koje informacije više vidim, a koje manje.“ (student FPN UNSA I godina, I ciklus)

Nadalje, primjetno je i odstupanje od poznavanja prethodnog oblika kojeg su ispitanici definirali bez poteškoća. U ovom slučaju, manji broj studenata nije siguran u opće poznavanje područja algoritamske pismenosti:

"S algoritamskom pismenošću nisam upoznat u potpunosti, ali znam stvari o Facebooku, Instagramu." (student FPN UNSA, I godina)

Naglašeni aspekt automatizacije procesa i olakšavanja rada vidljiv je u par osvrtu i istovremeno prelazi u tehničku domenu izučavanja i prakse:

„Algoritamska pismenost je efikasno iskorištavanje svega toga, automatizacije određenih procesa koji su nas samo usporavali tokom rada, poštivanje matematičke zakonitosti u svim informacijama koje stižu do nas.“ (student FPN UNSA I godina II ciklus)

„Algoritamska pismenost ulazi u svaku profesiju i olakšava rad (student FPN UNSA III godina I ciklus)

Analizirajući ukupan broj ispitanih studenata i osoblja, vidljivo je da su svi nastavnici i saradnici upoznati sa pojmom algoritamske pismenosti koji su definirali bez većih poteškoća, dok su studenti ponudili raznolike odgovore ističući nedovoljno poznavanje modela, nastavak MIP koncepta i tehničke vještine.

4.2. Obrazovanje i iskustvo

Tema obrazovanja i dosadašnjih iskustava u području algoritamske pismenosti pokazala je da nastavno i nenastavno osoblje Fakulteta političkih nauka nije pohađalo programe obuka koji su vezani specifično za ovu oblast. Studenti Fakulteta političkih nauka nisu pohađali predmete koji su tematizirali konkretno algoritamsku pismenost, dok studenti Katedre za informacijske nauke Filozofskog fakulteta jesu podučavani u sklopu predmeta, ali bi voljeli znati više o specifičnim aspektima.

„Što se tiče algoritamske pismenosti, moram priznati da nisam imala mnogo prilika za usvajanje tog znanja. S druge strane, medijska pismenost je često obrađivana na brojnim radionicama i seminarima.“ (student FPN UNSA, II godina II ciklus)

Iako su predodžbe i iskustva različita, gotovo svi studenti su izrazili želju za boljim razumijevanjem algoritama i sticanjem novih znanja u ovom polju s obzirom da pridaju važnost algoritamskoj pismenosti:

„Vrlo mi je bitno razumjeti što se događa u pozadini.“ (student FPN UNSA, I godina, I ciklus);

„Ja pridajem važnost ovoj temi jer moj posao često ima veze s internetom, ali i da ne radim ono što radim, smatrala bih ovo bitnim.“ (student FPN UNSA, IV godina);

„Pridajem sve više važnosti algoritamskoj pismenosti jer sam shvatila koliko je to kompleksno okruženje.“ (student FPN UNSA, III godina)

Bez obzira na stupanj poimanja i dubinu razumijevanja, nedovoljno doticaja sa preciznim i kontinuiranim aktivnostima algoritamske pismenosti uslovljava prepoznavanje potreba studenata, nastavnog i nenastavnog osoblja za dodatnim edukacijama.

4.2.1. Edukacije i kursevi

Pored studenata Katedre za informacijske nauke Filozofskog fakulteta koji su tokom prvog i drugog ciklusa studija slušali predmete⁶⁴ čije su tematske okosnice pokrivale različite društvene, kulturološke i kritičke dimenzije algoritamskog upravljanja, par studenata Odsjeka za politologiju Fakulteta političkih nauka pohađalo je međunarodne kurseve iz područja informacijske pismenosti. Pri tome, kursevi kojima su studenti prisustvovali prije dvije do tri godine ticali su se aspekata algoritamskog društva, ali ih nisu detaljnije razrađivali zbog fokusa na krovnim temama informacijskih nauka poput procesa pronalaženja, validiranja i diseminiranja informacija za istraživačke i akademske svrhe. Jedan u nizu međunarodnih kurseva u organizaciji Univerziteta u Hildesheimu (Njemačka) tokom posljednjeg zimskog izdanja bavio se intenzivno algoritmima, a ljetni program interkulturalnim aspektima umjetne inteligencije⁶⁵:

⁶⁴ Informacijska i medijska pismenost, Informacijsko društvo, etika i politika, Digitalna kultura i obrazovanje

⁶⁵ Univerzitet u Sarajevu nekoliko godina surađuje sa Univerzitetom u Hildesheimu na organizaciji ljetnih i zimskih škola i međunarodnih kurseva. Posljednje izdanje ljetnog kursa *Interkulturalni aspekti informacijske pismenosti i metapismenosti*, tokom jula 2023. godine uključilo je studente iz Njemačke, Bosne i Hercegovine, Indije i Poljske koji su u grupnom radu obrađivali teme poput upotrebe umjetne inteligencije u kreiranju znanja i istraživanju, AI kao kreativni alat, perspektive nastavnika i studenata te AI u kontekstu produkcije informacija.

Dalje znanje stekao sam na kursu koji sam pohađao preko Instituta za društvena istraživanja FPN UNSA u suradnji sa Univerzitetom u Hildesheimu. Tu sam bio na dva kursa. Prvi je bio malo specifičnije orijetisan na algoritme, a na drugom je priča bila oko umjetne inteligencije. (student FPN UNSA, II godina, I ciklus)

Ispitujući dalje opcije kurseva koje nudi Univerziteta u Sarajevu na temu algoritamske pismenosti, studenti i osoblje nisu prisustvovali obukama, seminarima ili radionicama. S obzirom da je pohađanje masivno otvorenog online kursa (MOOC) sastavni dio predmeta na prvog godini prvog ciklusa studija na Odsjeku sigurnosnih i mirovnih studija Fakulteta političkih nauka, manji broj studenata potvrdio je značaj masivno otvorenog online kursa za uvod u promišljanje o algoritmima, dok studenti drugih odsjeka nisu završili kurs, a veći dio njih nije svjestan postojanja mogućnosti, načina upisa te opcijama samozadatog tempa pohađanja. S druge strane, zabilježena su različita iskustva sa masivnim online kursom nastavnika i saradnika pri čemu je mali broj završio kurs, dok je većina upoznata sa postojanjem mogućnosti koje do sada nisu iskoristili. Nakon što su studenti drugih odsjeka upoznati sa sadržajem kursa, analizirane su njihovi stavovi i preporuke za unapređenje.

4.2.2. MOOC i moduli IX i X

Kako bi se dobio uvid u mogućnosti unapređenja postojećih resursa Univerziteta u Sarajevu, učesnici istraživanja naveli su mogućnost prilagođavanja masivnog otvorenog online kursa. S obzirom da je sadržaj kursa kreiran 2019. godine pratio do tada aktualna kretanja u području algoritama, umjetne inteligencije, informacijske sigurnosti i zaštite podataka, te da je u međuvremenu primijećen značajan otklon pri čemu nije riječ toliko o vremenskom rasponu, već masovnijem problematiziranju algoritamske kulture digitalnog doba, tehnološkim inovacijama i potencijalno novim sigurnosnim prijetnjama, potrebno je ispitati detaljnije opcije za njegovo unapređenje. Stoga su studenti i osoblje prepoznali potencijal opcija koje nude trenutno dostupni resursi te ponudili vlastite prijedloge za adaptaciju sadržaja Modula IX i X javnog otvorenog online kursa.

Nenastavno osoblje procijenilo je koheretnost cjelokupne strukture kursa i njegov značaj za sistematizaciju već postojećih znanja:

Niko nije potpuno medijski, informacijski i algoritamski nepismen. Međutim, o svojoj pismenosti nemaš struktuiranu predodžbu kao nečemu što ima i glavu i rep. To je taj online kurs. Na MOOC-u je sve predočeno, ali idalje ostaje osjećaj nelagode. (viši stručni saradnik FPN UNSA)

Utjecaj masivnog otvorenog online kursa najjasnije je vidljiv kroz jedinstven pregled svih modula pri čemu se znanja nadopunjuju kretanjem polaznika iz nižih i jednostavnijih ka višim i kompleksnijim modulima. Govoreći specifično o modulima koji tematiziraju algoritme, umjetnu inteligenciju i informacijsku sigurnost, nastavno osoblje istaklo je potrebu za dopunjavanjem:

„Treba ih updateovati i teorijski i praktično i u teoriji. Treba puno više primjera i interaktivnih modaliteta za učenje, igrice, kvizova koji će im biti zanimljiviji od samog teksta. Većina ljudi ne čita tekstove ili pročita površno, naslove, kraj i početak, ali interaktivnost intrigira, kao i izazovi i prepreke.“ (docentica FPN UNSA).

Imajući u vidu da je sadržaj modula IX i X uglavnom u tekstualnoj formi uz par kratkih edukativnih videosnimaka i infografika, nastavno osoblje istaklo je nužnost za predstavljanjem sadržaja u različitim formatima koji su prilagođeniji mladima. Osim promjene i dodavanja novih formata, predložena je revizija sadržaja baziranog na primjerima i interaktivnim elementima.

Slično viđenje imaju i studenti oba fakulteta jer navode primjere uvođenja kvizova za provjeru znanja specifično iz oblasti algoritamske pismenosti, što ne potpadaju pod opći kviz znanja kojeg polaznici pohađaju na kraju prelaska dvanaest modula kursa, niti pod postojeća opća pitanja za provjeru znanja na kraju svakog modula. Zbog čestog mistificiranja pojma algoritma i praksi „nevidljive algoritamske ruke“, studenti su izrazili interes za upoznavanje načina na koji algoritam radi kroz simplificirane primjere:

„U modulu o algoritmima bih volio da detaljnije upoznam ono što sam na nekim predmetima upoznao površno, da taj dio dodatno nadogradim u smislu toga kako jedan algoritam funkcioniše“ (student FPN UNSA, I godina II ciklus).

Vjerujući kako interaktivnost može pomoći boljem usvajanju pojmova, razumijevanju načina na koje algoritmi funkcionišu i izgrađivanju ličnih metoda za smanjivanje utjecaja personalizacije i osiguravanja zaštite sigurnosti podataka, najviše studenata istaklo je uvođenje kvizova za samoevaluaciju:

„Možda proširiti u smislu boljeg razumijevanja načina na koje se mi ponašamo – kviz gdje je mladi mogu da selektuju određene odgovore i da im na kraju rezultat pokaže koliko su oni algoritamski pismeni i da li kritički posmatraju sadržaj koji im se nudi. Mislim da bi ih potaklo da više razmišljaju o evaluaciji samih sebe“ (student FF, I godina II ciklus).

Dok većina studenata navodi nove modele za učenje i podučavanje o algoritmima uz pomoć modula na javnom otvorenom online kursu kako bi se poboljšalo korisničko iskustvo i kreiralo poticajno okruženje za praktične osnove algoritamske pismenosti, pojedini studenti obrazložili su specifične razloge zbog kojih je potrebno u module uvesti gemifikaciju i objašnjenje Chat GPT-a:

„Interakciju, mini *game* u kojoj bi neko mogao da izgradi veći osjećaj za digitalno okruženje, koje je dinamično, a definicije su statične, potrebne su ali nisu dovoljne da se razvije razumijevanje za dinamičnost. Ne mislim da je Chat GPT loš, ali nije adekvatno upotrebljen i sva kritika se bazira hoće li studenti prepisivati pomoću njega, a onda se zaboravlja da Chat GPT ne zna citirati, što može biti objašnjeno u modulu da se razvije diskurs u ispravnom pravcu.“ (student FF UNSA, III godina, I ciklus).

Kako bi se već problematizirani algoritamski fenomeni sagledali i sa drugačijih stanovišta, predloženo je uvođenje novih sadržaja, ali i pristupa njihovom kreiranju, a kao primjer navedeno je korištenje Chat GPT-a čije se implikacije na obrazovni proces uglavnom posmatraju iz ustaljenih perspektiva bojazni i potencijalnih opasnosti. Studenti koji imaju osnovna znanja o funkcionisanju algoritama voljeli bi dopuniti postojeća znanja sa složenijim primjerima algoritamskih procesa:

Kompleksniji, senzibilniji odnosi sa algoritmima i kako oni funkcionišu su još uvijek nejasni iz krajnje tehnološke perspektive. Njihov utjecaj na društvo je sasvim jasan, ali kako, zašto i odakle funkcionišu, to mi je još u magli. (student FF UNSA, I godina, II ciklus).

Posmatrajući odgovore ispitanika općenito, primijećene razlike u poimanju algoritama i dosadašnjim iskustvima uslovljavaju i drugačije potrebe, načine i pristupe edukacijama. Međutim, zajednička komponenta u promišljanjima svih ispitanika ostaje potreba za redefiniranjem i dopunjavanjem postojećih resursa koji će moći zadovoljiti sve kategorije polaznika i nuditi određeni set za usvajanje znanja, vještina i kompetencija onih sa višim i nižim stepenom iskustava.

4.3. Utjecaj platformi i društvenih mreža

Kako bi napravili uvod u propitivanje konkretnih aspekata algoritmizacije poput personalizacije sadržaja i narušavanja privatnosti te zaštite podataka, u razgovorima sa ispitanicima, bilo je potrebno prvo steći opći dojam o pogledima na ubrzan razvoj tehnoloških procesa i algoritamskih implikacija u svakodnevnim aktivnostima i komunikaciji sa osobama u okruženju. Ovaj uvod u specifične teme rezigniranosti i generacijskog jaza omogućio je

kasniju kontekstualizaciju dubljih razgovora, identificiranje osnovne promjene u svakodnevnom životu i navikama ispitanika te postavljanje algoritamske pismenosti u širi kontekst koji uzima u obzir opću svijest i stavove, utjecaj na socijalne dinamike i međuljudske odnose. U ovom odjeljku, učesnici istraživanja osvrnuli su se na generalnu rezigniranost o vezi algoritamskih implikacija te su komparirali odnos starijih generacija i mlađih naraštaja.

4.3.1. Rezignacija i indignacija

Nudeći pregled vlastitog okruženja te dijeleći crtice iz svakodnevnog promišljanja o digitalnoj transformaciji, nastavno, nenastavno osoblje i studenti komentirali su indiferentno ophođenje spram tema tehnološkog determinizma. Nenastavno osoblje dotaklo se nemogućnosti izbora glede utjecaja tehnologije i učestvovanja u online okruženju:

„Ali je osjećaj taj da smo svi kooptirani u nešto za šta nas niko nije ni pitao da li želimo, to je samo tako. On ima svoje beneficije, ali isto tako mislim da nezadovoljstvo dolazi prvenstveno od te stvari što je uzbuđenje i nada koje smo imali 90-ih kad se internet pojavio, mi smo vjerovali da će tehnologija i tehnosolucionizam riješiti dosta stvari. Sada nam je jasno da neće. Nisam potpuno skeptičan, medicina i dosta drugih stvari je napredovalo, ali idalje činjenica da ne možemo bez ovoga stvara ogromnu nelagodu. Svrha bivstvovanja jeste da imaš opcije. Ovo nije opcija više“ (viši stručni suradnik za kvalitet FPN UNSA).

„Mislim da smo gurnuti u to iskustvo bez ikakve informacije i pripreme.“ (viši stručni suradnik za nastavu FPN UNSA)

Studenti su također uglavnom pokazali negativnu percepciju vodeći se uvidima iz vlastitih sredina i diskusijama sa osobama iz okoline. Pritom je zapažena posebna kategorija studenata koji studiraju u Sarajevo, ali imaju dodatnu komparativnu perspektivu uslovljenu činjenicom ne dolaze iz Kantona Sarajevo, odnosno, da se u periodima bez nastavnih aktivnosti vraćaju u druge rodne gradove. U ovim slučajevima, studenti bolje uviđaju disrazmjer odnosa i kritičkog aspekta fakultetske sredine spram digitalnog algoritamskog okruženja izvan akademskog *filtera*, te su bili u stanju ponuditi širi spektar primjera i iskustava navodeći raznolike primjere:

„Ponekad mislim da živim dvojni život. Jedan u Sarajevu i jedan drugi u Livnu kada odem kući gdje sam se rodio. Tamo se često družim s ljudima koji se ne bave puno takvim stvarima i onda dobijem drugu perspektivu. Recimo, kako o tome razmišlja čovjek koji svoj ručak zaradi montiranjem PVC stolarije. Osjeti se razlika kad pričam sa ljudima koji studiraju, sa kojima se družim na fakultetu i privatno u Sarajevu i kada sam kući. Mislim da je čisto razlika u tome da

ovdje ljudi imaju puno više filtera medija, dok su drugi spužvasti na neki način.“ (student FPN UNSA, II godina, I ciklus)

Nastavno osoblje pokazalo je dvojaku perspektivu. Jedni vjeruju da je većina njihovih kolega otprilike upoznata sa konceptom, ali se mogu prepoznati i pojedinci bez temeljnog shvatanja teorijskog okvira i praktikovanja digitalne higijene koja počinje od medijske i informacijske pismenosti, dok kod osoba izvan akademske sredine primjećuju nedostatak tematiziranja i kritičkog gledanja na algoritame. Drugi pak uviđaju obrnutu situaciju jer dublje razgovore i dijeljenja iskustava obično imaju sa kolegama izvan fakulteta.

„Mislim da dosta toga ne razumiju, jedino kada im objasnim plastično. To jer znak da taj koncept nije dovoljno zastupljen u široj javnosti i pri tome mislim na cjeloživotno učenje.“ (docentica FPN UNSA)

„Ironija je da o ovim temama mogu pričati više sa prijateljima i poznanicima izvan nego unutar fakulteta. Naravno, ima bar dvoje-troje pojedinaca sa kojima se o ovakvim problemima i pitanjima može pričati. Ostale kolege drže se svojih uskih disciplinarnih granica i nemaju namjeru da izađu iz toga.“ (viši asistent FPN UNSA)

Obraćajući posebnu pažnju na element rezigniranosti unutar šire slike tehnološkog determinizma, gotovo svi ispitanici istakli su da među njihovim prijateljima, kolegama i obitelji vlada osjećaj pomirenosti sa postdigitalnim stanjem. Posebno se izdvajaju izjave koje su prikazale stupnjevanje indiferencije i različite odnose mladih spram tehnološkog determinizma. Naime, studenti su primijetili da mnogi mladi pasivno konzumiraju Internet zadržavajući stav da potonji nije *stvarni svijet*, dok drugi nisu informisani, ali iskazuju interes i žele naučiti više o nevidljivim načinima digitalnog upravljanja iz različitih razloga:

„Često čujem tu apokaliptičnu verziju u smislu da mlade nije briga, bitno im je samo da imaju Instagram. Mislim da ima i interesovanja kod mladih i ako ih to ne zanima zbog njih samih, onda uče da bi to znanje mogli prenijeti starijima“ (student FF UNSA, I godina II ciklus).

4.3.2. Generacijski i digitalni jaz

Tokom objašnjava vlastitih iskustava o općem razmišljanju o utjecaju platformi i društvenih mreža, značajan broj studenata osvrnuo se na problem generacijskog jaza objašnjavajući kako starije generacije unutar uže obitelji, znatno manje razumiju digitalne alate i algoritme, te iako su sposobni koristiti mobilne telefone i računalne uređaje, njihovo razumijevanje je više praktične prirode. Pojedini studenti podijelili su zamjećivanja o

svjesnosti uže obitelji i uvjerenja da nije riječ o općem nepoznavanju, već nedostatku terminologije i pojmovnog aparata kojim bi objasnili vlastita zapažanja:

„Što se tiče mog okruženja, znam da koriste društvene medije, osim nekih starijih kao što su majka i djed, oni nisu upoznati, ne pričaju o tome. Dok otac, mama i svi moji prijatelji i rodbina, oni izuzetno znaju šta je to. Ne znaju da se to zove algoritamska pismenost, ali znaju da algoritam postoji jer su vidjeli da Facebook i Instagram izbacuju reklame i preporuke“ (student FPN UNSA, II godina, I ciklus).

U okviru teme o generacijskom jazu, studenti su odnos starije populacije često upoređivali sa utjecajem platformi i društvenih mreža na djecu i mlađe generacije:

Ono što mene lično najviše zabrinjava jeste dostupnost svega toga djeci koja su izložena i tim sredstvima kao što je Facebook i platformama koje imaju vrlo slabu kontrolu. Najizloženiji su uzrasti djece osnovnih i srednjih škola koji koriste i vrlo su upućeni u način rada tih platformi, ali suština im nije jasna jer nisu dovoljno educirani po tom pitanju i onda često dolazi do cyber nasilja jer ne mogu da naprave jasnu distinkciju između stvarnog i lažnog svijeta. (student FPN UNSA, IV godina)

Primijećeno je i da u kontekstu mlađe populacije, izazovi cyber nasilja i nesporazuma postaju jasniji. Stoga par studenata prepoznaje da je odgovornost mladih, koji su većinom *digitalno* pismeniji, da podijele svoje znanje i iskustvo sa starijim i mlađim generacijama kako bi se smanjio jaz u razumijevanju digitalnog svijeta. Zajedno sa vlastitom odgovornošću, ispitanici su istakli i odgovornost društva, institucija, vladinih i nevladinih organizacija, uključujući tako formalno i neformalno obrazovanje u obučavanje djece za korištenje novih tehnologija od najranijih faza razvoja. Poseban problem studenti i osoblje vide u društvenoj platformi TikTok koja se uglavnom koristi za zabavu, ali je istovremeno potrebno obratiti pažnju na popularnost određenih sadržaja na društvenim platformama i razmotriti kako se mogu iskoristiti za edukativne svrhe. Upravo je podučavanje i učenje o utjecaju personalizacije sadržaja i uloge algoritama na oblikovanju onoga što korisnici vide i doživljavaju na društvenim platformama poput TikTok-a ili drugih medijskih i informacijskih kanala jedan od pristupa koji su ispitanici naveli.

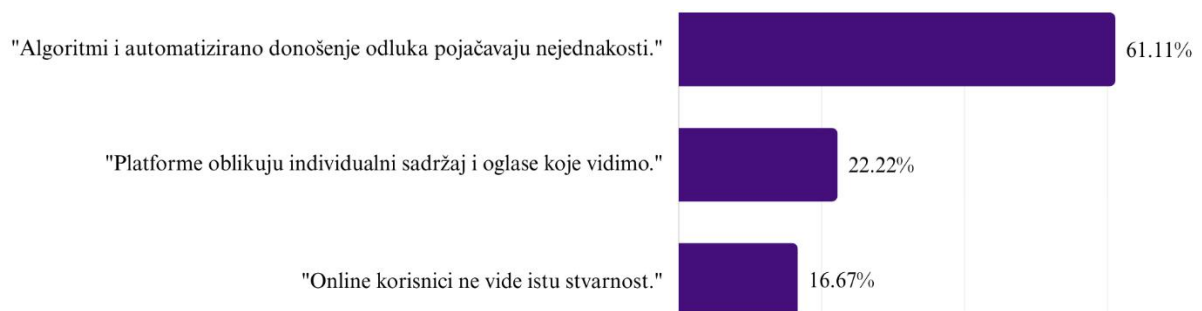
4.4. Personalizacija sadržaja

Kao uvod u detaljniji razgovor o korištenju algoritama za personalizaciju informacija i vijesti koje dobivaju, sa studentima, nastavnim i nenastavnim osobljem tematizirane su njihove

nedavne pretrage na nekoj od platformi poput Google-a, YouTube-a, Instagrama ili Facebooka. Na pitanje o tome da li su ikada osjetili da je ono što vide online bilo utjecano time ko su, šta su radili, čitali, gledali ili željeli kupiti, te da li ih je to zabrinulo, ispitanici istraživanja dali su uglavnom potvrdne odgovore navodeći primjere iz ličnog ili iskustva bližnjih osoba, pri čemu je prisutno manje odstupanje:

„Nije me zabrinulo, osjećao sam se super, bilo mi je zanimljivo. Pričao sam sa prijateljem i onda mi je izašao oglas kursa za njemački jezik. Bilo je super zabavno, nasmijali smo se i ja sam istražio podatke kako da upišem kurs iz njemačkog. Mislim da je to super stvar na način da nam se olakšava svakodnevni život,, (student FPN UNSA, III godina, I ciklus).

U nekoliko slučajeva, studenti personalizaciju informacija doživljavaju kao olakšavajuću i korisnu za svakodnevni život, jer može pružiti relevantne informacije i ponude koje odgovaraju individualnim potrebama i interesima korisnika. Onda kada prilagođavanje rezultata preferencijama ne vide kao pozitivno djelovanje umjetne inteligencije, personalizacija kod ispitanika izaziva strah i zabrinutost iz različitih razloga.



Grafikon 1: Šta brine studente i osoblje u vezi računarskih algoritama

Grafikon 1 prikazuje koji segmenti personalizacije sadržaja najviše brinu studente, nastavno i nenastavno osoblje. Više od polovine, tačnije 61,11% ispitanika vjeruje da je povećavanje nejednakosti u društvu najalarmantnija posljedica algoritmizacije života pojedinaca, dok 22,22% studenata i osoblja misli da oblikovanje predstavljenog sadržaja čini najveći problem, a 16,67% učesnika istraživanja kao najveći problem ističe to da online korisnici ne vide istu stvarnost. Više od polovine ispitanika istaklo je da društven nejednakosti jesu posljedica oblikovanja individualnog sadržaja, drugačije percepcije stvarnosti i prikupljanja podataka.

4.4.1. Prikupljanje zvučnih podataka

Tematizirajući specifično zabrinutost pri prvom izravnom i zapamćenom susretu sa personalizacijom informacija, studenti i nastavno osoblje dali su slične odgovore:

„Prvi put jeste, iskreno. Prvi put nisam znao o čemu je stvar, to je bilo sigurno prije dvije godine, u srednjoj školi kada sam malo više počeo koristiti Facebook i Instagram. Bilo mi je iznenađujuće da dobivam informaciju koju spominjem naglas svojim kolegama.“ (student FPN UNSA I godina);

„Meni je bio najveći šok kada sam shvatio da me telefon sluša. Izbilo me iz cipela kada am prvi put shvatio. Sada znam šta se dešava.“ (student FPN UNSA, I godina, II ciklus);

„Nije pretjerano iznenadilo i šokiralo, već se pričalo o tome kad se meni to desilo.“ (student FPN UNSA III godina, I ciklus)

„Dešavalo se svima. Pričam sa prijateljicom kako hoću da promijenim madrac i sutra uđem na Facebook, izađe mi dvanaest reklama za Dormeo ili neku drugu firmu koja proizvodi madrace i jastuke. Onda imam tu misao – da li je moj telefon prisluškivao konverzaciju kako mi treba novi madrac ili je ovo puka koncidencija.“ (student FF UNSA, I godina II ciklus)

Iz navedenih primjera moguće je čitati dvije vrste opažanja. Prvo, briga zbog personalizacije informacija na mrežnim platformama kod studenata i osoblja primijećena je prilikom prvog susreta sa prilagođavanjem sadržaja, nakon čega je zastupljen rezignirajući stav koji se izravno opisuje:

To se događa već godinama i postoji pregršt primjera čija je rezultanta da čovjek postane bezvoljan prema toj informaciji. (student FPN UNSA II godina, I ciklus)

Nakon akumulacije konkretnih iskustava tijekom vremena, ispitanici obično prelaze u atapično stanje svijesti. Drugo opažanje tiče se duboke zabrinutosti među sudionicima u vezi zvučnih segmenata i "prisluškivanja" njihovih uređaja. Ova zabrinutost proizlazi iz nekoliko razloga – narušavanje intimnosti razgovora, nedostatka vidljivosti, potencijala za zloupotrebu i nedostatka kontrole što stvara osjećaj povrede privatnosti i nepoželjnog nadzora. Na kraju, indikativno je također da su različiti primjeri koje su studenti i osoblje navodili kao odgovore na naredno pitanje o iskustvima kada platforme nisu bile usklađene a njihovim interesima, bili posljedica dijeljenja tehnoloških uređaja i zbog toga ne oslikavaju pogrešku algoritma.

4.4.2. Tehnokapital i manipulacije

Ne zaboravljajući da *Internet divovi* o kojima je prethodno bilo riječi nisu jedine stranice koje personaliziraju sadržaj na ekranu., ispitanici su podijelili percepcije o tome zašto online platforme prilagođavaju spektar informacija i pokušavaju oblikovati mišljenja i djelovanja. Većina ispitanika, bez obzira na nivo zabrinutosti, navela je slične razloge: 1. korporativnu korist – povećanje angažmana, kreiranje boljeg korisničkog iskustva i ovisnost, 2. političku korist – kreiranje filter mjehura i različite manipulacije i 3. komercijalnu korist. Prvi uočeni element tiče se korporativne, digitalne javne sfere:

„Mislim da je njihova korist sigurno tu, oni skupljaju na jedno mjesto ljude koji jedu jaja za doručak, na jednom mjestu skupljaju ljude koji jedu kobasice, i onda će lakše plasirati različite stvari za tu target grupu. Ne žele mijenjati društva na bolje ili na gore, jedina vodilja je profit. Ako skupiš dovoljno ljudi koji jedu kuhana jaja za doručak, ispostavi se da svi jedemo jaja za doručak.“ (viši stručni suradnik za kvalitet FPN UNSA)

„Stvaranje potreba dovodi do stvaranja ovisnosti, a kapitalizam je često generator tih potreba.“ (viši asistent FPN UNSA)

Sličan stav naveo je i student prvog ciklusa, ali bez kritičkog uklona:

„Vjerujem da se korporativna korist dešava, ali ja nisam ni u jednom trenutku razmišljao o tome na taj način. Ako je to korporacijska utakmica, ja idem na nju.“ (student FPN UNSA, III godina, I ciklus)

Drugi razlog za personalizaciju prepoznat je u političkoj koristi, a učesnici istraživanja izdvojili su nekoliko primjera gdje se takva upotreba naglašavala: tijekom američkih izbora 2016. godine⁶⁶, Brexita⁶⁷ i rata u Ukrajini. Navodeći da se radi o složenoj mreži političkih, komercijalnih i korporativnih interesa, student trećeg ciklusa naglasio je da iako se može činiti da je riječ o teorijama zavjere, stvarnost je često kompleksnija:

„Opet se postavlja pitanje tko stoji iza platformi i što im je cilj. Ako žele utjecati na promjenu vlasti, logično je da će generirati sadržaj koji potiče na proteste ili protiv vlasti, ili da će utjecati

⁶⁶ Tijekom predsjedničke kampanje u Sjedinjenim Američkim Državama 2016. godine, Donald Trump koristio je usluge kompanija za generiranje sadržaja koji promovira teorije zavjere i istovremeno podržava konzervativna stajališta komplementarna sa njegovom politikom. Koristeći se podacima o ponašanju korisnika na društvenim mrežama, prilagođavao je svoje političke govore kako bi privukao što veći broj glasača, a ovaj pristup se pokazao izuzetno uspješnim.

⁶⁷ Kako bi se ciljano utjecalo na glasače Cambridge Analytica, prikupljala je lične podatke o političkim preferencijama i interesima korisnika društvenih mreža, posebno Facebooka. Nakon analize i kreiranja marketinške kampanje identificirani su potencijalni glasači kako bi im dostavljali personalizirane političke poruke i reklame putem društvenih medija što je izazvalo kontroverze i podiglo etička pitanja zaštite privatnosti.

na to da se vlast promijeni. To se ne odnosi samo na zemlje koje nisu demokratske.“ (student FPN, III ciklus)

Na kraju, učesnici su naveli i komercijalnu korist, odnosno generiranje prihoda povećanjem interakcija i transakcija na platformama, što se može doimati kao *win-win* situacija jer korisnici dobivaju personaliziran sadržaj i ponude koje ih više zanimaju, dok platforme ostvaruju veće prihode kroz povećanu prodaju i oglašavanje.

„Koncept da me netko pokušava motivirati da ostavim neki novac postaje vrlo očigledan.“ (viši stručni suradnik za nastavu, FPN UNSA)

Gotovo svi ispitanici personalizaciju sadržaja, bilo da se radi o korporativnim, političkim i komercijalnim interesima, razumijevaju kao pristup koji može imati ozbiljne implikacije na privatnost i sigurnost korisničkih informacija.

4.5. Privatnost i sigurnost

Kako bi se u narednim sekcijama analize ispitalo usložnjeno razumijevanje povezanosti algoritamske pismenosti, zaštite podataka i informacijske sigurnosti, ispitanici su prvo predstavili vlastite predodžbe i stavove pojedinačnih područja. Kada je riječ o odnosu između zaštite podataka i informacijske sigurnosti, a sagledavajući odgovore ispitanika općenito, vidljiva su poimanja koja, svjesno ili nesvjesno, stavljaju naglasak na tehničke mjere:

„Prva ključna riječ koje se sjetim kada riječ o informacijskoj sigurnosti jeste enkripcija. Zaštita podataka, u suštini – maskiranje.“ (student FPN II godina, I ciklus)

S druge strane, ukoliko se informacijska sigurnost kao disciplina fokusira i na zaštitu podataka, naglašava se humanocentrični pristup:

„Kada se priča o informacijskoj sigurnosti, priča se o velikim sistemima. Znači, uvijek je prisutan taj *top-down* pristup, a pojedinac se nekako izgubi u masi. Tehnički dio informacijske sigurnosti je razrađen, ali u čitavoj priči nema pojedinca.“ (viši stručni suradnik za kvalitet, FPN UNSA).

Objašnjavajući predodžbe informacijske sigurnosti, ispitanici su posebno izdvojili dvije kategorije asocijativnog niza – zaštitu podataka i *povjerljivost* informacija kao jednu od tri komponente CIA modela.

4.5.1. Zaštita podataka i povjerljivost informacija

Stavovi nastavnog i nenastavnog osoblja u pogledu predodžbi informacijske sigurnosti i ličnih potreba za zaštitom podataka su ujednačeni ukoliko se posmatra njihova opća percepcija i kritički uklon:

„Što se tiče zaštite podataka, čini se da mnogi ljudi nisu dovoljno svjesni kako se njihovi lični podaci koriste u online svijetu. Činjenica da sve što se jednom pojavi *online* obično ostaje *online* zauvijek dodatno komplicira ovu situaciju.“ (viši stručni suradnik za nastavu, FPN UNSA)

S druge strane, slično kao i koncept informacijske i medijske pismenosti, studenti zaštitu podataka definiraju rašlanjajući i objašnjavajući osnovne pojmove:

„Zaštita može predstavljati proces čuvanja nečega na sigurnom, podaci su ono što svakodnevno govori o individuama i društvu, a zaštititi se trebaju podaci i informacije koji su važni. Mislim da su informacijska sigurnost i zaštita podataka u uzajamnoj vezi. Informacije i sigurnost, ako je nešto sigurno, onda je i čuvano i zaštićeno.“ (student FPN UNSA, III godina, I ciklus)

Iako su svi studenti manje ili više jasno definirali koncept zaštite podataka i povjerljivosti informacija, njihove predodžbe o potrebi za informacijskom sigurnosti značajno se razlikuju u pojedinim aspektima i često ne proizlaze iz poznavanja osnovnih pojmova. Većina studenata svjesna je rizika narušavanja podataka i povjerljivosti:

"Svjesna sam da sam dala svoje lične podatke u trenutku kada sam pristupila online svijetu." (student FPN, I godina, II ciklus)

„Zaštita podataka za mene znači osiguranje sigurnosti mojih ličnih informacija i informacija koje dijelim online.“ (student FPN UNSA, I godina, II ciklus)

Ipak, poznavanje potencijalnih prijetnji i rizika ne uslovljava često djelovanje po pitanju zaštite podataka i informacijske sigurnosti jer studenti ne prepoznaju razlog za prikupljanje, a mnogi pritom vjeruju da njihovi podaci nisu iskoristivi:

„Radi se opet o mojoj nebitnosti u funkcioniranju društva, a ako nešto dobro radi ove prirode, onda je to dobro, čak i ako nema garancija.“ (student FPN UNSA, II godina, I ciklus)

„Ja mislim da rizik ne postoji za mene jer nisam istaknuta ličnost ili neka javna osoba čiji podaci trebaju biti čuvani. Što se tiče interneta, lično ga posmatram kao pragmatičnu stvar za ostvarivanje ciljeva. Ne marim toliko za sigurnost i curenje mojih ličnih podataka jer to nikada nisam percipirao kao bitnu stvar.“ (student FPN UNSA, III godina, I ciklus)

Navodeći primjere narušavanja zaštite bankovnih, zdravstvenih i pristupnih podataka iz okruženja bliže i šire obitelji, pojedini studenti naglasili su i nedostatke ovakvog pristupa koji polazi od uvjerenja o nebitnosti vlastitih podataka i informacija za društvene procese:

„Ljudi se generalno slabo štite jer misle da su pitanja cyber sigurnosti američka kultura. Mislim da je to upravo nedostatak znanja i osviještenosti koliko može biti opasno. Ograničava ih ta ideja da nije bitno *ko smo mi* ili u krajnju ruku nepoznavanje, šta je najgore što se može desiti.“
(student FF UNSA, I godina, II ciklus)

Nedostatak informiranosti o načinima kako se lični podaci mogu zloupotrijebiti i stupnju ranjivosti na prijetnje u online svijetu studenti navode kroz primjer utjecaja medijskog oglašavanja i javnim raspravama gdje su naglašeni incidenti vezani ponajviše uz cyber sigurnost u Sjedinjenim Američkim Državama i drugim zapadnim zemljama zbog čega se stječe dojam da su takvi problemi ograničeni na specifične regije i ne predstavljaju prijetnju u Bosni i Hercegovini. Nadalje, osoblje i pojedini studenti uporište ideja da *nismo bitni* ili da naše lične informacije nisu relevantne za hakere ili zlonamjerne aktere, vide u nejasnoj predodžbi kako se kibernetički napadi provode.

Među odgovorima studenata i mlađeg osoblja postoji i konzistentna ideja o *početničkim greškama* dijeljenja povjerljivih podataka i informacija posebno u ranoj mladosti na društvenim mrežama, te o postepenom osvještavanju i mijenjanju pristupa tijekom vremena. Značajan broj studenata, nastavnog i nenastavnog osoblja također spominje situacije u kojima su podaci korišteni bez njihovog znanja ili pristanka, pri čemu su pojedini istakli i suočavanje s nedostatkom transparentnosti procesa prikupljanja i načina korištenja podataka ne samo velikih tehnoloških kompanija, ali i državnih institucija, organizacija i prodajnih lanaca.

4.5.2. Algoritamska pismenost za informacijsku sigurnost

Primijećeno je da studenti oba fakulteta odnos između informacijske sigurnosti i algoritamske pismenosti čitaju kroz poveznicu zaštite podataka i naglašavajući jedan od elemenata CIA modela, *povjerljivost* informacija.

„Zaštita podataka bi bila ova moja prva asocijacija. Ako već informacija jeste u svom digitalnom obliku tu gdje jeste, na koji je način možemo osigurati da *ne curi*. O bilo kojoj informaciji da se radi. WikiLeaks je isto curenje informacija, samo je pitanje ko je taj protagonist čije informacije cure.“ (student FPN UNSA II godina, I ciklus)

Ovisno od odsjeka i fakulteta na kojem studiraju i te poslova kojima se bave, studenti primjere pronalaze na online platformama, medijima i kroz rad u određenim institucijama, organizacijama i kompanijama. Tako je studentica zaposlena u javnom RTV servisu istakla odnos medija, algoritama i informacijske sigurnosti:

„Sve je međusobno povezano. Algoritamska pismenost, mediji i informacijska sigurnost čine složenu mrežu.“ (student FPN UNSA, I godina, II ciklus).

Studentica Katedre za informacijske nauke poveznicu između informacijske sigurnosti, zaštite podataka i pismenosti u ophođenju sa njima razumijeva unutar profesionalnih odgovornosti bibliotečke profesije:

„Upoznata sam sa terminom informacijske sigurnosti, ali obično ga povezujem sa zaštitom podataka u kontekstu poslovanja i firmi. Može biti povezano i sa zaštitom podataka i informacija o korisniku biblioteke“ (student FF UNSA, I godina, II ciklus).

Ispitanici sa Odsjeka sigurnosnih i mirovnih studija Fakulteta političkih nauka posebno su istakli humani pristup informacijskoj i digitalnoj sigurnosti općenito jer o njoj promišljaju primarno kao o načinu prepoznavanja opasnosti na internetu za pojedince:

„Kroz algoritamsku pismenost možemo naučiti kako prepoznati rizične situacije i kako donositi informirane odluke o svojoj digitalnoj sigurnosti.“ (student FPN UNSA, I godina, II ciklus).

Iako su definirali pojam informacijske sigurnosti, pojedini studenti drugih odsjeka Fakulteta političkih nauka nisu uspostavili jasnu poveznicu sa utjecajem algoritama:

„Imam percepciju kako mogu povezati ta dva pojma. Međutim, ne bih ih mogao odrediti tako u cjelini kako se postavlja, ali volio bih više naučiti o tome.“ (student FPN UNSA, III godina, I ciklus)

Ističući važnost zaštite podataka, studenti su priznali da se suočavaju s nedostatkom konkretnih vještina potrebnih za zaštitu i održavanje povjerljivosti svojih informacija. Istovremeno, neki studenti izrazili su zabrinutost zbog nedostatka praktičnog iskustva u vezi s algoritmima i informacijskom sigurnošću.

Jasno je da studenti različitih fakulteta i odsjeka imaju različite perspektive i razumijevanja kada je riječ o algoritamskoj pismenosti i informacijskoj sigurnosti. Dok su neki od njih, poput studenata interdisciplinarnog studija informacijske sigurnosti, izrazito svjesni važnosti ovih tema i spremni su ih istraživati i kontinuirano pratiti, drugi bi željeli više upliva teorijskih osnova i praktičnih obuka o mjerama zaštite u algoritamskom okruženju kako bi samoregulaciju mogli dovesti na viši nivo.

4.6. Kritička svijest i (samo)regulacije

S obzirom na primijećenu neujednačenost u odgovorima ispitanika, odnosno, različite stupnjeve razumijevanja, drugačija iskustva i težnje kada je u pitanju algoritamska pismenost, informacijska sigurnost i zaštita podataka, u nastavku analize ispitanici su praktični aspekti i koraci koje studenti i osoblje poduzimaju kako bi osigurali povjerljivost vlastitih informacija. Imajući u vidu da su određeni ispitanici prilikom razgovora ponudili i kritički uklon obrazovnih politika i potrebe za pronalaskom novih regulatornih modela, posljednja dva poglavlja analize, pored uvidu u prakse ispitanika spram personalizacije sadržaja i mjera zaštite privatnosti/povjerljivosti informacija, analiziraju gledišta potreba za regulatornim okvirima, standardizacijom i usklađenošću.

4.6.1. Ograničavanje personalizacije i mjere zaštite

Odgovori ispitanika u vezi sa načinima na koje se odnose prema personalizaciji sadržaja i zaštiti podataka pokazali su različite odgovore koji se bazično mogu podijeliti u tri grupe: ispitanici koji u personalizaciji primjećuju pozitivni element uštede vremena, oni koji poduzimaju osnovne preventivne korake zaštite odataka i one koji u personalizaciji vide potencijalnu prijetnju, ali zbog vlastite svjesnosti o postojanju i posljedicama eho-komora, vjeruju da visok nivo zaštite nije nužan. Govoreći o ograničavanju personaliziranog oglašavanja i reklamiranja, manji broj studenata izjavio je da ne pokušava limitirati njihov utjecaj. Pri tome, posebno se izdvajaju dvije grupe: studenti i osoblje koji ne vide problem u eho-komorama zbog odlike pragmatičnosti i uštede vremena, te ispitanici sa stavom da personalizacija može značiti prijetnju, ali zbog vlastite svjesnosti o utjecaju algoritama, vjeruju da visok nivo zaštite nije nužan, te štaviše, da ga mogu okrenuti u svoju korist:

„Identificiram se sa ličnošću umjetnika, a umjetnik mora biti otvorena knjiga. Zašto bi meni smetalo da Google ima moje podatke? Ta problematika me ne dotiče emocionalno i služim se njom za svoju korist. Ako želim da se bavim nekom temom, svjesno ću tražiti od algoritma da mi izbacuje informacije u vezi s tim. Odnos je simbiotičan, ali treba od parazita napraviti obostranu korist.“ (student FF UNSA, III godina, I ciklus)

Ostali ispitanici naveli nekoliko primjera korištenja aplikacija ili ličnih mjera za prevenciju. Većina ispitanika izdvojila je *ad blocker* i *incognito* način pretraživanja kao preventivnu mjeru personalizacije sadržaja:

„Radim kombinaciju različitih stvari. Incognito sam recimo na mobilnom telefonu, uvijek je u tom načinu rada, Samim tim ne moram brisati historiju.“ (viši stručni suradnik za kvalitet)

„Ja koristim *ad blocker* i brisanje povijesti, nekad pogledaš i nešto što nisi htio.“ (student FPN UNSA, II godina, I ciklus)

„Od svega, najviše koristim *ad blocker*, ne zbog privatnosti, već mi stvara nervozu kada mi iskaču prozori i reklame po ekranu. Brisanje povijesti nikada ne radim, zato što ne pretražujem ništa čega bih se stidio, a ako se odlučim pretraživati neku glupost, kao na primjer gdje se proizvodi određeni proizvod, i ako mislim da će rezultirati time da mi iskaču više takvih proizvoda, u tom trenutku koristim incognito način rada jer mi on smanjuje tu mogućnost.“ (student FPN UNSA, III godina, I ciklus).

Razlozi zbog kojih studenti koriste opciju brisanja povijesti pretraživanja i blokiranja reklama ili *incognito* način rada su različiti i nemaju uvijek za cilj zaštitu, ali svi ovi postupci kao krajnju posljedicu idalje imaju ograničavanje personalizacije. Istovremeno, primijećen je i disrazmjer u razumijevanju značenja određenih preventivnih mjera poput brisanja povijesti koju pojedini studenti ne vide kao mogući korak ograničavanja namjenskih pretraga, oglašavanja i reklamiranja.

Kada je riječ o uvođenju drugih i dodatnih mjera zaštite podataka i povjerljivosti informacija, nastavno, nenastavno osoblje i studenti naveli su korištenje drugih mrežnih pretraživača, poput DuckDuckGo, Brave ili metapretraživače, dok je studentica master studija informacijske sigurnosti podijelila iskustva o detaljnom i kontinuiranom praćenju novih mogućnosti sa pojačanim sistemom zaštite:

„Ne koristim određeni set browsera koji se standardno koristi, kao što su Mozilla, Chrome, Internet Explorer. Trudim se da nađem neke koji imaju integriran određeni set zaštite i to mi je jedan vid istraživanja kako bih saznala šta mogu koristiti lakše, bez reklama i skočnih prozora.“ (student FPN UNSA, I godina, II ciklus)

Nadalje, većina studenata i osoblja koristi opciju brisanja kolačića i koristi virtualne privatne mreže (engl. Virtual Private Network – VPN). Ipak, primarni razlog za VPN opciju nije u zaštiti privatnosti, već u dolasku do sadržaja koji je inače ograničen ili nedostupan za područje Bosne i Hercegovine i zemalja u regiji:

„Koristio sam VPN, ali jednom prilikom kada mi je trebalo istraživanje za predmet Demografija, a Sjedinjene Američke Države su blokirale podatke, pa smo virtualno bili u SAD-u.“ (student FPN UNSA, III godina, I ciklus)

„VPN koristim kada sam na odmoru.“ (docentica, FPN UNSA)

„Najviše koristim VPN i kolačiće povremeno, kad se sjetim da ih trebam. To su dvije stvari. VPN koristim zbog pristupa sadržajima, a uz to mi super dobro dođe i iz sigurnosnih razloga.“
(viši stručni saradnik za nastavu FPN UNSA)

Tematizirajući složenije sigurnosne mjere, studenti master studija informacijske sigurnosti, pojedini saradnici i studentica informacijskih nauka, nabrojali su *password manager* opciju, dvostruku identifikaciju za ključne setove podataka, te odvajanje računara za ličnu i profesionalnu upotrebu te različite mjere standarda ISO 27001.

„Nisam rigorozna jer uglavnom koristim Password Manager i imam tu kulturu stalnog mijenjanja šifri. Stalno pratim da li su šifre provaljene i korištene negdje. Koristim odgovarajuće softvere koji to provjeravaju. Mail adrese isto moraju biti zaštićene. Finansije su također važne, pa koristim dva-tri segmenta dvostruke autentifikacije obavezno.“ (student FPN UNSA, I godina, II ciklus).

Ocjenjujući odnos između vlastitih nastojanja u zaštiti privatnosti i kvalitete iskustva na internetu, učesnici intervjua naveli su srednji nivo zadovoljstva s obzirom da potpuna sigurnost podatak ne može biti zagarantovana, sigurnosni rizici povećavaju se recipročno sa tehnološkim razvojem ili zbog toga što smatraju da je stupanj sigurnih mjera koje koriste idalje nizak.

4.6.2. Regulacije i usklađenost

Prilikom tematiziranja oblika (samo)regulacije, odnosno, načina na koje ispitanici mogu djelovati kao pojedinci da bi osigurali zaštitu podataka i povjerljivost informacija koristeći se određenim tehnikama, aplikacijama i pristupima, zamijećen je kritički uklon na polju regulacija koji je nužan jer se ne tiče isključivo odgovornosti pojedinaca, već obaveza države prema zajednici:

„Prvo treba pronaći mehanizam koji će ih čuvati na sigurnom, bilo da se radi o državnoj regulaciji i internetu, shvatiti kako to funkcioniše.“ (student FPN UNSA, III godina, I ciklus)

„Vlasti trebaju bolje regulirati tehnološke kompanije kako bi se smanjila mogućnost zloupotrebe podataka i širenja lažnih informacija“ (student FPN UNSA, I godina, I ciklus)

Kao jedan od načina za uvođenje državnih regulacija, studenti prepoznaju *down-top* princip:

„Pošto veće države utječu na manje, teško je reći da bi jedna država mogla uvesti taj sistem, da se kontrolira Facebook. Onda bi država imala pritisak od međunarodnih agencija i kompanija. Ali naprimjer, pretpostavljam da bi bilo utjecajnije da to krene odozdo. Kažemo da mi zbog svoje pismenosti želimo regulaciju i onda bi se država pozvala na nas. Možda bi bilo utjecajnije.“ (student FPN UNSA, II godina, I ciklus)

Istovremeno, studenti koji navode da se osjećaju sigurno u digitalnom okruženju i naglašavaju da taj osjećaj sigurnosti često proizlazi iz pravnog aspekta koji predviđa potencijalne sankcije za kršenje privatnosti. Ispitanici osim osjećaja odgovornosti za vlastitu sigurnost te sigurnost drugih, očekuju da država igra ključnu ulogu u osiguravanju povjerljivosti informacija i zaštiti podataka.

Pored državnih regulacija, pojedini su naveli i sankcije u općem smislu:

"Svaka kompanija koja koristi informacije obavezna je da plati onome koji mu je dao tu informaciju." (student FPN UNSA, I godina, II ciklus)

Studenti informacijske sigurnosti razmatraju potrebu za pravednijom raspodjelom prihoda u kontekstu algoritamske ekonomije predlažući da kompanije koje koriste korisničke podatke trebaju platiti za korištenje podataka korisnicima koji su ih generirali. Ovaj pristup zahtijeva promjene u regulatornom okviru i poreznim pravilima. Komentirajući masivno otvoreni online kurs i pristupe obrazovnih politika, studenti su također naglasili su da tradicionalne metode edukacije nisu dovoljno efikasne u postizanju željenih ciljeva. Umjesto toga, predlažu integriranje pravne regulative, poput GDPR-a, s edukacijom kako bi se osvijestila važnost zaštite privatnosti i sigurnosti podataka. Drugi smatraju da bi korisnicima trebalo jasno predočiti koje informacije dijele i kako će se te informacije koristiti, što bi bilo popraćeno strožim zahtjevima i regulativom za aplikacije i online platforme kako bi se ograničila njihova sposobnost praćenja korisnika bez njihove svjesne saglasnosti.

Dotičući se potencijala standardizacije procesa informacijske sigurnosti unutar akademije i visokoškolskih obrazovnih institucija, nenastavno i nastavno osoblje prepoznalo je potencijal sistemskog pristupa uspostavljanja politika informacijske sigurnosti na razini Fakulteta političkih nauka i Univerziteta u Sarajevu:

„Ne samo da bi trebali proći dodatne obuke, već i sami sistemi za upravljanje informacijama i procesima moraju biti standardizirani. To ne mora nužno biti ISO standard, ali mora postojati sistem koji osigurava informacijsku sigurnost. Može biti interni standard koji smo mi razvili i

koji nije standardiziran izvan institucije, ali ključno je da postoji.“ (viši stručni suradnik za kvalitet FPN UNSA)

Uvođenjem standardiziranog sistema informacijske sigurnosti utjecalo bi se na povećanje digitalne higijene zaposlenika, ali i omogućilo usmjeravanje u pravcu povećanja kvalitete poslovnih procesa institucije koji se odnose na ključnu ciljnu skupinu – studente. Takvo povećanje kvalitete i umanjivanje rizika podrazumijeva reosmišljavanje nastavnih planova i programa čiji će ciljevi i ishodi učenja težiti praćenju promjena digitalne algoritimizacije i konkretiziranju utjecaja algoritamske obrade na digitalnu kulturu (Manovich 2013).

5. Diskusija rezultata

U ovom poglavlju diskutiramo prikazane rezultate sadržajne i tematske analize kako bismo ih povezali sa istraživačkim pitanjima IP1, IP2, IP3. Prilikom kodiranja intervjua izdvojeno je šest glavnih tema i dvanaest manjih tematskih okosnica uz koje se vezuje 53 koda pri čemu pojedine teme odgovaraju na više od jednog istraživačkog pitanja kao što i više tema odgovara na pojedina istraživačka pitanja. Za potrebe promišljanja rezultata analize, postojećih šest tema grupirano je tako da odgovaraju redosljedu IP1, IP2 i IP3.

5.1. Predodžbe pismenosti i algoritamska iskustva

Kako bi kasnije mogli diskutovati o poimanju kompleksnijih odnosa područja, disciplina i njihove međusobne uslovljenosti, poput algoritamske pismenosti, zaštite podataka i informacijske sigurnosti, te imajući u vidu da je namjerni uzorak uključio ispitanike koji su barem načelno upoznati sa konceptom medijske i informacijske pismenosti, prvi set grupiranih tema ponudio je odgovore na pitanje o dosadašnjim predodžbama i iskustvima algoritamske pismenosti studenata, nastavnog i nenastavnog osoblja.

Govoreći o shvatanju i aktivnostima na polju medijske i informacijske pismenosti, svi sudionici pokazali su jasno i koncizno poimanje oba koncepta, a stavljanje naglaska i preciznije određenje pojedinog područja nudili su u odnosu sa vlastitim stupnjem obrazovanja, odsjekom i fakultetom kojeg pohađaju. Tako studenti Fakulteta političkih nauka dublje razumiju medijsku pismenost, dok studenti Filozofskog fakulteta i nenastavno osoblje više pažnje posvećuju konceptu informacijske pismenosti. Integrirani model uglavnom se razumijeva kao neophodan zbog toga što se u obzir uzima 1. uslovljenost (medij služi za prijenos informacija), te 2. da UNESCO u svojim razvojnim i obrazovnim politikama promiče konsolidirani okvir.

Istaknuta potreba za naglašavanjem informacijske pismenosti posljedica je floskularizacije pojma medijske pismenosti kroz svođenje na prepoznavanje binarne opozicije lažnih/istinitih informacija, ali još bitnije, prepoznavanja nužnosti da se fenomenu pristupa interdisciplinarno vodeći se klauzom – informacija je inherentna svim disciplinama. U vremenu datafikacije, dok se metode za analize ekstrahovanih podataka usložnjavaju, postoji, više nego prije, potreba za evaluacijom izvora informacija jer idalje *nije sve informacija*, ali je metapodatkovni potencijal u dobu platformskog kapitalizma sada prepoznat u svim sferama djelovanja (Angwin 2014; Zuboff 2019), zbog čega se polje informacijskih nauka kontinuirano reaktualizira procesom širenja područja izučavanja i istraživanja na nestalni mrežni prostor.

Za razliku od MIP modela, studenti, nastavno i nenastavno osoblje algoritamsku pismenost određuju nepreciznije, ali idalje unutar okvira poznatih oblika ili kao njihov nastavak, pozadinu, ono što se dešava *iza*. Algoritamske implikacije, iako iniciraju današnje medijske, političke, sociološke i sigurnosne teme, nisu dovoljno problematizirane na studijskim grupama Fakulteta političkih nauka. Katedra za informacijske nauka postavila je teorijske temelje za kritičko promišljanje platformskog okruženja, ali trenutno na nivou Univerziteta u Sarajevu manjka obuka, predmeta i kurseva koji studentima mogu ponuditi strukturane programe, prilagođene njihovim interesovanjima i potrebama u stalnoj algoritamskoj modifikaciji postojećeg digitalnog okruženja. Bojazan od nepoznatih i nedovoljno analiziranih posljedica algoritamskog upravljanja utjecala je na pravac iskustvenih procesa studenata i osoblja – samostalno istraživanje o prikupljanu podataka, *prisluškivanju* i distanciranje od digitalnih uređaja kao uvođenje mjere za mitigaciju ekonomije pažnje. Autori studija algoritamske pismenosti (Head, Fister i MacMillan 2020) naglašavaju da „studenti ne bi trebali samostalno morati učiti ove ključne vještine o informacijama. Također, ne bi trebalo pretpostavljati da su sve njihove strategije nužno učinkovite“ (28) zbog čega se otvaranja pitanje prilagođenosti nastavnih praksi i obrazovnih politika jer „netransparentnost metoda platformskog informacijskog usluživanja nadilazi sposobnost i odgovornosti pojedinaca da kontroliraju relevantnost i privatnost.“ (Hibert 2018, 21).

5.2. Odnosi i uslovljenosti

U razgovoru o informacijskoj sigurnosti primijećen je dvostruki pristup – 1. humanocentrična perspektiva nastavnog i nenastavnog osoblja i 2. tehničko-tehnološka koju naglašavaju uglavnom studenti sa iskustvom u IT sektoru i studenti koji su imali manje doticaja sa disciplinom što je uslovlilo ograničavanje na osnovno i/ili parcijalno razumijevanje. Ova

podjela ukazuje na činjenicu da je disciplina informacijske sigurnosti u Bosni i Hercegovini još uvijek u početnim fazama razvoja budući da se idalje razmatraju samo njeni specifični segmenti. Nadalje, pri razmatranju uvođenja sistema informacijske sigurnosti unutar obrazovne institucije, moguće je govoriti o ISO 27001 standardu koji nužno ne podrazumijeva certifikaciju, već slijeđenje pojedinih kontrola iz Priloga 1, poput *A.7.2.2. Svjesnost o informacijskoj sigurnosti, obrazovanje i treninzi*. (ISO/IEC 27001:2013, 11).

Dok studenti načelno razumiju pojam informacijske sigurnosti, zaštitu podataka povezuju sa problemom digitalne privatnosti. Međutim, kada je riječ o odnosu između algoritamske pismenosti, informacijske sigurnosti i zaštite podataka, dolazi do povlačenja manje određenih poveznica. Postojanje svijesti o procesu personalizacije sadržaja i prikupljanja podataka obično kod ispitanika izaziva emocionalnu reakciju straha, zabrinutosti i anksioznosti, što nerijetko nema uporište u akcijama i uvođenju preventivnih mjera. Autori algoritamske studije (Head, Fister i MacMillan 2020) u rezultatima istraživanja navode sličan indiferentni pristup koji ne isključuje postojanje svijesti o zamkama personalizacije radi usmjeravanja akcije i pojačavanja podjela: „Međutim, ono što tačno kompanija može raditi s prikupljenim podacima o njima često je nepoznata varijabla.“ (11) Dok su neki razmatrali je li sposobnost korištenja određenih web stranica vrijedna žrtvovanja svojih podataka, drugi su tvrdili da je već prekasno. Pri tome, razlog za rezignaciju i indignaciju javlja se kao posljedica tehnološkog determinizma, osjećaja nemoći i prebacivanja odgovornosti za regulaciju algoritamskih procesa na državne vlasti i opće regulatorne okvire.

Interes studenata da se suprotstave radu velikih tehnoloških kompanija jeste značajan uvid u njihove percepcije i početni uslov za društveno odgovorno djelovanje, ali istraživanje sugerira da era algoritama zahtijeva ponovnu evaluaciju nastavnih strategija tijekom redefinicije i usložnjavanja fokusa medijske i informacijske pismenosti.

5.3. Algoritamska budućnost i sigurnosne mogućnosti

Gledajući prema budućnosti obrazovanja u algoritamskom društvu, svi ispitanici su pozvali na propitivanje postojećih obrazovnih praksi osvrnuvši se posebno na potencijal masivnog otvorenog online kursa čiji moduli o algoritmima i informacijskoj sigurnosti pružaju dobar teorijski osnov za propitivanje ove problematike, ali bi pritom mogli biti bolje uvezani u smislu objašnjavanja odnosa algoritamske pismenosti i informacijske sigurnosti. Činjenica da je većina ispitanika, usključujući i studente i nastavno i nenastavno osoblje, pozvala na dopune postojećeg MOOC-a koje bi bile bazirane na konkretnim vještinama, praktičnim savjetima,

kvizovima algoritamske pismenosti i jasnim primjerima algoritamskog djelovanja, ukazuje na dva indikatora: 1. obrazovni sistem još uvijek nije uspio odgovoriti na složene potrebe digitalne studentske populacije i 2. tehnološki solucionizam u obrazovni kontekst prodire kroz uvjerenje da će uključivanje više alata, aplikacija, gemifikacije i multimedijalnih sadržaja riješiti problem neuklađenosti nastavnih planova i programa sa ubrzanim algoritamskim razvojem, zanemarujući složeniji pristup uvođenja velikih istraživačkih programa koji bi kritičku teoriju konačno stavili u poziciju upravljača ovih procesa (Hibert 2018, 19).

Primijećene „defanzivne prakse“ (Head, Fister i MacMillan 2020) javljaju se kao oblik (samo)regulacije u pokušaju mitigiranja digitalnih sigurnosnih rizika koristeći se ponovno nizom aplikacijama, softvera i ličnim tehnikama koje kombiniraju nekoliko različitih pristupa. Bez obzira na pojedinačne težnje i akcije, nije primijećeno smanjenje osjećaja rezignacije i indignacije, što ukazuje na potrebu za razmatranjem dodatnih preporuka za integraciju i unapređenje algoritamske pismenosti na Univerzitetu u Sarajevu koje su namijenjene sudionicima obrazovnih procesa, top menadžmentu organizacionih jedinica Univerziteta, nastavnom i nenastavnom osoblju te donosiocima odluka.

Preporuka I: Prilagoditi javni otvoreni online kurs medijske i informacijske pismenosti (MIP MOOC) tako da odgovara potrebama studenata u algoritamskom okruženju;

Preporuka 2: Redefinirati nastavne planove i programe tako da kroskurikularno integriraju algoritamsku pismenost;

Preporuka 3. Uvesti sistem kontinuirane edukacije i osposobljavanja nastavnog i nenastavnog osoblja na Univerzitetu u Sarajevu u području algoritamske pismenosti.

Pored navedenih, preporuke trebaju uzeti u obzir da su studenti tijekom održavanja intervjua gotovo uvijek prepoznali kolege i vršnjake kao izvore informacija o algoritmima smatrajući da su bolje pozicionirani za postavljanje pitanja i suprotstavljanje personaliziranim sadržajima od starijih članova obitelji i nastavnika (Head, Fister i MacMillan 2020). U drugim slučajevima, povezivali su ovo lično iskustvo s širim razgovorima tijekom pojedinih predavanja i intervjua primjenjujući kritičku perspektivu na kompleksna pitanja vezana uz algoritme. Nasuprot tome, ne računajući studente koji su pohađali predmete medijske i informacijske pismenosti i studije informacijske sigurnosti te osoblje koje je imalo doticaj sa aktivnostima MIP integracije, ispitanici su izjavili da algoritmizacija nije problematizirana kroskurikularno. Stoga bi nedostatak sistemskog pristupa mogao biti umanjeno konvergencijom razumijevanja nastavnog osoblja o informacijama i društvu u okviru njihove discipline, kompetencija nenastavnog

osoblja za provođenje potrebnih mjera, te uvida i kreativnih praksi studenata kako bi se razvio nastavni plan koji zadovoljava potrebe studenata kao učesnika obrazovnih procesa i građana potičući ih na razmatranje oblika djelovanja, bilo primjenom obrambenih taktika ili zagovaranjem društvenih ili zakonodavnih promjena.

Zaključak

Razmatrajući percepcije i iskustva algoritamskih procesa kako bi se odgovorilo na postavljena istraživačka pitanja, ovaj magistarski rad bazira istraživanje na integraciji algoritamske pismenosti u obrazovne programe Univerziteta u Sarajevu, s naglaskom na Fakultet političkih nauka. Postojeći resursi poput nastavnog predmeta medijske i informacijske pismenosti, master programa informacijske sigurnosti, javnog otvorenog online kursa (MIP MOOC), strateških dokumenata i standarda, postavili su temelj za preciznije određenje područja istraživanja. Propitujući utjecaj, stanja i mišljenja o algoritamskoj pismenosti i informacijskoj sigurnosti, rad polazi od pretpostavki da algoritamske amplifikacije iniciraju izazove informacijske sigurnosti i potencijalne dileme u području zaštite podataka, te da je trenutni spektar metoda unutar holističkog pristupa potrebno prilagoditi i dopuniti shodno stalnim promjenama digitalnog okruženja.

Teorijska polazišta, sažeta u dva poglavlja na početku rada, ponudila su uvid u međunarodne preporuke i standarde informacijske sigurnosti s naglaskom na ISO 27001, kao i pregled studija, metoda i razvojnog toka dosadašnjeg strateškog pristupa i nastojanja da se integraciji medijske i informacijske pismenosti na Univerzitetu u Sarajevu pristupi holistički. Potom je metodološki okvir precizirao ciljeve i način istraživanja te odabir uzorka, pripremu instrumenata istraživanja i prostorno-vremensko određenje. Vodeći se metodologijom razvijenom za potrebe projekta informacijske pismenosti (Project Information Literacy) i istraživačke aktivnosti Harvard Graduate School of Education, te kombinirajući dvije kvalitativne metode, tematsku i analizu sadržaja, kodirani su podaci i grupirani segmenti materijala osamnaest intervjua sa ciljnim skupinama. Na kraju, analiza je otvorila prostor za diskusiju rezultata istraživanja o informiranosti i razumijevanju procesa automatiziranog prikupljanja, organiziranja i upravljanja metapodacima.

Predstavljani rezultati odgovaraju na istraživačka pitanja o dosadašnjim predodžbama i iskustvima algoritamske pismenosti studenata, nastavnog i nenastavnog osoblja, njihovih percepcija korelacije informacijske sigurnosti, algoritama i zaštite podataka te o mogućnostima

unapređenja kapaciteta i stanja algoritamske pismenosti na Univerzitetu u Sarajevu. Iako ispitanici posjeduju teorijske i praktične osnove uslovljene različitim stupnjem učešća u MIP aktivnostima, istraživanje je ukazalo na nužnost sistemskog kritičkog pristupa platformskom društvu i algoritmizaciju životnih sfera kroz uvođenje tematskih obuka nastavnog i nenastavnog osoblja te dopunu masivnog otvorenog online kursa medijske i informacijske pismenosti, specifično modula IX i X koji tematizirajući detaljnije umjetnu inteligenciju, algoritme, informacijsku sigurnost i zaštitu podataka.

Ograničenja istraživanja zasnivaju se na relativno malom broju ispitanika s obzirom da su pored studenata i osoblja Fakulteta političkih nauka uključena još dva studenta Katedre za informacijske nauke Filozofskog fakulteta, te imajući u vidu da je odabrani uzorak baziran na postojanju osnovnih predodžbi medijske i informacijske pismenosti. Obuhvatniji pregled stanja i perspektiva algoritamske pismenosti podrazumijeva doticaj i uključivanje više organizacionih jedinica u proces ispitivanja što bi omogućilo pretpostavke za sistemski, relevantniji prikaz i djelovanje na Univerzitetu u Sarajevu. Bez obzira na ograničenja istraživanja, rad postavlja osnove za daljnje fokusiranje na utjecaj i poziciju umjetne inteligencije u visokoškolskom obrazovanju kroz unapređenje kompetencija interpretacije, analize i kritičke evaluacije utjecaja algoritamskog okruženja na društvene procese.

Literatura

Angwin, Julia. 2014. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. USA: Times Books.

Astambayeva, Zhupat, Aziya Zhumabayeva, Marina Romanova, Nurbanu Nygymanova, Rabiga Bazarbekova, i Makhinur Nizamova. 2021. "Algorithmic Methodological and Mathematical Literacy of the Future Primary Education Teacher: Perspective of Learning Technology". *World Journal on Educational Technology: Current Issues*. 13 (October): 758–74. <https://doi.org/10.18844/wjet.v13i4.6263>. (Pristupljeno 23. septembra 2023)

Atack, Iain. 2022. "Human Security, Human Rights and Human Development" U *The Ethics of Peace and War*, 111-124. Edinburgh: Edinburgh University Press. <https://doi.org/10.1515/9780748680894-009> (Pristupljeno 23. 09. 2023)

Braman, Sandra. 2006. *Change of State: Information, Policy, and Power*. The MIT Press. <https://doi.org/10.7551/mitpress/1783.001.0001>. (Pristupljeno 23. septembra 2023)

Braun, Virginia, i Victoria Clarke, V. 2006. "Using thematic analysis in psychology." *Qualitative Research in Psychology*, 3(2), 773101.

<https://doi.org/10.1191/1478088706qp063oa> (Pristupljeno 23. septembra 2023)

The British Standards Institution (BSI). 2022. *The new ISO/IEC 27001:2022 standard*. <https://www.bsigroup.com/en-GB/iso-27001-information-security/isoiec-27001-revision/> (Pristupljeno 23. septembra 2023)

Carlsson, Ulla, ur. 2019. *Understanding Media and Information Literacy (MIL) in the Digital Age A Question of Democracy*. (UNESCO) Department of Journalism, Media and Communication (JMG), University of Gothenburg. (Pristupljeno 18. marta 2021)
https://en.unesco.org/sites/default/files/gmw2019_understanding_mil_ulla_carlsson.pdf

Carr, Nicholas. 2011. *The Shallows*. New York: WW Norton.

Castells Manuel. 2000. *The Rise of the Network Society*. 2nd ed. Oxford: Blackwell.

Collins Alan. 2010. *Contemporary Security Studies*. 2nd ed. Oxford: Oxford University Press.

D'Appollonia, Ariane Chebel. 2012. "Securitization after 9/11". U *Immigration and Insecurity in the United States and Europe*, 77–110. Ithaca, NY: Cornell University Press. <https://doi.org/doi:10.7591/9780801463914-007>. (Pristupljeno 23. 09. 2023)

Dijk, Jose van, Thomas Poell i Martijn de Waal. 2018. *The platform society: public values in a connective world*. Pristupljeno: mart 12. 2021.
<http://www.oxfordscholarship.com/view/10.1093/oso/9780190889760.001.0001/oso-9780190889760>

Dizdar, Senada, Džejla Khattab i Nadina Grebović-Lendo. 2016 "Understanding the Role of Libraries and Librarians in Information Literacy Implementation: Based on the Example of Students of the Faculty of Philosophy, University of Sarajevo". U: Knežević, Ratko et al., ur. *Proceedings: International Scientific Conference Western Balkan Information Literacy - Information Literacy in the Digital World, 8-11 June 2016*. (str. 173-178). Bihać/Limerick: Limerick Institute of Technology

Dizdar, Senada, i Lejla Hajdarpašić. 2014. "Razvoj informacijske pismenosti na Univerzitetu u Sarajevu". *Čitalište: naučni časopis za teoriju i praksu bibliotekarstva* 24 (maj 2014): 25-31. http://citaliste.rs/casopis/br24/dizdar_senada.pdf. Pristupljeno: mart 12. 2021.

Dogrueel, Leyla, Philipp Masur i Sven Joeckel. 2022. "Development and Validation of an Algorithm Literacy Scale for Internet Users". *Communication Methods and Measures* 16 (2): 115–33. <https://doi.org/10.1080/19312458.2021.1968361>.

Dogrueel, Leyla. 2021. "What Is Algorithm Literacy? A Conceptualization and Challenges Regarding Its Empirical Measurement". U *Algorithms and Communication*, ur. Monika Taddicken i Christina Schumann, 9:67–93. Digital Communication Research. Berlin. <https://doi.org/10.48541/dcr.v9.3>.

- Duff, Alistair S. 2004. "The Past, Present, and Future of Information Policy". *Information, Communication & Society* 7 (1): 69–87. <https://doi.org/10.1080/1369118042000208906>.
- Fakultet političkih nauka. 2021. *Elaborat interdisciplinarnog studijskog programa informacijske sigurnosti*. Univerzitet u Sarajevu – Fakultet političkih nauka
- Gemserv. 2019. *ISO/IEC 27001 and the General Data Protection Regulation (GDPR): How the ISO/IEC 27001 framework supports GDPR compliance*. London <https://gemserv.com/wp-content/uploads/2019/09/ISO-IEC-27001-and-GDPR-v1.0.pdf>
- Gladden, Matthew E. 2017. "An Axiology of Information Security for Futuristic Neuroprostheses: Upholding Human Values in the Context of Technological Posthumanization". *Frontiers in Neuroscience*. <https://doi.org/10.3389/fnins.2017.00605>.
- Gupta, Manish, i Raj Sharman. 2008. *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, 2008. <https://doi.org/10.4018/978-1-60566-036-3>.
- Hajdarpašić, Lejla i Džejlja Khattab. 2019. "Information Literacy of Library Science Students at the Faculty of Philosophy, University of Sarajevo." *Revista română de biblioteconomie și știința informării: revistă trimestrală editată de Asociația bibliotecarilor din învățământ- România* 15 (1): 8-15. Pristupljeno 12. 20. 2020. <http://www.rrbsi.ro/index.php/rrbsi/article/view/71/29>.
- Harper, Rebecca, 2022. *2022 Update -Everything You Need to Know*. ISMS Online. <https://www.isms.online/information-security/everything-you-need-to-know-about-the-iso-27001-2022-standard-update/> (Pristupljeno 16. septembra 2023)
- Head, Alison J., Barbara Fister, i Margy MacMillan. 2020. *Information literacy in the age of algorithms: Student experiences with news and information, and the need for change*. 15 January 2020. Project Information Research Institute. <https://projectinfolit.org/publications/algorithm-study/> (Pristupljeno 23. septembra 2023)
- Hibert, Mario. 2018. *Digitalni odrast i postdigitalna dobra*. Zagreb: Multimedijalni Institut i Institut za političku ekologiju. http://ipe.hr/wp-content/uploads/2019/01/Mario_Hibert-Digitalni_odrast.pdf. (Pristupljeno 23. septembra 2023)
- Hill, Jordan. 2022. "Policy responses to false and misleading digital content: A snapshot of Children's Media." Organisation for Economic Co-operation and Development, august 3. [https://one.oecd.org/document/EDU/WKP\(2022\)13/en/pdf](https://one.oecd.org/document/EDU/WKP(2022)13/en/pdf). (Pristupljeno 22. augusta 2023)
- Hodžić, Sanela. 2019. "Media and Information Literacy in Bosnia and Herzegovina: Numerous Civil Society Initiatives and Lack of Public Policies." U *Media and Information Literacy in the Western Balkans: Unrealized Emancipatory Potential*, 87-128. Sarajevo: Media and Civil Society Development Foundation Mediacentar.

- https://www.media.ba/sites/default/files/media_and_information_literacy_in_the_western_balkans_unrealized_emancipatory_potential_final.pdf. Pristupljeno 12. 5. 2020.
- Huskić, Sanel, Emir Vajzović i Mario Hibert. 2022. "Strategic positioning of media and information literacy." *Vjesnik bibliotekara Hrvatske* 65(2): 93-113. <https://hrcak.srce.hr/285508>. (Pristupljeno 12. 5. 2020)
- Information security management systems. 2023. *Requirements*. <https://www.iso.org/standard/27001#lifecycle> (Pristupljeno 12. 8. 2023)
- International Organization for Standardization. 2013. Information security, cybersecurity and privacy protection — Information security management systems — Requirements., ISO/IEC 27001:2013.
- International Telecommunication Union. 2023. *National Cybersecurity Strategies Repository*. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx>
- ISO Standards. 2022. ISO/IEC 27001
- IT Governance. 2022. *ISO/IEC 27001:2022 and ISO/IEC 27002:2022: Key Updates and Insights*. <https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates> Pristupljeno 12. 5. 2023.
- J. H. Saltzer i M. D. Schroeder. 1975. "The Protection of Information in Computer Systems". *Proceedings of the IEEE* 63 (9): 1278–1308. <https://doi.org/10.1109/PROC.1975.9939>.
- Jacobson, Trudi, Thomas Mackey i Kelsey O'Brien. 2021. "Visualizing the Convergence of Metaliteracy and the Information Literacy Framework". University Libraries Faculty Scholarship. 149. https://scholarsarchive.library.albany.edu/ulib_fac_scholar/149 (Pristupljeno 12. 8. 2023)
- Kenway, Jane i Helen Nixon. 1999. "Cyberfeminisms, Cyberliteracies, and Educational Cyberspheres". *Educational Theory* 49 (4): 457.
- Komatsu, Ayako, Daisuke Takagi i Toshihiko Takemura. 2013. "Human Aspects of Information Security". Ur. Steven M. Furnell i Nathan Clarke. *Information Management & Computer Security* 21 (1): 5–15. <https://doi.org/10.1108/09685221311314383>.
- Krause, Keith i Michael C. Williams, ur. *Critical Security Studies: Concepts and Cases*. NED-New edition. University of Minnesota Press, 1997. <http://www.jstor.org/stable/10.5749/j.ctttv088>. (Pristupljeno 12. 8. 2023)
- Kuhn, Thomas S. 1970. *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press.

- Kusotić, Dejan. 2022. "ISO 27001 2013 vs. 2022 revision – What has changed?". *Advisera*, 25. oktobar. <https://advisera.com/27001academy/blog/2022/10/25/iso-27001-iso-27002/> (Pristupljeno 10. septembra 2023)
- Lee, Alice i Clement So. 2014. "Media literacy and information literacy: Similarities and differences". *Comunicar Journal 42: Revolution in Education?* 21 (42): 137-145. <http://dx.doi.org/10.3916/C42-2014-13>. (Pristupljeno: juli 25. 2023)
- Ljubčić, Elma. 2023. *Kada bi BiH mogla dobiti strateški i zakonski okvir za cyber sigurnost*. januar 29. <https://balkans.aljazeera.net teme/2023/1/29/kako-bih-moze-povecati-otpornost-na-cyber-napade>. (Pristupljeno septembar 19. 2023)
- Lundgren, Björn i Niklas Möller. 2019. "Defining Information Security". *Science and Engineering Ethics* 25 (April). <https://doi.org/10.1007/s11948-017-9992-1>. (Pristupljeno septembar 19. 2023)
- Mackey, Thomas i Trudi Jacobson. 2010. "Reframing Information Literacy as a Metaliteracy". *College & Research Libraries* 72 (December): 62–78. <https://doi.org/10.5860/crl-76r1>.
- Magnuson, Marta. 2015. "Metaliteracy: Reinventing Information Literacy to Empower Learners by Thomas P. Mackey and Trudi E. Jacobson". *Portal: Libraries and the Academy* 15 (January): 198–99. <https://doi.org/10.1353/pla.2015.0006>.
- Mahmutović, Aida i Aida Trepanić. 2002. *Pravni i administrativni sistem koji kaska u prepoznavanju cyber sigurnosti*. Balkan Investigative Reporting Networ (BIRN), Sarajevo <https://detektor.ba/wp-content/uploads/2022/12/Cyber-sigurnost-FINAL-WEB-pages-1.pdf> (Pristupljeno: septembar 19. 2023)
- Manovich, Lev. 2013. *Software Takes Command*. New York: Bloomsbury Academic.
- Mansoor, Hasan M. H. 2023. "Diversity and Pluralism in Arab Media Education Curricula: An Analytical Study in Light of UNESCO Standards". *Palgrave Communications* 10 (1): 1–11. <https://doi.org/10.1057/s41599-023-01598->.
- Mayring, Philipp. 2010. *Qualitative Inhaltsanalyse. Grundlagen und Techniken* (Vol. 1). Beltz Verlag. https://www.beltz.de/fachmedien/sozialpaedagogik_soziale_arbeit/buecher/produkt_produktdetails/27650-qualitative_inhaltsanalyse.html (Pristupljeno 24. septembra 2023)
- Mijić, Branka. 2019. „Information Security in Bosnia and Herzegovina“. *FBIM Transactions* 7 (April): 91–99. <https://doi.org/10.12709/fbim.07.07.01.11>.

- Moghaddasi, Hamid, Samad Sajjad i Mehran Kamkarhaghghi. 2016. "Reasons in Support of Data Security and Data Security Management as Two Independent Concepts". U *The Open Medical Informatics Journal* 10 (October): 4–10.
<https://doi.org/10.2174/1874431101610010004>.
- Mouffe, Chantal. 2016. *O političkom*. Zagreb: Politička kultura
- OSCE. 2019. *Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini*. OSCE.
<https://www.osce.org/files/f/documents/4/8/438386.pdf> (Pristupljeno septembar 19. 2023)
- Puharić, Predrag i Muhamed Budimlić. 2008. "Information Safety (European Standards)". *Kriminalističke Teme* 8 (1-2):103-115.
<https://krimteme.fkn.unsa.ba/index.php/kt/article/view/302>.
(Pristupljeno septembar 19. 2023)
- Rašidović, Ešefa Beba. 2016. „Izborni predmet informacijske pismenosti 'Bibliotečko informacijske baze' u curriculumu Fakulteta za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu.” *Pregled* 57(2): 35-53.
- Ratta, Donatella Della. 2021. "Shooting 2011–21: Violence, Visibility, and Contemporary Digital Culture in Post-Uprising and Pandemic Times". *Film Quarterly* 75 (2): 68–75.
<https://doi.org/10.1525/fq.2021.75.2.68>.
- Rosado da Cruz, António Miguel, José Oliveira i Pedro Faria. 2020. *Zeroconf Network Retail Kiosk for Fish Products Traceability*.
<https://doi.org/10.23919/CISTI49556.2020.9141069>.
- Samokishyn, Marta. 2022. *The Role of Algorithmic Literacy in Academia and Beyond: Some Considerations*. novembar 2. <https://bccampus.ca/2022/11/02/the-role-of-algorithmic-literacy-in-academia-and-beyond-some-considerations/>. (Pristupljeno juni 14. 2023)
- Secure Privacy. 2020. *ISO 27001 and GDPR: Is it Enough for Website Compliance?* 20. novembar. <https://secureprivacy.ai/blog/iso-27001-and-gdpr-website-compliance>.
(Pristupljeno septembar 16. 2023)
- Silajdžić, Lamija. 2020. "Medijske navike i medijska i informacijska pismenost studenata komunikologije. *Časopis SaZnanje* (2): 322-332.
- Simić, Slavko i Branko Marković. 2020. *Međunarodni standardi – Abeceda ISO/IEC standarda u kontekstu digitalne transformacije i primene General Data Protection Regulation (GDPR)*. Banja Luka: Nezavisni Univerzitet Banja Luka.
- Sinclair, Jane, Russell Boyatt, Claire Rocks i Mike Joy. 2015. "Massive Open Online Courses: A Review of Usage and Evaluation". *International Journal of Learning Technology* 10 (January). <https://doi.org/10.1504/IJLT.2015.069450>.

- Stallings, William. 2016. *Cryptography and Network Security: Principles and Practice*. Pearson. https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-_principles-and-practice-7th-global-edition.pdf
- Stallings, William. 2021. *Network Security Essentials: Applications and Standards*. Pearson.
- Tajić, Lea. 2013. *Medijska pismenost u Bosni i Hercegovini*. Sarajevo. Internews u Bosni i Hercegovini. (Pristupljeno 1.11.2020)
https://epale.ec.europa.eu/sites/default/files/medijska_pismenost_u_bih.pdf.
- Terra, John. 2023. *What is Media and Information Literacy?* maj 3. Pristupljeno: juli 5. 2023.
<https://www.simplilearn.com/what-is-media-and-information-literacy-article>
- Tsujii, Shigeo, 2006. "Information security as interdisciplinary science based on ethics". *Information Security and Cryptology - ICISC 2005:2-2*.
https://doi.org/10.1007/11734727_2
- Tufekci, Zeynep. 2018. *Twitter and Tear Gas*. New Haven, CT: Yale University Press.
- Turčilo, Lejla. 2020. "Cjeloživotno učenje za medijsku i informacijsku pismenost: Proces odgajanja mislećih građana". U *Medijska i informacijska pismenost: istraživanje i razvoj*. Mario Hibert, Lejla Turčilo, Amer Džihana Emir Vajzović, ur. Emir Vajzović, 27-35. Sarajevo: Fakultet političkih nauka. Pristupljeno: septembar 23, 2023.
https://fnp.unsa.ba/b/wp-content/uploads/2020/12/MEDIJSKA-I-INFORMACIJSKA-PISMENOST-ISTRAZIVANJE-I-RAZVOJ_e-izdanje-1.pdf. Pristupljeno septembar 19, 2023.
- Univerzitet u Sarajevu. 2019. *Strategija razvoja Univerziteta u Sarajevu 2019–2023*.
https://www.unsa.ba/sites/default/files/dodatak/2019-05/Strategija%20razvoja%20UNSA_30042019_lektorisano.pdf Pristupljeno: septembar 19. 2023.
- Vajzović, Emir, Mario Hibert i Emina Adilović. 2023. "Transverzalno učenje: medijska i informacijska pismenost na Univerzitetu u Sarajevu". *Pregled: časopis za društvena pitanja*, no. 1 (Juli):437-55. <https://doi.org/10.48052/19865244.2023.1.437>
- Vajzović, Emir, Mario Hibert, Lejla Turčilo, Vuk Vučetić, i Lamija Silajdžić. 2021. *Medijska i informacijska pismenost: dizajn učenja za digitalno doba*. Sarajevo: Fakultet političkih nauka Univerziteta u Sarajevu. Pristupljeno: [dan.mjeseć.godina] https://fnp.unsa.ba/b/wpcontent/uploads/2021/04/MEDIJSKA-I-INFORMACIJSKA-PISMENOST-DIZAJNUCENJA-ZA-DIGITALNO-DOBA_e-izdanje-1.pdf.
- Vajzović, Emir. 2019. "Medijska i informacijska pismenost u sistemu cyber sigurnosti." *Kriminalističke teme XIX (5): 529-543*. Pristupljeno novembar 3. 2020.
<http://krimteme.fkn.unsa.ba/index.php/kt/article/view/240/237>. Pristupljeno septembar 19, 2023.

- Vajzović, Emir. 2020. „Digitalna transformacija sigurnosti i algoritamska demokratija.“ *Sarajevski žurnal za društvena pitanja* Fakultet političkih nauka (IX): 7-37. Pristupljeno: septembar 21, 2023. <https://www.ceeol.com/search/article-detail?id=962456>.
- Vajzović, Emir. 2020. “Medijska i informacijska pismenost: Strateški pristup”. U *Medijska i informacijska pismenost: istraživanje i razvoj*, by Mario Hibert, Lejla Turčilo, Amer Džihana Emir Vajzović, edited by Emir Vajzović, 27-35. Sarajevo: Fakultet političkih nauka. Pristupljeno: septembar 23, 2023. https://fpn.unsa.ba/b/wp-content/uploads/2020/12/MEDIJSKA-I-INFORMACIJSKA-PISMENOST-ISTRAZIVANJE-I-RAZVOJ_e-izdanje-1.pdf.
- Vijeće Evrope. 2023. *Media and Information Literacy*. Pristupljeno: august 3, 2023. <https://www.coe.int/en/web/digital-citizenship-education/media-and-information-literacy>.
- Vijeće ministara BiH. 2017. *Odluka o usvajanju politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017 - 2022. godine* (Službeni glasnik BiH, broj 38/17) <http://www.sluzbenilist.ba/page/akt/bM0k8gNBNCU=>
- Vijeće ministara BiH. 2022. *Odluka o usvajanju Smjernica iz politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine za period od 2017 - 2022. godine*. Službeni glasnik BiH, broj 62/22. <http://www.sluzbenilist.ba/page/akt/kf999pBB6Fs=>
- Vlada Kantona Sarajevo. 2022. *Strategija razvoja medijske i informacijske pismenosti u oblasti obrazovanja u Kantonu Sarajevo*. Sarajevo, april. Pristupljeno: septembar 23, 2023. <https://mon.ks.gov.ba/sites/mon.ks.gov.ba/files/2022-06/Strategija%20razvoja%20medijske%20i%20informacijske%20pismenosti.pdf>.
- Wilson, Carolyn, Alton Grizzle, Ramon Tuazon, Kwame Akyempong i Chi-Kim Cheung. 2011. *Media and information literacy curriculum for teachers*. Paris: UNESCO. Pristupljeno: mart 18. 2021. <https://unesdoc.unesco.org/ark:/48223/pf0000192971>.
- Wood, Charles. 2004. “Why Information Security Is Now Multi-Disciplinary, Multi-Departmental, and Multi-Organizational in Nature”. *Computer Fraud & Security* 2004 (January): 16–17. [https://doi.org/10.1016/S1361-3723\(04\)00019-3](https://doi.org/10.1016/S1361-3723(04)00019-3).
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. London, England: Profile Books.



FAKULTET
POLITIČKIH
NAUKA

Obrazac AR

UNIVERZITET U SARAJEVU – FAKULTET POLITIČKIH NAUKA

Stranica 75 od 76

IZJAVA o autentičnosti radova

Naziv odsjeka i/ili katedre: Odsjek za sigurnosne i mirovne studije
Predmet: Zaštita podataka

IZJAVA O AUTENTIČNOSTI RADOVA

Ime i prezime: Emina Adilović
Naslov rada: Algoritamska pismenost na Univerzitetu u Sarajevu: zaštita podataka i informacijska sigurnost
Vrsta rada: Završni magistarski rad
Broj stranica: 75

Potvrđujem:

- da sam pročitao/la dokumente koji se odnose na plagijarizam, kako je to definirano Statutom Univerziteta u Sarajevu, Etičkim kodeksom Univerziteta u Sarajevu i pravilima studiranja koja se odnose na I i II ciklus studija, integrirani studijski program I i II ciklusa i III ciklus studija na Univerzitetu u Sarajevu, kao i uputama o plagijarizmu navedenim na web stranici Univerziteta u Sarajevu;
- da sam svjestan/na univerzitetskih disciplinskih pravila koja se tiču plagijarizma;
- da je rad koji predajem potpuno moj, samostalni rad, osim u dijelovima gdje je to naznačeno;
- da rad nije predat, u cjelini ili djelimično, za stjecanje zvanja na Univerzitetu u Sarajevu ili nekoj drugoj visokoškolskoj ustanovi;
- da sam jasno naznačio/la prisustvo citiranog ili parafraziranog materijala i da sam se referirao/la na sve izvore;
- da sam dosljedno naveo/la korištene i citirane izvore ili bibliografiju po nekom od preporučenih stilova citiranja, sa navođenjem potpune reference koja obuhvata potpuni bibliografski opis korištenog i citiranog izvora;
- da sam odgovarajuće naznačio/la svaku pomoć koju sam dobio/la pored pomoći mentora/ice i akademskih tutora/ica.

Mjesto, datum

Potpis

Sarajevo, oktobar 2023.